Recent Advances in Biometric Technology for Mobile Devices

Abhijit Das*†[1], Chiara Galdi†[2], Hu Han[3], Raghavendra Ramachandra[4], Jean-Luc Dugelay [5], and Antitza Dantcheva[6]

[1,6]Inria, Sophia Antipolis, France
[2,5]EURECOM, Sophia Antipolis, France
[3] Institute of Computing Technology, CAS, China
[4] Norwegian University of Science and Technology, Norway

Abstract

The prevalent commercial deployment of mobile biometrics as a robust authentication method on mobile devices has fueled increasingly scientific attention. Motivated by this, in this work we seek to provide insight on recent development in mobile biometrics. We present parallels and dissimilarities of mobile biometrics and classical biometrics, enumerate related strengths and challenges. Further we provide an overview of recent techniques in mobile biometrics, as well as application systems adopted by industry. Finally, we discuss open research problems in this field.

1. Introduction

Biometric recognition on mobile devices has drawn increased attention of the scientific community in the last decades, as evidenced by a set of related competitions at prominent pattern recognition and biometrics conferences [23, 76, 45, 46, 38, 41, 44], as well as by a rapidly growing number of related publications (see Figure 1 for the period 1997-2017, according to Scopus, matching keywords include *biometrics*, *mobile devices*, and *smartphone*). This scientific attention has been fueled by the prevalent commercial deployment of mobile biometrics as a robust authentication method on smartphones and other mobile devices. In addition, commercial organizations are involved in research projects, such as the Abacus project, introduced at Google I/O 2015, which aimed at replacing password-based authentication by an biometric-based authentication system. Related monitored biometric modalities include face, fingerprint, voice, patterns of typing, based on which a multimodal trust score was computed. Associated results on a 40TB multi-modal database show a false acceptance rate (FAR) of 1:1,000,000 [13].

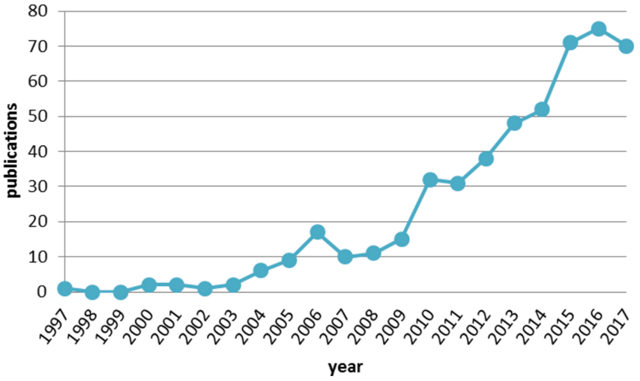

Figure 1. Graph of scientific papers published per year in the period 1997-2017 matching keywords including biometrics and mobile devices. From Scopus (https://www.scopus.com).

In addition, the *mobile biometrics market* is projected to significantly expand, according to Acuity Market Intelligence, indicating that in 2019 all smartphones will have at least one integrated biometric technology. Similarly, according to Statista [12], by 2020 mobile biometrics will additionally be pervasive on wearable devices. This comes at a time, when TrendForce estimates the global smartphone production for 2018 at around 1.5 billion units [3]. Further, the introduction of applications such as Apple-pay is curving the need for highly reliable and secure mobile authentication [4]. Finally, financial institutes and banks are aiming to introduce online transactions on mobile platforms with biometric authentication [6]. Hence, biometrics is considered as the next generation mobile payment technique and related biometrics-embedded mobile devices are becoming increasingly popular.

Motivated by the above, we here aim to adhere to previous review works, including Meng et al. [47], Wojciechowska et al. [75], Baldini et al. [21] and Neal et

*abhijit.das@inria.fr

†First and second author contributed equally.

al. [52], by revisiting latest commercial solutions and recent papers from the years *2017-2018*, as well as identifying added challenges that a biometric technology might face in mobile environment. Specifically we here place focal points on (a) what constitutes mobile biometrics and its specific challenges (Section 2) , (b) currently deployed commercial mobile biometric solutions (Section 3), (c) recent works in mobile biometrics (Section 4), as well as on (d) open research problems in the field (Section 5).

2. Mobile biometrics

A *classical biometric system* acquires biometric data from an individual (e.g., a fingerprint image), extracts a set of features from the data, and compares this feature set with templates in the database in order to verify a claimed identity or to determine an identity. Keeping in mind that this classical structure is also incorporated in mobile biometric systems, one could introduce following definition. A *mobile biometric system* is the entity that combines (i) embedded readers or sensors, as well as (ii) mobile applications, which process acquired data via (i), exploiting biometrics. Such a system can be built-in hand-held systems, as well as in smartphones or tablets [7].

2.1. Benefits of mobile biometrics

Mobile biometrics inherits a main part of benefits of classical biometrics, endorsing its own assets. Benefits associated to mobile biometrics include the following.

Portability: Due to compactness and high portability, mobile biometrics allows for an authentication at any time and in any place.

Cost effectiveness: The cost of performing biometric authentication on mobile devices is relatively low due to sensor technology and increasing computational power of the processing units embedded in the devices.

Market popularity and user acceptance: Due to the popularity and widespread use of mobile devices, the ease of use, as well as the acceptance of both, user and industry, have increased [37].

2.2. Challenges

Utilities related to mobile biometrics come along with challenges associated with acquisition, pre-processing, feature extraction, tempate storage that we proceed to describe.

Acquisition The sensors embedded in mobile devices, smartphones in particular, are constrained in *size* and *cost*. The former is of pertinence particularly for biometric traits such as fingerprints, palm prints, finger and hand veins. Additional factors concern the *quality* and *heterogeneity* of mobile-embedded microphones, which impact voice-based systems.

Sensor resolution may impact the accuracy of a biometric system based on face, periocular or, particularly, iris, since it relates to the amount of acquired features. However, the resolution of embedded digital cameras has greatly increased in the last decade. As an example, Samsung expanded from 8 to 13 megapixels between the 2011 Galaxy S2 and 2013 S4, then to 16 MP with 2014's Galaxy S5 [8]. In addition, new structured light RGB-D sensors have been recently deployed for smartphones, such as in iPhone X [5] or the recently announced Time of Flight (TOF) 3D Sensing Technology by Vivo [14], exploiting 3D face information, leading to an improved accuracy and robustness to presentation attacks.

