Biometric Systems Interaction Assessment: The State of the Art

Article *in* IEEE Transactions on Human-Machine Systems · June 2019

DOI: 10.1109/THMS.2019.2913672

CITATIONS
0

READS
35

7 authors, including:

R. Blanco-Gonzalo
University Carlos III de Madrid
30 PUBLICATIONS **140** CITATIONS
SEE PROFILE

Oscar Miguel-Hurtado
University of Kent
38 PUBLICATIONS **260** CITATIONS
SEE PROFILE

Chiara Lunerti
University of Kent
10 PUBLICATIONS **11** CITATIONS
SEE PROFILE

Richard Guest
University of Kent
128 PUBLICATIONS **588** CITATIONS
SEE PROFILE

Biometric Systems Interaction Assessment: The State of the Art

Ramon Blanco-Gonzalo, Oscar Miguel-Hurtado, Chiara Lunerti, Richard M. Guest, Barbara Corsetti, Elakkiya Ellavarason, and Raul Sanchez-Reillo

***Abstract*—The design and implementation of effective and efficient biometric systems presents a series of challenges to information technology (IT) designers to ensure robust performance. One of the most important factors across biometric systems, aside from algorithmic matching ability, is the human interaction influence on performance. Changes in biometric system paradigms have motivated further testing methods, especially within mobile environments, where the interaction with the device has fewer environmental constraints, which may severely affect system performance. Testing methods involve the need for reflecting on the influence of user-system interaction on the overall system performance in order to provide information for design and testing. This paper reflects on the state of the art of biometric systems interaction assessment, leading to a comprehensive document of the relevant research and standards in this area. Furthermore, the current challenges are discussed and thus we provide a roadmap for the future of biometrics systems interaction research.**

***Index Terms*—Accessibility, biometrics, human-computer interaction (HCI), usability.**

I. Introduction

BIOMETRICS is the study of human authentication by their physical and/or behavioral characteristics. The deployment and everyday usage of computer-based biometric authentication systems (e.g., based on fingerprints, face, or iris features) has substantially increased over recent years.

Nowadays, biometric recognition is widespread in banking [1], in automated border control (ABC) systems [2], in home automation systems and authentication on mobile devices. Since more and more people are using biometric applications on a daily basis, it had become appropriate to study biometric systems from a human-computer interaction (HCI) perspective. This means studying how people react to this new technology and understanding which interaction factors may influence the relationship between user and biometric devices and systems.

Moreover, novel biometric scenarios and devices have also introduced a range of new issues that require a re-engineering of conventional methods of implementation, for example, with new or tailored authentication algorithms with specific devices, sensors, and modalities. Besides conventional biometric modalities, such as fingerprint, face, or iris, the number of reliable alternative modalities has increased (e.g., gait recognition [3] or knuckle recognition [4]) and many others are under consideration (e.g., forehead recognition [5] or facial sketches [6]).

Many of the above-mentioned innovations have been motivated by the use of biometrics within mobile platforms. The requirement to protect access to mobile devices has grown with the ubiquity that smartphones, tablets, and laptops have in our daily lives, in particular, the storage of sensitive data, such as contacts, emails, and calendars, or making bank transfers and purchases over the Internet. The inherent mobility of these devices, along with their ever-growing capabilities, render them the ideal multipurpose computing device, but make it easy for them to become lost or stolen. Recently, biometrics has been increasingly used ahead of PIN and password for protecting the access to smartphones. Biometric systems prevent users from having to remember passwords and also provide safety against attacks, such as shoulder surfing [7].

The adoption of biometrics in mobile platforms has also been driven by presence of capture sensors embedded on the device itself [8], helping to reduce the cost of the authentication system deployment. Every mobile device has a microphone to make phone calls, and this can be used for voice recognition. The majority of devices also contain a camera and a touchscreen that can be used for face and signature verification, respectively. Recently, mobile devices have incorporated specific fingerprint and iris sensors allowing the use of fingerprint and iris verification.

As new usage scenarios and, indeed, biometric modalities evolve, the interaction between the user and the biometric sensor is potentially modified leading to a possible effect on the performance of the entire system. Traditionally, algorithms have been the main factor claimed to affect performance rates, but many other factors also influence successful outcome, such as the environment, biometric sensor quality, and characteristics changes, within the biometric sample and the user-system interaction [9], [10].

Manuscript received July 9, 2018; revised January 31, 2019; accepted April 1, 2019. This work was supported by the European Union's Horizon 2020 Research and Innovation Programme under the Marie Sklodowska-Curie grant agreement No 675087 ("AMBER"). This paper was recommended by Associate Editor F. Scotti. *(Corresponding author: Ramon Blanco-Gonzalo.)*

R. Blanco-Gonzalo, B. Corsetti, and R. Sanchez-Reillo are with the Department of Electronic Technology, University Carlos III of Madrid, 28911 Madrid, Spain (e-mail: rbgonzal@ing.uc3m.es; bcorsett@ing.uc3m.es; rsreillo@ing.uc3m.es).

