Smartphone Fingerprinting Combining Features of On-Board Sensors

Irene Amerini, *Member, IEEE*, Rudy Becarelli, Roberto Caldelli, *Senior Member, IEEE*, Alessio Melani and Moreno Niccolai

***Abstract*—Many everyday activities involve the exchange of confidential information through the use of a smartphone in mobility i.e. sending on e-mail, checking bank account, buying on-line, accessing cloud platforms, health monitoring. This demonstrates how security issues related to these operations are a major challenge in our society and in particular in the cyber-security domain. The proposed paper focuses on the use of the smartphone intrinsic and physical characteristics as a mean to build a smartphone fingerprint to enable devices identification. The basic idea proposed in this paper is to investigate how to generate a specific fingerprint that allows to distinctively and reliably characterize each smartphone. In particular, the accelerometer, the gyroscope, the magnetometer and the audio system (microphone-speaker) are taken into account to build up a composite fingerprint based on a set of their distinctive features. Many experiments have been carried out, by analyzing different classification methods, diverse features combination configurations and operative scenarios. Satisfactory results have been obtained showing that the combination of such sensors improves smartphone distinctiveness.**

***Index Terms*—Source identification, smartphones classification, features, fingerprint, MEMS sensors.**

I. Introduction

THE exchange of confidential information (images, videos, texts), through the use of a smartphone in mobility, involves many everyday activities like sending on e-mail, checking bank account, buying on-line, accessing cloud platforms, health monitoring. Username and password pair (something the user knows) is the usual modality to access personal accounts and to reach resources online so far. A stronger level of safeness [1] is achieved through the use of auxiliary devices (something the user has), such as smart cards, USB sticks, OTP generators in combination with username and password. Anyway, the mentioned auxiliary devices are not always available (must be in the user hand all the time) or usable (not easily pluggable in a mobile device). Moreover, when a continuous authentication is required, e.g. transferring a great amount of confidential data, the authentication issue become even more complicated; it is impossible asking to the user to insert the pair username-password again and again, and/or to require to use many times the previously mentioned auxiliary devices. The proposed paper focuses on the adoption of the smartphone intrinsic and physical characteristics as a mean to find a smartphone fingerprint and to enable device identification. Furthermore, since a smartphone is a personal item owned by a specific person, it should be possible to use the information on the device to detect and trace the person itself. Obviously privacy preservation is an issue to be considered and discussed in certain types of applications and it shall be studied as future work. The novel idea proposed in this paper is to investigate how to generate a specific fingerprint that allows to distinctively and reliably characterize each smartphone (or tablet), to be used as a univocal and trustworthy security component. Modern mobile phones are equipped with several on-board sensors such as accelerometer, gyroscope, magnetometer and so on; it is quite well-known that each one has peculiar anomalies due to the imperfections occurred during the manufacturing process that left traces in the acquired signals. The main goal of this paper is to combine such distinctive traces and exploit them in a comprehensive fingerprint for the identification of each specific device. The proposed methodology is firstly based on the individuation and validation of a set of distinctive features for each on-board sensor; in our experiments we considered, in particular, the accelerometer, the gyroscope, the magnetometer and the audio system (microphone-speaker). Their features are assembled in order to constitute a fingerprint of each device. According to these fingerprints, two classifiers are evaluated and comprehensive experimental tests to verify detection performances of the proposed method have been carried out. Furthermore, diverse operative conditions have been analyzed: smartphone position (hand-held or placed on tables of different materials), vibration motor on or off, geographical location and time. The fingerprint extraction and the consequent device identification could represent an important achievement for secure assessment, for example, of confidential information exchange, enforcing the reliability of the smartphone identity. The paper is organized as follows: Section II presents some previous works inherent the device sensor fingerprinting, while Section III describes the selected smartphone sensors. In Section IV the proposed methodology is introduced and in Section V extended experimental results are presented and discussed to evaluate the performances of the proposed technique; finally Section VI draws conclusions.

II. Related works

Device identification is a significant issue in multimedia forensics and that is witnessed by various techniques proposed so far devised to discerne among digital cameras, printers scanners and also smartphones. Already well established works demonstrated the possibility to identify digital cameras exploiting CCD sensor pattern noise extraction from

I. Amerini, R. Becarelli, A. Melani and M. Niccolai are with Media Integration and Communication Center (MICC), University of Florence, Florence, Italy. R. Caldelli is with National Interuniversity Consortium for Telecommunications (CNIT), Parma, Italy and with Media Integration and Communication Center (MICC), University of Florence, Florence, Italy.

images [2], [3], [4] proposing also the use of a fingerprint digest [5], [6]. The approach in [3] is also extended to work with video camera identification and video forgery detection [7],[8]. Others papers are devoted to exploit which kind of device has generated a certain digital image (e.g. a scanner, a digital camera, a computer generated content etc.) [9], [10], [11]. Regarding smartphone identification, some works use specific traces, like physical network ID interface, network traffic pattern [12], bluetooth signals track, and information extracted from the web browser or hidden in the header of email messages [13], [14] as device fingerprints. Another paper proposes a smartphone fingerprint on the basis of the combination of the installed applications on it [15]. On the other side, smartphone identification based on built-in sensors like accelerometer, gyroscope, magnetometer etc.. it is still in an early stage. In [16] only accelerometer sensor is analyzed and the fingerprint is extracted while the device is vibrating. The overall best results, obtained in [16], are for standalone chips, i.e., accelerometer connected to an Arduino board for data collection. This case has obviously a clear limitations in real scenarios where it is necessary to operate on a smartphone by an user. In [17] the fingerprinting of a loudspeaker and microphone is proposed in addition to the accelerometer. Data are collected when the device is lying on a surface with the z-axis perpendicular to it, first facing up and then facing down. The paper [18] presents a preliminary work with the perspective of understanding if some distinctiveness exists among smartphone sensors, in particular accelerometer, gyroscope and CCD, and how to combine them. Others works in literature propose a fingerprinting approach that uses the microphones and speakers to uniquely identify a device [19], [20]. The work in [21] introduces an important and thorough analysis on smartphone fingerprinting by means of sensors; in particular, it takes into account the combination of two sensors (accelerometer and gyroscope) to improve fingerprint reliability. In addition to this, it also investigates how to provide countermeasures such as calibration and obfuscation to avoid phone fingerprinting during web browsing for privacy preserving. In [22] smartphone identification takes place through the use of accelerometer and gyroscope with the objective to contrast MEMS components counterfeiting. In [23], magnetometer sensor is used for another task such as device pairing between two previously unassociated devices in close proximity while in [24] magnetometer, stimulated by motion patterns, is considered for smartphone identification. Differently from the others techniques briefly outlined in this section, in the current work, many sensors, such as accelerometer, gyroscope, magnetometer and speaker-microphone system, are singularly evaluated and then combined together to obtain a comprehensive fingerprint for the device identification. Features coming from the digital camera CCD sensor are not taken into account because taking pictures require a user involvement (i.e. acquiring a certain number of pictures with uniform content) and for the moment, it is important to limit, as much as possible, the interaction with the smartphone. Furthermore, more challenge operational cases have been evaluated, getting closer to a real scenario, in terms of sensor acquisition i.e. with vibration motor on or off, with audio stimuli or not and also regarding smartphone position during the acquisition (on a table or in the hand of the user). In addition, different geographical locations and time instants have also been considered for the sensors data acquisition.