While using mobile biometrics allows for identification at any time and in any place, it has to account for a great variability of *acquisition conditions*. Specifically *environmental* factors including illumination, temperature, humidity, noise, as well as *human* factors such as physical (e.g., resting, walking, seating) and psychological state of the user have a great impact on the quality of the biometric acquisition. For example, gait or movement based biometrics are restricted, when the user is resting. Table 1 gives an overview of further challenges and limitations of biometric modalities with regard to mobile environment and sensors.

Pre-processing Once acquired, biometric samples pass through a pre-processing step that aims to select from the raw data only the information necessary for biometric matching. This step may include *segmentation*, *noise reduction*, as well as shape and color *normalization*. For example, in the context of mobile iris recognition, segmentation has always been a challenge, in particular in the visible spectrum. Varying illumination, reflections, and occlusions make the process of extracting the iris area from an image extremely challenging [32, 64]. Illumination and pose normalization are indispensable to reduce intra-class variations for face [55].

Feature extraction Technological development has greatly reduced the gap between classical and mobile-based systems in terms of computational power. However the resources of a mobile device remain limited and the algorithms need to be designed to suit them. This brings to the fore the challenge of using memory and computationally intensive techniques, such as deep neural networks (DNNs) on mobile devices. This puts DNNs at direct odds with the power and performance constraints of embedded devices, necessitating algorithmic and software optimizations to make related algorithms suitable for deployment at the edge. It is essential that DNNs are executed within a power-constrained, computation-constrained, restricted environment, while maintaining the performance the networks would normally achieve in the cloud or even on a desktop PC [10]. Towards this, Qualcomm has recently unveiled the Vision Intelligence Platform, built to enable powerful visual computing and edge computing for machine learning on a wide range of IoT devices [11]. Other

Table 1. Challenges for biometric traits proposed for mobile environment.

Modality/Factors	**Environment**	**Physiological condition**	**Sensor**
Face	Illumination	Injury	Resolution
Fingerprint	Temperature and humidity	Fingerprint and skin condition	Size
Plamprint		Skin condition	
Signature	-	Physical and psychological state	Size, heterogeneity
Voice	Background noise		Heterogeneity
Iris	Illumination	Injury	Resolution
Gait	Ground condition	Physical and psychological state	Sensitivity
Heart rate	-		
Keystroke	Temperature and humidity		
Touch-based gestures			

companies developing processors for deep learning on mobile devices include Intel Movidius, HiSilicon, ARM, and MediaTek. Huawei claims that its neural processing unit (NPU) can perform image recognition of 2,000 pictures per second, which the company also alleges is 20 times faster than a standard CPU [2]. We note that such a development in computational power of mobile devices will beyond doubt promote research, as well as use of more sophisticated models for mobile biometric applications.

Template storage Given that user biometric data is encrypted and stored within mobile devices, it is relatively easy for an adversary to appropriate the data, if the mobile phone can be accessed [75]. While classical biometric systems are generally manipulated only by authorized personnel and are monitored (e.g., video surveillance), mobile devices are fully and only under the control of the owner. This security challenge requires the use of sophisticated *encryption* techniques to protect biometric data, as well as the employment of *presentation attack detection* to deny access to impostors.

3. Commercial solutions

In terms of sensor technology, smartphone biometrics in 2018 focused on Face ID (Apple), iris recognition (Samsung), with other brands *mainly* using capacitive fingerprint sensors “due to existing technical barriers”. Vivo, which recently launched an Android smartphones, featuring an optical under-display fingerprint sensor, grew in production volume by 17% in 2017. At MWC Shanghai 2018, Vivo revealed its Time of Flight (TOF) 3D Sensing Technology, which detects the time it takes emitted pulse light to return to the sensor to accurately map objects at up to three meters in front of it. It enables new opportunities in facial, gesture and motion recognition, 3D photography and Augmented Reality (AR), expanding the capabilities of the next generation of smart devices.

Bloomberg recently reported that Google may adopt an iPhone-style “notch” in forthcoming smartphones, which could enable it to integrate 3D facial recognition cameras (from `https://www.biometricupdate.com/` [25]). An overview of the most recent biometric commercial solutions is summarized in Table 2. The table illustrates that currently modalities deployed by commercial products are predominantly related to face, fingerprint and iris.

Regarding mobile biometrics applications, it is expected that industry standardization initiatives like Visas Secure Remote Commerce will drive growth in remote biometric transactions, as the integration of biometric hardware in smartphones will increase, according to the research carried out by Juniper [48]. It was also predicted that more than 80% of smartphones would have some form of biometric hardware built-in by 2023. While fingerprint sensors are still the most common form of biometric hardware, facial recognition and iris scanning hardware integration will become more common, exceeding 1 billion devices.

Further, software Biometrics-as-a-Service offerings will be the main innovation in the field, Juniper reported. Software-based facial recognition is already supported by 90% of current smartphones, and 80% can support voice biometrics for payments. These services and behavior tracking technologies will allow cloud services to perform authentication in the background and across platforms, and Juniper estimated more than 1.5 billion smartphones would use software-based biometrics by 2023 (from `https://www.biometricupdate.com/` [6]).

4. Recent academic advances

In this section we review the most recent and innovative work on mobile biometrics. Apart from biometric recognition itself, several other aspects have been investigated by the research community, such as presentation attack detection and continuous authentication. This Section covers in particular approaches to overcome the challenges presented in Section 2.

4.1. Uni-modal approaches

Tables 3 and 4 report recent work on mobile biometrics in the period 2017-2018. Specifically Table 3 reflects the fact that modalities such as iris, face and periocular are predominant in mobile biometrics, which have been the main focus of the recent literature. In addition, a set of challenges mentioned in Section 2 such as robustness to acquisition-condition and illumination have been addressed. Mobile

Table 2. Latest commercial solutions for mobile biometrics.