O. Miguel-Hurtado is with the Callsign, EC2V 6ET London, U.K. (e-mail: oscar.miguel@callsign.com).

C. Lunerti, R. M. Guest, and E. Ellavarason are with the School of Engineering and Digital Arts, University of Kent, CT2 7NT Canterbury, U.K. (e-mail: c.lunerti@kent.ac.uk; r.m.guest@kent.ac.uk; e.ellavarason@kent.ac.uk).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/THMS.2019.2913672

This review highlights the most relevant works related to user interaction on biometrics systems performance as one of the major influences of performance. This encompasses several factors, such as ergonomics, user acceptance, and efficiency. Poor user-system interactions usually negatively affect the whole system performance and furthermore might lead to users' rejection of the technology. It is therefore necessary to overcome these concerns by means of good practices in design and biometric implementations testing. In reviewing this area, we do not focus explicitly on HCI design considerations. Our review is instead focused on the analysis of the influence of the user-sensor interaction on the system performance. We do, however, acknowledge that HCI design and sensor interaction are intrinsically linked and, as such be approached in parallel.

In Section II, a historical review of previous work on the analysis of the interaction between users and biometric systems is provided. In Section III, we focus on how the recent introduction of biometrics authentication capabilities into mobile devices has brought a new range of challenges for implementation, while in Section IV we review the various national and international standards that exist within the area of biometrics and usability. Finally, in Section V, we discuss the current and future challenges for research and development in this field.

II. Historical Review

Several studies in HCI in biometrics were made by the U.S. National Institute of Standards and Technology (NIST) following the publication of ISO 9241-11:1998 "Ergonomic requirements for office work with visual display terminals (VDTs)—Part 11: Guidance on usability" [11]. ISO 9241-11:1998 explains how to identify the information necessary to consider when specifying or evaluating usability in terms of measures of user performance and satisfaction. Guidance is given on how to describe the context of use of a product and the measures of usability in an explicit way. This standard introduces the terms efficiency, effectiveness, and satisfaction as metrics of usability and consequently most subsequent research in user-biometric systems interaction uses these definitions. These three terms have usually been applied to measure the biometric systems' usability and are defined by ISO 9241-11:1998 as follows.

1) Effectiveness: "The accuracy and completeness with which specified users can achieve specified goals in particular environments."
2) Efficiency: "The resources expended in relation to the accuracy and completeness of goals achieved."
3) Satisfaction: "The comfort and acceptability of the work system to its users and other people affected by its use."

Even if these metrics are standardized, the way they are calculated could be flexible depending on the tasks and on the biometric system being evaluated.

In this section, the most important works in user-biometric system interaction are explored. First, by individual modalities: Fingerprint, face, handwritten signature, and then by multimodal assessment. Furthermore, we analyze studies on other aspects of the user interaction with biometric systems: Accessibility and user acceptance. Finally, we explore the use of frameworks to evaluate the users influence in biometric system performance.

A. Fingerprint Interaction

The first interaction experiments in biometrics were made with fingerprint recognition. As fingerprint was the first widely deployed modality, this was subject to early interaction concerns. The rationale behind these studies was to investigate the users' acceptance and perception on biometric recognition systems. For instance, in [12], Heckle *et al* asked 24 participants to make online payment presenting their fingerprint along with their personal data and their credit cards. At the end of the experiment, the 88% of the users rated fingerprints recognition very beneficial and the 46% of them found it comfortable in this context of use. Regarding their preference in terms of security, just the 35% of participants said that using biometric recognition increases the security. Authors argue that this lack of trust may depend on still poor understanding of biometric systems.

Moreover, since the appearance of fingerprint recognition in airports and access control (especially after 2006 with the appearance of the ePassport) the concept of "usability" ("The extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use") [11] arouse. Systems were required not only to reduce delays in recognition (leading, for example, to long queues in airports), but also make the user feel confident using fingerprint and therefore, potentially boost subsequent performance. As a result, the NIST Visualization and Usability Group [13] started working in this field in 2005.

In 2006 [14], NIST conducted a study to determine the influence of external factors, such as gender, age, and presence of feedback on the image quality of fingerprints, as well as the effect that habituation has on the user's interaction. In this study, participants were asked to provide their fingerprints twice a day, but in the first phase of the experiment, they were not allowed to view the sample images and were not given any kind of feedback from the system. In the second phase, they received indications from the operator through the user interface and real-time feedback as to fingerprint sample quality provided. With this information, the participants decided which sample to store (they were encouraged to provide a sample with a quality score—NFIQ—of 3 or higher). Outcomes from this study showed that younger participants provided higher quality prints than older participants, both in male and female subjects. Women submitted on average 20% poorer quality fingerprint images than men. Habituation with no feedback caused no effect in the quality of the images. On the contrary, when the feedback was provided in the second phase, there were habituation improvements that resulted in a higher quality of the fingerprints presented and in fewer attempts.