III. Smartphone sensors

On-board smartphone sensors allow the devices to sense information from the surrounding environment. The usage of these sensors permits to collect raw data that can be employed to modify the way the user acts on the device. A typical device, as a smartphone, is able to interact with multiple measurements, therefore requires to use a collection of different sensors. The leading technology adopted by manufacturers is named MEMS (Micro Electro-Mechanical Systems). This kind of technology is very useful to obtain reduced-sized instruments, using a productive process based on the capacitor operative principle. Furthermore, this process could introduce an unperceivable error on the generated signal that could be analyzed to extract a fingerprint from the device. These errors are originated by imperfections introduced during the productive process of the inner structure of the sensor. Anyhow, such imperfections do not alter the expected behavior of the instrument. In conclusion, a sensor can be seen as a tiny instrument, capable of some kinds of measurements, that is subjected to an error dependent by the productive process. It is necessary to demonstrate that this kind of error is unique and systematic in order to be used as fingerprint of the device. Each smartphone, both iOS and Android, are equipped with many different sensors like accelerometer, gyroscope, magnetometer, luminosity, camera, microphone, etc. This paper considers four of the most common sensors available on Android smartphone from the 2.3 O.S. version: accelerometer, gyroscope, magnetometer and microphone-speaker. A short analysis of the structure of each considered sensor, focusing on the relevant aspects, is shown hereafter. Since Android is the most widely used smartphone operating system so far we start our investigation considering only Android smartphones; though it could be interesting to expand this analysis on iOS smartphone and Windows Phone in the next future.

A. Accelerometer

The accelerometer is a sensor that allows to measure the acceleration of the device along three axes x, y and z and it is capable to acquire measurements in $\frac{m}{s^2}$. The main application of accelerometer sensor involves gesture recognition, device orientation and movement evaluation. As it can be guessed, this sensor is involved in every situation that concerns the motion context. In particular, MEMS accelerometers measure the acceleration of the device by evaluating the displacement between one or more movable plates and a single anchored plate. Considering these plates as part of a capacitor, the resultant variation of capacity induced by the displacement (caused by the acceleration) between plates reveal the actual amount of movement impressed to the device. The variation of the capacity can be measured and converted into an acceleration value. This concept may be extended to every axis, determining the amount of acceleration impressed to the device in each direction.

B. Gyroscope

The gyroscope is a sensor that allows to measure the rotation of the device ratio along three axes x,y and z and it is capable to acquire measurements in $\frac{rad}{s}$. This instrument may be used in combination with the accelerometer sensor to better evaluate the precise amount of motion impressed to the device. Technically, employing this sensor the device is able to sense its orientation respect to the canonical coordinate system. This instrument is realized by combining vibrating masses and metallic surfaces where the acceleration and hence direction change, can be detected measuring the amount of vibration originated by the movement. On the basis of the momentum conservation principle, the considered vibrating object continues to vibrate on the same plane, hence the vibration deviations may be used to estimate a change in the direction of the orientation. These deviations are caused by the Coriolis force, which is orthogonal to the vibrating object. The slightest imperfections in the electro-mechanical structure could introduce differences across chips [25].

C. Magnetometer

The magnetometer is a sensor that allows to sense the environmental magnetic field measuring its intensity along three axes x,y and z. This instrument is capable to acquire values in $Tesla$. The main application in which this sensor is involved concerns acquiring the orientation of the device regarding the Earth geomagnetic field. This procedure may enable the correct positioning of the device on a map if used in combination with the GPS module. To realize this kind of instruments the Hall structure is adopted. A standard Hall sensor relies on the operative principle of the Hall effect which defines that a beam of charged particles is deflected from its straight path in presence of a magnetic field. As said for other sensors, even this structure can be manufactured with MEMS techniques that may determine subtle imperfections, such as a non-perfect planarity of the conductive plate or an incorrect calibration of the Hall sensor to a reference voltage.

D. Microphone-speaker

The microphone is a sensor that permits to transduce acoustic pressure waves to an electrical signal. This instrument is capable to sense acoustic signals values in dB. Basically, it is used in combination with a loudspeaker to allow users to communicate, digitalizing pressure waves produced by the user's voice in electric signal sequences. The microphone structure is composed by many modules, each one processing physical measures. Defections in the area of the moving plate may occur during the productive process and impress slight deviations from the ideal response of the microphone. Even assuming that such imperfections are not considerable during the standard usage of the sensors, these features may be inspected to determine the uniqueness of each microphone instrument.

IV. Proposed method

A. Features extraction

As mentioned in the previous section, sensors readings are affected by anomalies due to sensors imperfections. Our goal is to detect these anomalies and exploit them as an asset to understand which device generated them. To accomplish this goal, we make use of a set of features computed on signals acquired by the different sensors. The overview of the features extraction procedure is depicted in Figure 1.

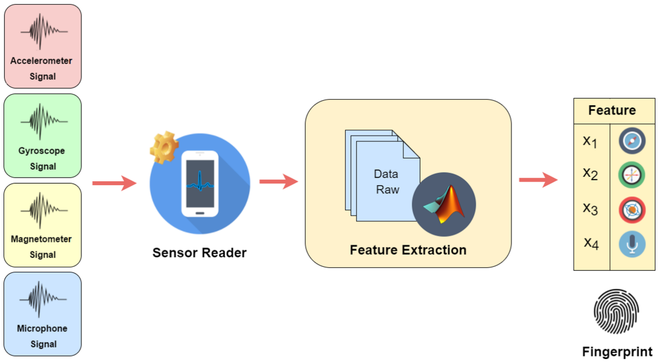


Fig. 1: Features extraction pipeline.

For each sensor using the Sensor Reader application (see Section V-A for a description of the application), the raw values along three axes of the smartphone at a certain time k are acquired (values have not been normalized [21]). So, for a given time-stamp k we have, for accelerometer, gyroscope and magnetometer, three vectors of the following form: $a(k) = (a_x, a_y, a_z)$, $\omega(k) = (\omega_x, \omega_y, \omega_z)$ and $m(k) = (m_x, m_y, m_z)$ respectively. In particular regarding accelerometer and magnetometer, a certain number of features are extracted in both time and frequency domains by using the MIRToolbox [26] starting from the following signals:

$$|a(k)| = \sqrt{a_x^2(k) + a_y^2(k) + a_z^2(k)}$$

$$|m(k)| = \sqrt{m_x^2(k) + m_y^2(k) + m_z^2(k)}$$

The frequency domain features are calculated using the interpolated $|a(k)|$ and $|m(k)|$ signals using bicubic spline (50Hz). In total a vector of 21 features (consisting of 10 temporal and 11 spectral features) is obtained to describe the accelerometer and the magnetometer (f_a and f_m respectively). In Table I all the features taken into consideration are outlined. Regarding the gyroscope, we consider data from each axis as a separate stream in the form of $\omega_x(k), \omega_y(k), \omega_z(k)$. In total a vector of 63 (21×3) features f_g is used to describe the gyroscope sensor for each device [21]. Finally, the last considered sensor is the microphone-speaker audio system, according to the paper in [17], 13 sine functions are reproduced through the smartphone speaker at increasing frequency (from 100 to 1300 Hz) and then recorded by the smartphone through the use of the microphone. From each of the frequency sample the frequency response of the audio system is computed i.e. a sinusoidal signal at the frequency of interest is compared with the acquired signal, returning a measure of the dissimilarity between them.

