A Survey of Techniques for the Identification of Mobile Phones Using the Physical Fingerprints of the Built-In Components

Gianmarco Baldini, *Member, IEEE*, and Gary Steri

***Abstract*—In recent years, several research studies have investigated the identification of electronic devices through their physical components and properties, both from a theoretical point of view and through extensive experimental studies. Results have shown that, in many cases, a very high identification accuracy can be obtained by exploiting imperfections and small differences in the electronic components, which are called fingerprints in this context. Part of these studies have focused on a specific category of electronic device, the mobile phone or smartphone, which is usually equipped with components, such as radio frequency front-ends, cameras, micro-electro-mechanical systems, microphones, and speakers that are likely to reveal fingerprints in their digital outputs and then allow the identification of the component and of the mobile phone itself. Keeping the focus on mobile phones, this paper provides a survey of the different techniques for mobile phone identification on the basis of their built-in components. This paper describes the methodology, the classification algorithms, and the types of features that are typically used in literature. Outstanding challenges and research issues are also identified and described, together with an overview of the potential applications of mobile phone fingerprinting. In addition, this paper analyzes the potential privacy risks associated to the tracking of the mobile phone on the basis of its fingerprints and the related mitigation techniques. Finally, it summarizes the main issues and identifies research opportunities and potential future trends for mobile phone fingerprinting.**

***Index Terms*—Fingerprint recognition, machine learning, radiofrequency identification, counterfeiting, security, telephone equipment.**

I. Introduction

THE IDENTIFICATION of electronic devices on the basis of their physical features has possible applications in different domains. In particular, if the device is a mobile phone, the capability to uniquely identify it by analysing the digital output of its components constitutes a powerful way to authenticate, but also to track, the device and its user. For these reasons, this topic has recently gained the attention of many research studies that have proposed several techniques for the identification of mobile phones using the physical characteristics of their built-in components. All these techniques are the focus of this survey.

Manuscript received September 26, 2016; revised February 28, 2017; accepted April 9, 2017. Date of publication April 17, 2017; date of current version August 21, 2017. *(Corresponding author: Gianmarco Baldini.)*

The authors are with the European Commission, Joint Research Center, 21027 Ispra, Italy (e-mail: gianmarco.baldini@ec.europa.eu; gary.steri@ec.europa.eu).

Digital Object Identifier 10.1109/COMST.2017.2694487

In this context, the physical features exploited for the identification of a specific device are called (hardware) *fingerprints*, while the term *fingerprinting* refers to the process through which these observable characteristics are extracted from the device in order to make it identifiable and distinguishable from another one of the same brand or even of the same model. The observation of these characteristics can be performed in several ways, and the aim of the paper is to show how a mobile phone can be identified and authenticated through different means and with different levels of accuracy on the basis of the physical fingerprints of its components.

The fingerprints are usually generated in the preparation of the base materials of the components and in the manufacturing process, and their insertion is accidental or intrinsic to the process itself. However, they can also be inserted on purpose like, for example, the Physical Unclonable Functions (PUF), physical entities embodied in the physical structure of a component [1]. In both cases, fingerprints are usually tiny variations in the electronic components which can be exploited for the identification of a mobile phone if they can generate observable characteristics that can be collected and analyzed with an adequate level of precision. The term *adequate* is relative to the type of imperfections and the way the observables are collected and evaluated.

The fingerprinting of electronic components has many similarities to the fingerprinting of human beings in biometrics. Indeed, some requirements for the fingerprinting defined in the biometrics domain [2] can also be adopted for the fingerprinting of mobile phones:

1) universality, which means that every mobile phone or its electronic components should have the characteristics that are used for its identification;
2) uniqueness, which indicates that no two components should have the same fingerprinting or physical characteristics;
3) permanence, which means that the characteristic should be invariant with time or with the environment conditions;
4) collectability, which indicates that the characteristics can be measured quantitatively.

Not all the requirements can be satisfied at the same time or to the same degree for all the components of a mobile phone. As we will see in the following sections of this paper, the current state of art of the identification techniques may allow only a limited degree of fingerprints permanence

(e.g., the features can vary in time or depending on the environment) or they may not be unique because the physical features are not specific enough to uniquely identify the mobile phone.

An important clarification has to be done about the terminology, in particular for terms identification, authentication and verification that, in the literature and papers we surveyed, are sometimes used with slightly different meanings. For this reason we provide the following definitions, which we will be used in the rest of this paper:

1) *Authentication*: is the process of confirming the claimed identity of a phone. Most of the techniques described in this paper have the objective to authenticate a phone through the physical fingerprints of their components, which are difficult or impossible to clone.
2) *Validation* or *Verification*: are synonyms of authentication as the concept is to verify or validate the claimed identity of the phone.
3) *Identification*: is the process by which a recognition system determines the identity of a device by comparing a captured device fingerprint with a set of reference fingerprint templates of known devices. The identification process requires a one-to-many comparison and it is more difficult than verification. Note that the identification in this context has a different meaning than in other contexts, where the identification is the process by which an entity claims to have a certain identity.
4) *Classification*: is the process by which mobile phones are classified in different classes or categories.

In the rest of this paper, we also distinguish between *inter-model* and *intra-model* classification. In inter-model classification, two mobile phones of different brand and model are classified in two different categories. In intra-model classification, two mobile phones of the same brand and model (but different serial numbers of course) are classified in two different entities. Obviously, intra-model classification is more difficult to achieve than inter-model classification, since different manufacturers may use different materials and components for different models.

While other papers have separately investigated the fingerprinting techniques and approaches for the specific components of a mobile phone, this is the first survey (to the knowledge of the authors) that identifies and describes the techniques for the whole set of built-in components in a comprehensive way. The goal is not only to describe the state of art but also to identify potential synergies among the different classification techniques and components and to propose new classification techniques, which exploit the combination of different components to improve accuracy or to address the outstanding challenges in identification and verification. An additional objective of this survey is to highlight the common identification elements and algorithms, which can be reused among different components. For example, the application of specific features and algorithms that are common in radio frequency fingerprints could also be employed in digital camera or micro-electro-mechanical systems (MEMS) fingerprinting.

The structure of the paper is the following: in Section II we identify and describe the main applications of mobile phone identification. In Section III we describe the main structure of a generic mobile phone for the consumer market with the aim to describe which components can be exploited for identification. Section IV describes the main techniques for identification of a mobile phone component (e.g., camera, RF front-end), identifying strengths and weaknesses. Due to the fact that many techniques use machine learning algorithms to classify and identify mobile phones, an introductory subsection on the main machine learning algorithms is presented. In the same section we also discuss how different techniques and components can be combined to improve the accuracy identification. Section V discusses the privacy risks, which can originate from the identification of mobile phones and describes ways to mitigate these risks (e.g., by adding noise to the digital output of the components). The section also discusses the potential trade-offs. Section VI summarizes the lesson learned from the analysis in the previous sections. Section VII analyzes future trends and potential new applications. Finally, Section VIII concludes the paper.

II. Applications of Mobile Phone Fingerprints

In this section, we identify and discuss the main applications of mobile phone identification on the basis of built-in components.

A. Fight Against Counterfeiting

As described in [3], the authentication of an electronic device, component or system is an important function in the fight against counterfeiting and Intellectual Property Rights (IPR) infringement in the electronics market. Guin *et al.* [3] have defined a taxonomy of the counterfeit Integrated Circuits (IC)s in different categories where the device identification methods described in this article can be useful. These categories include remarked, recycled, out-of-spec/defective or overproduced components. Recycled components are used IC components, which are remarked and repackaged, and then sold in the market as new. Because they are old and used, recycled components could have a different fingerprints than brand new components due to time wear or degradation. The remarking process includes the removal of markings on the package (or even on the die) and remarking with forged information. The reason for remarking is to obtain a higher specification (e.g., from commercial grade part to industrial or defense grade) and resell a cheaper component for a higher price. In this case, the difference in quality between high specification and low specification components could be identified through the techniques described in this article. For examples, Zhou *et al.* [4] show that clock stability in oscillators is directly related to the quality of hardware components. The application of radio frequency (RF) fingerprinting to fight counterfeiting is also described in [5]. Still further research work and studies are needed to evaluate how recycled and remarked electronic components produce different fingerprints from newly produced components. Out-of-spec or defective products can be subject to a similar analysis of remarked products because

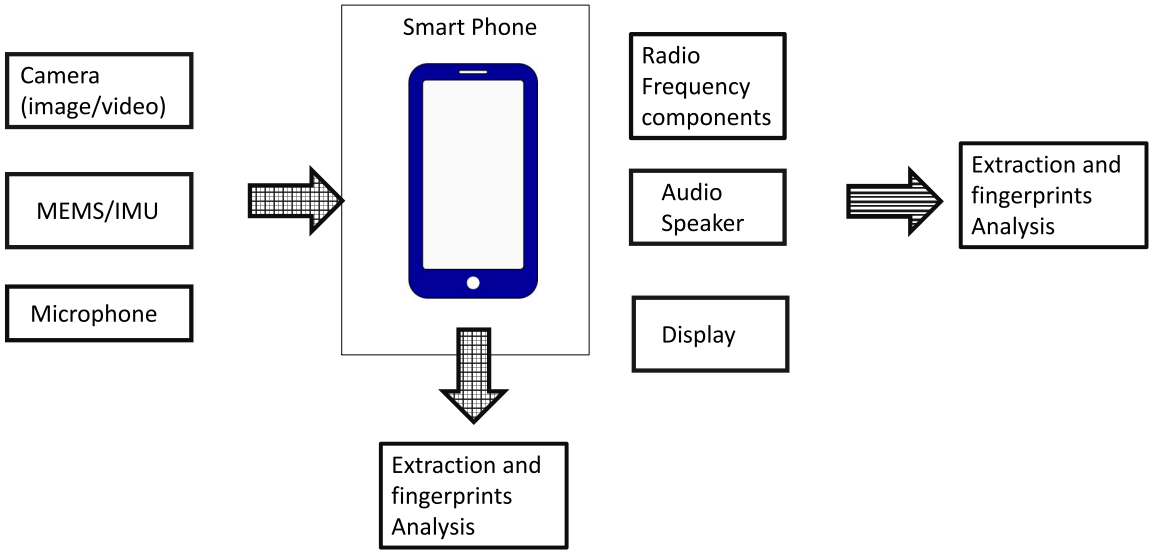

Fig. 1. Pictorial description of the main built-in components of a mobile phone, which can be used for fingerprinting.

they are built with components out of specifications or even defective. A key element for the identification of counterfeit electronic components in this category is the knowledge on how defects can modify the fingerprint of the component. For example, the research community could provide hints to investigators (e.g., a customs officer) that specific defects or low grade electronics modify the RF emissions or the data collected from the sensors in the mobile phone and that these differences can be detected by the application of specific statistical features. In another example, a low grade RF amplifier can have a distinct RF signature in comparison to a high grade amplifier and this can be detected by the analysis of the spectral response [6]. The final counterfeiting category of overproducing could be the more difficult to identify through fingerprints. Overproducing means that the electronic components are produced in the same foundry and with similar materials of proper components outside the proper contract as described in [3]. In this case, the counterfeiters gain is due to the infringement of the Intellectual Property Rights rather than use cheaper components and materials. As a consequence, the fingerprints due to material or features of the manufacturing line would not be usable to detect counterfeit products.

To summarize, the fight against the distribution of counterfeit products can exploit the techniques described in this paper for identification purposes: the goal is to find features and algorithms which can distinguish between counterfeit and proper mobile phones. Both supervised and unsupervised machine learning algorithms (see Section IV-D2) could be used for this purpose. The first set of algorithms could be used to identify if a mobile phone is a non-counterfeit item on the basis of a previously created reference library, while the second set of algorithms could be used to generate clusters of proper and counterfeit phones to support the identification (e.g., on the basis of the similarity to one of the clusters) of new mobile phones to be identified. Note that the focus in this case is both on *identification* and *validation*.

B. Authentication

Beyond fight against counterfeiting, the identification of the mobile phone has also other applications in the field of security. Multi-factor authentication using fingerprints has been proposed by many research papers like in [7] using built-in accelerometers or based on RF emissions in [8]. Here, we can distinguish between an implementation of the multi-factor authentication based on the digital output generated by the components of the mobile phone acquired externally by another device or the digital output generated by the components of the mobile phone acquired internally (see Figure 1). In the latter case, the multi-factor authentication can be more difficult than the former case because a compromised mobile phone could fabricate specific fingerprints. In this case, the integrity of the generated fingerprints must be protected using other means (e.g., cryptographic schemes) or the mobile phone could be cleaned from the malicious software before executing the test. In the case of an external device checking the fingerprints (e.g., RF emissions) the multi-factor authentication can be more effective because the processing of the observables is done by a device external to the mobile phone, which is not affected by a compromised mobile phone. An example of the authentication which exploits the RF physical fingerprints of WiFi device is demonstrated in [9]. The registration of RF fingerprints of specific wireless devices, which are allowed to operate in a specific system, could be an useful authentication mechanism in systems, where other authentication means are difficult to implement and it could be used prevent intrusion attacks. For example, RF fingerprints could be used to generate a 'white list' of authenticated wireless devices in MANETs and it could be used to implement intrusion detection (i.e., the intruder would have a different fingerprint from the 'white list'). See [10] for an example of the applicability of this approach in MANETs for intrusion detection where multimodal biometrics could be replaced or enhanced with RF fingerprints or other fingerprints. Beyond the exploitation of native fingerprints, specific fingerprints could be created

on purpose to enhance the identification and authentication as in the case of the PUF concept where specific physical structures, which are easy to evaluate but hard to predict, are inserted on purpose. There is an extensive literature on the design and deployment of the PUF concept. For example, Potkonjak and Goudar [11] provide a survey of the main PUF solutions to implement an authentication system. We note that cloning attacks on the PUF have been recently demonstrated even in a short time in [12]. The PUF concept can be applied to any component of the mobile phone even if it is mostly used in the RF based fingerprints. More details on the application of the PUF concept to mobile phone identification are provided in Section VII-A. A subcase of this security type of application is the concept of virtual proofs presented by Rührmair *et al.* [13]. The idea is that certain external physical properties of the mobile phone can be converted into digital data for authentication without any secret keys or tamper-proof hardware. This physical property is called Virtual Proof (VP) and is constructed from the response bits generated from an input image collected with the help of a light sensor. This can be applied to contexts like the Internet of Things (IOT) applications where conventional cryptographic algorithms can have limited use because of the computing and storage constraints.

To summarize, the use of the techniques described in this survey for this specific application are more focused on the *validation* of a specific mobile phone (e.g., the serial number) rather than the model identification. In comparison to traditional authentication schemes like the ones based on Public Key Infrastructure (PKI), an authentication approach provides the advantage that the authentication information is already embedded (i.e., as a physical property) in the mobile phone, while the implementation of a PKI scheme would require the set-up of a trust model and a distribution of cryptographic materials (e.g., private keys or certificates). Even if authentication based on PKI is well understood and it is currently implemented in many mobile communication systems, its set-up still requires considerable effort. The disadvantage of authentication based on fingerprints is that the fingerprint could be cloned or modified as written above. For these reasons, we recommend a combination of the two approaches with multi-factor authentication.

C. Criminal Investigation and Forensics

Another application of the mobile phone identification through its built-in components is for the criminal investigation and forensics. In this case the criminal investigators want to identify the mobile phone through collected digital output to understand if it is the same phone used in a criminal activity. One example is provided in [14], where the photos describing child abuse and collected from a Web-site or a computer are compared to the photos collected by a specific camera. By applying a camera identification technique based on the Sensor Pattern Noise (SPN) it is possible to confirm the identity of the camera under specific conditions and if the pictures have good quality. This can be a powerful tool for criminal investigation because it is not impacted by manipulation of the phone itself (e.g., removing the serial number of the phone). Additional details on this specific technique are provided in Section IV. In this application, the focus is again on the *verification* that the mobile phone is the one that collected and processed the digital artifact (e.g., image or accelerometer trace). Note that there is no control where the initial digital artifacts are collected and disturbances from the environment (e.g., background noise) could impact the validation accuracy.

D. Tracking

Another set of applications can exploit phone identification by tracking the activities of the users of a mobile phone (e.g., if (s)he is involved in illegal activities). For example, the collection and analysis of the radio frequency emissions of a mobile phone can be used by a law enforcer to track the movements of the mobile phone and his/her owner. The tracking of user through his/her mobile phone has already been investigated in literature by various authors with different means (see [15] for a description of a possible implementation and a survey on the topic). The possibility of using the RF emissions of the mobile phone for tracking has been described by Hunag *et al.* [16] where the system used to collect the RF observables is quite similar to the one described in this paper. In this application, the focus is both on the *verification* that the tracked phone is indeed the right one and the *identification* of a mobile phone among various phones in an area. In comparison to the other applications described in this section, some issues for mobile phone identification become more relevant. In particular, observables must be collected almost in real time to support tracking and, in the case of RF based identification, they may be subjected to attenuation or disturbances due to the distance where the observables are collected. Techniques based on the collection of internal acquired digital artifacts may not be appropriate because the phone's user may not desire to be tracked and the mobile phone may be configured to provide false fingerprints. In this case, similar considerations to the fight against counterfeiting application can be adopted. Externally based artifacts are preferable (e.g., RF emissions) even if they may be hampered by attenuation or fading effects as previously described. Note that the possibility of tracking an individual through the phone can also have negative implications for what concerns privacy risks. This will be discussed more in detail in Section V.

E. Quality Control

Finally, mobile phone identification could be used for the quality control of the mobile phone. In this case, fingerprints are collected from a mobile phone after the production phase to ensure that they are not dissimilar from the reference template of a specific model. If the fingerprints have a high degree of dissimilarity, this may point out to defects in the sensors or the electronic components or even the processing components of the mobile phones. After the production phase, the techniques described in this paper could also be used to give an indication of the status of the wear of the mobile phone. For example, an RF amplifier which generates fingerprints quite different from the reference template could be degraded and not able to support in a efficient way

TABLE I
SUMMARY OF THE APPLICATIONS

Application	Identification Validation	Model Specific phone	Notes
Fight against counterfeiting	Identification and Validation	Model	A compromised mobile phone could provide falsified fingerprints if they are internally acquired
Multi factor authentication (security)	Validation	specific mobile phone	The integrity of the fingerprints collected internally must be protected
Criminal investigation and forensics	Validation	specific mobile phone	Disturbances in the collection phase could decrease the validation accuracy
Tracking the activities of the users of a mobile phone	Identification and Validation	specific mobile phone	Externally based observables could be hampered by environment and distance
Quality control	Validation	Model	A golden reference template should be created for each model.

the mobile communications. Then the service provider may request it to be removed from the market. In this application, the focus is on *validation* against the reference template of the model.

F. Summary of the Applications

A summary of the analysis of this section is provided in Table I.

