Fingerprinting Smartphones From Embedded Transducers

PhD thesis - Summary
for obtaining the Scientific Title of PhD in Engineering from
Politehnica University Timișoara
in the Field of Computer and Information Technology
by

Eng. Adriana-Maria Berdich
PhD Supervisor: Prof. Bogdan Groza

May, 2023

Nowadays smartphones have a staggering amount of processing and memory capabilities. They are also equipped with various sensors, including loudspeakers, microphones, accelerometers, magnetometers and radio frequency sensors (such as NFC, UWB and GPS). These are generally referred to as transducers, components that convert one form of energy into another. Due to the manufacturing process, each transducer has unique properties that have the potential to be used as a fingerprint for the mobile device. Fingerprints based on software can also be used, but in this thesis, the focus is on hardware-based fingerprints. This is because they rely on the characteristics of transducers, which are embedded in the circuit board and are more challenging to replace. This makes the fingerprint more difficult to falsify.

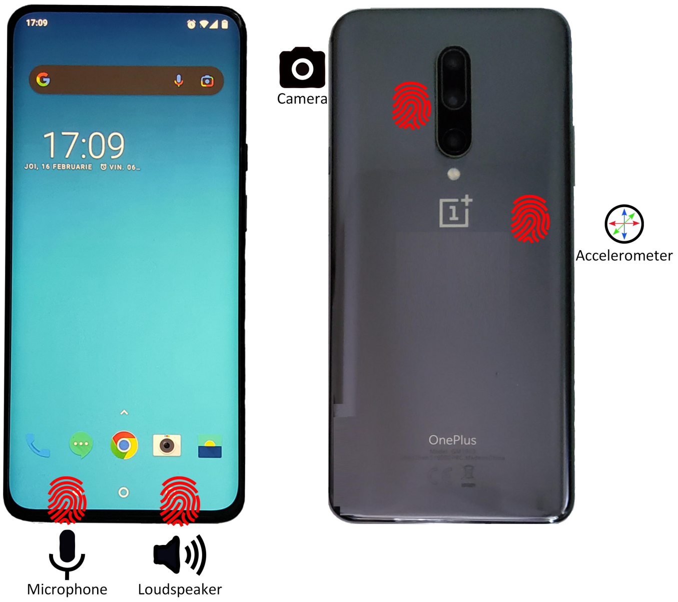

Fig. 1. A generic smartphone with sensors and transducers subject to fingerprinting

In Figure 1 a generic smartphone is illustrated with the sensors and transducers that can be subject to fingerprinting. Since the beginning of the 2000s, circuit identification using physical characteristics has been studied [1]. Later, Physically Unclonable Functions (PUFs), based on distinctive and erratic properties of the circuits, were proposed in [2] for security applications such as device authentication. Device-to-device (D2D) authentication is common in IoT scenarios. Using the characteristics of the device to ensure authentication is one way to eliminate user interaction, which is especially beneficial for embedded devices that lack user interfaces or inside vehicles where accessibility to the interface may be limited.

Research objectives. This thesis aims to fingerprint smartphones based on their sensors, i.e., accelerometers, loudspeakers, microphones and camera sensors and also briefly investigate such fingerprinting techniques for in-vehicle ECU. More specifically, the main objectives of this thesis can be summarized as follows:

1) Surveying the existing literature that addresses smartphone fingerprinting based on embedded sensors;
2) Collecting data from accelerometers, loudspeakers, microphones and camera sensors of different and identical smartphones to create comprehensive datasets;
3) Analyzing the collected data and finding the more reliable characteristics;
4) Fingerprinting smartphones based on accelerometer, loudspeakers, microphones and camera sensor characteristics which are the main four transducers used inside modern smartphones;
5) Analyze distinct classification algorithms and show that traditional machine learning algorithms may have better results than neural network algorithms;
6) Analyze and test how fingerprinting smartphone techniques can be extended to other components, using in-vehicle ECUs as an example.