TABLE I: List of time and frequency domain features.

Time Features	Frequency Features
Mean	Spectral Spread
Std-Deviation	Spectral Centroid
Average Deviation	Spectral Skewness
Skewness	Spectral Kurtosis
Kurtosis	Entropy
RMS	Flatness
Max	Roll Off
Min	Roughness
ZCR	Irregularity
Non-negative count	Spectral RMS
	Low Energy Rate

Therefore the fingerprint for the microphone-speaker audio system is a vector of 13 elements $f_{ms} = h(k_i)$ $(i = [1 : 13])$, containing the value of the frequency response for each of the reproduced sine function: $h(k_i) = \frac{|S_s(k_i)|}{|S_r(k_i)|}$, where S_s is the DFT (Discrete Fourier Transform) of the sensed signal and S_r is the DFT of the reference signal. Finally, a vector of 118 features ($f_a = 21, f_g = 63, f_m = 21, f_{ms} = 13$) is obtained.

B. Training and classification

In order to achieve device identification, we propose a methodology based on supervised classification on the basis of the features described in the previous section (f_a, f_g, f_m and f_{ms}). The overall identification procedure works as follow: the system is trained based on the acquired data; then device identification is accomplished by sending a new set of features (as test fingerprint) to a classifier. For the training procedure, let us consider the d-th smartphone out of all the possible D ones. First of all, through an application installed on the device d (Sensor Reader app, see Section V-A), a variable number of sensors readings from the accelerometer, the gyroscope, magnetometer and microphone are collected. From all the sensors readings, different sets of feature vectors are computed as previously described. The application finally sends to the server all the feature sets. At this point, the system can be trained: features are combined together and used to train a supervised classifier. The employment of the Naive Bayes and the Random Forest classifiers is foreseen [27]. The Naive Bayes is a probabilistic multi-class classifier based on theorem of Bayes [28] with strong (naive) independence assumptions between the features; Random Forest bases its operation on bagging and boosting techniques limiting the variance of different *weak* learners reducing the correlation between the trees that compose the forest. In addition to the classifiers two different approaches used to combine the features are introduced, named *Big-feature* and *Multi-voted*. The *Big-feature* approach provides an unique classifier, using as input a set of features obtained by the concatenation of the fingerprint generated from each of the acquired signal (see Figure 2 (top)). In this case an *unique fingerprint* $F = [f_a, f_g, f_m, f_{ms}]$ is associated to a device for a total of 118 features. The idea of linking the features from different sensors guarantees the generalization of the model, in fact, some sensors or more specifically, some features, could be more predictive of the others. In this way the classifier is able to give more weight to the most informative features, executing a feature selection process, internally, in order to maximize the likelihood between the training and test samples. On the other side, the *Multi-voted* approach involves an ensemble of classifiers. Each classifier is trained on a subset of features related to a specific sensor. The final classification result is obtained through a majority vote among the different outputs of each classifier (see Figure 2 (bottom)). Differently from the previous case *multiple fingerprints* (f_a, f_g, f_m and f_{ms}) are associated with the device. This ensures a high degree of flexibility in the case one of the classifier returns a discordant output from the others. In fact, the response is considered an outlier and hence ignored because it is less frequent and therefore probably incorrect. In terms of features, this approach allows to give less weight to the features of the discordant classifier, unbalancing the final decision in favor of the features that generate the most voted (frequent) result. A further aspect to be evidenced is that each vote is independent, so it is possible to have a discordant classifier for a certain element and consistent with another test element. The choice of using different classifiers per sensors permits to obtain a modular approach mitigating the effect of an incorrect calibrated sensor (or even missing) in the overall result of the classification. Once the system has been properly trained, each time a smartphone needs to be identified in the test phase, a few seconds sensors reading are collected; the n-uple of features f_a, f_g, f_m and f_{ms} are computed and the identification phase takes place exploiting one of the classifier described above (Naive Bayes, Random Forest) and then combing the features with the *Big-feature* and through the *Multi-voted* approaches.

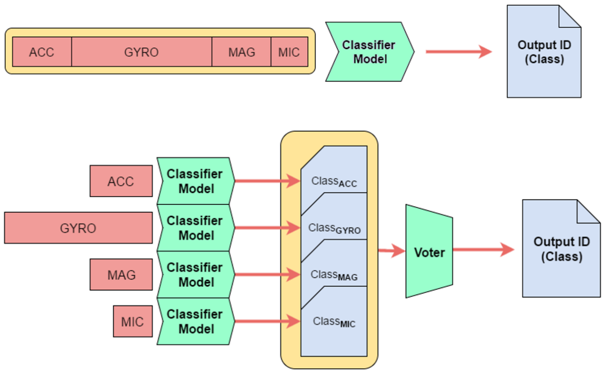


Fig. 2: The *Big-feature* (top) and the *Multi-voted* (bottom) approaches.

V. Experimental Results

In this section some of the different experimental tests that have been carried out are presented based on the technique illustrated above. First of all, the developed Sensor Reader application is described, then the set-up domain will be defined, together with the metrics adopted to verify the achieved results. Next, results obtained considering as fingerprint single sensors or a combination of them will be given, analyzing the aspects emerged from the use of different classifiers and approaches to compose the features. Lastly, it is reported an analysis on the spatial-temporal invariance issue related to the proposed fingerprinting method in order to demonstrate the reliability of the approach in a more uncontrolled scenario.

A. Sensor Reader application

Sensor Reader is a native Android application developed to extract signals originated by device sensors adopting Google APIs. This application permits to automate the acquisition of the signal coming from each sensor: accelerometer and gyroscope are recorded simultaneously and subsequently magnetometer and microphone are acquired. A calibration phase is not required to reduce as much as possible the user interaction because of the open operative context.

Acquisition	Duration	Data
Accelerometer + Gyroscope	120 s	(.csv)
Accelerometer + Gyroscope (vibration)	120 s	(.csv)
Magnetometer	120 s	(.csv)
Microphone-Speaker	39 s	data RAW (.pcm)

TABLE II: Sensor Reader acquisition details

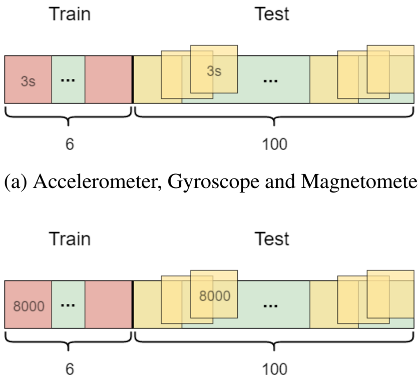
Acquisitions for MEMS are performed at the higher available frequency established by the Android operative system according to the characteristics of each smartphone both in terms of hardware resources and computational burden at that time. So acquisitions have been carried out in a very open scenario. The user can start the acquisition from all the sensors through a button, then the application proceeds to store data on the memory of the device by adopting the structure shown in Table II. Finally each acquisition set is compressed in a single zip file. In the last step the Android app sends the zip archive, via FTP, to a dedicated server.