III. THE MOBILE PHONE COMPONENTS

The components of a typical mobile phone for the consumer market that may be exploited for identification purposes are the following ones (see also Figure 1 for a pictorial description):

- RF components for transmission and reception of different cellular communication standards: Global System for Mobile Communications (GSM), Universal Mobile Telecommunications System (UMTS), Long Term Evolution (LTE);
- RF components for the transmission and reception of short range communications like Wi-Fi or Bluetooth;
- digital cameras to collect pictures and videos. Modern mobile phones usually have digital cameras capable to capture high resolution pictures;
- Global Navigation Satellite Systems (GNSS) receiver to process signals from various GNSS constellations like Global Positioning Systems (GPS), GLObal NAvigation Satellite System (GLONASS), the European system Galileo, the Chinese Baidou and others
- MEMS components, namely accelerometers, gyroscopes and magnetometers;
- Liquid-Crystal Display (LCD) screen;
- audio components like the microphone and loudspeaker.

Each of these components can have unique fingerprints which are due to the manufacturing process of the materials used to built them. They have also specific characteristics, which can support a higher or lower degree of accuracy in the identification and validation process. Fingerprints can be difficult to be generated if the component in the list only provides pre-processed data to the mobile phone, where the physical fingerprints have been somewhat filtered or degraded. For example, compression algorithms can degrade the fingerprints of a digital camera to a certain extent. In a similar way, a GNSS receiver may not provide the raw data of the GNSS signal but rather position, velocity and time information, which is not useful for fingerprint generation. From this point of view, the evolution of GNSS receivers and the future Android N operating systems for smartphones to support the provision of raw GNSS measurements [17] can facilitate the fingerprinting of GNSS receivers. In addition, some components can be highly sensitive to the environmental conditions (e.g., magnetometers in presence of magnetic material like iron) or have specific bias which change in time and therefore impacts the stability of the fingerprints in time (e.g., clock skew).

On the basis of the listed components, the approaches to classify and identify a mobile phone through their fingerprints are basically two:

1) the digital output generated by the components of the mobile phone is acquired externally by another device (receiver or sensor) that processes and analyzes those data in order to extract the fingerprints;
2) the digital output generated by the components of the mobile phone is acquired internally by a software module or a physically connected device, and then processed either internally or externally in order to extract the fingerprints.

The first category includes the analysis of the RF emissions (e.g., WiFi) where an external RF receiver can collect the emission and process them to extract the fingerprints. This approach is often called or considered a *passive* method from the mobile phone point of view, in the sense that the mobile phone might be totally unaware of the fact that its emissions are captured and processed for fingerprinting, since there is no need of a physical contact or interaction with the device. In this case, there is the risk that the external receiver or sensor introduces its own fingerprint as described in the rest of this paper (see a discussion on the problem of portability in Section IV).

In the second category, we include the analysis of a camera, where the generated images can be processed by an external system (or by the mobile phone itself if it is capable) to extract the fingerprints. Here, the raw data should be copied directly from the mobile, either with a physical connection or with a software that collects them. In this case, there is the risk that a manipulated or compromised (from a security point of view) mobile phone can provide false digital output to avoid detection. The user of a mobile phone may have an interest for not being tracked either legitimately (e.g., for privacy reasons as described in Section V) or because (s)he means to implement a malicious activity. For example, the timestamps of the digital output of the sensors can be manipulated. See [18] for the implementation of time manipulations of the records stored in a mobile phone. In addition, the software module, which processes the raw data from the sensor can introduce its own fingerprints. For example, the timing or format of the

digital output can change from a version of the software module to another. In other words, two mobile phones with same hardware (same brand and model and different serial number) may generate different fingerprints if the software processing the sensor data applies different algorithms (e.g., compression algorithms for images). This can be an issue for some applications or it may be an advantage to identify the mobile phone as a system composed by hardware and software. It is also possible to select features that are robust (i.e., constant) against different software processing algorithms. For example, features based on timing could be avoided in the selection of fingerprints if different versions of software introduce differences in time processing.

In the rest of the paper, we will call *observables*, the samples of digital output generated by the built-in components of the mobile phone, which are collected either externally or internally.

IV. Survey of the Techniques for Different Components of the Mobile Phone

Following the categorization described in the previous Section, here we identify the main techniques for mobile phone fingerprinting which have been reported by the research community until now.

A. Generic Methodology

The objective of this section is to describe the common methodology used to collect and process the observables from a mobile phone. Note that various papers have used different approaches for different components of the mobile phone and the presented methodology may not be applicable to all the cases and references identified in this paper. Still, it is useful to provide an overview of the most common approaches for identification and verification from a tutorial point of view.

The overall work-flow is presented in Figure 3 and each phase is described in the following steps:

1) *Data Collection*. The initial phase is to collect the observables or digital output from the mobile phone either internally (e.g., camera images) or externally (e.g., the RF signals in space) as described previously. In the first case the samples must be digitized from the analog observables, while in the second case the observables are usually already in a digitized form. In RF fingerprinting collection the signal must also be down-sampled from the carrier frequency to the base-band frequency.
2) *Filtering*. In both cases (internally or externally), the digital artifacts must often be subject to a filtering process to remove bias, noise, interferences or unwanted elements, which may pollute the fingerprints.
3) *Synchronization and Normalization*. There may be the need to normalize in power and synchronize the digital artifacts unless the wanted features are not removed by these processes. For example, an identification approach based on the time differences would not require synchronization (and actually it can compromise the identification itself). In most cases, normalization is needed to remove differences related to the environment where the observables were collected (e.g., brightness in images taken from the camera or different distances between mobile phone and receiver in the collection of the RF signals). While normalization of the response is usually straightforward, the synchronization of the responses must be precise and this can be difficult in noise conditions. A common approach used by various authors (see [19], [20]) is to detect the start of the transient in RF fingerprinting using variance trajectory, which is the variance calculated on a sliding window of the time series. An example of a GSM burst and the related variance trajectory is shown in Figure 2 (the image has been produced by the authors on basis of their experimental work on GSM fingerprinting). Other statistical features and approaches can also be used for synchronization (e.g., Rényi dimension trajectory in [21]).

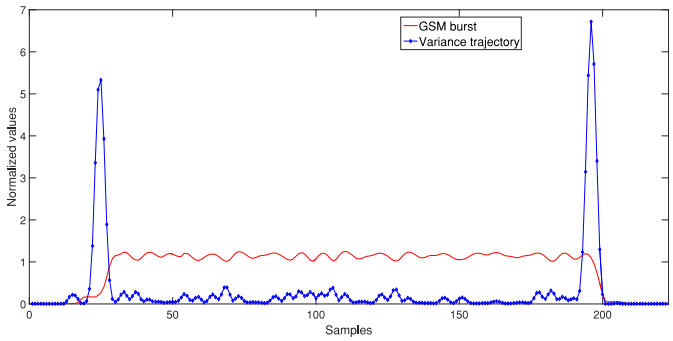

Fig. 2. Variance Trajectory applied to a GSM burst for synchronization.

4) *Content removal*. If the digital artifacts still contain content-related information this must be removed, otherwise the fingerprint creation process will be based on the content (e.g., voice in a GSM burst) rather than the physical characteristics of the built-in component in the mobile phone. The removal of the content can be achieved either by considering only parts of the observables, which are content independent or by averaging a large number of observables or by removing the content itself through an additional signal processing phase.
5) *Fingerprinting generation*. At this stage, different approaches (described in this section) can be used to generate the fingerprints or to perform the identification and verification: a) an instance based approach (e.g., correlation or mutual distance among digital artifacts generated from different mobile phones) or b) a feature based approach, where features are generated either by selection or extraction from the digital artifacts (e.g., variance of a GSM burst). A more detailed description of these two approaches is provided in Section IV-D1. Since the process of fingerprint generation is quite specific for each component of the mobile phone, the following sections will describe in detail the processes adopted in literature for each component.

B. Techniques Based on Signal Emitted by the Components of the Mobile Phone and Processed by an External System

In this category we investigate the verification and identification techniques based on external emissions of the mobile

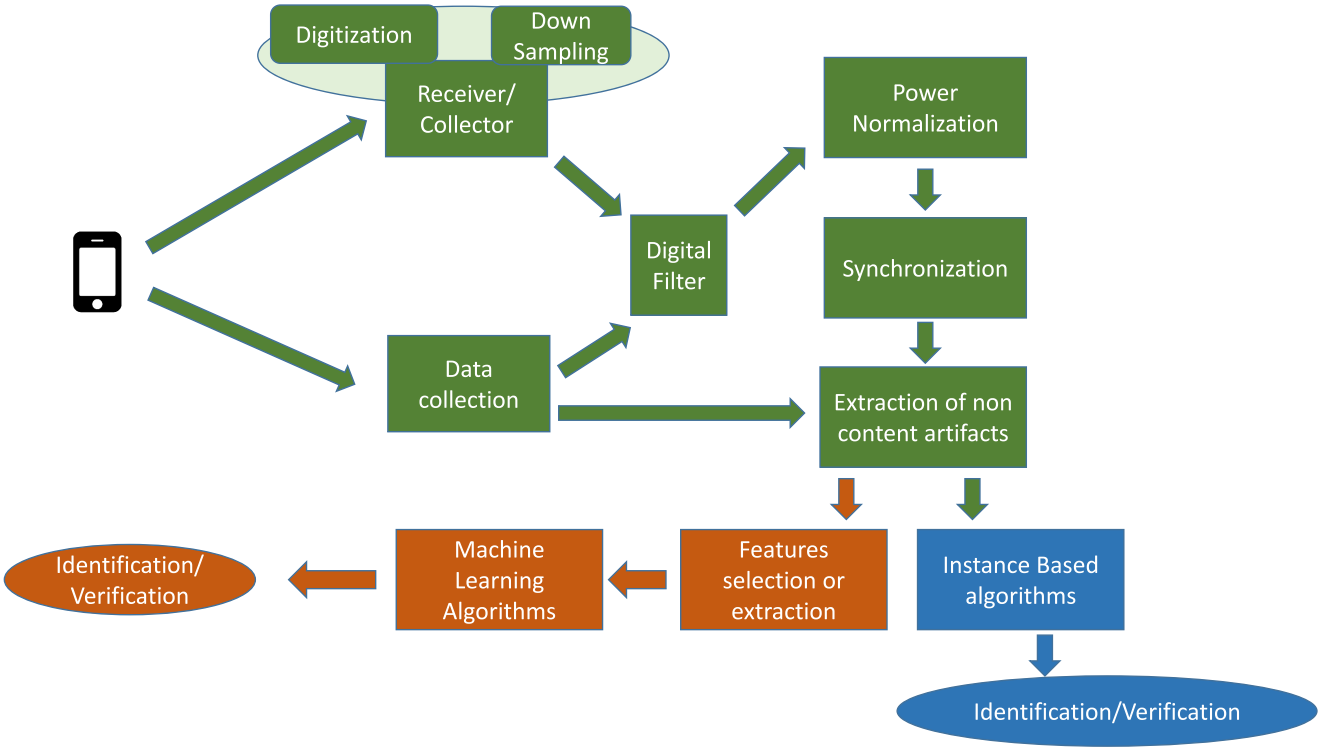

Fig. 3. Generic methodology for identification and verification.

phone, which are collected and processed by an external system. A considerable part of scientific literature has investigated the use of the emissions from the RF components of a mobile phone to identify the phone itself. As described in a recent survey on this topic [22], signal transmission in wireless communication provides various features that can be used for mobile phone fingerprinting. Similar conclusions are also provided by another survey on physical layer identification [23]. Relevant features for identification and verification can be found at all layers of the protocol stack, so that our analysis will be conducted for each layer starting from the physical one.

1) Analysis of the Radio Frequency Physical Layer of the Emitted Signal: Device identification based on the RF fingerprinting has been applied to many different wireless communication standards including:

- Wireless Local Area Network (WLAN) standards, i.e., Wi-Fi version 802.11a, 802.11b and 802.11n;
- GSM;
- UMTS;
- ZigBee;
- Bluetooth.

All these techniques exploit the imperfections and small differences in the radio frequency chain of the transmitter, which are present in the implementation of the various standards. A visual representation of these imperfections is visible in Figure 4 where the GSM bursts from different mobile phones are shown after the normalization and synchronization process (the image has been produced by the authors on the basis of their experimental work on GSM fingerprinting). Each mobile phone is represented by a different color. From the figure, we can see that physical imperfections generate small variations in the ramp up, midamble (the central part of the burst in Figure 4) or the ramp down. The content related parts of the GSM burst are usually not used for fingerprinting (the section between the central midamble and the ramps) because they contain the transmitted content (e.g., voice) and they are quite different among the various mobile phones. If the content related sections of the bursts are used, there is the risk that the fingerprint is based on the content rather than the physical fingerprints. From Figure 4, it is possible to see that each mobile phone has specific differences especially in the initial ramp up part, which can be used to distinguish the phones. In comparison, the differences in the central part of the burst (i.e., the midamble) are not so relevant and they provide lower classification accuracy. This analysis for the fingerprinting of the GSM phones is not novel and it is only provided here for tutorial purpose. A detailed experimental analysis is provided in [23].

These differences are reflected on the signals and they can be detected using the techniques described here. Wang *et al.* [24] have highlighted that any specific wireless protocol, which uses specific modulation schemes, bandwidths and Power Spectrum Density (PSD), can stimulate the RF frequency components in a different way and thus generate a different fingerprint. This means that the RF component implemented for a specific standard may generate a different fingerprint if the parameters of the transmitter change within the standard specifications. For example, the same transmission system implemented for the LTE can be requested to change the modulation scheme or the bandwidth due to environmental conditions or requests from the base station (e.g.,

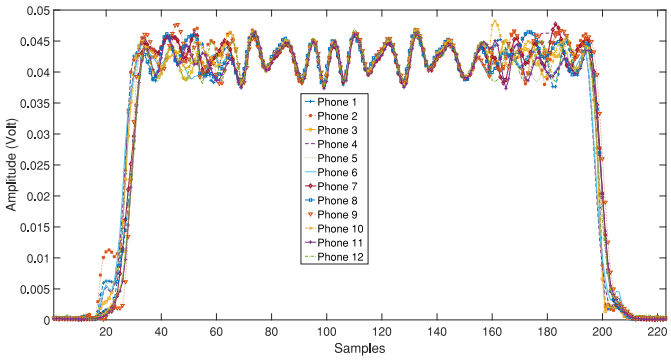

Fig. 4. GSM bursts from different phones collected by an external RF receiver.

to support higher traffic capacity). As a consequence the same transmission system and the same mobile phone could produce different fingerprints even if the same standard is used depending on the configuration and the context. Two examples from literature are provided in the following paragraphs.

Dubendorfer *et al.* [25], Reising *et al.* [26], and Patel *et al.* [27] have developed an identification framework based on the intrinsic characteristics of the devices in the radio frequency emissions which is called RF-DNA to associate them to the unique genetic features of a human being. The identification framework is based on Multiple Discriminant Analysis (MDA)/Maximum Likelihood (ML) and it has been applied to 802.11a in [28] and to GSM in [23]. The technique is based on the selection of statistical features of the collected and processed radio frequency signals emitted by the device. The collection of the signal in space is performed using a spectrum analyzer (E3238S), then the signals are down-converted, digitized and stored as complex in-phase and quadrature (I-Q) components. A filter is applied to the samples to remove unwanted interference and only the non-content sections of the bursts are used for fingerprinting. Then the statistical features of variance, skewness and kurtosis are applied to the bursts.

Dolatshahi *et al.* [29] have exploited the imperfections of the power amplifier to identify wireless devices. In particular the authors use the nonlinear characteristics of the power amplifiers and they model them with a Volterra series representation. The fingerprints are directly derived from the identified Volterra coefficients.

A significant issue in device identification based on the radio frequency physical layer is the quality of the receiver used to collect the radio frequency samples (e.g., observables). While the majority of the papers (e.g., [26]) have used high-end receivers like expensive spectrum analyzers and oscilloscopes, some authors have recently investigated the feasibility of fingerprinting with relatively low-cost receivers. An analysis of the impact on the identification accuracy between low-end and high-end receivers was recently reported in [27], where six different ZigBee devices of the same brand were analyzed using a high-cost receiver (i.e., NI PXIe-108) and a low cost software defined radio (i.e., the Universal Software Radio Peripheral (USRP) 2921 model). The cost ratio between the most expensive receiver and the low cost receiver was at least four. The results show a difference of accuracy approximately between 6% and 8% especially where Gaussian noise is present. Similar results were achieved in [20] with the 802.11a standard, where the high-end equipment is a PSA Agilent E4448A spectrum analyzer and the low-end are USRP receivers. In this case the cost ratio for the equipment was at least 10. The differences in accuracy are also higher: between 10% and 20% even in the presence of limited Gaussian noise (i.e., 10 dB for Signal Noise Ratio (SNR)). In addition, Rehman *et al.* [20] have noted a significant discrepancy in the accuracy results and suggested the use of more than one low-end receiver for the evaluation and validation of the RF fingerprinting techniques. The conclusion shown by these preliminary studies is the receivers can significantly impact the identification and verification accuracy. On the other hand, we note that both studies and similar studies by some of the same authors (see [30]) have not explored in detail how the different statistical features are less or more robust against the quality of the receivers.

Another important issue is related to portability, which is based on the consideration that a receiver used to collect the samples does also introduce a fingerprint in the measured observables. The receiver's fingerprint can negatively affect the use of samples collected using a specific receiver (e.g., for training) with other receivers (e.g., for identification and verification). In other words, the bias introduced by a receiver can compromise the *portability* of the fingerprints from one receiver to another. This issue has been experimentally investigated in [30] and [31] for 802.11a. The conclusion by both papers is not reassuring as it is demonstrated for the specific class of features used in the evaluation that the fingerprints cannot be re-used from high-end receivers to low-end receivers, and even with low-end receivers the risk of misclassification is very high. Both issues are very serious and they limit the practical applicability of RF fingerprinting for the applications identified in Section II. An example of the portability issue due to the discrepancies created by different receivers is shown in Figure 5, where the authors of this paper have collected the RF emissions from ZigBee devices using three difference receivers. The image represents a scatter plot in the bi-dimensional space on the two statistical features of variance and entropy. Different colors and shapes represent different receivers, which collect data from the same ZigBee device. The portability issue is also identified in the section of open research problems and future directions in the recent survey [22].

Different approaches could be proposed to overcome these problems. One approach is to evaluate more in detail which features are more or less robust against the quality of the receivers. To the knowledge of the authors of this paper, this approach has not been investigated in detail yet even if [22] suggests that features in modulation domain are typically more robust than those in waveform domain. Another approach proposed by [24] is that the bias introduced by the receivers could be filtered out in a subsequent phase, once the receiver features have been properly characterized. Wang *et al.* [24] propose to use the research results in wireless communication to mitigate the receiver's non-linearities and remove or

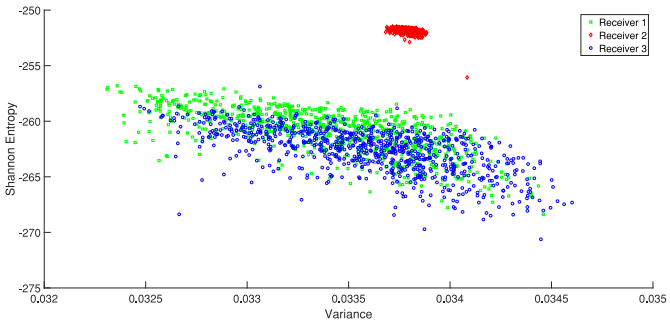

Fig. 5. Example of the portability issue for fingerprinting.

mitigate the receiver's fingerprints. In particular the following references are cited: [32] to mitigate non-linearities, [33] to mitigate non-linearities of the power amplifier and for experimental work in [34]. Still further studies and research are needed to investigate if this issue can be solved or mitigated.