Provider	Solution name	Sensor	Modality	Application
Samsung	Intelligent Scan	Infrared camera module and an infrared LED	Iris and face	Smartphone screen unlock, Secure Folder access, Samsung Pay
	Fingerprint scanner	Capacitive sensor	Fingerprint	
Huawei	Face unlock	RGB camera	Face	Smartphone screen unlock
	Fingerprint scanner	Capacitive sensor	Fingerprint	
Apple	Face ID	TrueDepth Camera	3D Face	Smartphone screen unlock, Apple pay, unlock banking app and Paypal
	Touch ID	Capacitive sensor	Fingerprint	
Vivo	Face ID	Time of Flight (TOF) 3D depth-sensing system with 300,000 sensor points	3D Face	Smartphone screen unlock
	Fingerprint scanner	Qualcomms ultrasonic In-Display Fingerprint Scanner	Fingerprint	
OnePlus	Face unlock	RGB camera	Face	Smartphone screen unlock
Google	Smart Lock	Depends on the smartphone	Voice, fingerprint, or face	Smartphone screen unlock

face recognition found to attend promising performance of AUC of 0.3 in both, constrained and unconstrained scenarios, validated on a private dataset. Noisy acquisition poses a remaining challenge in *iris recognition in the visible spectrum*. Specifically iris segmentation has shown to be challenging in this context [20]. Related recent advancement [20] employed weighted adaptive Hough transform on MICHE-II database and showed a high level of accuracy and more efficient computationally. In contrast to iris, the accuracy of periocular biometrics has significantly increased, given noisy acquisition, as experiments on the VISOB [63] and MICHE-II dataset showed. Therefore, it will be interesting to investigate viability of periocular biometrics in real life and moreover commercial devices for smart-phones having visible spectrum sensor. For both, iris and periocular biometrics publicly available datasets such as MICHE-II [26], VISOB [63], VSSIRIS [60] and CASIA-Iris Mobile V1.0 [77] have been employed. The detailed description of popular publicly available datasets can be found in Table 6.

In addition to classical biometric modalities, Table 3 showcases that recently *new physiological biometric traits* such as ECG, palmprint and hand geometry have been investigated in the context of mobile biometrics. Such traits have achieved accuracy of EER=0.5% for hand geometry and ECG, and EER = 7% for palmprint. Despite the fact that such traits are not yet established, related benefits are considerable. For example in the context of ECG, the spontaneous physiological signal is complementary to other physiological traits and can be used as a single trait for continuous authentication without user cooperation. It is notable that in most experiments related to new physiological trait, private datasets were explored, which brings to the need for public datasets that would enable benchmarking, in order to establish a state of the art. Recent works on mobile biometrics based on *behavioral traits* involve mainly gait, touch gesture, signature and keystroke (see Table 4). Among these traits gait is found to be the most investigated one. Significant results with very low EER=0.15% have been reported, considering both, constrained and unconstrained scenarios. We note that dataset size has been limited in such studies (maximum of 50 individuals). Similar to the new physiological traits the viability of behavioral traits for incorporation in commercial solutions is yet to be addressed and can be of great commercial interest.

Further advancements can be noticed in the *feature extraction techniques* for mobile biometrics. Similar to other computer vision and machine learning areas, mobile biometrics has rapidly and increasingly adopted DNN based methods (see Table 3). Given the skyrocketing performances of DNN-algorithms in recognition tasks, as well as the newest development of resource-preserving and lite DNN-architectures like Mobile Net [39], such architectures are expected to take over in mobile biometrics in the very near future.

The large heterogeneity of the mobile-embedded sensors and the rapid release of new models are not without consequences for mobile biometrics. As data comes from different acquisition sources, we face the challenge of *cross-sensor recognition*, which has been investigated for palmprint [70] and periocular [19]. Similar studies also are necessary for other traits. The challenge of cross-sensor recognition concerns mainly server based authentication system as opposed to standalone applications.

4.2. Multi-modal approaches

As in classical biometric systems, the use of multiple biometric modalities is beneficial in mobile environment, as it can overcome a number of above-mentioned limitations. For example the overall accuracy of the system can be improved, unfavorable conditions for one modality can be compensated by the others, as well as attacking a system based on multiple modalities is more challenging, since it would involve the replication of multiple modalities. Re-

Table 3. Recent development of mobile biometrics based on physiological traits. Abbreviations used: EER = Equal Error Rate; ISO = International Organization for Standardization; FNMR = False Non-Match Rate; AUC = Area Under Curve; AUROC = Area Under ROC curve; ROC = Receiver Operating Characteristics curve; RR = Recognition Rate; DEC = Decidability; ACC = Accuracy; CNN = Convolutional Neural Networks; LBP = Local Binary Pattern; SIFT = Scale Invariant Feature Transform

Work	Modality	Technique	Dataset	Performance	Mobile challenge
Barra et al., 2018 [22]	Hand geometry	Contact-less hand shape and geometry analysis in visible light	100 subjects	0.52% EER	Varying illumination
Wasnik et al., 2017 [72]	Face	Quality assessment by ISO standard	101 subjects	Error Reject Curve: at FNMR f = 0.1: iPhone 6 Plus AUC of 0.0334, Samsung S7 AUC of 0.03	Intra-class variation due to unconstrained acquisition
Rattani and Derakhshani, 2017 [62]	Iris	Iris co-training	VISOB	13.5% EER	Intra-class variation due to unconstrained acquisition
Galdi and Dugelay, 2017 [34]	Iris	Iris color and texture feature extraction; fusion at score level	MICHE-II	70% RR; 80% AUROC; 29% EER	Noisy iris recognition in visible spectrum
Abate et al., 2017 [16]	Iris	Statistical operators of Kurtosis and Skewness at pixel level; Self Organizing Map for clustering pixels of iris images	MICHE-II	65% RR; 18% EER; 89% AUROC; 1.80 DEC	Noisy iris recognition in visible spectrum
Ahuja et al., 2017 [18]	Periocular	Hybrid model: unsupervised and a supervised CNN, and Root SIFT model	MICHE-II VISOB	MICHE-II: 98.6 % AUROC; 5.3 % EER. VISIOB: 99.5% TPR at FPR of 0.001%	Intra-class variation due to unconstrained acquisition
Fernandez et al., 2017 [19]	Periocular	Log-likelihood score level fusion of several comparators	VSSIRIS	6% EER (-40% EER for cross-sensor)	Cross-sensor recognition
Ungureanu et al., 2017 [70]	Palmprint	Collaborative Representation Classifier via Regularized Least Squares classifier using Difference of Vertex Normal Vectors	81 subjects acquired with 5 smartphones	86% RR; 7.4% EER	Cross-sensor recognition
Tan and Perkowski, 2017 [68]	Electrocardiogram (ECG)	Two-stage classifier based on random forest and wavelet distance measure	184 subjects	99.52% ACC	Intra-class variation due to unconstrained acquisition

cent work on mobile based multi-modal biometrics is summarized in Table 5. One interesting recent trend of research relates to the fusion of physiological and behavioral traits, which brings to the fore high recognition accuracies (due to the physiological trait), as well as continuous authentication (due to the behavioral trait). Satisfactory results of EER = 2.4% have been achieved in this area for example employing face and voice [30]. This is only a recent trend and it will be important to explore different traits, in order to find reasonable combinations of physiological and behavioral traits to attend a robust and reliable mobile solution.