B. Set-up description

In order to evaluate the robustness and invariance of the illustrated method, various tests have been defined. Experimental tests have been carried out on 20 Android smartphones listed in Table III, heterogeneously selected among different brands and models. To better simulate real operative conditions, some of the selected devices are identical i.e. with same brand and model (four smartphones LGE NEXUS 5, two HUAWEI U9200 and two HUAWEI ALE-L21).

Device	Quantity	Invariance Test1	Android OS
LG NEXUS 5	4	✓ (1)	6.0.1
LG D320	1		4.4
LG NEXUS 4	1	✓ (1)	5.1.1
SAMSUNG GT-I9300	1		4.3
LG D802	1		5.1.1
SONY D5103	1	✓ (1)	4.4.2
SAMSUNG GT-I9515	1		5.0.1
SAMSUNG GT-I9505	1		5.0.1
SAMSUNG GT-I9105P	1		4.2.2
HUAWEI U9200	2	✓ (2)	4.1
HUAWEI G7-L01	1	✓ (1)	5.1.1
HUAWEI MT7-L09	1	✓ (1)	5.1.1
HUAWEI ALE-L21	2	✓ (1)	5.0.0
MOTOROLA XT 1072	1		5.0.2
WIKO FEVER	1		5.1

TABLE III: Experimental devices set. In the third column, the devices adopted for the *Invariance Test1* (Section V-E) are indicated (quantity is in brackets).



(a) Accelerometer, Gyroscope and Magnetometer

(b) Microphone-speaker

Fig. 3: Training and testing samples extraction from the acquired signal.

The signals acquired by the *Sensor Reader* app are subdivided and separately used for training and testing phases. Six fingerprint samples for each sensors are used to train the classifier. Different numbers of samples have been proven and this choice was taken with the intent to grant a reliable training phase but, at the same time, reducing, as much as possible, the impact of training phase for the user. In particular, in the case of accelerometer, gyroscope and magnetometer, each sample is obtained by processing a non-overlapped chunk of 3 seconds of the signal (see Figure 3(a)). In the case of the microphone, the sampling rate used ($8KHz$) for the trace acquisition is considered, so each fingerprint is calculated on 8000 samples (see Figure 3(b)). To build the test set, in total 100 partially overlapped (60% of overlapping) samples (each of them obtained processing 3 seconds of data or the 8000 samples) for each smartphone sensors are collected (Figure 3(a) and 3(b)). This solution allows to build a test set big enough to elaborate a sufficient statistic to evaluate the results, even though a small level of correlation is injected between subsequent samples. To demonstrate that this kind of correlation does not afflict the precision measures, another test has been conducted using tracks acquired by the same smartphones in a different location and at different time (see Section V-E).

Another issue that will be investigated in the following is the case of unknown device submitted to the system as test samples. This unknown smartphone will be referred as *alien*, i.e. device not in the training set but belonging to the test set. Please note that both the evaluated classifiers (Naive Bayes and Random Forest) assign a cost $c_i \in [0, 1]$ to each test input, so it is assumed that every prediction with cost lower than 0.5 is unreliable and the test sample will be categorized as a possible unknown device. The choice of the value 0.5 has been done by computing the Equal Error Rate (EER) as point of equilibrium between the False Acceptance Rate (FAR) and the False Rejection Rate (FRR) by ranging this threshold between 0 and 1 with step of 0.1. The EER (FAR=FRR) equals 2.8% when the threshold is 0.5. Furthermore, different configurations are evaluated and summarized in four scenarios simulating the user interaction with a smartphone:

- No Vibration-smartphone on Table (**NVT**): data are collected from each sensor when the smartphone is placed on a table and the vibration motor is turned off.
- Vibration-smartphone on Table (**VT**): data are collected from each sensor when the smartphone is placed on a table and the internal vibration motor is turned on;
- No Vibration-smartphone hold in Hand (**NVH**): data are collected from each sensor when the smartphone is hold in a user hand (tiny motion is allowed), the internal vibration motor is turned off;
- Vibration-smartphone hold in Hand (**VH**): data are collected from each sensor when the smartphone is hold in a user hand (tiny motion is allowed) and the internal vibration motor is turned on;

For sake of clarity, it is important to underline again that the vibration has been considered only to stimulate the accelerometer and the gyroscope while for the sensor microphone-speaker the sinusoidal tones have been used; this has been chosen to follow the approaches already present in literature. With regards to the magnetometer, being never used in combination before for smartphone fingerprinting, it has been decided not to introduce an additional stimulation, at least in this phase; anyway the issue of the interference with sources of electromagnetic fields has been considered in the experiments of Section V-E. According to the learning techniques illustrated in Section IV-B, two types of classification models have been tested out: the Naive Bayes and Random Forest discriminative approach with *Big-feature* and *Multi-voted* features combination. Obviously the goal is to evaluate the best learning approach in term of classification accuracy but also in terms of robustness when different variables are put into play. Each classification technique is tested over each scenario previously described but also in presence of *alien* device or not, defining a great variety of tests (e.g. *Multi-voted*, Naive Bayes learning technique in **NVH** scenario).
The obtained results have been evaluated in terms of *F-score* *($F1$)* which is defined as in Equation (1):

$$F1 = 2 * \left(\frac{Pr * Re}{Pr + Re} \right) = \frac{2 * TP}{2 * TP + FN + FP} \quad (1)$$

where $Pr = \frac{TP}{(TP+FP)}$ and $Re = \frac{TP}{(TP+FN)}$ stands for *Precision* and *Recall.*

C. Single sensor fingerprint evaluation

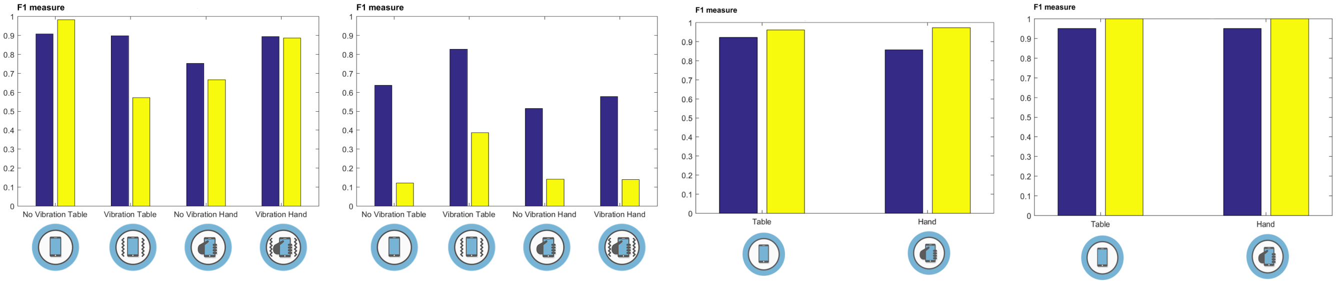
The first proposed experiment takes in exam the realization of a fingerprinting using a single sensor among accelerometer, gyroscope, magnetometer and microphone. This preliminary test is necessary as baseline to determine how much every single sensor is distinctive. What happen combining different kinds of sensors will be seen in sub-section V-D.