Future lines of research are also related to the selection of features. Most of the identified papers use similar sets of statistical features (e.g., variance, skewness, kurtosis, Shannon entropy, coefficients of the spectrum representation of the signal) and few papers have explored and compared the different features. While techniques to reduce the dimension of the feature space, or project the features to a transformed space have been investigated in some papers like [35] for ZigBee and [26] for WiFi, there is still considerable work to do in this area. For instance, it would be useful to re-use work done in other areas or more general studies like [36], which investigates thousands of interpretable features from time series in literature. The selection of the features can also take advantage of the structure of the signal embedded in the observables. For example, the cyclostationary components of the signal in [37], where Nguyen *et al*. exploit the fact that, in OFDM signals, second-order cyclostationary statistics or Second-Order Cyclostationary Feature (SOCF) can be used for identification. This is only applicable if the signal emitted from the RF component has cyclostationary components, but this is often the case in wireless communication standards as described in [38]. Another approach would be to transform the signal in another space, where the extraction of significant features could be easier. For example, this is investigated in [39] where the Hilbert-Huang Transform is used.

An additional concern is that not many research papers have investigated the effective cost of the fingerprints in terms of complexity, requested processing power and size of the database of fingerprints.

We note that most of the reviewed papers perform an experimental analysis but there are minor and limited attempts to define a theoretical model for fingerprints which can be validated with the experimental results. In a similar way, the type of noise applied to simulate realistic conditions for identification and verification is usually Gaussian noise and this is often applied in the post processing phase (e.g., in MATLAB). One of the main reasons for these limitations in the surveyed papers is the difficulty to model the hardware imperfections in the different components (e.g., filters, amplifiers), which compose the front end of a mobile phone and therefore the fingerprints. In an effort to overcome this limitation, the authors in the recent paper [24] acknowledge this issue and present a theoretical model, which identifies the main components both in the transmission/emission chain and the environment.

Finally, another potential challenge for RF fingerprinting is related to the future evolutions of wireless communication standards like 5G and cognitive radio [40]. For example, the complexity of the communications structure in future communication systems can hamper the extraction of useful information from the RF emissions. While, the GSM bursts or the WiFi standards produce very clear bursts to which feature extraction can be easily applied, this may not be true in the future. In addition, the implementation of cognitive radio networks with underlay spectrum usage (where signals with a very low spectral power density can coexist, as a secondary user, with the primary users of the frequency band(s)) can also make difficult the process of feature extraction. Further research is needed in this area.

2) Techniques Based on the Analysis of the Medium Access Control (MAC) and Above Layers: Various references have reported the use of the MAC and above layers to identify or verify the identity of a device. One of the initial works was [41] where Kohno *et al*. have exploited the Transport Communication Protocol (TCP) timestamps option from RFC 1323 to estimate a device's clock skew and, thereby, fingerprint a physical device including wireless devices. The approach can be applied without the device's cooperation, and it doesn't require any modifications of the applications running on the device.

Radhakrishnan *et al.* [42] have proposed GTID: A Technique for Physical Device and Device Type Fingerprinting, which is based on information leaked by a device through its network traffic to identify a device and a device's type. The authors use statistical techniques to capture time-variant behavior of network traffic. The objective is to identify devices through the generated traffic and the difference in timing like clock skews using Artificial Neural Networks (ANN) for classification. The approach is validated with a very large experimental study with 300 GB of collected traffic, where realistic effects like MAC congestion were also analyzed. Finally, the authors have also investigated the robustness of the approach against specific attacks like the emulation of a valid device.

Cristea and Groza [43] exploit the Internet Control Message Protocol (ICMP) timestamp-based fingerprinting to identify mobile phones over a WLAN. As in the previous references, the authors uses the small differences in timing and they compute the clock skew of the device with linear programming techniques. The authors exploited the possibility that the ICMP timestamp option is often enabled in mobile phones and very likely there is only a small minority of users that are aware of this setting. The authors suggest that the problem can be alleviated by the user, which can either disable the ICMP timestamp requests or change the slope of the offset.

3) Techniques Based on Display Identification: The display of a mobile phone could also be used for fingerprinting even if there are no reported works on this area for mobile phones. The possibility to identify monitors through their RF

emissions has been demonstrated by Mo *et al.* [44], where an accuracy of more than 98% was achieved for LCD monitors. Two machine learning techniques were used: the ANN and the Support Vector Machine (SVM). The SVM provided much better results compared to ANN. The RF emissions were captured with a near field probe in a frequency range between 0 and 600 MHz and a spectrum analyzer. This equipment is rather expensive for a practical use of the applications identified in Section II. In addition, only LCD screens for computers and laptop were analyzed in [44], while the focus of this paper is on mobile phones' displays. Modern mobile phones use different technologies to build the display, which may indicate that the same fingerprinting approach may not be valid for all the different types of mobile phones. The fingerprinting of the display has also a limited use for some of the applications identified in Section II but it may be valuable in the application of fight against counterfeiting because the display is a significant part of the cost of a mobile phone on the basis of the published bill of materials of many mobile phone manufacturers. A producer of counterfeit phones may use lower quality materials for the display and an identification algorithm could help to identify counterfeit mobile phones.

We also note that modern displays for mobile phones do also have a touchpad function, which could be stimulated to produce unique fingerprints of the capacitive display but no work has been reported so far, even if authors have demonstrated the possibility to generate fingerprints of users thanks to the touchpad function in [45], which indicates that a high level of granularity is possible.

4) Techniques Based on Clock Differences: Another technique is to evaluate the clock drift of the mobile phone. While recent mobile phones have a very precise clock, which could also be synchronized with the GNSS, subtle clock differences could be used to differentiate mobile phones and their models. The clock differences can be extracted from various digital artifacts already examined in the previous sections. For example, from the radio frequency observables collected by an external receiver. In comparison to the techniques already described before, the generation of the fingerprints based on the clock is slightly different. In the example of the radio frequency fingerprinting, it is the timing of the occurrence of the bursts that generates the fingerprints rather than the statistical features extracted from the bursts or the mutual correlation among the bursts. The clock differences can be applied to any of the previous techniques and digital observables, where a difference in clock is relevant enough for identification and verification. As described in Section IV-B2, many techniques used the clock skew calculated from ICMP [43], TCP [41] or for various protocols as in [42].

Another approach to identify a wireless device proposed in [46] is based on the analysis of the unique characteristics of the phase noise of the transmitter's RF oscillator. In these papers, the authors have used the autocorrelation function of the Phase Lock Loop (PLL) output in 8 devices obtaining a good identification accuracy. In addition, Polak and Goeckel [46] have repeated the measurements at a distance of months to investigate the stability of the fingerprints and the impact of aging. The advantage claimed by Polak and Goeckel [46] in comparison to approaches based on the characteristics of RF power amplifiers is that these latter fingerprints can change when the transmitter's power-mode changes, while this is not the case for the PLL.

C. Techniques Based on the Internal Digital Output Generated by the Electronic Components of the Mobile Phone

1) Techniques Based on the Camera Identification: Identification of mobile phones with image acquisition capability (e.g., with digital cameras) can be achieved by characterizing the image artifacts caused by the Complementary Metal Oxide Semiconductor (CMOS) sensor [47] and/or by any of the post-processing steps (de-mosaicing filter [48], Joint Photographic Experts Group (JPEG) compression [49], etc.). This process is also called *image source identification*.

The overall image acquisition process in digital cameras is shown in Figure 6. Here we provide a brief description of the image acquisition and processing flow before the storage of the images themselves. Similar schemas and descriptions have been provided by Orozco *et al.* [50] and Swaminathan *et al.* [51], and the schema adopted in this paper is derived from them. Even if different manufacturers may implement in a slightly different way the various elements of the overall flow, the basic schema is similar.

The first element of the flow are the lens or lens system, as it may be more complex than a simple lens. The lens system can introduce aberrations in the stored image, which can be used to fingerprint the camera. Aberrations can include astigmatism, spherical, coma, radial distortion, field curvature and chromatic aberration as described in [50]. In addition, there may be components or functions to regulate the focal length of the lens, the shutter speed or the aperture size. All these functions are considered part of the lens element. Dust on the lens can also be used for fingerprinting but obviously the dust is not a permanent fingerprinting, so it is not a reliable identification feature.

The second element in the flow is usually represented by a filter like an antialiasing filter, which has the function to clean and smooth the signal prior to the analogue to digital conversion.

As described in [50], when an image is captured, it is necessary to measure three or more bands for each pixel. This may require a sensor for each band. Many camera manufacturers prefer to use a Color Filter Array (CFA) in front of the sensor. The CFA is a set of color sensors. Each sensor in the CFA blocks out a certain portion of the spectrum, allowing each pixel to detect only one specific color. In the case that a CFA is implemented in the camera, the digitized sensor output must be interpolated in a subsequent phase by using color interpolation algorithms to obtain all three basic colors for each pixel (see [52]). After interpolation, the images may be subject to different processing operations, which might include color correction, white balancing, gamma correction, lens distortion removal, lens vignetting correction, denoising and other functions. All these operations produce the final non-compressed raw image S_R. The raw image is then compressed (e.g., JPEG format) to produce S_C and then stored.

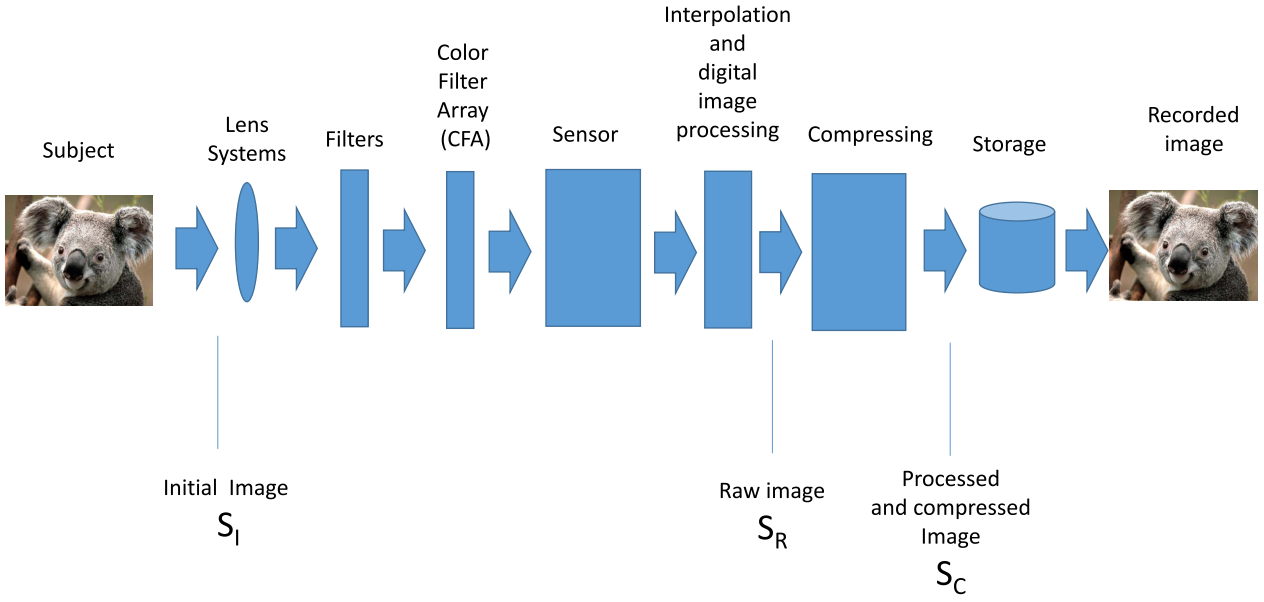

Fig. 6. Process for acquisition, processing and storage of image in a digital camera in a mobile phone.

All the components described before can contribute to generate fingerprints, which can be used to identify a specific model or brand or a specific camera (i.e., serial number from a model or brand). As described in the pioneering work by Lukas *et al.* [52], there are various sources of imperfections and noise, which can be present into the different stages of the image acquisition process. For example, even if the sensor takes a picture of an uniformly lit scene, the resulting digital image can still exhibit minor changes in intensity among the pixels. These changes are due to various hardware imperfections or differences among cameras, which include lens radial distortion, chromatic aberrations, dust on the lens, sensor pattern noise, high-International Organization for Standardization (ISO) sensitivity noise (especially at very high values, up to ISO 6400 or 12800 in modern digital cameras), white noise and shot noise. Some of these noises (e.g., high-ISO noise, white noise and shot noise) have a random distribution and if a large number of frames are used and they are added or averaged together, the noises tend to cancel out.

Here we describe the various identification techniques for each of the components. See also [53] for a recent survey on camera identification.

Lens. Low quality wide angle lenses, which are widely used for cost reasons can introduce radial distortion which has been used by Choi *et al.* [54] to obtain a 91.28% accuracy for identifying the camera source. The dust particles present in front of the imaging sensor can also create a pattern in all the captured images. Dirik *et al.* [55] exploit the presence of the dust particles for a camera identification method based on detection and matching of these dust-spot characteristics. In [55], the dust spots in the image are detected using a Gaussian intensity loss model. The authors are able to perform camera identification with low false positive rates, even under heavy compression and down-sampling. A potential issue is the permanence of these fingerprints in time, which limits the application of this technique.

CFA. The CFA and the digital image processing block in Figure 6 can employ particular sets of algorithms, which may be proprietary to the camera manufacturer, brand, or model. Because these algorithms impact all the processed images, they can be used as a fingerprint. It is obvious that these algorithms are not related to the specific camera but rather to the model, so they can be used for inter-model identification but not intra-model identification.

Sensor. The specific fingerprints of the sensor are the most used by the research community. The two most common types of imaging sensors in digital cameras are (at the time of writing this paper) a Charge Coupled Device (CCD) and a CMOS. As described in [56] and other sources, both consist of large number of photo detectors, which are commonly called pixels. The pixels (made of silicon) convert the photons in electrons using the photoelectric effect. The amount of electrons generated by each pixel depends on the dimension of the photosensitive areas, the homogeneity of the silicon material and the presence of imperfections. While, the dimension of the photosensitive area can be directly linked to the model and brand of the digital camera in the mobile phone, the imperfections generated in the pixel manufacturing process can be used for intra-model identification in a very similar way to radio frequency components for RF fingerprinting. In addition, other types of noise can be present or generated by the sensor: the shot noise, which represents random variations in the number of photons processed by the pixel or the readout noise, which is created in the sensor readout. These random components can be averaged out and they are not likely to be used to uniquely identify the camera or model. In addition to the pixel imperfections, other systematic defects can be used for fingerprinting including hot and dead pixels and dark-currents, which are noiselike patterns collected by the camera when the lenses are covered.

In his preliminary work on SPN [52], Lukas *et al.* suggested that not all the non-random noises or disturbances are recommended for camera identification. In relation to the noises

and imperfections identified above, Lukas *et al.* distinguish between photo-response non-uniformity noise (PRNU) which includes all the non-random noises and its main component Pixel Non-Uniformity (PNU), which is defined as the different sensitivity of pixels to light caused by the inhomogeneity of silicon wafers and imperfections during the sensor production process [52]. Here we note the similarity of the camera identification approach to the RF identification approach also based on imperfections during the manufacturing process. The advantage of PNU is that it is not much affected by ambient temperature or humidity and it is quite stable in time, while other non-random noises can change in time. For example, new dead pixels can appear in the camera as a consequence of its use. As a consequence only PNU is recommended for camera identification.

The most common technique based on PNU is the SPN, which is based on the non-uniformity of each sensor pixel sensitivity to light, which can be used as inherent fingerprint of a video capture device and therefore of the mobile phone. In comparison to other types of noise or imperfections having random distribution, the sensor pattern noise is a deterministic component, which stays the same for different frames and it is strengthened after being added up. Due to this property, sensor pattern noise can be used for camera identification. As described in [56], the PRNU factor can be estimated separately for each color channel (e.g., red, green and blue), thus it is possible to obtain three fingerprints of the same dimensions. As these fingerprints are highly correlated, the three fingerprints are usually converted to a single gray fingerprint using the RGB to obtain gray scale conversion.

The process to extract the SPN has been thoroughly investigated in recent years. A summary of the process is provided here, and we refer the reader to [52] and [56] and other sources. The goal is to determine if an image has been taken with a specific camera of a mobile phone. From a set of images, the SPN noise residual is extracted. The images which are more adapt to the extraction of the SPN based fingerprint are the ones with high luminance and smooth content [56]. For example, the out-of-focus image of a cloudy sky or a white wall could be optimal. It is reported that tens of images are usually enough to get a good SPN. Then, a hypothesis testing problem is formulated for camera identification, which is used to link the identity of the mobile phones. Note that the hypothesis testing problem can be based on previously recorded images. For the application of fight against counterfeiting of electronic products, a set of images in optimal conditions (as described above) can be used to create a reference library. Then, the mobile phone under test can be used to get pictures to be evaluated.

Kulkarni and Mane [57] have improved the basic SPN approach by applying Gray level Co-occurrence Matrix (GLCM) to the sensor noise from the images. Then features like Contrast, Homogeneity, Entropy and Correlation are extracted. The authors have shown that the hybrid system used for the SPN extraction along with the GLCM feature extraction yields better results than the basic SPN. Another improvement to the basic SPN identification has been proposed by Li and Li [58], where it is noted that during the image acquisition process not every color component of each pixel is physically captured. Instead, the authors interpolate the missing color components by involving the adjacent pixels according to the CFA. The assumption is that physical components are more reliable than virtual components to identify the fingerprints. Then, Li and Li [58] propose a Couple-Decoupled PRNU (CD-PRNU) approach where the physical and virtual color components are decoupled in the processed and stored images collected by the mobile phone. The goal is to prevent the interpolation error of the virtual components from contaminating the physical components during the discrete wavelet transformation process. The results show the improvement of this approach in comparison to the conventional SPN extraction approach.

Compression algorithms. A compression algorithm can be implemented in slightly different ways among different brands and models. Choi *et al.* [49] have exploited the differences in compression algorithms to differentiate camera models. As in similar cases, this technique can be used for inter-models identification rather than intra-model identification.

Combination of elements. In addition to the use of specific components in the pipeline shown in Figure 6, some researchers have also used all the components together. For example, Xu *et al.* [59] have applied an image statistical model to the whole image formation pipeline. In particular, the authors have applied moments of 1-D characteristic functions generated from the given image, their prediction-error 2-D arrays, its JPEG 2-D array and moments of 2-D characteristic functions generated only from JPEG 2-D array. We note that this approach is similar to the application of statistical analysis to the RF fingerprinting, even if the type of features is clearly different.

Video based identification. The camera and consequently the mobile phone can also be identified by video recordings. As described in [60], the camera identification based on videos can be performed by applying the sensor pattern noise to each frame of a video. However, videos can be contaminated by blocking and blurring, which can decrease the identification or verification accuracy. Chen *et al.* [60] have calculated that even with a rate of about 500 kbps, more than 20 minutes of video are needed to get a decent accuracy. For this reason the authors have proposed additional identification methods based on the mitigation of the blocking and blurring effects (e.g., by using the part of the frame not subject to blurring) and the combination with the wireless fingerprints of the video-camera on the basis of the consideration that wireless cameras often capture the scene and stream to another device or a sink in real time. These new identification methods perform significantly better than the previous ones in term of accuracy. Even if this is a good example on the power of combining different techniques to improve accuracy in camera and mobile phone identification, this may not be applied to all types of mobile phones where the video will be stored in the mobile phone itself. The combination of the techniques based on different components of a mobile phone will be discussed more in details in Section VII-D.