Further studies on fingerprint and interaction focused on ergonomics: Feedback is highly important, but also users' comfort when using biometrics. Effective ergonomic systems lead to higher user's satisfaction and better biometric samples. In 2007 [15], NIST analyzed anthropometric and ergonomic factors of biometric deployments, specifically to assess the influence of the surface height of the sensor on the quality and the acquisition time of fingerprint images. Seventy-five NIST employees took part in this study. Each participant donated five fingerprint images at four different scanner standard heights:

26 in (work table height), 32 in (desk height), 36 in (counter height), and 42 in (standing counter height). Efficiency, effectiveness, and user satisfaction assessed following donation. The results showed that the time to complete the tasks as well as the quality of the print images was affected by the work surface height, in particular for the thumbs. At 26 in, it was possible to collect the images with the highest quality and 36 in provided the fastest acquisition time. Participants preferred 32 or 36 in work surface height, while they found a 42-in height uncomfortable for use.

A further study in 2008 [16], considered fingerprint images collected from four different scanner angles (0°, 10°, 20°, and 30°), given the same scanner heights from the previous experiment [12]. This study aimed to find the optimum angle to position the fingerprint scanner in terms of efficiency, effectiveness, and satisfaction. Results revealed that different angles did not affect the transaction time (efficiency) and the quality of the fingerprint images (effectiveness); however, the angle of the scanner can be adjusted to improve the user satisfaction.

Having performed several laboratory-environment experiments, NIST assessed fingerprint system interaction in operational environments. One of the first attempts was a usability study to assess the fingerprint capture of 10-print image in an airport scenario, analyzing the impact of the type of instructional information provided to users (poster, video, and verbal) on the efficiency, effectiveness, and user's satisfaction [17]. Efficiency was measured as the time required to complete the 10-print scan, the effectiveness as the number of participants who were unable to complete the task, and the number of errors incurred by those who successfully completed the task. Finally, satisfaction was measured with a survey after completing the test. Three hundred participants took part in the experiment receiving instruction in three different formats: poster, verbal instruction, and soundless video. Only 56% of the participants that received instruction by poster were able to complete the task successfully. Poster information resulted to be least efficient and effective, while verbal and video instruction performed equally well. The minimum time required to capture a 10-print sequence was approximately 30 s. Without an operator to give assistance, the process took on average from 48 to 64 s, and only 78% of the users completed the task successfully, compared to 98% and average time from 50 to 54 s when assistance was provided.

Building on these studies, other research groups have carried out interaction experiments using fingerprint recognition in operational environments. In 2010, Fernandez-Saavedra *et al*. performed a usability evaluation of commercial solutions of fingerprint access control [18]. Along with the event logs and matching results, the user's interactions were video recorded with two cameras (upper view and semi-lateral view). The users' feedback was collected via interviews. Within this study, effectiveness, users' satisfaction, false reject rate (FRR), and false accept rate (FAR) were analyzed. The results indicate that the time spent and the number of errors are higher in the scenarios, where users must place the fingerprint scanners at a different height as the recommended by suppliers (70–75 cm in desk devices).

In 2006, Kukula *et al*. analyzed the ergonomic principles of a biometric system in order to examine issues related to fingerprint acquisition [19]. Users interacted with swipe fingerprint sensors and an interface which provided different messages as feedback (e.g., "move right" or "move left"). The results showed that the thumb, pointer/index, and middle fingers had fewer acquisition problems in comparison with the ring and little fingers of both hands due to lesser finger dexterity of the lateral fingers.

In 2010, Kukula *et al*. validated the human biometric sensor interaction (HBSI) model (see Section II-D) by means of an evaluation of three swipe fingerprint sensors [20]. The authors analyzed the failure to acquire (FTA) (14.38% overall), with FTD accounting for 30.71% of the overall FTA rate. They concluded that users cannot always successfully interact with a swipe fingerprint biometric device, yet algorithm developers believe that there are few problems or issues with their device or algorithm, which is indeed a serious concern for biometric recognition.

Further studies [21]–[23] carried out by NIST aimed to test the usability of five different contactless fingerprint devices, using a contact-based fingerprint device as the baseline. Participants were required to use the devices three times: The first time without instructions, the second, receiving verbal instruction, and the third, watching a video. Efficiency was measured as the time required for completing the tasks, effectiveness by task success, and the quality of captured fingerprints. Finally, satisfaction was measured through participants' opinion about the easiness and the intuitiveness of the devices. In the second and third studies, participants rated the contactless devices as easier and faster to use. Conversely, in the first study, participants rated the contact device as the easier to use and the most intuitive. The authors argue that this fact is motivated by the lack of intuitiveness of the contactless device used. Thus, NIST highlighted the necessity of educating people to properly use contactless scanners.

B. Face System Interaction

An image of the travelers' face is a common characteristic that all passports across the globe contain. With the introduction of e-passports in 2006, facial verification in border control scenarios became commonplace. This was followed by a number of large-scale facial user interaction studies.

In 2008, NIST made a usability evaluation of a facial biometric system, which included an initial inspection of the operational settings in use to identify interaction components and the most common user interaction mistakes [24]. Based on this, NIST designed a usability experiment to determine if addressing human factors for face image capture could improve the overall image quality without introducing additional tasks to the operator. Based on the common user interaction issues, the NIST usability team analyzed whether improving the face image capture station layout would better assist both the operator and the , resulting in better quality face images captured. Three hundred participants joined the experiment. The results clearly showed an overall improvement on the quality of the images based on 20 image quality attributes.