a) Accelerometer case: The first considered sensor is the accelerometer and to analyse its predictivity, various classification tests have been performed varying the type of classifier. Let $N_d = 20$ the number of devices; each of them represented by a single signal track acquired by our native Android application Sensor Reader. Each track has been split into two set of samples (train and test, as described in Figure 3). Let $N_{fp} = 6$ the number of fingerprint samples used to compose the training set (each composed by $f_a = 21$ features) extracted from the first part of the track. The learning matrix $\mathcal{D}$ is therefore composed by $N_d \times N_{fp} = 120$ rows and $f_a = 21$ columns. Let $N_{fp'} = 100$ the number of fingerprint samples used to compose the test set (with the same number of features of the training fingerprint samples) extracted from the second part of the track. The test matrix $\mathcal{T}$ is then composed by $N_d \times N_{fp'} = 2000$ rows and 21 columns. This train/test configuration has been adopted for every acquisition configuration. The result for each considered scenario (**NVT**, **VT**, **NVH**,**VH**) is shown in Figure 4(a) where the two proposed classifiers (Naive Bayes in blue and Random Forest in yellow) are evaluated. In particular, it can be seen that the Naive Bayes classifier provides a satisfactory performance, in fact the classification rate is on average over 0.8 except for the **NVH** case. The Random Forest classifier, instead, has obtained good results both for **NVT** and **VH** cases with $F1$ around 0.9; on the contrary, the others two configurations have given unsatisfactory performances (especially for the **VT** scenario with $F1$ around 0.6). Furthermore, it can be observed that the use of vibration does not provide a coherent improvement for both the situations (Hand and Table).

b) Gyroscope case: Taking into account the gyroscope sensor, analogous prediction tests have been performed as for the accelerometer. Adopting N_d, N_{fp} as before, but considering each sample composed by $f_g = 63$ features. So the learning matrix $\mathcal{D}$ is composed by $N_d \times N_{fp} = 120$ rows and $f_g = 63$ columns. The test matrix $\mathcal{T}$ is composed by $N_d \times N_{fp'} = 2000$ rows and 63 columns. Results of tests conducted for each scenario are shown in Figure 4(b) reporting the *F-score* value. The results obtained with gyroscope sensor are quite low respect to the accelerometer case: very low performance has been reported with Random Forest classifier and while Naive Bayes has shown good performance only for the Vibration-Table (**VT**) case with $F1$ around 0.8.

c) Magnetometer case: According to the experiments conducted with accelerometer and gyroscope, the same N_d and N_{fp} have been adopted. Considering $f_m = 21$ features extracted for each sample N_{fp}, the learning matrix $\mathcal{D}$ is composed by $N_d \times N_{fp} = 120$ rows and $f_m = 21$ columns. The test matrix $\mathcal{T}$ is composed by $N_d \times N_{fp'} = 2000$ rows and 21 columns. The results in Figure 4(c) are reported only for two scenarios the No Vibration-Table (**NVT**) and the No Vibration-Hand (**NVH**); the two classifiers are evaluated as before. The vibration was not turned on during the acquisition of magnetometer signal. The magnetometer sensors seems to be very distinctive since the classification performance are quite high for both the classifiers with on average $F1 = 0.95$.

d) Microphone-speaker case: Finally, the microphone sensor is involved in another set of experiment. Using the same N_d and N_{fp} and considering $f_s = 13$ features. The learning matrix $\mathcal{D}$ is composed by $N_d \times N_{fp} = 120$ rows and $f_{ms} = 13$ columns and the test matrix $\mathcal{T}$ by $N_d \times N_{fp'} = 2000$ rows and 13 columns. The results on **NVT** and **NVH** scenario are shown



(a) (b) (c) (d)

Fig. 4: Single sensor classification results (F1-score, in blue *Naive Bayes* and in yellow *Random Forest*): (a) accelerometer, (b) gyroscope, (c) magnetometer and (d) microphone-speaker.

in Figure 4(d). The device vibration engine in this particular case is excluded because of the possible interference with the sound emitted during the microphone recording. The obtained results are very promising, $F1$ equals to 1 when the Random Forest classifier is used and is over 0.95 for Naive Bayes.

D. Sensors combination fingerprint evaluation

After having been shown that an effective fingerprint can be extracted from each sensor (especially from accelerometer, magnetometer and microphone), tests have been focused to maximize the prediction by combining features from all the considered sensors. As introduced in Section IV-B, two different approaches have been investigated to combine sensors features: the *Big-feature* and the *Multi-voted* approach. Each approach has further been evaluated and used to train the two classifiers; *alien* devices, as anticipated at the beginning of this Section, are introduced as well in the investigation.

a) Big-feature approach set-up: Let N_d, N_{fp}, $N_{fp'}$ and f_a, f_g, f_m, f_{ms}, as previously discussed, this approach combines features extracted from different sensors in a new unique feature, simply concatenating each single feature with the schema $\{f_a, f_g, f_m, f_{ms}\}$. Let $F_{big} = 118$ the number of features obtained summing up each sensor features; as result, the training matrix $\mathcal{D}$ is composed by $N_d \times N_{fp} = 120$ rows and $F_{big} = 118$ columns, and the test matrix $\mathcal{T}$ is composed by $N_d \times N_{fp'} = 2000$ rows and $F_{big} = 118$ columns.
In the case of *alien* devices, two smartphones have been excluded from the training set construction, in order to evaluate the robustness of the proposed method to deal with unknown devices. As consequence the test matrix $\mathcal{T}$ remains untouched, but the training matrix $\mathcal{D}$ is then composed by $(N_d - 2) \times N_{fp} = 108$ rows and 118 columns.

b) Multi-voted approach set-up: The defined variables of the precedent approach are maintained but conversely to the *Big-feature* approach, this one requires a classifier and subsequently a training matrix $\mathcal{D}$ and a test matrix $\mathcal{T}$ for each sensor. So, for example, the input for the accelerometer classifier is defined by $\mathcal{D}_a$ (composed by $N_d \times N_{fp}$ rows and f_a columns) and $\mathcal{T}_a$ ($N_d \times N_{fp'}$ rows and f_a columns), and so on for each sensor. In the case of *alien* devices, the approach follows the same rule as *Big-feature*, excluding the same two devices from each $\mathcal{D}$ matrix.