2) Techniques Based on the Microphone Identification: This technique is similar to the identification of mobile phones

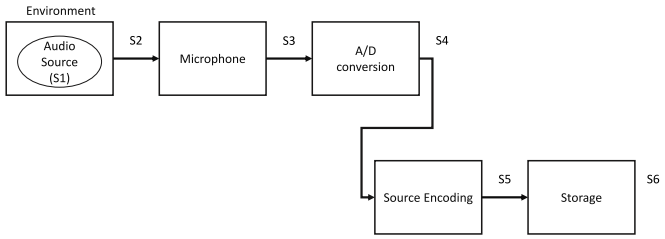

Fig. 7. Components of the audio processing.

with the image acquisition capability described before; however, it is applied to audio samples instead of images or video. As for other components, the differences in the production create microphones with slightly different transfer functions for the audio signal collected in the space.

Verification and identification of mobile phones with audio acquisition capability (e.g., mobile phones, tablets, webcams, camcorders, cordless phones) can be achieved by analysing the response of the audio circuit to a standard stimulus (e.g., a standard tone). Because of the nominal values of the electronic components and the different designs employed by the various manufacturers, the microphones of the different mobile phones introduce a different convolution distortion of the input audio signal (i.e., frequency response), which becomes part of the recorded audio.

Some work [61]–[64] has been already done in this direction in the context of digital forensics to exploit such phenomena, which will be described in detail here.

The typical design of a microphone system and the transfer functions used in the audio collection and recording are well described in literature. Here we use the descriptions and definitions from [65], which gives an overview of the whole chain as described in Fig. 7. We use the signal representation in frequency.

The initial audio signal is represented by the function $S_1(f)$. This audio can be created by an electronic source or by a natural source. The original signal $S_1(f)$ is influenced by Echo impact or by the environment in general. As a consequence, the signal $S_2(f)$ captured by the microphone can be expressed as:

$$S_2(f) = S_1(f) \bullet F_{Echo} + S_{Env}(f) \tag{1}$$

where F_{Echo} represents the effect due to the presence of echoes and reverberations. $S_{Env}(f)$ generally represents the other environment effect or the presence of background noise.

The signal S_2 is then collected and processed by the microphone itself and its components, which may include the diaphragms, pre-amplifiers, AD components and others. Indeed, the most common microphones for mobile phones are MEMS today, even if the technology is still evolving.

The combination of the analog audio processing and the AD processing can be represented by the following functions:

$$S_3(n) = Quantization(Nbits, sampling(f_s, S_3(t))); \tag{2}$$

$$S_3(f) = \int F_{mic}(f) \bullet S_2(f) + N_{mic}f + N_{ENF}(f)df \tag{3}$$

where $S_3(f)$ is obviously the Fourier transform of $S_3(t)$. $S_3(n)$ is the quantization of $S_3(t)$ by the Analog Digital Converter (ADC) with a sampling frequency of f_s. Note, that a quantization error should also be introduced in the equations above. On the other side, Marco and Neuhoff [66] show that the quantization error can be modeled as additive white noise and it has negligible correlation with the signal and an approximately flat power spectral density especially with high resolution quantization. As a consequence, in most cases, it can be considered as non-relevant for the identification of the microphone fingerprints even if this assumption could be challenged by future research and for specific types of audio signals. In our model, it is included in F_{MIC}. N_{ENF} is the Electric Network Frequency (ENF) influence, which is considered constant and negligible for classification and identification [65]. F_{mic} is the transfer function of the microphone and its components (including pre-amplifiers and ADC). This is the transfer function most commonly used for classification and identification as it usually contains the specific fingerprints of the microphone. N_{mic} denotes the thermal noise that the microphone generates and it is usually understood that it does not contain fingerprints.

$S_3(n)$ is then processed through encoding where several encoder options are available: Pulse Code Modulation (PCM), MPEG-2 Audio Layer 3 (MP3) or Advanced Audio Coding (AAC). The encoding algorithm usually does not introduce fingerprints but it can introduce an impact on the fingerprints in F_{MIC}. Finally, $S_3(n)$ is stored in the memory of the mobile phone. Usually, this last step is not considered in the detection of fingerprints.

As written before, the efforts by the researchers is to identify relevant fingerprints in F_{mic} and to mitigate the impact of the external environment noise and echoes $S_{Env}(f)$ and F_{Echo} or internal noise, which can degrade the fingerprints at different levels.

Kraetzer *et al.* [67] have investigated the impact of the environment where the mobile phone is present and they propose that the environment used for the collection of the fingerprints for training is mostly similar to the environment used to collect the samples for verification and identification. This approach may not be applicable in some of the applications described in Section II. Another mitigating approach is based on the application of de-reverberation algorithm, which can mitigate the impact of the echoes F_{Echo}, but this would require the application of this algorithm in the collection phase, which is again a strong limitation for some applications.

The most common approach to identify the fingerprints is through the application of features to the recorded audio signals. Hanilci *et al.* [64] use the Mel-Frequency Cepstrum Coefficient (MFCC) for the definition of the features as it is commonly employed as a feature to characterize speakers and, in their paper, they apply it to the identification of the brand and model of the mobile phone.

The motivation to choose the MFCC is because the envelope of the spectrum multiplied by a filter bank is more useful for identification in comparison to the speech spectrum itself. Then the authors apply SVM to a set of 14 different phones. Apart from two phones, which are of the same model and brand, all the other phones have different brands and models, so the analysis is mostly for inter-model verification and identification rather than intra-model. The authors point out

that one of the most challenging problems for the application of SVMs in speech processing is the huge amount of data to be processed. For example, in [64], the features are extracted from 30 ms frames with a 50% frame shift and the training test data for a set of speech samples is a sequence of vectors rather than a single vector. As a consequence, the Generalized linear discriminant sequence (GLDS) kernel was used to perform the classification. The 14 phones were submitted to a recording phase with 100 different speech samples. Then the feature extraction based on MFCC was applied to the recorded samples. As described before, the classification and identification was performed with SVM and the GLDS kernel function. The resulting accuracy is quite high: around 95% for specific type of phones. The performance of SVM was also compared to another algorithm: the Vector Quantizer (VQ), which is a quantization technique from signal processing that allows the modeling of probability density functions by the distribution of prototype vectors. Initially used as a compression algorithm, it has also been used for speaker classification [68]. Hanilci *et al.* [64] prove that SVM is superior to VQ.

The use of MFCC as statistical features has also been adopted in [67], where the identification is performed by a Naive Bayes classifier at a short-time frame level on 4 microphones. Accuracies on the order of 60-75% have been reported, which seems to indicate the SVM is a better classifier.

Another set of features was used in [63], including the random spectral feature. In [63], raw feature vectors of large size are obtained through the averaging of the log-spectrogram of a speech recording along the time axis. The parameters of each component of the Gaussian mixture model for the speech recorded by a specific device are stacked to compose the fingerprints. A sentence from the TIMIT database (also used by the other papers) is used as an input to 21 cell-phones of various models from seven different brands. There were no phones of the same model and brand (i.e., no inter-model classification). Landlines phones were also used but they are not considered in this survey. The features were then fed to three distinct classifiers: the Sparse representations Classifier (SRC), the SVM and Nearest Neighbour (NN). In a recent paper [69], Zou *et al.* have used sparse representation based classification methods for a set of 15 mobile phones applied to the built-in microphone. As in the other papers, the authors use MFCC based features to construct the learning dictionary. The authors obtain a very good inter-model classification but a limited intra-model classification.

3) Techniques Based on Accelerometers or Gyroscopes: Modern mobile phones contain electro-mechanical components like accelerometers and gyroscope, which do also contain specific physical characteristics exploitable for fingerprinting. Figure 8 shows the digital output generated by the gyroscopes embedded in three different smartphones when each smartphone is submitted to the same specific motion pattern (the image has been produced by the authors on basis of their experimental work on MEMS fingerprinting). We note subtle differences among the three digital outputs, which can be used to identify the specific smartphone.

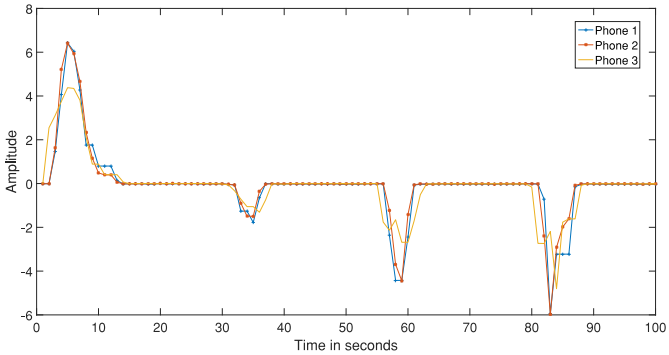

Fig. 8. Gyroscope response in three mobile phones stimulated by a specific motion pattern.

The extraction of fingerprints from accelerometers or gyroscopes (commonly implemented with MEMS) and their use for device and user identification was first described in [70] and [71]. Both studies showed how data collected from MEMS (mainly accelerometers), also remotely by cloud applications, could actually lead to the fingerprinting of the sensor and the device, thus allowing the identification of the user.

The analysis in [70] considers both embedded and stand-alone sensors, from which data are collected while the device (a mobile phone) or the stand-alone MEMS is vibrating. *Traces* of 2 seconds of duration are analyzed in order to extract the fingerprints using statistical features and supervised learning to distinguish between different sensors. When the classifier is trained with vibrations of at least 30 seconds, the calculated precision and recall are above 87%, but many variables like the type of sensors (built-in or stand-alone), the presence of casing and surface on which the device is lying, may result in different levels of accuracy for each of these cases. For example, the casing reduces the precision and recall to 60%, while the identification of the sensors on different surfaces can reach almost 80%. In addition, the best results are obtained for stand-alone sensors, thus limiting the applicability for the identification of mobile phones. From this point of view, [71] (which extracts fingerprints also from microphone and loudspeaker) proposes a more realistic scenario in terms of users identification from their mobile phones. Here the data of accelerometers in mobile phones from over 10 thousand mobile devices are acquired using a JavaScript code running on the browser. Then, the samples are collected when the device is lying with the Z axis in vertical position (first facing up and then down), so no vibrations or complex movements are required (only the gravity force is used to measure the acceleration on the sensor). However the results present very different level of accuracy when only few devices in the lab are analyzed and when data from more than three thousand devices are collected through a webpage. In the first case the percentage of correct identification reaches 85%, while in the second one only 15%.

The fingerprints of accelerometers or other built-in MEMS components can be used for multi-factor authentication as proposed in [7], but other applications can be also for detection of counterfeit smart phones or other electronic devices.

Baldini *et al.* [72] present the experimental identification of smartphones using their built-in accelerometers and gyroscopes. Data are collected when the phones are subject to repeatable movements performed by a high precision robotic arm, so that a considerable data set from which extracting several statistical features is obtained. Then, using a SVM classifier, phones of the same brand and model are identified with an accuracy higher than 90% for some combination of features. The analysis presented in [72] allows to identify which are the best features for each sensor and so on. Results show that built-in accelerometers and gyroscopes, if properly stimulated, can be used to extract fingerprints that allow a very precise intra-model identification, thus confirming the applicability for anti-counterfeiting or other applications.

4) Techniques Based on Magnetometers: Another component of the MEMS in the phone is the magnetometer, which can be used as a compass. The use of the magnetometers in the mobile phones has been exploited for navigation in [73] and for security applications. In particular, Jin *et al.* [74] have used the magnetometers to pair smartphones in close proximity by exploiting correlated magnetometer readings. In another application, Jiang *et al.* [75] have used the magnetometers to receive information from a test electromagnet system. At the time of writing this paper, there is no published research work, which investigates the application of magnetometers to identify and fingerprint mobile phones through their magnetometers apart for a preliminary pre-print research work where the built-in magnetometers of a mobile phone are stimulated using an external solenoid [76]. We can envisage that a significant challenge would be the repeatability of the fingerprints in different times or context as the magnetometers are quite sensible to the presence of magnetic fields (e.g., metallic objects) or they would require periodic calibration.

5) Analysis on the Complexities and Performance of the Different Techniques: Here we summarize the key differences from the point of view of the design and deployment complexities of the different techniques and their performance. A significant difference is when the data is collected by an external entity (e.g., RF fingerprinting) or internally by the mobile phone itself. In the first case, the impact on the performance of the mobile phone is negligible because all the data collection and processing is done externally. In the second case, the impact on the mobile phone is not negligible and it can vary according to the type of fingerprint. For the MEMS sensors like accelerometers, gyroscope and magnetometers, a specific application must be installed in the mobile phone to collect the data, process it and eventually distribute it to an external processing entity. While the collection of data from MEMS is supported by various libraries and applications, there is the risk that different applications provide different results and thus different fingerprints. In addition, if the fingerprints are used for an application, which requires on-time identification, the impact on the run-time performance of mobile phone can be significant both because a process will be running (e.g., the AndroSensor application to collect data from accelerometers) and because data may be sent to an external entity (e.g., a cloud server) for further processing, which impacts the connectivity performance of the mobile phone. In image, audio or video based identification, the performance impact can be minor as the image processing and storage is usually done by built-in components of the mobile phone, even if the connectivity can be impacted if the collected data must be sent to an external entity. While there is no performance impact on the mobile phone itself when the data is collected externally to the mobile phone, there are still complexities to address. For example, the collection of the RF signal may not be executed in ideal conditions with presence of interference, attenuation or fading effects that hinder the identification process as described in [24]. A potential issue is that the presence of such disturbances (e.g., interference) may be evident only in the post-processing phase of the observables. A significant issue for the applicability of mobile phone identification in various applications is the stability of the fingerprints in time or for different environmental conditions. While some papers investigated the classification stability in time (e.g., observables taken in different months) for specific components (e.g., accelerometers in [72] and RF oscillators [46]) and found that the impact of components aging for a duration of months is limited (i.e., classification accuracy does not change significantly), many more studies are needed to specifically investigate the impact of aging or different environmental conditions [77]. Additional details on this issue, which could a potential research area are presented in Section VII. In relation to the applications identified in Section II and Table I, each built-in component provides advantages or disadvantages for the different applications. A qualitative summary of the feasibility of the different components for different applications is provided in Table II. Note that this analysis is based on the current state of art in literature and this may change on the basis of future findings from the research activities.

D. Features and Algorithms

This section provides an overview on the features and the algorithms used for identification and verification. In the first subsection, we describe how the fingerprints can be extracted from the observables collected from the different components of the mobile phone. In the second subsection, we describe the algorithms used for classification, identification and verification.

1) Generation and Selection of Fingerprints: In this section, we describe how the fingerprints can be generated from the digital output collected either internally or externally from the mobile phone. The goal is to identify the unique or specific characteristics of the built-in component and/or the mobile phone, which can be used to fingerprint the mobile phone.

There are two different approaches for fingerprinting generation, which are also mentioned in [22]: passive or active generation of the fingerprints. In the first approach, the entity responsible for identification or verification collects the observables when the mobile phone is in a operating mode and it is executing a specific function (e.g., communication). For example, a RF receiver can extract the variance from the GSM bursts transmitted by a mobile phone. In the second approach, the mobile phone is stimulated by various means to trigger a response. For example, a message can be injected, or the

TABLE II
RELATION BETWEEN COMPONENTS AND APPLICATIONS

Component	Applications	Note
Radio Frequency front end	Fight against counterfeiting, forensics, tracking, quality control, multi factor authentication	An external system is needed to collect the fingerprints
Display	Fight against counterfeiting, quality control	Limited research work has been done to prove its feasibility
Clock differences	Fight against counterfeiting, quality control, forensics	Further work is needed to ensure fingerprints stability
Digital Camera	Fight against counterfeiting, quality control, forensics	Forensics is the primary investigated application
Microphone	Multi factor authentication, forensics	Forensics is the primary investigated application
Accelerometers, Gyroscopes and Magnetometers	Fight against counterfeiting, forensics, tracking, quality control, multi factor authentication	The implementation of the application requires an installed and active program on the mobile phone to collect and process the sensor data

accelerometers of the mobile phones are stimulated by a specific motion pattern applied to the mobile phone itself. The advantage of the first approach is that it is more covert than the second one and it is usually easier to implement as no specific action is needed. The advantage of the second approach is that it provides greater control for the generation of the fingerprints. For example, the stimulating pattern can be chosen to improve the specificity of the fingerprints and therefore the overall identification or verification accuracy.

Another important element in fingerprint generation is the selection and composition of the specific characteristics in the observables. If we consider the digital observables as time-series, then the research work on the analysis and classification of time series can be used for classification purposes.

In this paper, we adopt the wide classification proposed in [36]. When the time series of a set of observations encode meaningful patterns that can be easily compared, new time series can be classified by matching them to similar instances with a known classification (supervised learning) or by clustering them in clusters with similar patterns (unsupervised learning). In [36] this approach is called *instance-based classification*. Another approach is based instead on the representation of the time series using a set of derived properties, or features, and thereby transforming the temporal problem to a static one. In [36] this approach is called *feature-based classification*. In some cases, the two approaches can be combined. For example, the correlation of a new time-series of observations against a golden reference (e.g., a synthetic modulation scheme) could be used as features of the new time series.

The advantages and disadvantages of two approaches are summarized here even if we note that this summary can be a simplification since the effectiveness of each approach depends on the type of fingerprinting, the structure of the observables and other factors. In addition, it is also possible to combine the two approaches, as shown in some of the paper we identified.

The advantage of the *feature based* approach is that it transforms a temporal problem in a static one and the classification and identification can be therefore more computationally efficient once the statistical features have been generated. Another advantage is the presence of many statistical features that can be used for classification. This provides a larger set of tools for identification even if there is the risk that some statistical features are similar or correlated and they do not provide a significant increase in accuracy. The disadvantage of the feature based approach is that it usually requires a statistical significant number of observables from the mobile phone to perform an accurate identification and verification. For examples, if the number of collected RF bursts is relatively limited in number, the feature instances may not be large enough for a correct classification. On the contrary, the instance-based approach can be applied even with a limited number of time series granted that they are long enough. Another disadvantage of the feature based approach is that it is not known a-priori which are the most significant features for the component under investigation. This justifies the large number of papers using a feature-based approach where the most significant effort is focused on the identification of the best features. Another aspect, still to be investigated, is the robustness of the two different approaches against different environmental conditions (e.g., presence of RF interference, multi-path fading and attenuation). This aspect is highlighted and further elaborated in the section of Future Trends and research opportunities Section VII.

Regarding the feature based classification, many papers focuses on the selection of the best features from the many available in literature. A priori knowledge of the type of time series can provide useful insights on the type of statistical feature to apply. For example, in wireless communication protocols like GSM and WiFi the information is usually implemented in time bursts (as described in Figure 4 for GSM). As a consequence, skewness is an appropriate statistical features to identify specific distortions in the symmetry of the bursts.