Major contributions. In this thesis, several smartphone transducers, i.e., accelerometers, loudspeakers, microphones and camera sensors are fingerprinted. In addition to smartphone sensors, ECU fingerprinting is also analyzed. The contributions of this thesis can be summarized as follows:

1) Several comprehensive datasets were built containing:
    - Accelerometer data collected in different transportation modes: tram, train, car, bike, walk and shake [3];
    - 3,000 samples collected with 28 smartphones loudspeakers [4];
    - 19,200 samples collected with 32 smartphones microphones [5];
    - 300 dark photos collected with 6 identical smartphone cameras [6];
2) Several classification algorithms were used and their performance was analyzed in various scenarios, also using some signal processing techniques when needed [4], [5], [6], [7], [8];
3) Identification of smartphones from identical and different models of transducers (accelerometers, loudspeakers, microphones and cameras) was performed [4], [5], [6], [7];
4) Sensor identification in the presence of different types and levels of noise (additive white Gaussian noise or environmental noise) was performed [4], [5];
5) Device-to-device and in-vehicle authentication scenarios were addressed as applications for smartphone identification [3].

These major contributions are reflected by the following publications in relevant ISI journals and conferences. In [3] the author explored smartphone pairing based on accelerometer data collected from different transportation environments. For this, several accelerometer measurements were collected using smartphones in a train, tram, car and bike and later analyzed for the design of the protocol. Smartphone fingerprinting based on accelerometer data was analyzed in [7]. Experiments with 5 identical and 5 different smartphones were done in order to fingerprint them based on characteristics extracted from the accelerometer. In [4] smartphone fingerprinting based on loudspeaker characteristics is addressed. A dataset was built, containing records from 16 identical and 12 different smartphones, that play a linear sweep signal and it publicly released to serve for future works. Smartphones were identified based on the roll-off characteristics of the emitted sounds. Also, recurrent neural networks were used for a more accurate classification. In [5], microphone fingerprinting is addressed. A dataset was built, containing experiments with 16 identical smartphones that record locomotive, barrier, horn and tier sounds played by a high-fidelity audio system. The dataset also contains live recordings of a car honk, hazard lights and wiper sounds recorded with 16 different smartphones. The power spectrum of each signal was extracted from the recorded sounds and used as input for several machine learning classifiers to separate the smartphones. This dataset was also made public to serve for future investigations. Smartphone fingerprinting based on camera characteristics was discussed by the author in [6]. The characteristics extracted from 50 images collected using 6 identical smartphones were used as input for several classification algorithms in order to fingerprint the smartphones. The machine learning algorithms used for smartphone identification in the previously mentioned papers were also used in [9] to fingerprint in-vehicle ECUs based on an existing dataset. The author also contributed to other research papers focused on vehicle-to-smartphone interaction which, although they are not part of the main body of this work, provided a great opportunity for the author to gain even more insights into the security of the smartphone-vehicle ecosystem. These works discuss car to smartphone interaction [10], vehicle access rights based on cloud services [11], smartphone based access to vehicles [12] and audio-visual key exchange between smartphone and vehicle [13].

To sum up, the author has contributed to 11 papers on mobile system security and their presence within the in-vehicle environment, out of which the first 7 form the main body of the current thesis:

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.

Chapter II briefly presented the principles of operation behind smartphone transducers, i.e., accelerometers, loudspeakers, microphones and camera sensors. The most popular feature extraction methods, popular classification algorithms and an overview of evaluation metrics were presented. This chapter also illustrated some application scenarios and preventive measures against the exploitation of smartphone fingerprinting as a privacy leak. Regarding each sensor presented in the thesis, the related works showed the following. Accelerometers were widely used for device authentication (pairing) and it is surprising that only a few works discussed smartphone fingerprinting based on accelerometers. Loudspeakers were employed much less frequently in research than microphones were. It is possible that less research was done on device fingerprinting based on audio signals from loudspeakers because, while such data is simple to evaluate, it is more challenging to collect. There are several publicly available datasets for microphones (the majority of them focusing on speech recognition and criminal investigations), which are also utilized for device identification based on microphone characteristics. To the best of the author’s knowledge, the only public dataset available for loudspeaker identification is the result of the research done for this thesis. The topic of camera fingerprinting was addressed by the largest body of research works compared to all other sensors, based on the works surveyed in this thesis. This is expected given that consumers frequently submit images to several websites, making such data relatively easy to gather and likely leading to privacy concerns. Additionally, photos can be used to extract a wide variety of samples and attributes and numerous public datasets were available.