c) Test results: In the following, the results obtained with the two approaches combining different features are discussed. Others tests have been carried out combining two of them (accelerometer and gyroscope) and then adding magnetometer obtaining gradual improvement; in this paper for the sake of conciseness the combination of the four sensors is reported. In Figure 5 it is possible to evaluate the results in terms of *F-score* comparing different configurations (concerning features combination approaches, classifiers, operative scenarios and presence/absence of *alien* devices). It can be seen, as general, that the performances of the four sensors in combination are improved with respect to the single sensor cases with *F-score* on average around 0.9. In particular, in the case of Naive Bayes classifier the *Multi-voted* approach (column 5) seems to be preferred respect to the *Big-feature* (column 1) giving an higher $F1$ score (i.e **NVT** scenario $F1 = 0.96$ vs $F1 = 0.8$). On the other hand, such improvement is not appreciable for the Random Forest classifier, in fact high $F1$ values are obtained both with *Big-feature* and *Multi-voted* approach showing a more stable behavior (column number 3 and 7 respectively). Furthermore, the proposed approach is also robust to the introduction of unknown devices (denominated *alien*; second, fourth, sixth and eighth column of the Figure 5), in fact the performances are in line respect to the case without unknown devices. The achieved results are very promising since in some cases, for example for the configuration *Big-feature*, Random Forest, *alien* (two unknown devices), **NVT** and **VH** scenarios a 100% of correct classification is obtained. To better evidence the obtained results, in Table IV F1-score, Precision and Recall specifically for the alien experiment are reported. In particular, such results are computed by averaging on all the cases where two devices are randomly and repeatedly left out of the training set (i.e. training set of 18 smartphones and test set of $18 + 2$). Table IV again demonstrates the good resilience of the proposed system also in presence of unknown devices. Furthermore, it is important to highlight that in the case of two LG-Nexus5 taken out as aliens and two other LG-Nexus5 instead belonging to the training set performances are completely in line with the other test situations. Results, by averaging on the four classification methods, are the following for F1-score: $F1_{NVT} = 83.91\%$, $F1_{VT} = 99.31\%$, $F1_{NVH} = 94.96\%$ and $F1_{VH} = 97.38\%$. Moreover in Figure

6, a comparison between the case of the composite (4 sensors) fingerprint and those ones with three-sensors and two-sensors is pictured. The single sensor cases have been omitted for sake of readability: anyway they are averagely comprised in the range 80%-90% except for the gyroscope that is lower. It can be observed that there is a significant improvement of the F1 score (averaged over the different classification methods) when the composite fingerprint is considered.

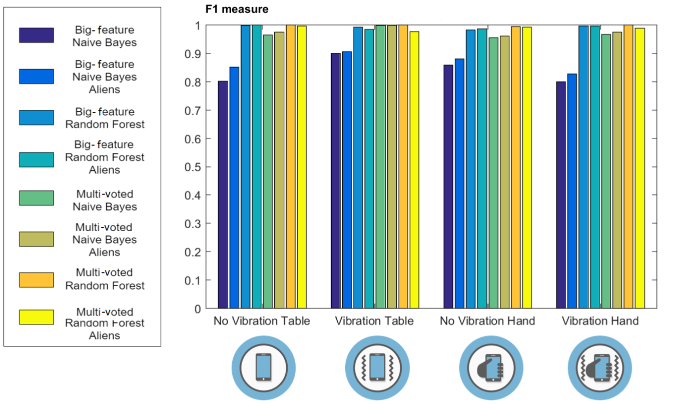


Fig. 5: Comparison among *Big-feature* and *Multi-voted* approaches, Naive Bayes and Random Forest classifiers with presence/absence of *alien* devices (the case of Motorola XT-1072 and Wiko Fever smartphones left as aliens is pictured).

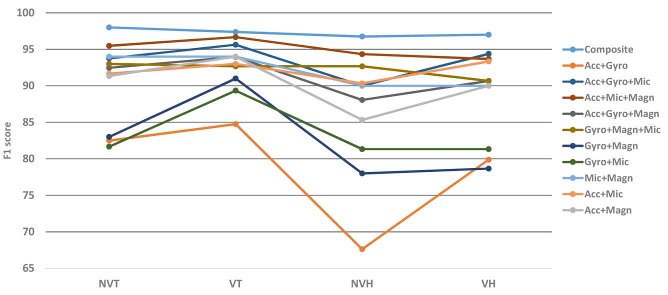


Fig. 6: Comparison of F1 score among the *Composite (4-sensors)* fingerprint, *(3 sensors)* and *(2 sensors)* fingerprint, averaged on all the classification methods.

E. Fingerprint invariance

After having shown that a smartphone can be reliably recognized within a set through the combined action of sensors fingerprints, we have tried to investigate if this still holds when test samples are acquired in different operative conditions, places and times beside the training samples as normally would happen in an operative scenario. To check such fingerprint invariance, additional tests with new tracks acquired in disparate working contexts on some sub-sets of devices used in the previous experiments have been performed. Hereafter three specific tests are reported.

a) Invariance Test1 (spatio-temporal): In this case, test samples have been acquired approximately 30-40 kilometers far from the training acquisition site and about one month later than the time of the training track. We have also tried to change the level of altitude (e.g. from 60 to 350 meters) and to add some environmental complexities such as the proximity of magnetic fields (see Figure 7 where #1 indicates the presence of a wi-fi hot-spot and #2 and #3 a train station). This has been done to understand if changes in the gravitational and magnetic fields (moreover the Earth magnetic field is not linear neither on the Earth surface nor during time) could determine some variations in sensor behavior and consequently in performances. The number of devices belonging to the sub-set used in this experiment is $N_d = 8$ and they are indicated in Table III. Tests have been conducted maintaining the same structure adopted for the previous experiments (the classifier is trained on 20 classes as before), using the same matrices structure, but avoiding the inspection on *alien* devices. The test matrix $\mathcal{T}$ is composed by $N_d \times N_{fp'} = 800$ rows and number of features variable according to the considered sensor. The results of the experiment for the all the four single sensors and the composite fingerprint cases are presented, as examples, in Table V where the difference of the $F1$ score between the current experiment (named *Invariance Test1*) and the previous one obtained in Section V-C and V-D, called here *Baseline Test*. It is possible to see that the performances on single sensors seem to generally decrease in this case. On the other side, in the case of composite fingerprint (four sensors) the performances tend to remain stable. Only in the most difficult case (when the smartphone is in the hand of the user, **NVH** and **VH**) $F1$ score slightly decrease, but not significantly.

Scenario	Acc	Gyro	Mag	Mic-Speaker	Composite
NVT	-0.03	-0.07	-0.04	-0.02	00.00
VT	-0.14	-0.03	—	—	+0.01
NVH	-0.13	+0.03	-0.12	-0.04	-0.02
VH	+0.03	-0.03	—	—	-0.04

TABLE V: *Invariance Test1 Spatio-temporal* (Random Forest, *Multi-voted*): difference of $F1$ score between the new one (*Invariance Test1*) and the previous case (*Baseline*).