The identification of a small subset of features is critical to improve the efficiency for the verification and identification process because the calculation of statistical features requires a big amount of time or memory storage, which actually should be minimized. Two basic approaches, well known in literature, are possible: *feature selection* and *feature extraction*. Feature selection is defined in [78] as follows: "given a set of candidate features, select a subset that performs the best under some classification system. This procedure can reduce not only the cost of recognition by reducing the number of features that

need to be collected, but in some cases it can also provide a better classification accuracy due to finite sample size effects". Various algorithms have been defined in an extensive literature for feature selection. The identification of the algorithms for feature selections is out of scope of this paper and the reader can refer to various references for a description of the algorithms and the various domains where they can be applied. Starting from the initial work of [78], a more recent paper [79] has investigated the surveyed algorithms from an experimental point of view. Even more recently, Fulcher and Jones [36] have investigated the performance of thousands of time-series features collected from literature. The authors have introduced a method that compares across these features to construct feature-based classifiers automatically. The other approach is feature extraction where a new set of features is built from the original feature set. One well know feature extraction technique is the Principal Component Analysis (PCA), whose goal is to find an orthonormal, ordered basis such that i-th dimension represents as much variance as possible while keeping the orthonormality with the other dimensions. Note that feature extraction involves a transformation of the features, which often is not reversible because some information is lost in the process of dimensionality reduction. This could be an issue for fingerprint identification, because the relationship between the feature and its physical meaning may be lost. For example, the skewness may represent the distortion of a WiFi burst while a synthetic feature generated with PCA may not have a clear physical meaning. This difference can be relevant for fingerprinting collection when the observables are measured and collected in a noisy environment that impacts the different features in a different way. For example, it may be possible to define theoretical models to evaluate the impact of fading effects on specific RF features like variance, but the same approach would be quite difficult to apply for extracted features. In the following paragraph, we describe how the authors in literature have applied the approaches identified before.

Regarding feature-based classification, in radio frequency physical layer fingerprinting, statistical features such as variance, skewness and kurtosis are used in various papers like [25] for ZigBee standard, in [28] for WiFi and in [23] for GSM. In all these papers MDA with maximum likelihood ML estimation is used as a supervised classification algorithm. As described in [28], MDA is an extension of Fisher linear discriminant (FLD) process for more than two classes. For a 3-class problem, the Fisher-based MDA process projects higher dimensional data onto a 2-dimensional Fisher plane to maximize the inter-class distances and to minimize the intra-class distances. Even if MDA/ML has proven to be effective in many classification problems, Klein *et al.* [28] report that it does not provide implicit insight into the relevance of each feature for fingerprinting. This issue prevents the identification and removal of features, which provide little or even conflicting information to the classifier. As a consequence, the authors have adopted in [26] the Generalized Relevance Learning Vector Quantization Improved (GRLVQI) classifier first presented in [80] to perform feature Dimensional Reduction Analysis (DRA). For device identification, the advantages of GRLVQI are described in [26] and briefly summarized here: 1) feature selection if performed in conjunction with classification, which is more cost effective than trying the classification process with different set of features, 2) the classification process is well-suited for cases where the number of inputs are comprised by noisy or inconsistent data and 3) a relevance ranking is assigned to each RF-DNA fingerprint feature, which provides a direct measure relating feature significance to the classification decision. While GRLVQI is more cost effective in the selection of the features (e.g., 90% reduction for the number of required features), the overall accuracy presented in [26] is not significantly higher than the one obtained by using MDA/ML, when it is applied to WiFi and Wireless Medium Access (WiMAX) signals and it is actually lower in some cases. We note that the statistical features used in [26] are similar to the ones chosen in the previous papers (see [23], [25], [28]) with the addition of standard deviation. Other authors have expanded this set of features or applied it both in time or the frequency domain.

Yuan *et al.* [81] use an expanded set of features after applying the Hilbert Huang Transform (HHT) on the signal in space. In particular, the authors apply the Energy frequency distribution entropy, kurtosis and skewness both in the HHT-based timefrequency plane thus obtaining a very high accuracy.

The second approach (*instance based*) is to use correlation among the observables collected from the mobile phones. In this case, the objective is to evaluate the degree of correlation between the observables. Observables from the same mobile phone or the same model should be more correlated than observables from different phones and models. Different types of correlation algorithms can be used: Euclidean distance between the observables, Pearson correlation and so on.

A summary of the statistical features and correlation algorithms used for the classification and identification in literature is provided in Table III, which aims to summarize the results from the research community and to identify the most appropriate features for the different built-in components of a mobile phone.

The table lists in the first column the type of feature used for fingerprinting. In the second column, a brief description of the feature is provided. Then, the third column identifies which components of the mobile phone have been used for fingerprinting. The fourth column lists all the research works where the feature has been used. When more than one component has been listed in the third column, the reference in the fourth column does also identify the component and the standard when applicable (e.g., RF WiFi).

From the summary Table III, we note that each set of components has a preferred set of features, as already described in the previous sections. Statistical features like Skewness and Kurtosis are common in RF related components because most of the communication standards are based on the transmission of bursts in the time domain. Variations in the skewness or kurtosis can be clearly identified in the fingerprinting extraction process. MFCC based features are quite common in microphone identification because they are based on voice processing, but there is no reported study on the application of other statistical features. SPN is mostly used in camera identification as expected.

TABLE III
SUMMARY OF THE STATISTICAL FEATURES OR CORRELATION FOR MOBILE PHONE IDENTIFICATION ON THE BASIS OF THE BUILT-IN COMPONENTS

Feature	Brief Description	Component	References
Instantaneous Magnitude or Phase	It is the magnitude or phase of the signal or its error from an ideal reference	RF	[82]
Standard Deviation	Standard deviation is the standard error of the estimated mean [83]	RF	[26]
Variance	The variance is the mean squared varion of a distribution from its mean [83]	RF, MEMS	[26], [19] (RF WiFi), [84] (RF WiFi), [85] (RF WiMAX), [72] (MEMS)
MFCC	Mel-frequency cepstral coefficients is a representation of the short-term power spectrum of a sound	Microphone	[63], [64], [86], [69]
Skewness	The skewness characterizes the degree of asymmetry of a distribution around its mean [83] or the standardized third population moment about the mean	RF, MEMS	[26],[81], [25] (RF ZigBee), [85] (RF WiMAX)
Kurtosis	Kurtosis measures the relative peakdness or flatness of a distribution [83] or the standardized fourth population moment about the mean	RF, MEMS	[26],[81], [25] (RF ZigBee), [85] (RF WiMAX)
Error Vector Magnitude	Error Vector Magnitude (EVM) is the measure used to quantify the performance of a digital radio transmitter or receiver in terms of how far the constellation points are far from the ideal locations	RF	[87] (RF WiFi), [82] (RF GSM)
Shannon Entropy and other entropy features	Shannon entropy is the expected value of the information contained in a signal	RF	[88]
Features based on wavelet-series	Wavelet series is a representation of a square-integrable function by a certain orthonormal series generated by a wavelet for a specific signal (see [89])	RF	[28] (RF WiFi), [90] (RF WiMAX), [91] (RF UMTS)
Compressed Sensing	A signal having a sparse representation can be recovered from a small set of linear, nonadaptive measurement [92]	RF	[93]
Coefficients of the Power Spectral Density	Spectral energy distribution per unit time	RF, Microphone	[20] (RF WiFi), [94] (RF UMTS), [95] (Microphone)
Hilbert-Huang Transform	Hilbert-Huang Transform (see [96])	RF	[39]
Clock Skew or Timing Analysis	Clock skew is the difference in the arrival times of clock in different components of an electronic device [97]. Clock skew is part of the more general timing analysis	Network	[43], [98], [42]
Sensor Pattern Noise	SPN measures the pixel nonuniformity noise caused by different sensitivity of pixels to light [52]	Camera	[99] [52], [47], [50], [58], [50]
Analysis of processing algorithms (e.g., JPEG)	Processing algorithms used by the mobile phone to process the sensor data	Camera	[49]

2) Algorithms: Machine learning algorithms, can be classified in the following broad categories [100]: supervised algorithm, unsupervised algorithms, reinforcement learning and hybrid algorithms (which combine elements of the previous three categories). See also [101] for a similar taxonomy in sensor networks. Based on the survey conducted in literature, the most applied categories for fingerprinting are supervised algorithm and unsupervised algorithms and we are going to describe the application of these two categories in the following sections.

a) Supervised learning: Supervised algorithms represent the category where a training set of correctly identified observations is available, and classifiers are built on the basis of a set of mutually exclusive and predefined classes of classified (i.e., labeled) data. In the application of supervised algorithms, the correctly identified observations are used as a training data set, while a separate testing data (unclassified data) set is used for identification and verification. For mobile phones identification or verification, this means that the fingerprints must be collected in a preliminary phase and stored in a reference library. In a subsequent phase (e.g., forensics process), the observables from a new or unknown phone (depending on the application) are compared to the existing library to identify the phone or to verify its identity. For example, in a security application like a multi-factor authentication, a reference library of valid mobile phones, which are granted access to specific rights, is built. This reference library creates a *white list* of mobile phones. In a subsequent phase, the observables from the mobile phone to be identified and verified are collected and processed using a supervised algorithm to provide an indication that the tested mobile phone is what it claims to be and it can be granted access. In this case, the creation of the reference library is the most critical and complex step.

The main supervised learning algorithms are identified in the rest of this section, which anyway does not have the ambition to provide a detailed analysis of each algorithm, as there is an extensive bibliography on each of them. The objective is to provide a high level description in relation to the identification and validation of mobile phones and the potential advantages or disadvantages. For a more detailed description we refer the reader to the cited references.

1) The K Nearest Neighbors algorithm (KNN) algorithm classifies a data sample on the basis of the labels of the nearest data samples (neighbors). Different functions can be used to determine how near or distant are the samples. The most common function is the Euclidean distance, but other distance metrics like the Mahalanobis or Minkowski distances can be used. The advantage of the KNN is that it is computationally efficient, as it does not need high computational power in the training phase. However, the classification phase could be more computational intensive than in other algorithms. This could be

an issue for some fingerprinting applications where the classification efficiency is more important than building the reference library (i.e., in the training phase). In addition, the disadvantage of KNN is that it may not perform in a optimal way when a large number of dimensions is used (see [102]). In general, the performance of the KNN algorithm depends on the distance metric used to identify nearest neighbors, which should be adapted to the particular problem, which must be solved [103].

2) Learning Tree or Decision Trees, where the algorithm iterates through the input data by using the features properties to reach a specific category, which is more similar to the labeled data (see [104] for a detailed description of the concept of decision trees). One feature of the decision trees is that their performance is more linked to the structural information contained in the data (i.e., fingerprints). Decision tree has been used for identification by various authors with good results (see Table IV) but it has the following advantages and disadvantages for identification on the basis of the fingerprints [105]. The implementation of decision trees is usually very simple and efficient if the data is well structured. An additional advantage is that they perform well even with high dimensional data sets. The disadvantages of the decision trees are the long training time and that the orders of the features in tree nodes have adverse effect on performance, so that an analysis and selection of the features would be needed before the deployment of the fingerprint system in the field.
3) SVM is a supervised algorithm, which learns to classify the data points (e.g., originating from the observables), from the labeled training samples (e.g., the reference fingerprints). SVM separates the labeled set in two areas on a multi-dimensional surface by using a separating function, which can be of different types: linear, Radial Basis Function (RBF), polynomial, sigmoidal are the most common. Since the multi-dimensional surface is divided in two areas, SVM is a binary classifier and it can be directly used to distinguish between two mobile phones or for validation (to validate the claimed identity of a mobile phone). See [106] for a detailed description of SVM. The extension of SVM to multi-classifier identification has been proposed by Crammer and Singer [107] and it is available in different libraries: the machine learning toolbox by MATLAB, LIBSVM and PRTools. Different multi-classifier techniques have been proposed in literature like One-Against-One (OAO), One-Against-All (OAA) or Directed Acyclic Graph-Support Vector Machine (DAGSVM) and an analysis of the advantage or disadvantages of each technique is presented in [108]. There are no special recommendations for the fingerprinting problem analyzed in this paper as it depends on the type of component and its observables. The advantage of the SVM for fingerprint classification is that it is well known for its high level of accuracy and robustness against outliers. SVM is less prone to overfitting than other methods [109]. SVM is also quite efficient for binary classification, which is very important in the verification phase. The disadvantage is that SVM can be slow in the learning process and it can require a large amount of training time. On the other side, this may not be a problem for many applications described in Section II because the creation of the initial reference library of fingerprints may be a time consuming process anyway. Some algorithms used in SVM like Quadratic Programming (QP) methods can be computationally and memory demanding, so other Kernel methods should be preferred in fingerprint classification.
4) Bayesian Classifiers are statistical classifiers and they predict the class membership probability, that is the probability that a given sample belongs to a particular class. See [110] for a detailed description of Bayesian Classifiers. A specific category of Baynesian classifier is the Naïve Bayes Classifier, where it is assumed that all variables contribute toward classification and are mutually correlated. This may be true for some specific category of fingerprints because they originate from the same physical components (e.g., the RF equipment). One advantage of Bayesian methods is that they adapt the probability distribution in an efficient way without over-fitting. Another advantage of Bayesian statistics is that it requires a limited number of training samples, which is useful when it is difficult to obtain a large number of fingerprints for training. The disadvantage is that they are less accurate in comparison to other classifier. See [105] and [111] for an analysis of the Bayesian classifier against the other classifiers.
5) Neural network is a set of connected input and output units where each connection has a weight associated with it. The network performs the learning process by adjusting the weight to predict the class label of the input sample. A commonly used neural network classifier is the back propagation algorithm, which performs the learning process on a multilayer feed-forward neural network. The algorithm learns by processing a data set of training samples in a iterative way. At each iteration, the algorithm compares the network prediction for each sample with the actual target value and adjusts accordingly the weights in each layer. See [112] for a description of the back propagation algorithm and adaptive neural networks in general. The advantage of neural networks is that they are able to tolerate noisy data or outliers in the fingerprints and observables. They are usually able to classify patterns they have not been trained on, thus being useful in identifying new models or components. The disadvantage is that the classification requires a very long learning time, but this (as in the case of SVM) may not be an issue, since the creation of a reference library may anyway require considerable time to collect and extract the fingerprints. The tuning of the neural networks may require some a-priori knowledge of experimentation to narrow down the list of parameters, which are specific for a type of component (e.g., accelerometer). At the time of writing this paper, some authors have started in [113] to investigate the possibility to fingerprint wireless devices

by using Convolutional Neural Networks (CNN) and Deep Neural Networks (DNN), which offers flexibility to learn features across a wide range of tasks and demonstrates improved classification accuracy against current day approaches. O'Shea *et al.* [113] have demonstrated that the application of CNN and DNN provides greater accuracy than conventional machine learning classifiers (e.g., SVM and KNN) especially in low SNR conditions. Still, O'Shea *et al.* [113] recommend further investigation and experimental work in this area.

Each machine learning algorithm has its own strengths and weaknesses depending on the data set and the context or application where the algorithm is employed. Various papers have attempted to provide an analysis and a comparison of the different algorithms (see [101], [105], [111]). While we refer the reader to the cited references, here we try to summarize the key elements for the objective of identification and verification of the mobile phones through the fingerprints of the built-in components. Generally SVM and neural networks tend to perform better with multi-dimensional and continuous features [105], which is usually the case for fingerprints classification.

Neural networks and SVM are characterized by a time consuming learning process. However this is not a major issue in this context because the collection of fingerprints to build the reference library can also be quite time consuming due to synchronization and normalization processes. In comparison to other classifiers, Neural networks, SVM and Decision Trees have usually a high accuracy, which is quite important because many applications identified in Section II depend on a very high accuracy (e.g., multi-factor authentication).

Variance is an important factor in the observables used to generate the fingerprints, because it is a measure of the contribution to error of deviations from the central tendency [105]. Errors in the observables can be present for many reasons (e.g., RF bias in the receiver, impact of different environmental conditions on clock skew). Decision Tree, Neural Networks and SVM are usually characterized by high variance sensitivity and special care must be applied to avoid the danger of overfitting. Mitigation techniques against over-fitting can be based on the application of cross validation (e.g., K-fold) or the repetition of the collection of observables in different times or days. The testing or execution phase (e.g., when a fingerprint is verified against the training set) should be minimized in terms of time and storage space. From this point of view, the KNN algorithm uses a large training space and its execution space is at least as big as the training space [105], resulting in a strong disadvantage.

We note that some machine learning algorithms require the tuning of some parameters (e.g., scaling factor in SVM) that influence the identification accuracy.

The identified work in literature for supervised learning is quite extensive and it is reported in Table IV together with the other approaches.

b) Unsupervised learning: Unsupervised learning is the category of algorithms where a training set is missing and the algorithms must find the hidden structure from data not previously labeled or classified. For mobile phone identification or verification, unsupervised algorithms often mean that similar fingerprints from different logical devices are grouped together and mapped to the same cluster. For example, in the application of the fight against counterfeiting, the observables from a set of mobile phones of the same model and brand can be evaluated using an unsupervised algorithm to identify potential counterfeit mobile phones. Since counterfeit mobile phones are usually manufactured with components of lower quality to save money or in different manufacturing plants and with different materials, the fingerprints of the counterfeit mobile phones will be different from the genuine phones. A potential identification process for counterfeit phones could be implemented with a process where observables from a mixed group of mobile phones (where the identity of the genuine mobile phones is well known) are collected and analyzed. The counterfeit phones should have different statistical features or a low degree of correlation with the subset of valid mobile phones. The advantage of this approach is that the creation of the reference library is not needed as the presence of valid phones is used for this purpose. The main disadvantage is that the testing entity must have a significant number of valid phones of the same type and model. This is not practical in most of the situations apart from the forensic labs of a manufacturer of mobile phone. On the other side of the coin, registration of device fingerprints ahead of time is not always feasible in practice, thus supporting approaches based on unsupervised learning. Another application of unsupervised learning is in the security domain when multiple phones with different fingerprints assume the same identifier. In this case, identity spoofing attacks could be mitigated: for example, the spoofer will be outside the cluster of valid phones [22].

There are various unsupervised learning techniques in literature. Here we described only a limited set applied to fingerprints identification and verification.

1) K-Means Clustering, where observables are partitioned into a number of clusters where each observation belongs to the cluster with the nearest mean, which serves as a prototype of the cluster.
2) Hierarchical clustering seeks to build a hierarchy of clusters. An example of hierarchical clustering applied to camera identification is provided in [114].
3) Unsupervised Bayesian Learning, which is the application of Bayesian networks to unsupervised learning. One example of this technique is in [115], where the feature space of a single device is modeled by a multivariate Gaussian distribution with unknown parameters. The non-parametric Bayesian Learning approach is then applied to the multivariate Gaussian distribution to identify the cluster.
4) PCA, a multivariate method for data compression and dimensionality reduction. PCA aims to extract important information from data and to present it as a set of new orthogonal variables called principal components. Note that PCA is often used in mobile phones identification to reduce a large set of features used for fingerprinting definition as in [26] for the RF component and in [116] for the camera component.
5) Techniques based on neural networks applied to unsupervised learning.