Chapter III discussed smartphone pairing in several transportation modes based on accelerometer data and also smartphone fingerprinting based on accelerometers. Accelerometer data was collected using three smartphones in different transportation modes, i.e., tram, train, car, riding a bike, with the smartphones in the pocket, while walking with the smartphones in the pocket and by shaking the smartphones in the hand. Accelerometer signals differ substantially depending on the mode of mobility. The findings from this thesis demonstrated that acquiring enough entropy from the accelerometer data was possible in order to create a session key in all transportation environments. Low-entropy extractions can also lead to secure session keys by relying on guessing-resilient protocols (that allow matching such values without exposing them to a brute-force adversarial search). Several signal processing methods were used, i.e., simple scaling, sigma-delta modulation, high-pass filtering, and smoothing. Most of the filtering methods employed gave comparable results. However, simple scaling of the accelerometer measurements was the most suitable choice due to its simplicity. The entropy was increased by extending the feature vectors with sigma-delta modulation, but this required more computations because more features had to be traded. Given the variations in transportation modes, specific parameters may be advantageous depending on the case and the trade-off between the level of security and pairing probability. By addressing the adversarial advantage and the pairing success rate, a more precise image of this approach was provided. The key exchange protocol starts with temporal synchronization between the smartphones, followed by data collection, processing, and splitting of the data into multiple windows. These windows are then used to generate the keys, which are transferred between the smartphones via Bluetooth connection using the EKE-DH and SPEKE protocols. SPEKE is a guessing-resistant protocol that was proposed in [14]. The key-exchange between two smartphones is described in outline in Figure 2. The computational time for the pairing operation using EKE-DH is between 25ms and 230ms for share calculation and between 39ms and 411ms for key recovery for both the 1024-bit and 2048-bit modules. In the case of SPEKE, the computational time is between 20ms and 145ms for share calculation and between 7ms and 70ms for key recovery. The computational time also depends on the smartphone's performance. This chapter also discussed smartphone fingerprinting based on accelerometer sensors. Data was collected using 5 identical and 5 different smartphones. Over 40 minutes of data were collected with each smartphone at a sampling rate of 10ms. Seven time-domain features, i.e., Kurtosis, Skewness, SNR, STD, RMS, peak value, and SINAD were extracted from the accelerometer data. These features were then used as input for five classification algorithms, i.e., NN, KNN, SVM, Ensemble, and Decision Trees. The Ensemble classifier provided maximum recognition accuracy of 100% for the dataset, which includes instances from five separate and identical phones. The results demonstrated that classical machine learning algorithms can produce good results for fingerprinting smartphones based on accelerometer sensors. Using more sophisticated deep learning architectures seem unnecessary, especially when training data is limited.

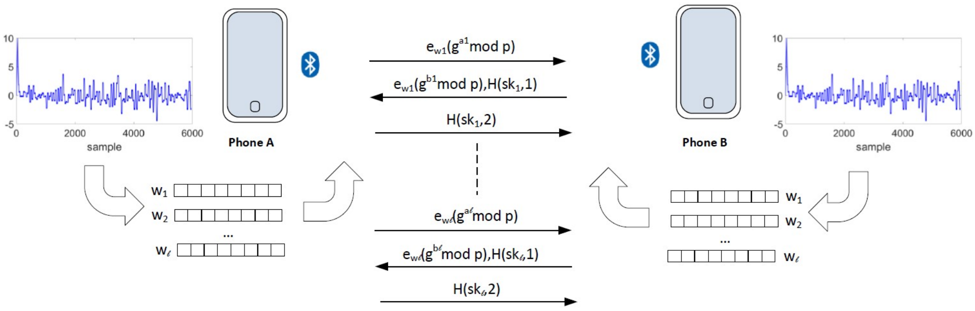
10
5
0
-5
0
2000
4000
6000
sample
Phone A
$e_{w1}(g^{a1} \text{mod } p)$
$e_{w1}(g^{b1} \text{mod } p), H(sk_1,1)$
$H(sk_1,2)$
$e_{w\ell}(g^{a\ell} \text{mod } p)$
$e_{w\ell}(g^{b\ell} \text{mod } p), H(sk_\ell,1)$
$H(sk_\ell,2)$
Phone B
w_1
w_2
...
w_ℓ