Further facial usability experimentation evaluated how the use of a face overlay could improve the quality of the captured face images [25]. Several usability factors were analyzed in this work: effectiveness (quality of the captured images), efficiency (task time), user satisfaction, and affordance (a measure of the intuitiveness of the system). In order to analyze these factors, facial images were stored for offline quality assessment. About 53.2% of the images were perfectly centered and 45.4% were partially centered. The face overlay resulted in an easy to use system, with no impact on the efficiency of the capturing process and users expressed satisfaction in knowing whether the image was framed properly.

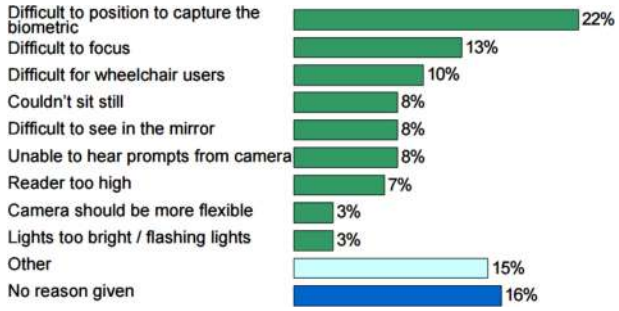

Fig. 1. Example of UKPS surveys results, where users were asked about their concerns when interacting with the iris recognition system [29].

C. Signature System Interaction

In recent years, handwritten signature recognition has been used increasingly, mostly due to growth in mobile devices: Signing documents is a common action and, in general, people feel comfortable donating a signature. New scenarios and devices have brought challenges to designers who have recently started to test interaction in these systems (further studies on handwritten signature have been made for mobile device implementations and are cited in Section III). Works in this area aim to improve ergonomics and produce the most appropriate feedback for users, therefore reducing FTA. One of the first specific works in this area is the integration of dynamic signature verification with the HBSI model [26] (see Section II-D). The authors revealed the complexity of the potential interactions according to the scenario (signing an important contract, in the supermarket, etc.). Another outcome of this work is a complete mapping of the HBSI presentation metrics for paper, ink, and virtual inking devices following their interaction flow charts.

Further experimentation in [27] aimed to assess the enrolment success rate and the user's preferences across three different signature input devices with different modes of feedback to the users. During the experiment, 42 users signed on two common signature capture devices, showing that users have different preferences among those devices (e.g., 93% of users preferred a device that they successfully enrolled on). This study also showed that right-handed users are more successful enrolling on all three of the sensors. Moreover, authors claim that usability issues regarding visual feedback or familiarity may negatively affect the biometric performance.

D. Testing More Than One Modality

One of the earliest studies conducted by NIST in this line [28] aimed to create a biometric database with the goal of collecting 10 000 comprehensive sets of biometric samples. For this purpose, a portable biometric workstation was developed consisting of nine digital cameras for capturing the image of the face from different angles, two different fingerprint scanners, and an iris scanner. To analyze the usability, NIST conducted an experiment to assess the time of each biometric capture and whether the interface facilitated the flow of the workstation. Eight NIST employees took part in the experiment acting as operators of three different scenarios, and they were asked to answer a questionnaire at the end of each session. The number of errors and time needed for each biometric capture decreased through the sessions, while satisfaction generally increased with the use.

The state of the art in biometric access control systems commonly contains multiple biometric modalities. An increase in user interaction with multiple biometrics in a single interaction has led to further research in this area.

Border controls/passports featuring biometric technology are widely deployed. In this context, the U.K. Passport Service Trial (UKPS) [29] in 2005 was the first major usability evaluation, gathering customer experience data when using fingerprint, face, and iris recognition systems. More than 10 000 users participated in this trial with 750 subjects exhibiting some kind of disability. The outcomes of the UKPS include effectiveness (enrolment and verification times), efficiency (enrolment and verification success rates), and satisfaction results in addition to several users' opinions and recommendations. Participants did not consider in general the level of intrusion as an issue, but the time taken of the overall experience was rated worse than expected. The analysis compared results among the three different sample groups: quota (2000 participants chosen to match the target population), opportunistic (7266 recruited from the area around and within the trial centers), disabled (750 pan-impairment participants), and demographic traits, such as age and gender. In general, fingerprint recognition was the preferred modality, but some groups felt more comfortable with iris recognition. Nevertheless, the disabled participant group found the iris recognition very challenging. An example of the surveys' results regarding difficulties found when interacting with iris recognition is in Fig. 1. This study also shows demographic (age and gender) difference for costumer perceptions and reactions.