4.3. Presentation attack detection

With the wide use of biometric technologies on mobile devices, presentation attack detection (PAD) is gaining high pertinence. While in this context biometric modalities such as fingerprint, palm print, and iris [74] are of lesser concern, face, which is easily acquired or obtained from social media and the related PAD on mobile devices, has attracted increased attention in recent years [74, 56]. Promising results have been reported for different face presentation attacks, such as the photo attack, and the video replay attack. Zero-effort and live minimal-effort impersonation attacks under realistic scenarios were investigated in Muaaz and Mayrhofer [49]. A dataset of 35 participants, five professional actors, who are specialized in mimicking body movements and body language were employed to investigate gait based spoofing for techniques, proposed for mobile devices. Notable in this context is the OULU-NPU database [24], which is a mobile face PAD - database including real-world variations, including 5940 videos corresponding to 55 subjects recorded in three different environments using high-resolution frontal cameras of six different smartphones. In a recent work [61], Raja et al. presented a new approach exploring the intrinsic characteristics of the smartphone camera to capture a number of stack images in the depth-of-field. The proposed system was entirely developed on the

Table 4. Recent development of mobile biometrics based on behavioral traits. Abbreviations used: CNN = Convolutional Neural Networks; DTW = Dynamic Time Warping; RF = Random Forest; EER = Equal Error Rate; FMR = False Match Rate; GMM = Gaussian Mixture Model; ACC = Accuracy; SVM = Support Vector Machine

Work	Modality	Technique	Dataset	Performance	Mobile challenge
Gadaleta and Rossi, 2018 [33]	Gait	Multi-stage decision making framework using CNNs and SVMa to classify walking cycles	50 subjects	0.15% EER	Transparent user authentication
Li and Bours, 2018 [42]	Holding of phone	Gyroscope and accelerometer based feature extraction, RF based classification, feature-level fusion	304 subjects	22.72% EER	Continuous authentication
Fierrez et al., 2018 [29]	Touch	GMM and SVM	UMDAA-02 [43]	Up to 3.1% EER	Inter-session comparison
Muaaz and Mayrhofer, 2017 [49]	Gait	DTW distance between gait cycles	35 subjects	0% FMR	Impersonation Attack
Wasnik et al. 2017 [73]	Gait	Fusion of multiple comparators using Subjective Logic	48 subjects	1.31% EER	Natural variations
Fernandez-Lopez et al., 2017 [28]	Gait	Representative gait cycles selection	23 subjects	17.17% EER	Cross-comparison of gait cycles
Tolosana et al., 2017 [69]	Signature	Feature-based (global system) and time functions-based (local system)	e-BioSign [71]	Intra-device: 10.1% EER; inter-device: 24.3% EER; mixed writing tools: $<$1% EER	Intra-device, inter-device, and mixed writing tool
Sun et al., 2017 [67]	Keystroke	Binary-class identification based on multi-view deep learning	40 subjects	93% ACC	Continuous authentication

Table 5. Recent development of mobile biometrics based on multimodal systems. Abbreviations used: CNN = Convolutional Neural Networks; DTW = Dynamic Time Warping; LBP = Local Binary Pattern; EER = Equal Error Rate; RR = Recognition Rate; HOG = Histogram of Oriented Gradients; AUROC = Area Under ROC curve; ROC = Receiver Operating Characteristics curve; FRR = False Rejection Rate; FAR = False Acceptance Rate.

Work	Modality	Technique	Dataset	Performance	Mobile challenge
Zhang et al., 2018 [78]	Iris and periocular	CNN feature based weighted fusion of iris and periocular	CASIA-Iris-Mobile-V1.0	0.60% EER	Multi-modal recognition
Findling et al. [30], 2018	Gait and face	Acceleration based gait match-on-card authentication	Yale-B [1], Panshot Face Unlock Database [31], Gait dataset [50]	Gait: 11.4% ERR; Face: 2.4-5.4% EER	Match-on-card biometric recognition
Galdi et al., 2018 [35]	Face and source digital camera	HOG; Sensor Pattern Noise	SOCRatES	97% RR	Secure authentication
Ahmed et al., 2017 [17]	Iris and periocular	Multi-Block Transitional Local Binary Patterns; Fusion at score level	MICHE-II	1.22% EER; 2.56% FRR at FAR =0.001	Intra-class variation due to unconstrained acquisition
Gofman et al., 2017 [36]	Face and voice	Hidden Markov Models	54 subjects	11.87% ERR	Intra-class variation due to unconstrained acquisition

smartphone and exploited a stack of images with varying focus to effectively determine the presentation attacks. In 2017, a competition on generalized face PAD in mobile authentication scenarios [23] was conducted, illumination conditions and presentation attack instruments (PAI) were employed to implement the attacks. The deep learning-based methods achieved impressive results. A future study was proposed, combining match scores with both PAD and quality measures, in order to improve the resilience of face verification systems.

Table 6. Publicly available datasets used in recent work on mobile biometrics.

Dataset	Modality	Subjects	Acquiring setup
MICHE	Ocular images	92	iPhone 5, Samsung Galaxy S4, Samsung Galaxy Tab II
VISOB	Ocular images	550	iPhone 5s, Samsung Note 4 and Oppo
VSSIRIS	Ocular images	28	Nokia Lumia 1020 and iPhone 5S
CASIA mobile V1.0	Ocular in NIR	630	Mobile devices
UMDAA-02	Touch gesture & face	48	Nexus 5
e-BioSign	Signature	70	Samsung Galaxy Note 10.1 and Samsung ATIV

Spoofing detection for mobile biometrics performed a large development-leap, addressing a set of challenges associated to classical modalities. In contrast, such PAD solutions have not been commercially deployed yet. Moreover, PAD for modalities proposed recently in the context of mobile biometrics (for example multi-modal system based on fusion of physiological and behavioral) is yet to be explored. Moreover, in contrast to classical biometrics, where PAD-techniques are associated to one specific biometric system and one specific acquisition sensor, mobile biometrics related PAD - techniques need to be robust to a number of acquisition sensors. This constitutes a challenging open research problem.