Fig. 2. Data collection and key-exchange between two smartphones

Chapter IV approached smartphone fingerprinting based on loudspeaker characteristics. Smartphones can be fingerprinted using the methods summarized in this thesis, possibly making them useful as smart keys identifiable based on physical characteristics. In this thesis, an effective fingerprinting technique was investigated that can be quickly applied to identify smartphones based on loudspeaker roll-off characteristics. An in-vehicle infotainment system was used for the experiments, which recorded the sounds emitted by 28 loudspeakers (16 identical and 12 different). Each loudspeaker emitted a linear sweep signal with a duration of about 10s. The distance between the infotainment system and the loudspeakers was 1 meter. In this setup, 3,000 measurements were taken. A suggestive depiction of the setup is shown in Figure 3 The power spectrum was extracted from each signal recorded by the infotainment unit and it was then used to either determine the slopes of the low and high roll-offs or to do more complicated machine learning techniques. Also, using 4 smartphones, measurements at different volume levels, i.e., 50%, 75%, 100% and orientation angles, i.e., 0°, 45° and 90°, were done. According to the findings, loudspeaker roll-offs offer a reliable fingerprint that is more resistant to variations in volume levels. In contrast, for some techniques, the volume level may be deceptive. While the slope of the roll-offs alone was adequate to identify different smartphone models, deep-learning methods were required for a more thorough analysis of loudspeakers coming from the same smartphone models. The discrimination between such identical loudspeakers can be done with an accuracy of 90–99% using the LSTM and BiLSTM neural network designs. The impact of noise was also analyzed, keeping in mind that in a real-world scenario, background noises are present and can affect the fingerprinting mechanism of the loudspeakers. Two significant types of noise were taken into account: additive white Gaussian noise (AWGN), which imitates the impacts of several random processes seen in nature and may also account for noise inside cars, and street noise, which is unique to the situation involving cars. In [15], the attenuation of the sound from the loudspeaker to the microphone was also simulated using the additive white Gaussian noise. The separation between loudspeakers was still visible after identical noise was introduced to the recordings. Repeated measurements taken inside the vehicle with the left window opened revealed a less distinctive separation. One specific application scenario was the use of smartphones inside vehicles, which is why most of the experiments conducted in this chapter employed a car's head unit to record the smartphone sounds. Regardless of the recorder, the identification had a high success rate, indicating that in-vehicle infotainment units are usable in such scenarios.

Chapter V investigated smartphone microphone fingerprinting employing the signal power spectrum and various supervised machine learning methods (including Linear Discriminant (LD), Ensemble-Subspace Discriminant, Fine Tree, Fine KNN and Linear SVM). The analysis was concentrated on three separate scenarios, as shown in Figure 4: scenario A, fingerprinting smartphones from different brands and models based on human speech, scenario B, fingerprinting identical smartphones based on environmental sound using prerecorded sounds and scenario C, fingerprinting smartphones from different brands and models based on live recordings. For scenario the already-existing MOBIPHONE dataset [16] was used. This dataset contains a human voice recorded with 21 smartphones from various manufacturers and models. The dataset for each smartphone includes 24 audio samples from 12 male and 12 female speakers. For scenario B, special recordings were done using 16 microphones from the same smartphone (a Samsung Galaxy S6) that were utilized to capture road and vehicle noise (locomotive, barrier, car honk and car tiers) that was then played by a high-fidelity audio system. For scenario C a special dataset was created by recording the sound on 16 smartphones both outside and inside a car. Each smartphone records three different sounds: can honk, hazard lights and car wipers. Additional noise was introduced to all scenarios to make classification more difficult. The LD classifier acted perfectly in the first two cases. The final scenario was the more challenging.

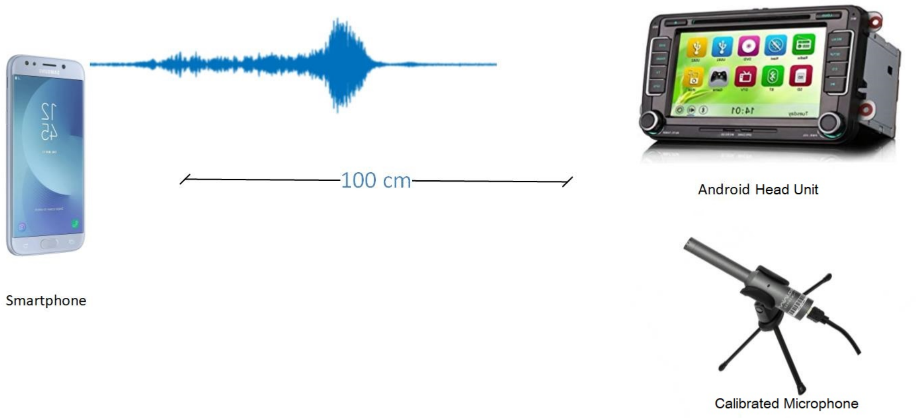

Fig. 3. Suggestive depiction of the setup: an Android infotainment unit or microphone records sound emitted by a smartphone