TABLE IV
SUMMARY OF THE ALGORITHMS USED IN MOBILE PHONE IDENTIFICATION

Algorithm	Description	Component	References
KNN	KNN is based on the Euclidean distance between a test sample and the specified training samples [117].	RF,MEMS, Microphone	[118] (RF WiFi), [119] (RF UMTS), [87] (RF WiFi), [50] (Camera), [120] (Camera), [63] (Microphone), [64] (Microphone)
SVM	SVM is a supervised machine learning algorithm for binary classification described in [121].	RF,MEMS	[82] (RF GSM), [72] (MEMS), [50] (Camera), [63] (Microphone), [64] (Microphone), [122] (Camera), [123] (Camera)
Random Forest	Random forests are a combination of tree predictors such that each tree depends on the values of a random vector sampled independently and with the same distribution for all trees in the forest [124]	RF	[125] (RF Zwave), [126] (RF ZigBee), [27] (RF ZigBee)
MDA with ML	MDA with ML estimation is a multi-class extension of FLD process for more than two classes	RF	[28] (RF WiFi), [25] (RF ZigBee), [84] (RF WiFi), [85] (RF WiMAX), [90] (RF WiMAX)
Neural Networks	Neural networks machine learning algorithms described in [127]	RF	[26], [98], [42], [113]
Sparse representation	Sparse representation is to search for the most compact representation of a signal in terms of linear combination of atoms in an overcomplete dictionary [128]	Microphone	[86] (K-SVD)
Instance-based classification	Instance-based classification based on Time or Spectral Correlation	RF, camera, Microphone	[19] (RF WiFi), [58] (Camera), [95] (Microphone)
Hierarchical clustering	definition of an hierarchy of clusters	Camera	[114] (Camera)
Unsupervised Bayesian Learning	Unsupervised application of Bayesian learning	RF	[115] (RF ZigBee)

The identified work in literature for unsupervised learning is quite limited and it is reported in Table IV together with the other approaches.

c) Summary of machine learning algorithms: A summary of the algorithms identified in the previous paragraphs is provided in Table IV.

From the summary we notice that SVM is the most common algorithm used for classification, followed by KNN. These two algorithms are used across all the different built-in components of the mobile phone. Algorithms based on neural networks have been scarcely used until now, but the cited references are quite recent and future research papers may adopt more frequently this type of algorithms including Deep Network approaches.

V. PRIVACY RISKS AND MITIGATION

The identification of mobile phones through their fingerprinting is useful for the applications described in Section II. However, it has also drawbacks related to the possibility of tracking mobile phones once their fingerprints are known. Even if tracking of mobile phones through their fingerprints can represent a significant privacy risk, there are also significant limitations in a realistic environment, which have been already partially described here. For example, wireless propagation attenuation and multi-path fading effects in a urban environment can severely impact the tracking of a mobile phone even with a-priory knowledge of its RF fingerprints associated to the mobile phone, as the RF observables will be highly degraded. Even for internally generated fingerprints, which do not suffer from propagation aspects (e.g., sensor pattern noise of the camera or MEMS fingerprints) it is possible to identify and define mitigation techniques. A preliminary analysis has already been presented in [129], where similar privacy issues have been identified and mitigation techniques have been recommended. The aim of this paper is to widen the analysis presented in [129] for the specific set of physical fingerprints.

In the following subsections, we describe the potential limitations of the tracking and the related mitigation techniques for the two main classes of built-in components.

A. Privacy Risks and Mitigation With External Processing Techniques

In this section we investigate how privacy risks can arise from the application and deployment of external processing techniques. The main built-in components, whose emissions can be used to track the mobile phone, are the RF components. In fact, for the other built-in components (i.e., display and loudspeaker), the fingerprinting and analysis processes are quite difficult to achieve even in ideal conditions as described in the previous sections. For example, in a practical scenario with background audio noise, the observables collected by an external sensor will also include the noise components, which are unpredictable (e.g., they vary depending on the environment). The fingerprinting of the emissions from the RF components may also be degraded in a realistic environment but to a minor degree and in different conditions. One difference with audio fingerprinting is that the radio spectrum policy

usually defines specific licensed bands for use by a specific radio access technology or standard. Even in the case of unlicensed bands (like WiFi), the RF component can transmit in a specific channel that can be filtered out and decoded, in opposition to the audio signal of a mobile phone loudspeaker that can be interfered in different frequency bands. Instead, one similarity with audio fingerprinting is linked to the impact of attenuation and multi-path fading due to obstacles. In a typical tracking scenario, an observer can collect observables of the mobile phone to be tracked at a considerable distance from the phone to avoid visual detection. Free-space propagation loss will considerably decrease the power of the RF emissions received by the observer. As noted before, a low SNR decrease the identification accuracy. Beyond the basic free-space propagation loss, the presence of obstacles in the path between the RF component or in the surrounding environment will introduce both attenuation and multipath fading effects. Even if the impact of multipath fading must still be investigated by the research community, we can reasonably guess that it will also decrease the identification accuracy. We note that these problems will be present both in the initial phase of collecting a fingerprint of the RF component and in the subsequent phases of identifying the RF component from its emissions. An additional issue is the lack of portability of the receivers (see [30], [31]), since a typical privacy threat scenario may include different observers in different positions (see [130] for a description of an implementation of a privacy threat based on the observation of RF emissions in the road transportation sector) and with different receivers. Even if all these limitations do not completely preclude the possibility of a privacy threat, they raise the bar for the difficulty to implement this privacy threat for the external processing techniques.

B. Privacy Risks and Mitigation With Internal Processing Techniques

In this section we investigate how the application of internal processing techniques can generate privacy risks. The identification of a mobile phone can be used to track its owner. In comparison to what described in Section V-A, the observables are not impacted by the distance at which an attacker implements the privacy threat. For example, the SPN from the images taken by a camera can be examined hundreds of kms from where the images were taken. Then, different protection techniques must be implemented to mitigate privacy risks. In this paper, we propose two main approaches:

1) the specific features of the built-in components in the mobile phone can be altered by removing specific bias (e.g., through filtering) or by adding noise to obfuscate their specific information about the mobile phone. This approach must not negatively impact the correct functioning of the smartphone and its provided services. For example, the clock skew could be eliminated by resynchronizing the phone either using GNSS or other techniques like the Reassemble TCP option in OpenBSD, which modifies the TCP timestamps in outgoing packets on the device with random and monotonically increasing numbers [129]. While the elimination of the clock skew does not negatively impact the proper functioning of the mobile phone and it can actually be beneficial, other fingerprints are not based on the same bias and their removal could have a negative impact. For example, the fingerprints present in accelerometers and gyroscopes can be mitigated by introducing white gaussian noise in the observables to obfuscate the specific features. The negative impact of this approach is that the addition of white Gaussian noise may degrade the signal originating from the sensors to the point that they will be unusable by applications using the accelerometers. For example, an application using accelerometers to correct location information from GNSS will be negatively impacted by the addition of Gaussian noise. This disadvantage does not apply to all the components investigated in this paper. For example, the removal of SPN in the image does not have an impact on imaging applications. The recommendation is to adopt this approach case by case. Beyond the specific techniques described here (e.g., addition of Gaussian white noise), there is a large body of work in the obfuscation of sensor artifacts, which could be exploited. See [131] for a general discussion on privacy mitigation techniques for images collection and processing, which could also be applied to fingerprinting.
2) In the second approach, the access to the fingerprints can be restricted only to specific categories of users and applications. For example, policy frameworks can be implemented to prevent the distribution of the fingerprints collected by the mobile phone as described in [129]. Indeed, this is one of the most common approaches adopted or investigated by the research community working on privacy threats. Various references have proposed policy framework to mitigate privacy risks, which could be applied to the specific fingerprint context. See [132] for a policy based framework, which is used to regulate the flow of data from Internet of Things (IoT) devices or for a more general framework like [133].

We note that the two approaches can be combined. The policy framework can implement the obfuscation techniques described in 1) rather than not allowing the access to the fingerprints. In other words, all the users will be able to access the digital artifacts generated by the sensors but some users will be able to see the original artifacts while other users will only see obfuscated or noise added artifacts.

VI. Lesson Learned

Following the analysis presented in the previous sections of this paper, here we summarize the key issues and obstacles for the identification and verification of mobile phones based on the fingerprints of their built-in components, i.e., we give an overview of the lessons learned. Some of these issues will be discussed again in Section VII along with the related research opportunities.

A. Dependency of the Fingerprints on Time or Environmental Conditions

The fingerprints of the built-in components can change in time or for different environmental conditions (e.g., temperature, humidity), as they are based on the physical properties of the material used to build the components. Different components have different degrees of stability against time or environmental conditions either because they are physically protected (by the case of the mobile phone) or they are designed with stability as a key requirement (e.g., RF components for cellular communications must be quite stable to support effective wireless communication services in the lifetime of the mobile phone). There are not many studies on the reliability of fingerprinting in time or environmental conditions, even if these aspects are taken into consideration in some of the papers identified in the previous sections (the measurements are repeated in different days or weeks). The research work on PUF can also provide insight in mitigation techniques against time or environmental changes (see [134]).

B. Security Threats on the Fingerprinting Generation Process

The process of collecting the observables and generating the fingerprints could be subject to security attacks with the goal to manipulate, fake or clone the fingerprints. Security threats can be present both for fingerprints based on internal digital output (e.g., collected by the mobile phone from its built-in accelerometer) or an external digital output (e.g., collected by an external RF receiver, see Figure 1). For internal-based fingerprints, there is the risk that a manipulated or compromised (from a security point of view) mobile phone can provide false observables to avoid detection and tracking through fingerprinting. The user of a mobile phone may have an interest for not being tracked either legitimately (e.g., for privacy reasons as described in Section V) or because (s)he means to implement a malicious activity. For example, the timestamps of the digital output of the sensors can be manipulated or the observables generated internally by the mobile phone (e.g., from the camera or MEMS) could be artificially created by malicious agents running in the mobile phone (e.g., a malware), through replication of valid fingerprints. In a similar way, fingerprints generated externally (e.g., RF fingerprints) could be captured by a malicious entity and used to clone a valid device. Various techniques could be used to mitigate these threats: a) a challenge-response approach, where the stimulation of the sensor (e.g., a specific image or vibration of the mobile phone) is the challenge and the digital output to create the fingerprint is the response, b) information flows protected with integrity checks to ensure that the sensor data is not manipulated. This area requires further investigation from a research point of view.

C. Interference and Noise

Fingerprints generated by an external device (e.g., RF based fingerprints) could be degraded by the presence of wireless interference or background RF noise. In a similar way, fingerprints generated on TCP traffic could be impacted by congestion on the communication link and varying levels of load on a node [42]. Background noise could hamper microphone based fingerprinting. Interference, congestion and noise could not be entirely eliminated in practical scenarios, but risks can be mitigated by the application of appropriate filters or improved features and classifiers as described in the previous sections.

D. Portability

This is a general issue for most of the fingerprints. The agent that collects the fingerprints can introduce its own fingerprint, compromising the portability of the fingerprints from one agent to another. This issue impacts not only the RF fingerprints (as the receiver will introduce different bias in the collection phase) but it may also impact the internally generated fingerprints. A mobile phone can download and activate a different firmware version of the built-in component, which can introduce variations in the fingerprint (e.g., software of the GNSS receiver). Portability of fingerprints is an open problem.

VII. Future Trends and Research Opportunities

The following future trends and possibilities are envisaged for mobile phone identification on the basis of their built-in components:

1) Artificial insertion of unique features in the mobile phone. Instead of using the spontaneous physical differences in the phones, intentional imperfections could be inserted in the manufacturing process. One example for RF detection is the concept of PUF, but similar approaches and techniques can be used with other components like a camera. An example of the use of the PUF concept to camera identification was initially proposed in [135] and further elaborated in [136]. The PUF concept is discussed in detail in the subsequent Section VII-A. The advantage of this approach would be a more effective support for multi-factor authentication in a way that cryptographic means could be correlated with the insertion of the intentional imperfections in the manufacturing phase.
2) Most of the results from the research community has been so far based on empirical evaluations of the observables without the definition of a clear model. It would be useful to define specific models which could help to identify the most appropriate algorithms and features for identification. In addition, some models could be used to identify the intrinsic limitations of the fingerprinting process and how this can be overcome.
3) New components or wireless standards will be included in mobile phones in the near future. For example, Near Field Communication (NFC), actually already present in many models, or other components.
4) While some authors have already proposed the combination of different features to improve identification, there is still work to do in the combination of different components whenever possible.
5) The stability of the fingerprints in time or for different environmental conditions still requires further research.

6) Most of the research was conducted on observables collected in ideal or almost ideal conditions. While various authors have started recently to investigate the impact of disturbances (e.g., fading conditions, non ideal light conditions), further research is needed to support the applicability of fingerprinting concepts in practical applications.
7) Security threats could be present on the fingerprinting process itself.

Each of these aspects will be discussed in the following subsections.

A. Intentional Fingerprints

The major part of the analysis presented in this paper is related to the collection and analysis of the unintentional fingerprints, i.e., the imperfections and specific physical features *unintentionally* created in the built-in components of the mobile phone during the manufacturing process. There is also the possibility of *intentionally* inserting specific physical features to support the applications identified in Section II. One example is the concept of PUF, which has been initially proposed in [137] to support security (e.g., the generation of secret keys). The PUF is built by introducing specific electronic elements in the IC to generate delay or time variations of the electronic information transmitted in wires and transistors of the electronic component [137]. These variations are reproducible and measurable across in manufacturing processes and they could be applied to any electronic circuits used in the built-in components of a smartphone. A recent tutorial on PUF is described in [138], where various examples of PUF implementation are described. In particular a Ring-Oscillator PUF is presented, which is based on the variation in delay of the inverters in ring oscillators. The consequence is that each ring oscillator will have a slightly different operating frequency, which can be used as a fingerprint (see the clock skew fingerprint described in Section IV-B4 of this paper). Another recent example of the PUF implementation for creating the fingerprint of a camera is provided by Cao *et al.* [136], where a CMOS PUF was implemented to support fingerprinting generation for security (multi-factor authentication) and anti-counterfeiting applications. The advantage of inserting the PUF in the built-in component of a mobile phone is to improve the identification or verification accuracy and to increase the resilience to changes in environmental conditions, which can be a significant challenge in this context, as discussed in the rest of this paper. The trade-off is obviously a higher price of the components and a more complex design and manufacturing process.

B. Models for Fingerprinting

As shown previously, most of the cited work is based on the experimental evaluation of verification and authentication algorithms. Theoretical models for describing the genesis of the fingerprints and their collection and classification are relatively scarce. These models could be helpful to mitigate bias or disturbances in the collection phase or to identify the most relevant features without resorting to complex and lengthy features selection processes. A recent contribution [24], called Wireless Physical Layer Identification (WLPI), aims to close this gap at least for the fingerprinting at the RF physical layer. Wang *et al.* [24] provide a systematic and mathematical description of the whole WLPI process, which is based on the following elements:

1) modeling of the signal processing at the transmitter;
2) modeling of the signal propagation between TX and RX antennas along the wireless channel between the transmitter and the receiver;
3) signal reception and processing at the receiver;
4) extraction, identification and classification of the radio frequency physical layer features.

As described before, existing models from literature can help to define elements 2) and 3). In particular for element 2), wireless propagation models (e.g., for fading) can be used to identify which components of the model contribute more significantly to the fingerprint or its degradation. For element 3), models on the electronic devices and receiver front-ends can be used. In particular, the characterization and calibration of electronic components is quite important in RF measurements and many models presented in literature can be used to this purpose. Finally, statistical features can have strong or weaker dependencies on the bias introduced by elements 2) and 3) (e.g., entropy on the presence of noise). At the moment of writing this paper, the authors do not report detailed studies on the evaluation of the statistical features on the basis of the bias introduced by elements 2) and 3) in relation to fingerprinting.

Each of these elements contribute to the fingerprint of the RF device to be identified, which is basically related to 1). However the other elements may degrade the definition of the fingerprint by introducing bias and distortions.

Another important aspect in this survey is to define the limits for identification and validation on the basis of the fingerprints. Even if we discussed in this paper the various factors which can contribute to create limits for fingerprinting, theoretical studies could be helpful to identify the theoretical limits for the different types of fingerprints. For example, Chu *et al.* [139] have addressed this problem by proposing a theoretical framework for forensic-ability (one of the applications identified in Section II). Then, the authors applied the model to image processing and identification.

A similar analysis for the RF fingerprints have been proposed in [140], where Gungor and Koksal focus on the authentication problem in the presence of an adversary. In the proposed scenario, both the legitimate transmitter and the adversary are furnished with unique fingerprint channels and a possible secret key, which is available at the legitimate nodes. The authors demonstrate that authentication without keys is possible via RF fingerprints when the legitimate channel cannot be simulated. This analysis is useful for the application of multi-factor authentication as it can be used to evaluate how robust is a RF fingerprint for security purposes.

C. Future Components

Mobile phones are continuously evolving and new functions and components have been added in recent year. MEMS were

not available until few years ago but they are now widespread in the medium-high end mobile phones. In a similar way, the resolution of the camera has improved drastically in recent years and the identification of a camera is proportional to its resolution (sensor pattern noise is less pronounced due to averaging material inhomogenities over a relatively larger area [52]).

The concept of modular phones, where mobile phones can be assembled with many different components is proposed by recent projects like the Project ARA [141] and Phonebloks [142]. The concept is to build a smartphone out of interchangeable parts that can be replaced by the user to customize the smartphone depending on the need or the context: add a wide-angle camera module for tourist trips or a better battery for business reasons. This is in contrast to current designs, characterised by a very high level of integration that makes almost impossible to replace individual components [143]. An example of potential add-ons for the mobile phone is the spectrometer described in the patent application [144], where an optical spectroscopic sensor is integrated with a mobile communication device to utilize various functions of a wireless communication network. Another example described in [145] is the integration of a polarized microscope into a generic mobile phone to support the rapid diagnostic tests of the malaria disease for field use.

At the moment, it is difficult to predict which potential add-ons will be proposed for the mobile phones. In some cases, these add-ons will be implemented for niche markets and they will not have widespread development. Depending on the technology used to implement them, some of the techniques presented in the previous sections can be extended to the add-ons as well. For example, in a mobile phone with a polarized lens, specific add-ons can be fingerprinted using image based recognition algorithms similar to the ones described in Section IV-C1.

D. Combination of Fingerprints Components

Most of the techniques described in Section IV are based on the fingerprint of a single component, while identification algorithms could exploit the combination of data from different sensors. In fact, Dey *et al.* [70] (one of the first works on fingerprinting through built-in accelerometers) have suggested the possibility to combine sensors such as gyroscope and accelerometer in order to increase the ability to discriminate between mobile phones. Different classifier combination methods proposed in literature can be applied to this specific context. Tax *et al.* [146] give a well cited overview of the most common classifier combination methods. To the knowledge of the authors, at the time of writing this survey, there is a limited research work on the combination of different fingerprints. We survey here the few works proposed in literature. Tax *et al.* [146], combine different classifiers used to fingerprints the RF components of Wireless Open-Access Research Platform (WARP) platforms, which is a type of Software Defined Radio (SDR). The authors perform a weighted voting where the probability of detection for each of the weak classifiers previously identified is assigned with normalized weight. The weight is based on the probability of detection, which is found during the signature learning phase. Tax *et al.* [146] noted in the conclusions that the combined classifiers perform well in the presence of a large set of observables, while its performance is not very good for small number of observables.