Sasse in [30] reports the usability results from another ABC experiment: The BioPII study. Two thousand airport staff members were recruited for this project and asked to use four biometric systems (1 iris, 1 face, and 2 fingerprints recognition based implementation). Their task was to enroll themselves two times every day for two months. The users who respected this timing had lower error rates compared to participants who skipped donation days. This supports the fact that the user experience (UX) may affect the performance of the whole systems. Moreover, even if at the end of the trial, the users rated their experience with the systems positive and satisfying, several user interaction issues emerged. For example, the iris scan was often confused

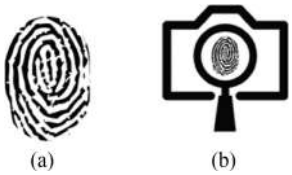

Fig. 2. NIST symbols for "Biometric in use" [31].

with a normal camera to which users have presented the whole face. The authors argue that in the future, a better interface design could eradicate all these issues.

E. User Acceptance in Biometrics

A key concept in user-biometric system interaction is the degree of trust that users put on the technology. Biometric recognition may sometimes be considered as intrusive, especially some modalities, such as iris recognition, where donation of samples maybe seen as unnatural or invasive. A lack of confidence may derive in biometrics misuses or the technology rejection. Thus, the topic of user acceptance has been deeply researched in biometric recognition. Traditionally, user acceptance was measured through surveys and interviews. One element of user interaction in which researchers have paid more attention is the feedback provided to users, typically consisting of symbols, images, or videos. The importance of understandable objective presentation and communication of use can be viewed for the following two reasons.

1) Biometric recognition is a novelty for many people who do not know how to use it.
2) In scenarios, such as airports, people from many different cultures (including different languages and habits) will use biometrics.

NIST has undertaken a comprehensive set of work with symbols in biometric systems. In one of their first studies [31], a set of symbol variants was proposed and evaluated in three phases by interviewing participants that had no background in biometrics. As a result, two symbol variants were considered, with the recommendation of using one when only fingerprint is in use [see Fig. 2(a)] and the other when further modalities are being used [see Fig. 2(b)].

Continuing the NIST work on biometrics symbols, in [32], they evaluated a set of symbols in six case studies with a total of 186 participants from United States and four Asian countries to consider also any cultural implications. The set included 20 individual symbols and 4 procedural symbols. Four of them caused confusion to all the participants from different cultures, indicating the need for an alternative design, while the remaining symbols showed mixed results and require further studies to determinate the feasibility of representing the intended meaning.

1) Surveying Biometrics: Surveys and interviews are used as a common measurement tool of user acceptance. When biometric recognition appeared as an alternative to other security solutions, a number of surveys gathering user's opinions were undertaken.

One of the first works surveying biometrics was carried out by Jones *et al*. in 2007 [33]. Within this paper, preliminary results of a survey of 135 users regarding biometrics (iris, fingerprint, signature, voice, hand geometry, and face) and other authentication technologies (passwords, RFID tags, smartcards, digital certificates, and other tokens) were discussed. Most respondents were unfamiliar with most of the technologies in question and expressed uncertainty about their use. Nevertheless, biometrics was shown to be the most popular means of authentication, followed by passwords, and tokens. The results also show that the usefulness of individual technologies depends on the context of use. Participants thought that biometrics would be more useful than tokens in most of the contexts analyzed (building access, computer access, hospital, financial transactions, retail store, and online retail) and more useful than passwords for building accesses, retail stores, and doctor's offices or hospitals.

Elliot *et al*., also, in 2007, conducted a survey of 391 individuals on issues relating to biometric technology [34]. Authors claimed that the results from this survey are in line with previous surveys, where a relevant percentage of respondents had not previously heard of biometrics. Those who had heard of biometrics expressed several concerns, including cleanliness of the devices and safety (with respect to iris and retinal identification).

When biometric recognition started to be used in applications, such as banking, many research groups carried out surveys and interviews in order to understand the user's willingness to interact with biometric systems. In 2009, Tassabehji *et al*. surveyed the e-banking security with biometrics, modeling user attitudes, and acceptance [35]. This study, carried out by an online questionnaire fulfilled by 113 people, revealed that user perceptions of biometrics security positively influenced their attitude and intention to use biometrics for online banking services. In 2009, Gunson *et al*. researched the user acceptance in voice recognition also for mobile banking with 204 telephone banking customers [36]. Users found voice recognition based on digits more usable than that based on sentences, and a majority of participants would prefer to use digits.

In [37], the authors assessed different dialogue designs for speaker recognition in automated telephone banking. Three strategies for voiceprint authentication were experienced by 120 participants: One-Factor (speaker recognition based on customers' eight-digit account number and six-digit sort code); One-Factor with challenge (a randomly generated digit string); and Two-Factor (One-Factor plus secret information known only to the caller). Once the three designs were tested, users were asked to fill a questionnaire. Participants found the Two-Factor design the most secure. Results also showed that 88.1% of users are likely to use voiceprint recognition in banking.

Even when it is not widely implemented, biometric recognition was suggested to be present in automated teller machines (ATMs) as a convenient solution instead of the current PIN. Coventry published a study in 2004 about HCI and user acceptance of these self-service systems when being used with biometrics [38]. The conclusion is the existence of a gap between laboratory and real life. Moreover, the author suggests that "biometric technologies do not resolve the usability/security trade off" and that "further research is required to understand the

relationship and find the balance between security and usability." Another study [39] shows the possibility of using fingerprint and palm vein recognition at the ATM, revealing that only 20% of the participants would not register to use biometric technologies. Within the study, it is not clear how much of this result is due to usability issues or underlying negative attitudes toward biometrics.