4.4. Continuous user authentication

Another recently explored novel area of research concerns continuous user authentication on mobile devices. The idea is to continuously monitor the identity, impeding presentation attacks of impostors. Crouse et al. [27] presented a related method based on face and Inertial Measurement Units (IMU). The effectiveness was evaluated on data collected from multiple Android smartphones and found to produce that the proposed person specific score level fusion achieved 9% in increase in true acceptance rate (TAR) in compression to the commercial off-the shelf (COTS) matcher.

Efficient and low latency detection of intruders in mobile active authentication can be found in Perera and Patel [57]. A classical authentication system considers only a single enrolled subject. However, with the emergence of mobile devices, this concept has changed since a mobile device may be accessed by more than one user. In an additional work of Perera and Patel [58], the issue of performance degradation associated to multiple user authentication (as opposed to single user authentication) has been addressed. The authors interpreted this challenge in an open-set framework and introduced the notion of probability of negativity to alleviate the effect of multiple users in authentication and further introduce a simple fusion scheme with the existing authentication methods to increase the intruder detection accuracy.

A major limitation of physiological modalities relates to the inability to authenticate the user continuously, when the information that the system is created to monitor, is not provided. On the other hand, due to the sporadic nature of human behavior, it currently seems impossible to solely rely on a behavioral system. Hence, an additional form of authentication is required to robustly handle different scenarios. Another important aspect is that a fair comparison between current works is not possible, due to the use of private datasets and nonuniform performance measures. Therefore, it would be of great interest to use established standards, that we proceed to enlist below.

4.5. Standards for mobile biometrics

Similar to traditional biometrics, towards the evaluation of the performance of a mobile biometric system, various types of standards have been defined. They are enlisted below.

Biometric Authentication: The performance evaluation of the biometric authentication on mobile devices is quantified in terms of the verification. However, the performance metrics for mobile devices are similar to that of the conventional biometrics systems. The recommended metrics following ISO/IEC 19795-1:2006 [15] include the False Acceptance Rate (FAR) and False Reject Rate (FRR). The ISO/IEC 19795-1:2006 [15] also provides the guidelines on evaluation protocols, data collection procedures, plotting of Receiver Operating Characteristics curve (ROC) and Detection Error Trade off (DET) curves. It is to be noted that, the performance reporting in terms of Equal Error Rate is not recommend following ISO/IEC 19795-1:2006 [15].

Presentation Attack Detection: To evaluate the presentation attack detection algorithms on the mobile environments, the ISO/IEC 30107-3 [40] has recommended two important metrics namely: Bona fide Presentation Classification Error Rate (BPCER) and Attack Presentation Classification Error Rate (APCER). BPCER is defined as proportion of bona fide presentations incorrectly classified as attacks while APCER is defined as proportion of attack presentations incorrectly classified as bona-fide presentations. In addition one can also report the performance of the proposed method by reporting the value of BPCER while fixing the APCER to 5% and 10% corresponding to recommendations from IS0/IEC 30107-3 [40].

Vulnerability of the biometric system: Following the ISO/IEC 30107-3 [40], the vulnerability (or attack success rate) of the biometrics systems under attacks can be quantified using the metric - Impostor Attack Presentation Match

Rate (IAPMR) which is defined as the proportion of impostor attack presentations using the same Attack Instrument species (morphed or averaged) in which the target reference is matched in a full-system evaluation of a verification system. For extended analysis on quantifying vulnerability on both academic and commercial biometric systems please refer to [65].

5. Open research problems

Deviating from above described research areas, there are a number of novel aspects, which we proceed to identify. We envision that the addressing of such open research problems would advance the field socially, economically and technologically. We identify below three such open research problems.

5.1. Novel sensors and modalities

As mentioned above, the performance of a biometric system is among others a function of the acquisition technology. Hence, exploring new sensor technology, as well as analyzing cross-sensor authentication will certainly push the performance accuracy.

Exploring the viability of novel modalities for mobile biometric will also be beneficial. For example in Munalih and Ardianto [51] finger vein recognition was one of the promising new modalities. In the commercial sector, Hitachi and Fujitsu actively research finger vein technologies. Recently, they have created a small and thin finger vein scanner for mobile devices. With the invention of the compact finger vein scanner, smart devices embedded with finger vein technology will soon be available on the market [9].

5.2. Novel applications

Since mobile phones are ubiquitous, novel applications are being proposed in the context of mobile biometrics [59], encryption and decryption of digital fingerprint are explored as digital signature. One application of high impact, benefiting from mobile biometrics relates to *health monitoring*. Herein physiological signal measurement using mobile devices is a field with recent rapid development. One of the important applications is heart rate (HR) estimation, which reflects the physical and emotional activities, e.g., exercise, emotion changes, illness, etc. The advantage of performing HR estimation using mobile devices is that it reduces the dependency to medical equipment, and thus improves the convenience to the users. However, robust HR on mobile devices is non-trivial because of the limited sensors in many of the mobile devices; in particular, not all the mobile devices have a photo plethysmography sensor and not all the scenarios are contact based. In this situation, it is required to perform physiological measurement such as HR measurement remotely (without contact) based on the commonly available visible light image sensor on mobile devices [53, 54]. The unconstrained illumination condition, pose variations, and low PSNR of the physiological signal captured by the visible light sensor pose great challenges to the measurement task. The literature of this area of research is not vast and there are many open research problem. Therefore, we expect it to be one of the directions for future research pertaining to mobile biometrics.