The combination of fingerprints from different components in the smartphone can improve identification and verification accuracy. The following combinations are suggested here: the fingerprints from different RF wireless devices could be combined using a weighting scheme. The RF acquisition would require a RF receiver able to acquire different signals in space in different frequencies. While this could be difficult to achieve years ago, SDR based receivers at low cost can acquire today RF signals in a large span of frequencies. As mentioned previously, the fingerprints of gyroscopes and accelerometers can be combined when the smartphone is subject to a specific motion pattern. Fingerprints based on video capture can be obviously related to the combined fingerprints of camera and microphones. The clock skew or bias can appear as a fingerprint in various observables (e.g., RF samples, digital output from the sensors including the GNSS receiver). Through the analysis of different observables, the evaluation of the clock bias could be ehnanced in comparison to a single digital output. Finally, different versions of the software and firmware present in the smartphone can generate slightly different fingerprints. For example, the compressing algorithms for image processing can be different between two software versions (see [49] for camera identification).

E. Fingerprints Stability

As pointed out in Section IV-C5, the stability of the fingerprints in time or for different environmental conditions is a critical issue that can hamper the deployment of many applications based on fingerprints. While some papers investigated the classification stability in time (e.g., observables taken in different months) for specific components (e.g., accelerometers in [72] and RF oscillators [46]) and found that the impact of components aging for a duration of months is limited (i.e., classification accuracy does not change significantly), many more studies are needed to specifically investigate the impact of aging or different environmental conditions [77]. The impact of aging or environmental changes may also be different for the different types of components and different statistical features. In other words, different statistical features will be more or less robust against the impact of aging. A potential way forward to address this issue would be to review the extensive literature on the impact of aging on electronic components (see [147], [148]) for each component (e.g., accelerometer, gyroscope), and define models that can be correlated with the features extraction process. Then, the features most robust against aging could be selected. Depending on the type of component, both theoretical work and experimental campaigns are needed in different environmental conditions (e.g., humidity, temperature) to further address this issue.

F. Quality of the Collected Observables

Many reviewed papers are based on the collection of observables in ideal conditions and with ideal equipment. In the case

of RF fingerprinting, high-end spectrum analyzers are used with Line of Sight (LOS) conditions between the receiver and the mobile phone. In the case of microphones, the data are collected in an ideal sound environment with no background noise. In the case of MEMS fingerprinting, the presence of background vibrations can compromise the classification process. Even if recent papers (e.g., [24] and [42]) have investigated and tried to mitigate challenging environments, further research work is needed. This is especially important for applications where there is no control on the environment for data collection (e.g., criminal investigation, forensics).

G. Resilience Against Security Attacks to the Fingerprinting Process

As described in Section VI, fingerprints or the digital outputs on which they are generated could be subject to security attacks aimed at modifying or cloning the fingerprints. If mobile phones fingerprinting aims to be employed in the various applications identified in Section II, additional research efforts are needed to secure the fingerprinting process.

VIII. Conclusion

This survey has reviewed the state of art on the identification and verification of mobile phones through their built-in physical components. Today, mobile phones are very complex systems equipped with a wide range of sensors, communication interfaces and other components whose unique features can be exploited to identify a mobile phone in a wide range of applications. From a security point of view, the advantage of mobile phone fingerprints is represented by the difficulty to replicate them, since they are based on the intrinsic physical features of phone's components. In addition, the widespread deployment of mobile phones makes fingerprinting an easy and cost effective approach to authentication beyond the conventional methods (e.g., based on cryptographic means). This survey has shown that researchers can have a wide range of techniques and algorithms to fingerprint mobile phones through their built-in components. Very high accuracy can be achieved (especially for inter-model identification) in a controlled test bed environment, but there are still considerable challenges that hamper the practical exploitation of mobile phone fingerprinting in realistic scenarios and require further research work. In particular, the issue of portability of the fingerprints remains an open problem especially for RF based fingerprinting. This paper has also discussed privacy issues related to the identification and tracking of mobile phones and the related mitigation techniques. Finally, the paper has taken into consideration the evolution of the mobile phones, which will probably widen the set of fingerprinting options and the feasibility of their practical implementations in a wide range of applications and future trends.

References

[1] C. Böhm and M. Hofer, *Physical Unclonable Functions in Theory and Practice*. New York, NY, USA: Springer, 2012.

[2] A. K. Jain, L. Hong, S. Pankanti, and R. Bolle, "An identity-authentication system using fingerprints," *Proc. IEEE*, vol. 85, no. 9, pp. 1365–1388, Sep. 1997.

[3] U. Guin *et al.*, "Counterfeit integrated circuits: A rising threat in the global semiconductor supply chain," *Proc. IEEE*, vol. 102, no. 8, pp. 1207–1228, Aug. 2014.

[4] H. Zhou, C. Nicholls, T. Kunz, and H. Schwartz, "Frequency accuracy & stability dependencies of crystal oscillators," Dept. Syst. Comput. Eng., Carleton Univ., Ottawa, ON, Canada, Tech. Rep. SCE-08-12, 2008.

[5] V. Lakafosis *et al.*, "RF fingerprinting physical objects for anticounterfeiting applications," *IEEE Trans. Microw. Theory Techn.*, vol. 59, no. 2, pp. 504–514, Feb. 2011.

[6] S. Bachir, N. E. Calinoiu, and C. Duvanaud, "New RF power amplifiers modeling and identification for wideband applications," *Analog Integr. Circuits Signal Process.*, vol. 83, no. 2, pp. 161–172, 2015.

[7] T. Van Goethem, W. Scheepers, D. Preuveneers, and W. Joosen, "Accelerometer-based device fingerprinting for multi-factor mobile authentication," in *Engineering Secure Software and Systems*. Cham, Switzerland: Springer, 2016, pp. 106–121.

[8] W. E. Cobb, E. D. Laspe, R. O. Baldwin, M. A. Temple, and Y. C. Kim, "Intrinsic physical-layer authentication of integrated circuits," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 14–24, Feb. 2012.

[9] D. Shan, K. Zeng, W. Xiang, P. Richardson, and Y. Dong, "PHY-CRAM: Physical layer challenge-response authentication mechanism for wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1817–1827, Sep. 2013.

[10] J. Liu, F. R. Yu, C.-H. Lung, and H. Tang, "Optimal combined intrusion detection and biometric-based continuous authentication in high security mobile ad hoc networks," *IEEE Trans. Wireless Commun.*, vol. 8, no. 2, pp. 806–815, Feb. 2009.

[11] M. Potkonjak and V. Goudar, "Public physical unclonable functions," *Proc. IEEE*, vol. 102, no. 8, pp. 1142–1156, Aug. 2014.

[12] G. T. Becker, "The gap between promise and reality: On the insecurity of XOR arbiter PUFs," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst.*, St.-Malo, France, 2015, pp. 535–555.

[13] U. Rührmair *et al.*, "Virtual proofs of reality and their physical implementation," in *Proc. IEEE Symp. Security Privacy*, San Jose, CA, USA, May 2015, pp. 70–85.

[14] R. Satta and P. Stirparo, "On the usage of sensor pattern noise for picture-to-identity linking through social network accounts," in *Proc. Int. Conf. Comput. Vis. Theory Appl. (VISAPP)*, vol. 3. Lisbon, Portugal, 2014, pp. 5–11.

[15] M. Ibrahim and M. Youssef, "CellSense: An accurate energy-efficient GSM positioning system," *IEEE Trans. Veh. Technol.*, vol. 61, no. 1, pp. 286–296, Jan. 2012.

[16] J. S. Hunag, R. Harwahyu, and R.-G. Cheng, "Study of low cost mobile phone tracking system," in *Proc. Int. Symp. Next Gener. Electron. (ISNE)*, Taipei, Taiwan, May 2015, pp. 1–4.

[17] *Google Opens Up GNSS Pseudoranges*. Accessed on Aug. 10, 2016. [Online]. Available: http://gpsworld.com/google-opens-up-gnss-pseudoranges/

[18] H. Pieterse, M. S. Olivier, and R. P. van Heerden, "Playing hide-and-seek: Detecting the manipulation of android timestamps," in *Proc. Inf. Security South Africa (ISSA)*, Johannesburg, South Africa, Aug. 2015, pp. 1–8.

[19] W. C. Suski, II, M. A. Temple, M. J. Mendenhall, and R. F. Mills, "Using spectral fingerprints to improve wireless network security," in *Proc. IEEE Glob. Telecommun. Conf. (GLOBECOM)*, New Orleans, LA, USA, 2008, pp. 1–5.

[20] S. U. Rehman, K. Sowerby, and C. Coghill, "Analysis of receiver front end on the performance of RF fingerprinting," in *Proc. IEEE 23rd Int. Symp. Pers. Indoor Mobile Radio Commun. (PIMRC)*, Sydney, NSW, Australia, Sep. 2012, pp. 2494–2499.

[21] L. Sun and W. Kinsner, "Fractal segmentation of signal from noise for radio transmitter fingerprinting," in *Proc. IEEE Can. Conf. Elect. Comput. Eng.*, vol. 2. Waterloo, ON, Canada, May 1998, pp. 561–564.

[22] Q. Xu, R. Zheng, W. Saad, and Z. Han, "Device fingerprinting in wireless networks: Challenges and opportunities," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 94–104, 1st Quart., 2016.

[23] D. R. Reising, M. A. Temple, and M. J. Mendenhall, "Improved wireless security for GMSK-based devices using RF fingerprinting," *Int. J. Electron. Security Digit. Forensics*, vol. 3, no. 1, pp. 41–59, 2010.

[24] W. Wang, Z. Sun, S. Piao, B. Zhu, and K. Ren, "Wireless physical-layer identification: Modeling and validation," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 9, pp. 2091–2106, Sep. 2016.

[25] C. K. Dubendorfer, B. W. Ramsey, and M. A. Temple, "An RF-DNA verification process for ZigBee networks," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Orlando, FL, USA, 2012, pp. 1–6.

[26] D. R. Reising, M. A. Temple, and J. A. Jackson, "Authorized and rogue device discrimination using dimensionally reduced RF-DNA fingerprints," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 6, pp. 1180–1192, Jun. 2015.

[27] H. Patel, M. A. Temple, and B. W. Ramsey, "Comparison of high-end and low-end receivers for RF-DNA fingerprinting," in *Proc. IEEE Mil. Commun. Conf.*, Baltimore, MD, USA, Oct. 2014, pp. 24–29.

[28] R. W. Klein, M. A. Temple, and M. J. Mendenhall, "Application of wavelet-based RF fingerprinting to enhance wireless network security," *J. Commun. Netw.*, vol. 11, no. 6, pp. 544–555, Dec. 2009.

[29] S. Dolatshahi, A. Polak, and D. L. Goeckel, "Identification of wireless users via power amplifier imperfections," in *Proc. IEEE Conf. Rec. 44th Asilomar Conf. Signals Syst. Comput. (ASILOMAR)*, Pacific Grove, CA, USA, 2010, pp. 1553–1557.

[30] S. U. Rehman, K. W. Sowerby, and C. Coghill, "Radio-frequency fingerprinting for mitigating primary user emulation attack in low-end cognitive radios," *IET Commun.*, vol. 8, no. 8, pp. 1274–1284, May 2014.

[31] S. U. Rehman, K. W. Sowerby, S. Alam, and I. Ardekani, "Portability of an RF fingerprint of a wireless transmitter," in *Proc. IEEE Conf. Commun. Netw. Security (CNS)*, San Francisco, CA, USA, Oct. 2014, pp. 151–156.

[32] F. H. Gregorio, S. Werner, J. Cousseau, J. Figueroa, and R. Wichman, "Receiver-side nonlinearities mitigation using an extended iterative decision-based technique," *Signal Process.*, vol. 91, no. 8, pp. 2042–2056, Aug. 2011. [Online]. Available: http://dx.doi.org/10.1016/j.sigpro.2011.03.011

[33] F. H. Gregorio, T. I. Laakso, and J. E. Cousseau, "Receiver cancellation of nonlinear power amplifier distortion in SDMA-OFDM systems," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process.*, vol. 4. Toulouse, France, May 2006, p. IV.

[34] T. Lee and H. Ochiai, "Characterization of power spectral density for nonlinearly amplified OFDM signals based on cross-correlation coefficient," *EURASIP J. Wireless Commun. Netw.*, vol. 2014, no. 199, pp. 1–15, 2014.

[35] T. J. Bihl, K. W. Bauer, M. A. Temple, and B. Ramsey, "Dimensional reduction analysis for physical layer device fingerprints with application to ZigBee and Z-Wave devices," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Tampa, FL, USA, Oct. 2015, pp. 360–365.

[36] B. D. Fulcher and N. S. Jones, "Highly comparative feature-based time-series classification," *IEEE Trans. Knowl. Data Eng.*, vol. 26, no. 12, pp. 3026–3037, Dec. 2014.

[37] N. T. Nguyen, R. Zheng, and Z. Han, "On identifying primary user emulation attacks in cognitive radio systems using nonparametric Bayesian classification," *IEEE Trans. Signal Process.*, vol. 60, no. 3, pp. 1432–1445, Mar. 2012.

[38] A. Napolitano, "Cyclostationarity: New trends and applications," *Signal Process.*, vol. 120, pp. 385–408, Mar. 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0165168415003138

[39] J. Zhang, F. Wang, O. A. Dobre, and Z. Zhong, "Specific emitter identification via Hilbert–Huang transform in single-hop and relaying scenarios," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 6, pp. 1192–1205, Jun. 2016.

[40] A. Attar, H. Tang, A. V. Vasilakos, F. R. Yu, and V. C. M. Leung, "A survey of security challenges in cognitive radio networks: Solutions and future research directions," *Proc. IEEE*, vol. 100, no. 12, pp. 3172–3186, Dec. 2012.

[41] T. Kohno, A. Broido, and K. C. Claffy, "Remote physical device fingerprinting," *IEEE Trans. Dependable Secure Comput.*, vol. 2, no. 2, pp. 93–108, Apr./Jun. 2005.

[42] S. V. Radhakrishnan, A. S. Uluagac, and R. Beyah, "GTID: A technique for physical device and device type fingerprinting," *IEEE Trans. Dependable Secure Comput.*, vol. 12, no. 5, pp. 519–532, Sep./Oct. 2015.

[43] M. Cristea and B. Groza, "Fingerprinting smartphones remotely via ICMP timestamps," *IEEE Commun. Lett.*, vol. 17, no. 6, pp. 1081–1083, Jun. 2013.

[44] F. Mo, Y.-H. Lu, J.-L. Zhang, Q. Cui, and S. Qiu, "A support vector machine for identification of monitors based on their unintended electromagnetic emanation," *Progr. Electromagn. Res. M*, vol. 30, pp. 211–224, May 2013.

[45] C. Holz, S. Buthpitiya, and M. Knaust, "Bodyprint: Biometric user identification on mobile devices using the capacitive touchscreen to scan body parts," in *Proc. 33rd Annu. ACM Conf. Human Factors Comput. Syst.*, Seoul, South Korea, 2015, pp. 3011–3014.

[46] A. C. Polak and D. L. Goeckel, "Wireless device identification based on RF oscillator imperfections," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 12, pp. 2492–2501, Dec. 2015.

[47] T. Filler, J. Fridrich, and M. Goljan, "Using sensor pattern noise for camera model identification," in *Proc. 15th IEEE Int. Conf. Image Process.*, San Diego, CA, USA, Oct. 2008, pp. 1296–1299.

[48] S. Bayram, H. T. Sencar, and N. Memon, "Sensor fingerprint identification through composite fingerprints and group testing," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 3, pp. 597–612, Mar. 2015.

[49] K. S. Choi, E. Y. Lam, and K. K. Y. Wong, "Source camera identification by JPEG compression statistics for image forensics," in *Proc. IEEE Region 10 Conf. TENCON*, Hong Kong, Nov. 2006, pp. 1–4.

[50] A. L. S. Orozco *et al.*, "Smartphone image acquisition forensics using sensor fingerprint," *IET Comput. Vis.*, vol. 9, no. 5, pp. 723–731, Sep. 2015.

[51] A. Swaminathan, M. Wu, and K. J. R. Liu, "Digital image forensics via intrinsic fingerprints," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 1, pp. 101–117, Mar. 2008.

[52] J. Lukas, J. Fridrich, and M. Goljan, "Digital camera identification from sensor pattern noise," *IEEE Trans. Inf. Forensics Security*, vol. 1, no. 2, pp. 205–214, Jun. 2006.

[53] T. V. Lanh, K.-S. Chong, S. Emmanuel, and M. S. Kankanhalli, "A survey on digital camera image forensic methods," in *Proc. IEEE Int. Conf. Multimedia Expo*, Beijing, China, Jul. 2007, pp. 16–19.

[54] K. S. Choi, E. Y. Lam, and K. K. Y. Wong, "Source camera identification using footprints from lens aberration," in *Proc. Electron. Imag.*, 2006, pp. 60–69.

[55] A. E. Dirik, H. T. Sencar, and N. Memon, "Digital single lens reflex camera identification from traces of sensor dust," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 3, pp. 539–552, Sep. 2008.

[56] J. Fridrich, "Digital image forensics," *IEEE Signal Process. Mag.*, vol. 26, no. 2, pp. 26–37, Mar. 2009.

[57] N. Kulkarni and V. Mane, "Source camera identification using GLCM," in *Proc. IEEE Int. Adv. Comput. Conf. (IACC)*, Bengaluru, India, Jun. 2015, pp. 1242–1246.

[58] C.-T. Li and Y. Li, "Digital camera identification using colour-decoupled photo response non-uniformity noise pattern," in *Proc. IEEE Int. Symp. Circuits Syst.*, Paris, France, May 2010, pp. 3052–3055.

[59] G. Xu, Y. Q. Shi, and W. Su, "Camera brand and model identification using moments of 1-D and 2-D characteristic functions," in *Proc. 16th IEEE Int. Conf. Image Process. (ICIP)*, Cairo, Egypt, Nov. 2009, pp. 2917–2920.

[60] S. Chen, A. Pande, K. Zeng, and P. Mohapatra, "Live video forensics: Source identification in lossy wireless networks," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 1, pp. 28–39, Jan. 2015.

[61] R. Aggarwal, S. Singh, A. K. Roul, and N. Khanna, "Cellphone identification using noise estimates from recorded audio," in *Proc. Int. Conf. Commun. Signal Process. (ICCSP)*, Apr. 2014, pp. 1218–1222.

[62] D. Garcia-Romero and C. Y. Espy-Wilson, "Automatic acquisition device identification from speech recordings," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process.*, Dallas, TX, USA, 2010, pp. 1806–1809.

[63] C. L. Kotropoulos, "Source phone identification using sketches of features," *IET Biometrics*, vol. 3, no. 2, pp. 75–83, Jun. 2014.

[64] C. Hanilci, F. Ertas, T. Ertas, and Ö. Eskidere, "Recognition of brand and models of cell-phones from recorded speech signals," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 625–634, Apr. 2012.

[65] L. Cuccovillo, S. Mann, M. Tagliasacchi, and P. Aichroth, "Audio tampering detection via microphone classification," in *Proc. IEEE 15th Int. Workshop Multimedia Signal Process. (MMSP)*, Pula, Croatia, 2013, pp. 177–182.