More recently, the study of user acceptance in biometrics has moved to other scenarios, such as mobile devices or Internet-based systems, in line with novel deployment platforms of new applications using biometric recognition. In 2015, Blanco-Gonzalo *et al*. surveyed 589 users before and after using three fingerprint sensors thought to be embedded in smartphones [40]. Participants were asked about several aspects regarding biometrics in general and fingerprint recognition in particular. Results show the importance of ergonomics in biometrics and the distrust of a high percentage of users of using biometrics for high security tasks, such as banking transactions.

Krol *et al*. published a study about user acceptance and perceived usability of face recognition as a CAPTCHA replacement [41]. Results show that participants found the face recognition to be more suitable to use in some service contexts. However, the experiment also shows the distrust of many users in taking face pictures and uploading them to an app in Internet.

In 2017, Zimmermann and Geber [42] surveyed the user interaction with different authentication schemes (biometric and nonbiometric) to understand the users' perception and preferences. Thirty five participants were enrolled in the experiment and were asked to authenticate themselves using eight different technologies (text password, graphical password, gesture recognition, fingerprint recognition, face recognition, iris recognition, speech recognition, and ear shape recognition). They were provided with a workstation comprising of a Sony VAIO notebook with fingerprint sensor, two monitors (one connected with the FaceLAB system able to capture the biometric features, and one used to provide feedback during the tasks), a microphone, and video cameras. At the end of the task, users answered questions about their perception of security within the tested schemes. The results show that, even if participants were more familiar with passwords, they preferred mainly biometrics because of its uniqueness and unforgeability.

F. Accessibility and Biometrics

The use of biometric technologies for common everyday end uses (especially within mobile scenarios) indicates that technology is not only restricted to high security scenarios anymore. In order to ensure that technology is easy to use for a wider percentage of the population, accessibility issues need to be considered.

Biometric recognition systems are not commonly designed to be accessible, focusing more on security rather than usability. As a result, there are not many works in this area within the literature. Nevertheless, some research groups have recently focused on increasing the UX in biometrics and various works on accessibility have arisen.

One of the first initiatives in the field was the conference Accessible Biometrics in 2005 [43]. The conference's intention was to inspire the development of innovative methodologies and solutions that support disabled people in their use of these new systems, even identifying novel applications to extend the usage of these technologies. The conference covered an overview of biometric technologies, an assessment of the market opportunities (and in particular those in the financial sector), usability issues, testing, and the role of standards.

Among early studies devoted to improving the accessibility of biometric systems were those carried out by the University of Surrey [44], [45]. A series of experiments allowed blind users to take selfies with a small camera guided by audio feedback having been provided with prior instructions. The findings suggest the importance of appropriate design of HCI as well as alternative feedback design based on the audio cue.

Visual disabilities were also studied by NIST within an accessibility test to investigate how users with visual disabilities interact with fingerprint systems [46]. The study involved ten participants that performed three different trials where they presented their biometrics to the sensor. Participants were able to locate the device guided by a tone and using a textured surface to identify the position to properly present their fingerprints. From the study, it resulted that audio tones were effective to localize the scanner, and all, but one participant, were able to identify the right-hand position using the textured surface.

Early studies with the elderly started in 2013 when Sasse *et al*. published the chapter usable biometrics for an ageing population [47] within the book Age Factors in Biometric Processing [48]. This work covers opportunities and challenges that ageing presents for researchers, developers, and operators of biometric systems. One of the important messages of this research is that the lack of usability and accessibility of current authentication products involves an opportunity to well-designed biometric recognition systems.

In 2013, Sanchez-Reillo *et al*. [49] published a biometric recognition prototype for people with accessibility concerns to interact with an ATM (by fingerprint and signature). The interface was adapted to the standard EN 301 549 "Accessibility requirements suitable for public procurement of ICT products and services in Europe" and the fingerprint sensor was connected to a mobile device via USB. The authors claim that their approach is generic and easily adaptable to the specific particularities of disabled people. Further studies have evaluated mobile accessible apps on smartphones when used by people with accessibility concerns (summarized in [50]). Results show poor fingerprint performance due to low fingerprints quality (fingerprints erode with time). On the other hand, signature recognition results are in the line of the state of the art. Authors claim that signing was familiar to most of the participants. Through these series of works, the authors conclude that developing universal accessible apps is nearly impossible due to the wide range of different existing accessibility issues. Therefore, their findings suggest that a convenient accessible design must rely on individual subject characteristics.

G. User-Biometric System Interaction Assessment

Only a few works have been carried out to evaluate the interaction between users and biometrics. In parallel to the NIST research on usability, the HBSI framework was developed by Kukula and Elliot [51]. The framework enables biometric systems interaction to be labeled and logged by the operator alongside users' feedback and the biometric system outputs for later analysis. The HBSI framework's purpose is to use common biometrics measurements (sample quality and system performance), ergonomics (physical and cognitive), and usability (efficiency, effectiveness, and satisfaction) to evaluate the functionality and performance of a biometric system.