When noise was added, the LD produces poor identification results for two specific phones (the LG and Nexus 7). The LD classifier may still be preferred because it utilizes little memory and has a short runtime. Other conventional machine learning classifiers performed worse than LD in terms of accuracy. These fingerprints have a wide range of potential uses. For example, verifying ownership of a specific phone to serve as a second authentication token with physical characteristics that cannot be cloned. However, such fingerprinting could also be abused by mobile applications to fingerprint devices without access to device-unique identifiers. Malicious apps (or libraries hidden within) with high-fidelity access to microphone samples already have a more significant impact on security and privacy [17] than the additional device fingerprint.

In Chapter VI, smartphone fingerprinting based on their camera sensors was also investigated using the low and mid-frequency AC coefficients obtained from the DCT of dark photos. The investigation showed that the blue channel is more effective at recognizing the camera. A dark picture needs to be taken for this purpose, by holding the smartphone against the user's palm. Six machine learning algorithms were employed to identify the devices, i.e., Nearest Neighbor (KNN), Ensemble-Subspace Discriminant, Support Vector Machines, Linear Discriminant, Naive Bayes and a wide neural network. For the classification, 50 photos were taken using six identical cameras from Samsung Galaxy J5 smartphones. The 2-D adaptive noise-removal filter from Matlab called the wiener2 filter was employed to process the original image. With 10x10 local neighborhoods, this filter calculates the variance and the local mean surrounding each pixel. To recover the pixel variations, the residual noise was computed as the difference between the original picture and the filtered image. The residual noise was divided into 8x8 non-overleaping blocks. The 2-D DCT was computed for each block and the low and mid-frequency AC coefficients were extracted. Each 8x8 block was converted into an array of 35 elements using the zigzag sequence, which was then concatenated to produce the fingerprint. The data processing steps are described in Figure 5. Due to prediction time and memory requirements, samples of 100 or 1000 rows of 35 columns were used from each image

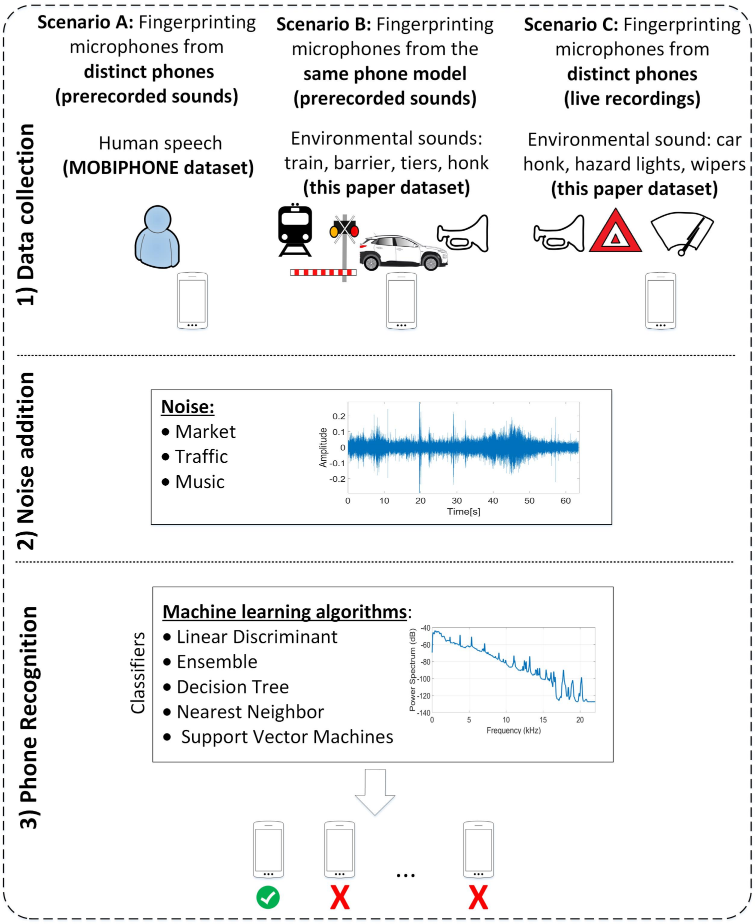
1) Data collection
Scenario A: Fingerprinting microphones from distinct phones (prerecorded sounds)
Human speech (MOBIPHONE dataset)
Scenario B: Fingerprinting microphones from the same phone model (prerecorded sounds)
Environmental sounds: train, barrier, tiers, honk (this paper dataset)
Scenario C: Fingerprinting microphones from distinct phones (live recordings)
Environmental sound: car honk, hazard lights, wipers (this paper dataset)
2) Noise addition
Noise:
• Market
• Traffic
• Music
Amplitude
Time[s]
3) Phone Recognition
Classifiers
Machine learning algorithms:
• Linear Discriminant
• Ensemble
• Decision Tree
• Nearest Neighbor
• Support Vector Machines
Power Spectrum (dB)
Frequency (kHz)
...