5.3. Novel privacy challenges

Storing biometric data on mobile devices raises additional challenges such as the protection of personal sensitive data / template protection. While the data should be protected from being stolen, the recovering of biometric information from the stolen data or linking the template to a person must be prevented. These concepts are referred to as *irreversibility* and *unlinkability*. Currently, template protection has received limited attention in the mobile biometrics literature. To this extent, in [66], Stokkenes et al. proposed a method for securing multiple biometric templates on smartphones, applying the concepts of Bloom filters along with binarized statistical image features descriptor. Obtained results indicate the robustness of the proposed system to preserve user privacy, while not compromising the inherent authentication accuracy without protected templates. On the other hand, template protection in classical biometrics has witnessed numerous works mainly based on four approaches: cancelable biometrics, BioHashing, Biometric Cryptosystems, and two-way partially homomorphic encryption, which can be easily adopted in the context of mobile biometrics. In addition to the above, the evaluation and analysis of modalities and relating technologies on larger scale are necessary to establish the scalability of mobile biometrics in real-life scenarios.

6. Conclusions

This article reviews biometric literature for mobile devices and suggests that research in mobile biometrics is on the rise. This is due to the recent commercial prevalence of mobile biometrics. In this article, we reviewed some of the recent methods, showing that face, fingerprint, and iris, are quite successfully deployed on mobile devices and largely accepted by the public. We discussed the benefits, limitations, as well as challenges with respect to biometric acquisition, processing, and biometric data storage and protection. Finally, we elaborated on some of the open research problems in the field.

Acknowledgement

A. Das was supported by the research program FER4HM funded by Inria and CAS. C. Galdi and J.-L. Dugelay were supported by the EU Horizon 2020 research and innovation programme under grant agreement No. 700259. H. Han was supported by the External Cooperation Program of CAS (grant GJHZ1843). R. Raghavendra was supported by the Research Council of Norway under Grant No. IKTPLUSS 248030/070. A. Dantcheva was supported by the French Government (National Research Agency, ANR) under grant agreement ANR-17-CE39-0002.

References

[1] https://computervisiononline.com/dataset/1105138686.

[2] https://fieldguide.gizmodo.com/what-do-the-ai-chips-in-new-smartphones-actually-do-1820913665.

[3] https://press.trendforce.com/press/20180213-3067.html.

[4] https://www.apple.com/apple-pay/.

[5] https://www.apple.com/lae/iphone-x/specs/.

[6] https://www.bayometric.com/biometrics-improve-customer-service-online-banking/.

[7] https://www.biometricupdate.com/biometric-news/mobile-biometric-news.

[8] https://www.gsmarena.com/.

[9] https://www.pcworld.idg.com.au/article/562256/hitachi-finger-vein-scanner-could-secure-large-venues/.

[10] https://www.qualcomm.com/invention/research/projects/deep-learning.

[11] https://www.qualcomm.com/products/qualcomm-vision-intelligence-platform.

[12] https://www.statista.com/chart/11122/the-future-of-mobile-biometrics.

[13] https://www.youtube.com/watch?v=lgrrynqhegc.

[14] http://www.vivo.com/en/about-vivo/news/vivo-showcases-pioneering-tof-3d-sensing-technology-mwc-shanghai-2018.

[15] ISO/IEC 19795-1:2006 - Information technology – Biometric performance testing and reporting – Part 1: Principles and framework. Technical report, Mar. 2006.

[16] A. F. Abate, S. Barra, L. Gallo, and F. Narducci. Kurtosis and skewness at pixel level as input for som networks to iris recognition on mobile devices. *Pattern Recognition Letters*, 91:37–43, 2017.

[17] N. U. Ahmed, S. Cvetkovic, E. H. Siddiqi, A. Nikiforov, and I. Nikiforov. Combining iris and periocular biometric for matching visible spectrum eye images. *Pattern Recognition Letters*, 91:11 – 16, 2017. Mobile Iris CHallenge Evaluation (MICHE-II).

[18] K. Ahuja, R. Islam, F. A. Barbhuiya, and K. Dey. Convolutional neural networks for ocular smartphone-based biometrics. *Pattern Recognition Letters*, 91:17 – 26, 2017. Mobile Iris CHallenge Evaluation (MICHE-II).

[19] F. Alonso-Fernandez, K. B. Raja, C. Busch, and J. Bigun. Log-likelihood score level fusion for improved cross-sensor smartphone periocular recognition. In *2017 25th European Signal Processing Conference (EUSIPCO)*, pages 271–275, Aug 2017.

[20] N. Amjed, F. Khalid, R. W. O. Rahmat, and H. B. Madzin. Noncircular iris segmentation based on weighted adaptive hough transform using smartphone database. *Journal of Computational and Theoretical Nanoscience*, 15(3):739–743, 2018.

[21] G. Baldini and G. Steri. A survey of techniques for the identification of mobile phones using the physical fingerprints of the built-in components. *IEEE Communications Surveys Tutorials*, 19(3):1761–1789, thirdquarter 2017.

[22] S. Barra, M. De Marsico, M. Nappi, F. Narducci, and D. Riccio. A hand-based biometric system in visible light for mobile environments. *Information Sciences*, 2018.

[23] Z. Boulkenafet, J. Komulainen, Z. Akhtar, A. Benlamoudi, D. Samai, S. E. Bekhouche, A. Ouafi, F. Dornaika, A. Taleb-Ahmed, L. Qin, et al. A competition on generalized software-based face presentation attack detection in mobile scenarios. In *Biometrics (IJCB), 2017 IEEE International Joint Conference on*, pages 688–696. IEEE, 2017.

[24] Z. Boulkenafet, J. Komulainen, L. Li, X. Feng, and A. Hadid. Oulu-npu: A mobile face presentation attack database with real-world variations. In *2017 12th IEEE International Conference on Automatic Face Gesture Recognition (FG 2017)*, pages 612–618, May 2017.

[25] C. Burt. Smartphone growth to slow in 2018 as mobile biometrics mostly stay the course, trendforce predicts, https://www.biometricupdate.com/201802/smartphone-growth-to-slow-in-2018-as-mobile-biometrics-mostly-stay-the-course-trendforce-predicts, Feb 2018.

[26] M. Castrillón-Santana, M. De Marsico, M. Nappi, F. Narducci, and H. Proença. Mobile iris challenge evaluation ii: results from the icpr competition. In *Pattern Recognition (ICPR), 2016 23rd International Conference on*, pages 149–154. IEEE, 2016.

[27] D. Crouse, H. Han, D. Chandra, B. Barbello, and A. K. Jain. Continuous authentication of mobile user: Fusion of face image and inertial measurement unit data. In *2015 International Conference on Biometrics (ICB)*, pages 135–142, May 2015.