In [20], the HBSI model was applied to the use of three common fingerprint devices. Data were collected from 85 individuals over three visits that accounted for 25 867 user interactions. This experiment validates the HBSI and the new metrics derived from the FTA analysis. Thus, the HBSI metrics show that incorrect interactions are less in index and middle fingers than for ring and little. Further work has analyzed other modalities, such as hand geometry [52]. In this work, the authors mapped the HBSI metrics for hand geometry interactions and performed an experiment to validate the model. Outcomes of that research showed that there are differences across the different training methodologies at the enrolment stage and verification stage: The group who has seen a demonstration performed slightly better than the group who has watched a video.

The HBSI framework was also applied in further scenarios, such as in automated border control (ABC) gates in [53]. The authors divided the process in two parts (named models): A generic model used to define the enrolment and the verification; and then an identity claim process, which analyzed every step of the verification. Then, they utilized the HBSI framework to assess the user interaction with the system. A total of 440 users participated in the experiment, interacting with an ABC system at an airport departure gate. During the first phase, passengers entered their electronic passport into a standalone kiosk and received the boarding pass. Then, in the second phase, passengers inserted the boarding pass into a gate reader and after that a biometric face verification subsystem matched the users' live photo with the picture read from their passports. A total of 30.96% of interactions were affected by user interaction errors, meaning that 139 users did not understand completely what to do or were distracted during interaction. This fact allowed the authors to conclude that user behavior is a predominant factor for the performance of ABC systems. They suggested applying the HBSI framework during the evaluation of these processes to understand how to reduce errors and improve the usability and the performance of the entire control system.

More recently, the HBSI model has been expanded to include other types of presentations, including false claims, attacks, and token interactions. These types of interactions have been brought together to complete the full HBSI model, allowing a full categorization of an interaction for any identity claim scenario.

H. New Application Contexts

The papers mentioned in this section are a clear example of how biometrics can be applied to support infrastructures and society. In the last decade, the evolution of technology has allowed the application of biometrics in different environments (e.g., e-border, e-health, e-coaching, e-voting). Several European projects: BODEGA (proactive enhancement of human performance in border control) [54], FastPass (improve security and efficiency in border checks) [55], FIDELITY (ensure e-Passport privacy, security and usability), [56] and SMILE (smart mobility at the European land borders) [57] have assessed the HCI of biometric-based ABC systems. Other researchers are studying how biometrics can increase user acceptance and trust in e-voting contexts [58]. Privacy issues related to e-health are also widely investigated [59].

All the works cited are characterized by a human-centric perspective in which the needs and the security of the user are the end goal. This means enhancing usability and, at the same time, guaranteeing users' privacy. User acceptance and privacy issues behind the new applications may represent the future challenges in biometric HCI research. For example, nowadays biometric applications are moving from a server-centric model to a user-centric one and therefore, it will be necessary to study the changes in terms of security and in user trust and/or user resistance. Additionally, more and more biometric systems are applied in the public surveillance. Thus, it has become necessary to include new trends like the ambient intelligence [60] and affective computing [61] in biometric-based HCI. By proposing biometric systems that ensure high security levels, it will be possible increase the user trust and apply biometrics in different contexts. This can make biometric applications notable even in private contexts, such as private access control systems or private e-payments.

III. Mobile Biometric Platform Interaction

With biometric recognition established in across numerous mobile contexts (smartphones, tablets, wearables, etc.) a series of user interaction studies have been carried out. This section summarizes the main works on biometric interaction on mobile devices.

A. Challenges

The deployment of biometrics on mobile devices as a convenient solution for guaranteeing security in low-risk interactions (e.g., unlocking devices or small-scale payments) motivated a series of new challenges to user-system interaction. In [62], Sanchez-Reillo *et al*. describe these challenges and propose strategies to overcome them. One example is the lack of computational power of mobile devices that, with the progression of technology, is starting to be solved. A similar observation can be made for the internal memory needed to store the biometric templates on the devices. The algorithm of the system should be suitable for any kind of mobile device, smartphone, or tablet, and these can differ for shape, dimension, and operating system supported. The capturing sensors, such as microphone or

fingerprint sensor might be placed in different positions, touchscreens might have different dimensions and sensitiveness, cameras may have different resolutions depending on the model of the device, etc. There is no control in the way the user interacts with the device, also as to where the interaction will happen, making the surrounding environment an important variable to take into consideration.

The main challenges for mobile systems interaction between the user and the device are the time spent in the interaction (the longer the higher probability of users' rejection), ergonomics (e.g., devices' size or use of stylus), and the user acceptance of the technology: Are users willing to use biometrics in their mobile devices?