[66] D. Marco and D. L. Neuhoff, "The validity of the additive noise model for uniform scalar quantizers," *IEEE Trans. Inf. Theory*, vol. 51, no. 5, pp. 1739–1755, May 2005.

[67] C. Kraetzer, A. Oermann, J. Dittmann, and A. Lang, "Digital audio forensics: A first practical evaluation on microphone and environment classification," in *Proc. 9th Workshop Multimedia Security*, Dallas, TX, USA, 2007, pp. 63–74.

[68] F. Soong, A. Rosenberg, L. Rabiner, and B. Juang, "A vector quantization approach to speaker recognition," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process. (ICASSP)*, vol. 10. Tampa, FL, USA, Apr. 1985, pp. 387–390.

[69] L. Zou, Q. He, and J. Wu, "Source cell phone verification from speech recordings using sparse representation," *Digit. Signal Process.*, vol. 62, pp. 125–136, Mar. 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1051200416301865

[70] S. Dey, N. Roy, W. Xu, R. R. Choudhury, and S. Nelakuditi, "AccelPrint: Imperfections of accelerometers make smartphones trackable," in *Proc. Netw. Distrib. Syst. Security Symp. (NDSS)*, San Diego, CA, USA, Feb. 2014, pp. 1–16.

[71] H. Bojinov, Y. Michalevsky, G. Nakibly, and D. Boneh, "Mobile device identification via sensor fingerprinting," *CoRR*, vol. abs/1408.1416, pp. 1–14, Aug. 2014. [Online]. Available: http://arxiv.org/abs/1408.1416

[72] 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.

[73] E. L. Grand and S. Thrun, "3-axis magnetic field mapping and fusion for indoor localization," in *Proc. IEEE Conf. Multisensor Fusion Integr. Intell. Syst. (MFI)*, Hamburg, Germany, Sep. 2012, pp. 358–364.

[74] R. Jin, L. Shi, K. Zeng, A. Pande, and P. Mohapatra, "Magpairing: Pairing smartphones in close proximity using magnetometers," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 6, pp. 1306–1320, Jun. 2016.

[75] W. Jiang, D. Ferreira, J. Ylioja, J. Goncalves, and V. Kostakos, "Pulse: Low bitrate wireless magnetic communication for smartphones," in *Proc. ACM Int. Joint Conf. Pervasive Ubiquitous Comput.*, Seattle, WA, USA, 2014, pp. 261–265.

[76] G. Baldini, G. Steri, R. Giuliani, and V. Kyovtorov, "Mobile phone identification through the built-in magnetometers," *CoRR*, vol. abs/1701.07676, Jan. 2017. [Online]. Available: http://arxiv.org/abs/1701.07676

[77] S. U. Rehman, K. W. Sowerby, S. Alam, and I. Ardekani, "Radio frequency fingerprinting and its challenges," in *Proc. IEEE Conf. Commun. Netw. Security*, San Francisco, CA, USA, Oct. 2014, pp. 496–497.

[78] A. Jain and D. Zongker, "Feature selection: Evaluation, application, and small sample performance," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 19, no. 2, pp. 153–158, Feb. 1997.

[79] L. C. Molina, L. Belanche, and A. Nebot, "Feature selection algorithms: A survey and experimental evaluation," in *Proc. IEEE Int. Conf. Data Min. (ICDM)*, Maebashi, Japan, 2002, pp. 306–313.

[80] M. J. Mendenhall and E. Merenyi, "Relevance-based feature extraction for hyperspectral images," *IEEE Trans. Neural Netw.*, vol. 19, no. 4, pp. 658–672, Apr. 2008.

[81] Y. Yuan, Z. Huang, H. Wu, and X. Wang, "Specific emitter identification based on Hilbert–Huang transform-based time-frequency-energy distribution features," *IET Commun.*, vol. 8, no. 13, pp. 2404–2412, Sep. 2014.

[82] J. Hasse, T. Gloe, and M. Beck, "Forensic identification of GSM mobile phones," in *Proc. 1st ACM Workshop Inf. Hiding Multimedia Security*, Montpellier, France, 2013, pp. 131–140.

[83] W. H. Press, *Numerical Recipes 3rd Edition: The Art of Scientific Computing*. New York, NY, USA: Cambridge Univ. Press, 2007.

[84] R. Klein, M. A. Temple, M. J. Mendenhall, and D. R. Reising, "Sensitivity analysis of burst detection and RF fingerprinting classification performance," in *Proc. IEEE Int. Conf. Commun.*, Dresden, Germany, Jun. 2009, pp. 1–5.

[85] M. D. Williams, S. A. Munns, M. A. Temple, and M. J. Mendenhall, "RF-DNA fingerprinting for airport wimax communications security," in *Proc. 4th Int. Conf. Netw. Syst. Security (NSS)*, Melbourne, VIC, Australia, Sep. 2010, pp. 32–39.

[86] L. Zou, Q. He, and X. Feng, "Cell phone verification from speech recordings using sparse representation," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process. (ICASSP)*, Brisbane, QLD, Australia, 2015, pp. 1787–1791.

[87] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," in *Proc. 14th ACM Int. Conf. Mobile Comput. Netw.*, San Francisco, CA, USA, 2008, pp. 116–127.

[88] C. E. Shannon, "A mathematical theory of communication," *ACM SIGMOBILE Mobile Comput. Commun. Rev.*, vol. 5, no. 1, pp. 3–55, 2001.

[89] A. Graps, "An introduction to wavelets," *IEEE Comput. Sci. Eng.*, vol. 2, no. 2, pp. 50–61, 1995.

[90] D. R. Reising, M. A. Temple, and M. E. Oxley, "Gabor-based RF-DNA fingerprinting for classifying 802.16e wimax mobile subscribers," in *Proc. Int. Conf. Comput. Netw. Commun. (ICNC)*, Jan. 2012, pp. 7–13.

[91] A. Chouchane, S. Rekhis, and N. Boudriga, "Defending against rogue base station attacks using wavelet based fingerprinting," in *Proc. IEEE/ACS Int. Conf. Comput. Syst. Appl.*, Rabat, Morocco, May 2009, pp. 523–530.

[92] E. J. Candès and M. B. Wakin, "An introduction to compressive sampling," *IEEE Signal Process. Mag.*, vol. 25, no. 2, pp. 21–30, Mar. 2008.

[93] C. Zhao, X. Wu, L. Huang, Y. Yao, and Y.-C. Chang, "Compressed sensing based fingerprint identification for wireless transmitters," *Sci. World J.*, vol. 2014, Apr. 2014, Art. no. 473178.

[94] P. Scanlon, I. O. Kennedy, and Y. Liu, "Feature extraction approaches to RF fingerprinting for device identification in femtocells," *Bell Labs Tech. J.*, vol. 15, no. 3, pp. 141–151, Dec. 2010.

[95] H. Malik and J. Miller, "Microphone identification using higher-order statistics," in *Proc. AES Int. Conf. Audio Forensics*, 2012, pp. 2–5.

[96] N. E. Huang, *Hilbert-Huang Transfor and Its Applications*, vol. 16. Hackensack, NJ, USA: World Sci., 2014,

[97] J. P. Fishburn, "Clock skew optimization," *IEEE Trans. Comput.*, vol. 39, no. 7, pp. 945–951, Jul. 1990.

[98] A. S. Uluagac, S. V. Radhakrishnan, C. Corbett, A. Baca, and R. Beyah, "A passive technique for fingerprinting wireless devices with wired-side observations," in *Proc. IEEE Conf. Commun. Netw. Security (CNS)*, Oct. 2013, pp. 305–313.

[99] X. Lin and C.-T. Li, "Preprocessing reference sensor pattern noise via spectrum equalization," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 1, pp. 126–140, Jan. 2016.

[100] E. Alpaydin, *Introduction to Machine Learning*. Cambridge, MA, USA: MIT Press, 2014.

[101] M. A. Alsheikh, S. Lin, D. Niyato, and H.-P. Tan, "Machine learning in wireless sensor networks: Algorithms, strategies, and applications," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 1996–2018, 4th Quart., 2014.

[102] K. S. Beyer, J. Goldstein, R. Ramakrishnan, and U. Shaft, "When is 'nearest neighbor' meaningful?" in *Proc. Int. Conf. Database Theory*, Jerusalem, Israel, 1999, pp. 217–235.

[103] K. Q. Weinberger, J. Blitzer, and L. K. Saul, "Distance metric learning for large margin nearest neighbor classification," in *Proc. Adv. Neural Inf. Process. Syst.*, Vancouver, BC, Canada, 2005, pp. 1473–1480.

[104] J. Qinlan, "Introduction of decision trees," *Mach. Learn.*, vol. 1, no. 1, pp. 81–106, 1986.

[105] S. B. Kotsiantis, "Supervised machine learning: A review of classification techniques," in *Proc. Conf. Emerg. Artif. Intell. Appl. Comput. Eng. Real Word AI Syst. Appl. eHealth HCI Inf. Retrieval Pervasive Technol.*, 2007, pp. 3–24. [Online]. Available: http://dl.acm.org/citation.cfm?id=1566770.1566773

[106] C. Cortes and V. Vapnik, "Support-vector networks," *Mach. Learn.*, vol. 20, no. 3, pp. 273–297, 1995.

[107] K. Crammer and Y. Singer, "On the algorithmic implementation of multiclass kernel-based vector machines," *J. Mach. Learn. Res.*, vol. 2, pp. 265–292, Dec. 2001.

[108] C.-W. Hsu and C.-J. Lin, "A comparison of methods for multiclass support vector machines," *IEEE Trans. Neural Netw.*, vol. 13, no. 2, pp. 415–425, Mar. 2002.

[109] X. Wu *et al.*, "Top 10 algorithms in data mining," *Knowl. Inf. Syst.*, vol. 14, no. 1, pp. 1–37, 2008.

[110] N. Friedman, D. Geiger, and M. Goldszmidt, "Bayesian network classifiers," *Mach. Learn.*, vol. 29, nos. 2–3, pp. 131–163, 1997.

[111] D. R. Amancio *et al.*, "A systematic comparison of supervised classifiers," *PLoS ONE*, vol. 9, no. 4, pp. 1–14, 2014.

[112] B. Widrow and M. A. Lehr, "30 years of adaptive neural networks: Perceptron, madaline, and backpropagation," *Proc. IEEE*, vol. 78, no. 9, pp. 1415–1442, Sep. 1990.

[113] T. J. O'Shea, J. Corgan, and T. C. Clancy, "Convolutional radio modulation recognition networks," in *Proc. Int. Conf. Eng. Appl. Neural Netw.*, Aberdeen, U.K., 2016, pp. 213–226.

[114] O. M. Fahmy, "An efficient clustering technique for cameras identification using sensor pattern noise," in *Proc. Int. Conf. Syst. Signals Image Process. (IWSSIP)*, London, U.K., Sep. 2015, pp. 249–252.

[115] N. T. Nguyen, G. Zheng, Z. Han, and R. Zheng, "Device fingerprinting to enhance wireless security using nonparametric Bayesian method," in *Proc. IEEE INFOCOM*, Shanghai, China, Apr. 2011, pp. 1404–1412.

[116] R. Li, C.-T. Li, and Y. Guan, "A compact representation of sensor fingerprint for camera identification and fingerprint matching," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process. (ICASSP)*, Brisbane, QLD, Australia, Apr. 2015, pp. 1777–1781.

[117] T. Cover and P. Hart, "Nearest neighbor pattern classification," *IEEE Trans. Inf. Theory*, vol. 13, no. 1, pp. 21–27, Jan. 1967.

[118] S. U. Rehman, K. W. Sowerby, and C. Coghill, "Analysis of impersonation attacks on systems using RF fingerprinting and low-end receivers," *J. Comput. Syst. Sci.*, vol. 80, no. 3, pp. 591–601, 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0022000013001220

[119] I. O. Kennedy *et al.*, "Radio transmitter fingerprinting: A steady state frequency domain approach," in *Proc. IEEE 68th Veh. Technol. Conf. VTC Fall*, Calgary, AB, Canada, 2008, pp. 1–5.
[120] Y. Huang, J. Zhang, and H. Huang, "Camera model identification with unknown models," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 12, pp. 2692–2704, Dec. 2015.
[121] C. J. C. Burges, "A tutorial on support vector machines for pattern recognition," *Data Min. Knowl. Disc.*, vol. 2, no. 2, pp. 121–167, 1998.
[122] O. Çeliktutan, B. Sankur, and I. Avcibas, "Blind identification of source cell-phone model," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 3, pp. 553–566, Sep. 2008.
[123] Y. Sutcu, S. Bayram, H. T. Sencar, and N. Memon, "Improvements on sensor noise based source camera identification," in *Proc. IEEE Int. Conf. Multimedia Expo*, Beijing, China, Jul. 2007, pp. 24–27.
[124] L. Breiman, "Random forests," *Mach. Learn.*, vol. 45, no. 1, pp. 5–32, 2001. [Online]. Available: http://dx.doi.org/10.1023/A:1010933404324
[125] H. J. Patel and B. W. Ramsey, "Comparison of parametric and non-parametric statistical features for Z-wave fingerprinting," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Tampa, FL, USA, Oct. 2015, pp. 378–382.
[126] H. J. Patel, M. A. Temple, and R. O. Baldwin, "Improving ZigBee device network authentication using ensemble decision tree classifiers with radio frequency distinct native attribute fingerprinting," *IEEE Trans. Rel.*, vol. 64, no. 1, pp. 221–233, Mar. 2015.
[127] B. Hammer and T. Villmann, "Generalized relevance learning vector quantization," *Neural Netw.*, vol. 15, nos. 8–9, pp. 1059–1068, 2002.
[128] K. Huang and S. Aviyente, "Sparse representation for signal classification," in *Proc. Adv. Neural Inf. Process. Syst.*, Vancouver, BC, Canada, 2006, pp. 609–616.
[129] V. K. Khanna, "Remote fingerprinting of mobile phones," *IEEE Wireless Commun.*, vol. 22, no. 6, pp. 106–113, Dec. 2015.
[130] M. Gerlach and F. Guttler, "Privacy in VANETs using changing pseudonyms—Ideal and real," in *Proc. IEEE 65th Veh. Technol. Conf. VTC Spring*, Dublin, Ireland, Apr. 2007, pp. 2521–2525.
[131] J. R. Padilla-López, A. A. Chaaraoui, and F. Flórez-Revuelta, "Visual privacy protection methods," *Expert Syst. Appl.*, vol. 42, no. 9, pp. 4177–4195, Jun. 2015. [Online]. Available: http://dx.doi.org/10.1016/j.eswa.2015.01.041
[132] R. Neisse, G. Steri, I. N. Fovino, and G. Baldini, "Seckit: A model-based security toolkit for the Internet of Things," *Comput. Security*, vol. 54, pp. 60–76, 2015.
[133] D. Ghosh, A. Joshi, T. Finin, and P. Jagtap, "Privacy control in smart phones using semantically rich reasoning and context modeling," in *Proc. IEEE Symp. Security Privacy Workshops (SPW)*, San Francisco, CA, USA, May 2012, pp. 82–85.
[134] R. Kumar, H. K. Chandrikakutty, and S. Kundu, "On improving reliability of delay based physically unclonable functions under temperature variations," in *Proc. IEEE Int. Symp. Hardw.-Oriented Security Trust (HOST)*, San Diego, CA, USA, 2011, pp. 142–147.
[135] K. Rosenfeld, E. Gavas, and R. Karri, "Sensor physical unclonable functions," in *Proc. IEEE Int. Symp. Hardw.-Oriented Security Trust (HOST)*, Anaheim, CA, USA, Jun. 2010, pp. 112–117.
[136] Y. Cao, L. Zhang, S. S. Zalivaka, C.-H. Chang, and S. Chen, "CMOS image sensor based physical unclonable function for coherent sensor-level authentication," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 62, no. 11, pp. 2629–2640, Nov. 2015.
[137] D. Lim *et al.*, "Extracting secret keys from integrated circuits," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 13, no. 10, pp. 1200–1205, Oct. 2005.
[138] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: A tutorial," *Proc. IEEE*, vol. 102, no. 8, pp. 1126–1141, Aug. 2014.
[139] X. Chu, Y. Chen, M. C. Stamm, and K. J. R. Liu, "Information theoretical limit of media forensics: The forensicability," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 4, pp. 774–788, Apr. 2016.
[140] O. Gungor and C. E. Koksal, "On the basic limits of RF-fingerprint-based authentication," *IEEE Trans. Inf. Theory*, vol. 62, no. 8, pp. 4523–4543, Aug. 2016.
[141] *Project Ara*. Accessed on Aug. 10, 2016. [Online]. Available: http://www.projectara.com/
[142] *Phone Bloks*. Accessed on Aug. 10, 2016. [Online]. Available: https://phonebloks.com/en
[143] V. S. Venkitachalam, V. Namboodiri, S. Joseph, E. Dee, and C. A. Burdsal, "What, why, and how: Surveying what consumers want in new mobile phones," *IEEE Consum. Electron. Mag.*, vol. 4, no. 2, pp. 54–59, Apr. 2015.
[144] S. X. Wang and X. J. Zhou, "Spectroscopic sensor on mobile phone," U.S. Patent 7 420 663, Sep. 2, 2008.
[145] C. W. Pirnstill and G. L. Coté, "Malaria diagnosis using a mobile phone polarized microscope," *Sci. Rep.*, vol. 5, Jul. 2015, Art. no. 13368.
[146] D. M. J. Tax, M. Van Breukelen, R. P. Duin, and J. Kittler, "Combining multiple classifiers by averaging or by multiplying?" *Pattern Recognit.*, vol. 33, no. 9, pp. 1475–1485, 2000.
[147] S. Mahato and G. Gielen, "Impact of transistor aging on RF low noise amplifier performance of 28nm technology: Reliability assessment," in *Proc. IEEE 20th Int. Conf. Electron. Circuits Syst. (ICECS)*, Abu Dhabi, UAE, Dec. 2013, pp. 413–416.
[148] B. Zhao, Y. Wang, H. Yang, and H. Wang, "The NBTI impact on RF front end in wireless sensor networks," in *Proc. IEEE Circuits Syst. Int. Conf. Test. Diagnosis*, Chengdu, China, Apr. 2009, pp. 1–4.

Gianmarco Baldini completed the degree in electrical engineering with specialization in wireless communications from the University of Rome "La Sapienza" in 1993. He was a Senior Technical Architect and a System Engineering Manager with Ericsson, Lucent Technologies, Hughes Network Systems, and Finmeccanica. In 2007, he joined the Joint Research Centre, European Commission, as a Scientific Officer. He has co-authored over 70 research papers in the areas of wireless communications, GNSS, and security. His current research activities focus on Internet of Things, GNSS, machine learning, and security.

Gary Steri received the master's degree in information technologies and the Ph.D. degree in computer science from the University of Cagliari in 2006 and 2011, respectively. He is a Post-Doctoral Researcher with the Joint Research Center, European Commission, Ispra, Italy. His research activity first focused on security and authentication of wireless networks, and then moved on wireless sensor networks for environmental survey and wearable inertial measurement units for human motion tracking. His current activity at the JRC focuses on security aspects of Internet of Things, device-to-device authentication, and high accuracy positioning systems for intelligent transport applications.