[28] P. Fernandez-Lopez, J. Sanchez-Casanova, P. Tirado-Martín, and J. Liu-Jimenez. Optimizing resources on smartphone gait recognition. In *2017 IEEE International Joint Conference on Biometrics (IJCB)*, pages 31–36, Oct 2017.

[29] J. Fierrez, A. Pozo, M. Martinez-Diaz, J. Galbally, and A. Morales. Benchmarking touchscreen biometrics for mobile authentication. *IEEE Transactions on Information Forensics and Security*, 13(11):2720–2733, Nov 2018.

[30] R. D. Findling, M. Holzl, and R. Mayrhofer. Mobile match-on-card authentication using offline-simplified models with gait and face biometrics. *IEEE Transactions on Mobile Computing*, pages 1–1, 2018.

[31] R. D. Findling and R. Mayrhofer. Towards secure personal device unlock using stereo camera pan shots. In *International Conference on Computer Aided Systems Theory*, pages 417–425. Springer, 2013.

[32] M. Frucci, C. Galdi, M. Nappi, D. Riccio, and G. Sanniti di Baja. Idem: Iris detection on mobile devices. In *Pattern Recognition (ICPR), 2014 22nd International Conference on*, pages 1752–1757. IEEE, 2014.

[33] M. Gadaleta and M. Rossi. Idnet: Smartphone-based gait recognition with convolutional neural networks. *Pattern Recognition*, 74:25 – 37, 2018.

[34] C. Galdi and J.-L. Dugelay. Fire: Fast iris recognition on mobile phones by combining colour and texture features. *Pattern Recognition Letters*, 91:44 – 51, 2017. Mobile Iris CHallenge Evaluation (MICHE-II).

[35] C. Galdi, M. Nappi, J.-L. Dugelay, and Y. Yu. Exploring new authentication protocols for sensitive data protection on smartphones. *IEEE Communications Magazine*, 56(1):136–142, Jan 2018.

[36] M. I. Gofman, S. Mitra, and N. Smith. Hidden markov models for feature-level fusion of biometrics on mobile devices. In *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*, pages 1–2, Nov 2016.

[37] A. Goode. Bring your own finger how mobile is bringing biometrics to consumers. *Biometric Technology Today*, 2014(5):5 – 9, 2014.

[38] M. Günther, A. Costa-Pazo, C. Ding, E. Boutellaa, G. Chiachia, H. Zhang, M. de Assis Angeloni, V. Štruc, E. Khoury, E. Vazquez-Fernandez, et al. The 2013 face recognition evaluation in mobile environment. In *Biometrics (ICB), 2013 International Conference on*, pages 1–7. IEEE, 2013.

[39] A. G. Howard, M. Zhu, B. Chen, D. Kalenichenko, W. Wang, T. Weyand, M. Andreetto, and H. Adam. Mobilenets: Efficient convolutional neural networks for mobile vision applications. *arXiv preprint arXiv:1704.04861*, 2017.

[40] ISO/IEC 30107-3:2017 Information technology – Biometric presentation attack detection – Part 3: Testing and reporting. Standard, International Organization for Standardization, Sept. 2017.

[41] E. Khoury, B. Vesnicer, J. Franco-Pedroso, R. Violato, Z. Boulkcnafet, L. M. Fernández, M. Diez, J. Kosmala, H. Khemiri, T. Cipr, et al. The 2013 speaker recognition evaluation in mobile environment. In *Biometrics (ICB), 2013 International Conference on*, pages 1–8. IEEE, 2013.

[42] G. Li and P. Bours. A novel mobilephone application authentication approach based on accelerometer and gyroscope data. In *2018 International Conference of the Biometrics Special Interest Group (BIOSIG)*, 2018.

[43] U. Mahbub and R. Chellappa. Path: person authentication using trace histories. In *Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), IEEE Annual*, pages 1–8. IEEE, 2016.

[44] S. Marcel, C. McCool, P. Matějka, T. Ahonen, J. Černockỳ, S. Chakraborty, V. Balasubramanian, S. Panchanathan, C. H. Chan, J. Kittler, et al. On the results of the first mobile biometry (mobio) face and speaker verification evaluation. In *Recognizing Patterns in Signals, Speech, Images and Videos*, pages 210–225. Springer, 2010.

[45] M. De Marsico, M. Nappi, F. Narducci, and H. Proença. Insights into the results of miche i - mobile iris challenge evaluation. *Pattern Recognition*, 74:286 – 304, 2018.

[46] M. De Marsico, M. Nappi, and H. Proença. Results from miche ii mobile iris challenge evaluation ii. *Pattern Recognition Letters*, 91:3 – 10, 2017. Mobile Iris CHallenge Evaluation (MICHE-II).

[47] W. Meng, D. S. Wong, S. Furnell, and J. Zhou. Surveying the development of biometric user authentication on mobile phones. *IEEE Communications Surveys & Tutorials*, 17(3):1268–1293.

[48] J. Moar. Juniper research: https://www.juniperresearch.com/.

[49] M. Muaaz and R. Mayrhofer. Smartphone-based gait recognition: From authentication to imitation. *IEEE Transactions on Mobile Computing*, 16(11):3209–3221, Nov 2017.

[50] M. Muaaz and R. Mayrhofer. Smartphone-based gait recognition: from authentication to imitation. *IEEE Transactions on Mobile Computing*, 16(11):3209–3221, 2017.

[51] A. Munalih and W. Ardianto. *Finger vein biometrics: The future for a mobile authentication system*. 2017. cited By 0.

[52] T. J. Neal and D. L. Woodard. Surveying biometric authentication for mobile device security. *Journal of Pattern Recognition Research*, 1:74–110, 2016.

[53] X. Niu, H. Han, S. Shan, and X. Chen. Continuous heart rate measurement from face: A robust rppg approach with distribution learning. In *IEEE IJCB*, pages 642–650, Oct. 2017.

[54] X. Niu, H. Han, S. Shan, and X. Chen. Synrhythm: Learning a deep heart rate estimator from general to specific. In *ICPR*, Aug. 2018.