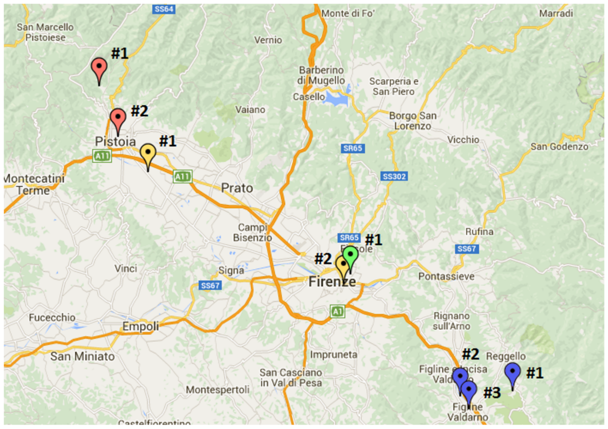


Fig. 7: Different acquisition test sites.

b) Invariance Test2 (different sensor stimulation): In this second test we have tried to understand if changing the way sensor stimulation is performed could affect smartphone

F1 (Precision/Recall) (%)	**NVT**	**VT**	**NVH**	**VH**
Big Features Naive Bayes	80.01 (86.50/74.44)	98.79 (99.17/98.43)	96.73 (99.78/93.88)	99.12 (99.31/98.94)
Big Features Random Forest	90.97 (95.50/86.86)	97.60 (98.57/96.67)	99.16 (99.50/98.84)	97.61 (97.88/97.35)
Multi-voted Naive Bayes	87.15 (91.00/83.62)	97.58 (99.77/95.50)	95.16 (98.75/91.84)	96.60 (97.74/95.52)
Multi-voted Random Forest	82.25 (86.50/78.40)	99.56 (99.92/99.20)	96.40 (99.30/93.70)	97.43 (97.45/97.42)

TABLE IV: Detailed results for alien test. Two devices are left out as aliens repeatedly: F1-score, Precision and Recall (in brackets) averaged over all these cases are presented.

Operative scenarios	**F1**	**Precision**	**Recall**
NVT audible $(0.1 - 1.3)$KHz	0.987	1.000	0.975
NVT inaudible $(15 - 21)$KHz	0.971	1.000	0.945
NVH audible $(0.1 - 1.3)$KHz	1.000	1.000	1.000
NVH inaudible $(15 - 21)$KHz	0.945	1.000	0.909

TABLE VI: Results on *Invariance Test2*: audible versus inaudible frequencies.

Nexus5	**A**	**B**	**C**	**D**	**E**	**F**	**G**
A	**88.64**	0.00	0.00	0.00	0.51	14.39	23.48
C	0.00	0.25	**93.18**	0.00	0.00	0.26	0.00
D	0.00	0.00	0.00	**99.75**	0.00	0.00	0.00
Inter-model	0.00	0.00	0.00	0.00	0.00	0.00	0.00
ALIENS	11.36	**99.75**	6.82	0.25	**99.49**	**85.35**	**76.52**

TABLE VII: *Invariance Test3 Intra-model* (Random Forest, *Big Feature*): confusion matrix. Results in percentage have been averaged over the four operative scenarios NVT, VT, NVH and VH.

classification. In particular, we have taken into consideration the sounds used for the sensor microphone-speaker. New test acquisitions have been done for 4 smartphone: two LG Nexus5 both belonging to the as-before training set of 20 and two alien devices, one Motorola XT1072 (same model but different with respect to that within the training set) and a Samsung SM-G800F. Such acquisitions have been carried out through the stimulation audio signals both in the audible range $(0.1 - 1.3$KHz) used for training and in an inaudible non-overlapped frequency range $(15 - 21$KHz with a step of 0.5KHz). This has been done with a two-fold purpose: first, understanding if the system depends on the audio stimulation and second, trying to avoid unpleasant audio tones during the acquisition that would reduce feasibility in a possible authentication phase. We have analyzed the case of the single sensor microphone-speaker and the 20-device trained classifier (e.g. audible frequencies and previous locations/times) to classify the new test smartphones acquisitions. Results are listed in TableVI; they have been averaged over the different classification methods (Naive Bayes and Random Forest) and the situations of phone on the table and in-hand are evidenced. It can be seen that performances are stable though slightly decrease when test acquisitions have been made with inaudible frequencies, that is when test conditions are decoupled with respect to those of training. Further experiments have been done by considering the case of the composite fingerprint; again the same trained classifier (now on composite features) is asked to classify test composite fingerprints acquisitions whose component, related to the sensor microphone-speaker, has been now generated with inaudible audio tracks. Achieved results confirm, also in this circumstance, the same performance stability as for the single sensor case.

c) Invariance Test3 (intra-model): In this third test, we have taken into account 7 different LG Nexus 5 (i.e. same brand and model) and made new acquisitions in diverse times (in a temporal range of around three weeks) and locations (different places in Italy, not only around Florence as in the previous experiment). In particular, 3 out of 7 devices (indicated with the letter A, C and D) belong to the initial training set of 20 smartphones (see Table III) and the remaining 4 (indicated with the letter B, E, F and G) are not included within the training set, consequently they should be classified as aliens. From the results in Table VII it can be observed that the 7 test devices are correctly associated with their corresponding classes with satisfactory values and, in particular, devices unknown to the system are individuated as aliens. It is worthy to underline that there are not inter-model errors that is LG Nexus 5 smartphones are not wrongly exchanged with other models (17 phones of the training set) but, at most, with other devices of the same kind; this happens for aliens phones and for those contained within the training set and basically indicates, as expected, that there are some similarities among the sensors of the devices of the same brand and model. In particular, in last column of the Table VII, it is to point out that the smartphone "G" is often wrongly detected as "A", but this performance is mainly determined by a poor result for the case NVH. Such experiment permits to have a vision of the whole system behavior in an open application scenario with a test set composed by devices all of the same typology.

VI. Conclusion

The basic idea proposed in this paper is to investigate how to generate a specific fingerprint that allows to distinctively and reliably characterize each smartphone to build an univocal fingerprint. In particular, the accelerometer, the gyroscope, the magnetometer sensors and the audio system (speaker-microphone) of the smartphone have been taken into account. Different experiments have been presented by considering diverse classification procedures and operative scenarios; satisfactory results have been obtained especially when all the sensors are used in combination. A significant level of smartphone distinctiveness has been achieved also demonstrating a sufficient robustness to spatio-temporal changes, different sensor stimulation and intra-model invariance. Future works will be devoted to the study of a more open-set scenarios increasing the number of smartphones involved and also to design an authentication protocol based on sensors fingerprint to be used in all those applications that require a strong mobile authentication. Future research will be dedicated to analyze the issue of fingerprint spoofing.

REFERENCES

[1] W. Stallings, *Cryptography and Network Security: Principles and Practice*. Prentice Hall Press, 2010.

[2] M. Goljan, J. Fridrich, and T. Filler, “Managing a large database of camera fingerprints,” in *SPIE Conference on Media Forensics and Security II*, 2010.

[3] M. Goljan and J. Fridrich, “Sensor fingerprint digests for fast camera identification from geometrically distorted images,” in *SPIE Conference on Media Watermarking, Security, and Forensics*, 2013.

[4] “Blind image clustering based on the normalized cuts criterion for camera identification,” *Signal Processing: Image Communication*, vol. 29, no. 8, pp. 831 – 843, 2014.

[5] S. Bayram, H. T. Sencar, and N. Memon, “Sensor fingerprint identification through composite fingerprints and group testing,” *IEEE Trans. on Inf. For. and Sec.*, vol. 10, no. 3, pp. 597–612, March 2015.

[6] D. Valsesia, G. Coluccia, T. Bianchi, and E. Magli, “Compressed fingerprint matching and camera identification via random projections,” *IEEE Trans. on Inf. For. and Sec. (TIFS)*, vol. 10, pp. 1472–1485, 2015.