Fig. 4. Overview of the methodology and scenarios used in this chapter

and device as input for the classifiers. The wide neural network, which had an accuracy of 97% for 1000 samples and roughly 70% for 100 samples, had the best results. The conventional KNN algorithm also gave promising outcomes, with an accuracy of about 80% for both 100 and 1000 samples. In order to prove the security level, the Shannon and minimum entropy values were computed on the original image and on the retrieved AC coefficients. The security level is good enough since the lowest entropy is still often in the region of 2-3 bits for each byte from the coefficients, which is twice as much as in the case of the unprocessed photos.

Last but not least, in Chapter VII, due to the interest of the author in the area of automotive security, a side objective of the current reasearch was the application of fingerprinting technologies on Electronic Control Units. Since a dataset containing physical fingerprints was already public [18], the application of the previous machine learning toolset from Matlab was immediate. This chapter presents the results of the author in this direction, and it is no surprise that these techniques that yield good results for smartphones, perform well in this area too. Five machine learning algorithms: Linear Discriminant (LD), Decision Trees (Tree), SVM, KNN and a wide neural network (NN), which were also used for smartphones, were also used here to

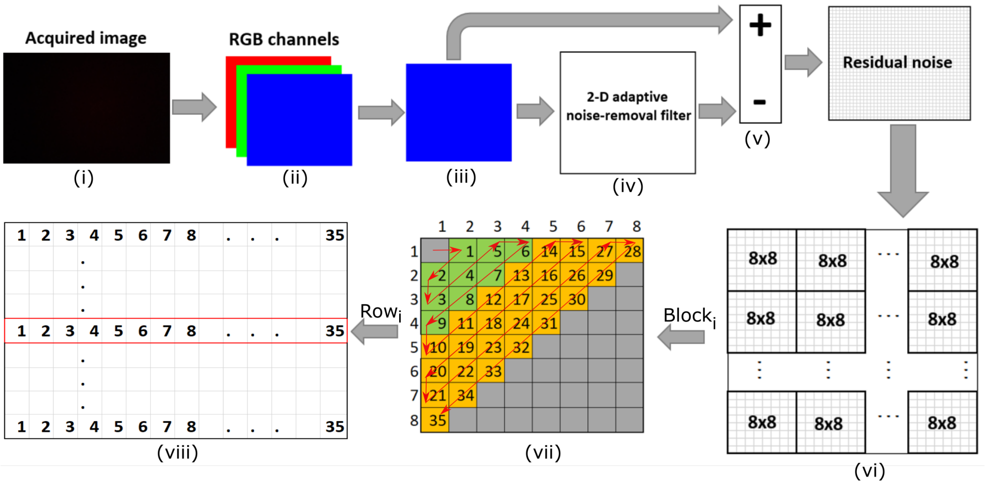

Fig. 5. Process of extracting fingerprints: from picture capture to AC coefficients

fingerprint 51 ECUs based on a publicly available dataset. The classifiers were tested on all features from the dataset. When all features were used, NN reached an accuracy of 99.9%, while when only two features were used, the ECUs performance of the KNN was not so good. Suggesting, as already known in the literature, that a reduced number of features is not sufficient for accurate classification.

Chapter VIII concludes this thesis. To sum up, this thesis provided positive results for the classification of smartphones based on four transducers: accelerometers, loudspeakers, microphones and cameras. One of the main findings of this research was that traditional machine learning algorithms can give even better results than more complicated deep neural network architectures for sensor fingerprinting. Comprehensive datasets were also publicly released for loudspeaker and microphone data evolving more than 60 smartphones. The results of this PhD work have been submitted and accepted for publication in relevant ISI journals and conferences.

References

[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.