[55] J. Olivares-Mercado, K. Toscano-Medina, G. Sanchez-Perez, H. Perez-Meana, and M. Nakano-Miyatake. Face recognition system for smartphone based on lbp. In *2017 5th International Workshop on Biometrics and Forensics (IWBF)*, pages 1–6, April 2017.

[56] K. Patel, H. Han, and A. K. Jain. Secure face unlock: Spoof detection on smartphones. *IEEE Transactions on Information Forensics and Security*, 11(10):2268–2283, Oct. 2016.

[57] P. Perera and V. M. Patel. Efficient and low latency detection of intruders in mobile active authentication. *IEEE Transactions on Information Forensics and Security*, 13(6):1392–1405, 2018.

[58] P. Perera and V. M. Patel. Efficient and low latency detection of intruders in mobile active authentication. *IEEE Transactions on Information Forensics and Security*, 13(6):1392–1405, June 2018.

[59] E. Rahmawati, M. Listyasari, A. S. Aziz, S. Sukaridhoto, F. A. Damastuti, M. M. Bachtiar, and A. Sudarsono. Digital signature on file using biometric fingerprint with fingerprint sensor on smartphone. In *2017 International Electronics Symposium on Engineering Technology and Applications (IES-ETA)*, pages 234–238, Sept 2017.

[60] K. B. Raja, R. Raghavendra, V. K. Vemuri, and C. Busch. Smartphone based visible iris recognition using deep sparse filtering. *Pattern Recognition Letters*, 57:33–42, 2015.

[61] K. B. Raja, P. Wasnik, R. Raghavendra, and C. Busch. Robust face presentation attack detection on smartphones : An approach based on variable focus. In *2017 IEEE International Joint Conference on Biometrics (IJCB)*, pages 651–658, Oct 2017.

[62] A. Rattani and R. Derakhshani. Online co-training in mobile ocular biometric recognition. In *2017 IEEE International Symposium on Technologies for Homeland Security (HST)*, pages 1–5, April 2017.

[63] A. Rattani, R. Derakhshani, S. K. Saripalle, and V. Gottemukkula. Icip 2016 competition on mobile ocular biometric recognition. In *Image Processing (ICIP), 2016 IEEE International Conference on*, pages 320–324. IEEE, 2016.

[64] N. Reddy, A. Rattani, and R. Derakhshani. A robust scheme for iris segmentation in mobile environment. 2016. cited By 1.

[65] U. Scherhag, A. Nautsch, C. Rathgeb, M. Gomez-Barrero, R. N. J. Veldhuis, L. Spreeuwers, M. Schils, D. Maltoni,

P. Grother, S. Marcel, R. Breithaupt, R. Ramachandra, and C. Busch. Biometric systems under morphing attacks: Assessment of morphing techniques and vulnerability reporting. In *2017 International Conference of the Biometrics Special Interest Group (BIOSIG)*, pages 1–7, Sept 2017.

[66] M. Stokkenes, R. Ramachandra, K. B. Raja, M. Sigaard, M. Gomez-Barrero, and C. Busch. Multi-biometric template protection on smartphones: An approach based on binarized statistical features and bloom filters. In C. Beltrán-Castañón, I. Nyström, and F. Famili, editors, *Progress in Pattern Recognition, Image Analysis, Computer Vision, and Applications*, pages 385–392, Cham, 2017. Springer International Publishing.

[67] L. Sun, Y. Wang, B. Cao, P. S. Yu, W. Srisa-an, and A. D. Leow. Sequential keystroke behavioral biometrics for mobile user identification via multi-view deep learning. In Y. Altun, K. Das, T. Mielikäinen, D. Malerba, J. Stefanowski, J. Read, M. Žitnik, M. Ceci, and S. Džeroski, editors, *Machine Learning and Knowledge Discovery in Databases*, pages 228–240, Cham, 2017. Springer International Publishing.

[68] R. Tan and M. Perkowski. Toward improving electrocardiogram (ecg) biometric verification using mobile sensors: A two-stage classifier approach. *Sensors*, 17(2):410, 2017.

[69] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, A. Morales, and J. Ortega-Garcia. Benchmarking desktop and mobile handwriting across cots devices: The e-biosign biometric database. *PLOS ONE*, 12(5):1–17, 05 2017.

[70] A. Ungureanu, S. Thavalengal, T. E. Cognard, C. Costache, and P. Corcoran. Unconstrained palmprint as a smartphone biometric. *IEEE Transactions on Consumer Electronics*, 63(3):334–342, August 2017.

[71] R. Vera-Rodriguez, R. Tolosana, J. Ortega-Garcia, and J. Fierrez. E-biosign: stylus-and finger-input multi-device database for dynamic signature recognition. In *IWBF*, pages 1–6, 2015.

[72] P. Wasnik, K. B. Raja, R. Ramachandra, and C. Busch. Assessing face image quality for smartphone based face recognition system. In *2017 5th International Workshop on Biometrics and Forensics (IWBF)*, pages 1–6, April 2017.

[73] P. Wasnik, K. Schafer, R. Ramachandra, C. Busch, and K. Raja. Fusing biometric scores using subjective logic for gait recognition on smartphone. In *2017 International Conference of the Biometrics Special Interest Group (BIOSIG)*, pages 1–5, Sept 2017.

[74] D. Wen, H. Han, and A. K. Jain. Face spoof detection with image distortion analysis. *IEEE Transactions on Information Forensics and Security*, 10(4):746–761, Apr. 2015.

[75] A. Wojciechowska, M. Choraś, and R. Kozik. The overview of trends and challenges in mobile biometrics. *Journal of Applied Mathematics and Computational Mechanics*, 16, 2017.

[76] M. Zhang, Q. Zhang, Z. Sun, S. Zhou, and N. U. Ahmed. The btas competition on mobile iris recognition. In *Biometrics Theory, Applications and Systems (BTAS), 2016 IEEE 8th International Conference on*, pages 1–7. IEEE, 2016.

[77] Q. Zhang, H. Li, Z. Sun, Z. He, and T. Tan. Exploring complementary features for iris recognition on mobile devices. In *Biometrics (ICB), 2016 International Conference on*, pages 1–8. IEEE, 2016.

[78] Q. Zhang, H. Li, Z. Sun, and T. Tan. Deep feature fusion for iris and periocular biometrics on mobile devices. *IEEE Transactions on Information Forensics and Security*, 13(11):2897–2912, Nov 2018.