[7] N. Mondaini, R. Caldelli, A. Piva, M. Barni, and V. Cappellini, “Detection of malevolent changes in digital video for forensic applications,” in *SPIE Conference on Security, Steganography, and Watermarking of Multimedia Contents*, E. J. Delp and P. W. Wong, Eds., vol. 6505, 2007.

[8] M. Chen, J. Fridrich, M. Goljan, and J. Lukas, “Source digital camcorder identification using sensor photo response non-uniformity,” in *SPIE Conference on Security, Steganography, and Watermarking of Multimedia Contents*, vol. 6505, 2007, pp. 65 051G–65 051G–12.

[9] S. Lyu and H. Farid, “How realistic is photorealistic?” *IEEE Transactions on Signal Processing*, vol. 53, no. 2, pp. 845–850, 2005.

[10] N. Khanna, G. T.-C. Chiu, J. P. Allebach, and E. J. Delp, “Forensic techniques for classifying scanner, computer generated and digital camera images,” in *Proc. of IEEE ICASSP*, Las Vegas, USA, 2008.

[11] R. Caldelli, I. Amerini, and F. Picchioni, “A DFT-based analysis to discern between camera and scanned images,” *International Journal of Digital Crime and Forensics*, vol. 2, no. 1, pp. 21–29, 2010.

[12] C. Arackaparambil, S. Bratus, A. Shubina, and D. Kotz, “On the reliability of wireless fingerprinting using clock skews,” in *Proc. of the Third ACM Conf. on Wireless Network Security*, 2010, pp. 169–174.

[13] K. Takeda, “User identification and tracking with online device fingerprints fusion,” in *Security Technology (ICCST), 2012 IEEE International Carnahan Conference on*, Oct 2012, pp. 163–167.

[14] N. Nikiforakis, A. Kapravelos, W. Joosen, C. Kruegel, F. Piessens, and G. Vigna, “Cookieless monster: Exploring the ecosystem of web-based device fingerprinting,” in *Proceedings of the 2013 IEEE Symposium on Security and Privacy*, ser. SP ’13, 2013, pp. 541–555.

[15] S. Seneviratne, A. Seneviratne, P. Mohapatra, and A. Mahanti, “Predicting user traits from a snapshot of apps installed on a smartphone,” *SIGMOBILE Mob. Comp. Comm. Rev.*, vol. 18, no. 2, pp. 1–8, 2014.

[16] S. Dey, N. Roy, W. Xu, R. Choudhury, and S. Nelakuditi, “Accelprint: Imperfections of accelerometer make smartphones trackable,” in *NDSS Symposium*, 2014.

[17] H. Bojinov, Y. Michalevsky, G. Nakibly, and D. Boneh, “Mobile device identification via sensor fingerprinting,” *CoRR*, vol. abs/1408.1416, 2014. [Online]. Available: http://arxiv.org/abs/1408.1416

[18] I. Amerini, P. Bestagini, L. Bondi, R. Caldelli, M. Casini, and S. Tubaro, “Robust smartphone fingerprint by mixing device sensors features for mobile strong authentication,” in *Media Watermarking, Security, and Forensics*. Ingenta, 2016, pp. 1–8.

[19] Z. Zhou, W. Diao, X. Liu, and K. Zhang, “Acoustic fingerprinting revisited: Generate stable device id stealthily with inaudible sound,” in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS ’14, 2014, pp. 429–440.

[20] A. Das, N. Borisov, and M. Caesar, “Do you hear what i hear?: Fingerprinting smart devices through embedded acoustic components,” in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS ’14, 2014, pp. 441–452.

[21] ——, “Tracking mobile web users through motion sensors: Attacks and defenses,” in *23rd Annual Network and Distributed System Security Symposium, NDSS’16*, 2016.

[22] G. Baldini, G. Steri, F. Dimc, R. Giuliani, and R. Kamnik, “Experimental identification of smartphones using fingerprints of built-in micro-electro mechanical systems (mems),” *Sensors*, vol. 16, no. 6, p. 818, 2016.

[23] R. Jin, L. Shi, K. Zeng, A. Pande, and P. Mohapatra, “Magpairing: Pairing smartphones in close proximity using magnetometers,” *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 6, pp. 1306–1320, June 2016.

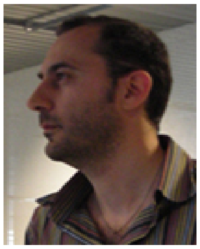
[24] G. Baldini, F. Dimc, R. Kamnik, G. Steri, R. Giuliani, and C. Gentile, “Identification of mobile phones using the built-in magnetometers stimulated by motion patterns,” *Sensors*, vol. 17, no. 4, 2017.

[25] O. Willers, C. Huth, J. Guajardo, and H. Seidel, “MEMS gyroscopes as physical unclonable functions,” in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, Vienna, Austria, Oct. 2016, pp. 591–602.

[26] O. Lartillot and P. Toiviainen, “MIR in Matlab: A toolbox for musical feature extraction from audio,” in *International Society for Music Information Retrieval Conference (ISMIR)*, 2007,

[27] T. J. Hastie, R. J. Tibshirani, and J. H. Friedman, *The elements of statistical learning: data mining, inference, and prediction*, ser. Springer series in statistics. New York: Springer.

[28] D. Barber, *Bayesian Reasoning and Machine Learning*. Cambridge University Press, 2012.



Roberto Caldelli (M’11-SM’17) received the degree in electronic engineering and the Ph.D. degree in computer science and telecommunication from the University of Florence, Florence, Italy, in 1997 and 2001, respectively. From 2005 to 2013, he was an Assistant Professor with the Media Integration and Communication Center, University of Florence. In 2014, he joined the National Inter-University Consortium for Telecommunications (CNIT) as a Permanent Researcher. His main research activities, witnessed by several publications, include digital image processing, interactive television, image and video digital watermarking, and multimedia forensics. He is member of the IEEE IFS-TC.

Rudy Becarelli graduated in Electronic Engineering in February 2004 at University of Florence with a thesis concerning motion estimation algorithms and their applications. He has been involved in research and development activities at University of Florence since 2004, he has obtained PhD in Computer Science, Systems and Telecommunications at the University of Florence on April 2016. Research activities mostly concern with digital watermarking, interactive TV and image forensics.

Irene Amerini (M’17) received the Laurea degree in computer engineering in 2006 and the Ph.D. degree in computer engineering, multimedia and telecommunication in 2010, both from the University of Florence. She is currently a post-doc researcher at the Media Integration and Communication Center, University of Florence, Italy. She was a visiting scholar at Binghamton University, NY, in 2010. Her main research interests focus on secure media and multimedia forensics.

Alessio Melani graduated in computer engineering from the University of Florence in 2016 with a thesis on smartphone sensors fingerprinting. His main research interests are machine learning and multimedia forensics. Currently he works for Engineering Ingegneria Informatica S.p.A and he is involved in design and realization of large J2EE systems based on JAX-RS paradigm.

Moreno Niccolai graduated in computer engineering from the University of Florence in 2016 with a thesis on machine learning system for digital forensics applications. His main interests are multimedia forensics, IoT systems and J2EE applications development. Currently he works for Engineering Ingegneria Informatica S.p.A. as front-end web developer for the e-health care environment.