B. Ergonomics in Mobile Biometrics

Ergonomics in mobile biometrics are related to the shape of the devices, how users handle those devices and where is the biometric (or nonbiometric-specific) sensor. In works carried out by UC3M [63], [64], users were required to use handwritten signature recognition in mobile devices within the most common scenarios. The authors found a high correlation between devices and scenarios. Thus, light and small devices achieved better usability results (efficiency, effectiveness, and satisfaction) in those scenarios where users hold the device in their hands. Subjects may have a different interaction depending on the dimensions of the device they are using. Blanco-Gonzalo *et al*. [64] focused on the online signature, asking participants to interact with four different types of device: A tablet, a smartphone, a tablet-PC, and a digitizer. Efficiency, effectiveness, learnability, and satisfaction were analyzed through three sessions; with a week in between; 20 users were asked to sign using the four different devices in five different scenarios representing the most common situations that might occur in real life. A big decrease in error rates and time was noticed between the first and the second session, but not between the second and the third one, meaning that by that time, participants obtained habituation to the system. This observation makes it clear that training is really important to reach better performance. The results demonstrate that the preferred devices were the digitizer with the stylus and the tablet with the fingertip, even though these do not correspond to the best performance.

Not only can the dimension of the device influence the user-system interaction, but also a reduction in size of the capturing sensors. The authors in [65] study the impact that a small fingerprint scanner can have on the quality and the performance of the biometric system. A database of more than 1 80 000 fingerprint images was collected for this purpose, involving the contribution from 589 participants. The performance was analyzed using a publicly available and a commercial algorithm in two different scenarios. The first scenario compared cropped images obtained from enrolment and authentication using the same small sensor implemented on the mobile device. The second scenario used full-size images obtained from enrolment with a larger external sensor and compared them with cropped images from the mobile device sensor. The results from the study showed that failures to enroll (FTE) and FAR rates increase for image of smaller size, and the quality of the cropped images deteriorate. The impact of using small sensors on mobile devices can be reduced using a large external scanner for the enrolment. Comparison with full-size reference images did not impact time and rates.

With the aim of creating an authentication system that allowed users to store secure identities within their smartphone, the EU cofounded the Private Identity as a Service (PIDaas) project [66]. In 2016, Miguel-Hurtado *et al*. [67], [68] conducted two studies to evaluate the human interaction with the main voice user interface for the PIDaaS platform, the PIDaaS mobile application (PMA), through the application of the HBSI framework. The study aimed to assess the PMA in common scenarios. So, the authors recreated a typical working scenario comprising a desk, a chair, a computer, and a smartphone (iPhone 5S). The participants were asked to register on the PIDaaS platform and then to record their voice template through the PMA. They also were video recorded during the whole experiment by two video cameras and two web cameras. The results obtained allowed an analysis of usability in terms of efficiency, effectiveness, and satisfaction. There was an interaction time and error decrease between sessions 1 and 2, but no such decrease was noticed between the second and the third session. Regarding satisfaction, participants positively evaluated the PMA and the voice authentication system.

C. User Acceptance of Mobile Biometrics

The perception of users of biometric recognition in mobile devices is really important as those who do not feel confident using it will opt for other technologies (e.g., PIN or patterns). Fear of forgeries or distrust in the smartphones' security is a common reason for rejecting the use of biometric recognition.

First user acceptance experiments analyzed preferences between the use of the PIN against the use of biometrics and the use of different biometric modalities on the mobile device. Trewin *et al*. applied the well-known system usability scale (SuS) in 2012 within a usability evaluation of three authentication modalities: Voice, face, and gesture as well as password entry using a mobile device [69]. SuS scores revealed preferences for passwords (78%), gestures (77%), and face recognition (75%). The combination of two biometric modalities were disliked by the participants, had higher FTA and lower performance. Therefore, it did not result in good user acceptance.

In 2015, Bhagavatula *et al*. published findings on user acceptance using iOS (fingerprint) and Android (face) biometrics authentication [70]. A survey about perception of biometrics and ease of use (Android and iOS PIN/Android face and iOS fingerprint) under different lighting conditions, ergonomics (sitting and walking), and other factors, was completed by 198 participants. The authors reached several conclusions, such as most of the participants preferred fingerprint unlock over face unlock or a PIN. Most of the users also perceived fingerprint unlock as more secure and convenient than a PIN.

The interaction that users have with mobile biometric platforms is the main factor that influences the decision to adopt biometrics as a security method. In [71], De Luca *et al*. conducted an online survey to understand the reasons for using (or

not using) biometric systems on mobile devices. The survey focused only on users from Apple's Touch ID and Android's Face Unlock, because they represent the most common systems at the time of the study. Three hundred and eighty three responses were collected from different categories of users: Current users, former users, and nonusers. Results show that usability has bigger influence on users than privacy and security.

The research in [72] analyzed the risk perception and behavior that users have on the interaction with security mechanisms on mobile devices. Data were collected through an online survey with 260 participants and a field study with 52 participants. From this study, it was found that users spend up to 9% of total usage time to unlock the device, and that protecting the access to the device is considered unnecessary in 24.1% of the cases. Also, shoulder surfing was not wholly perceived as a concern by 64.9% of the participants.

Mainly, smartphones are thought as personal objects, but in real life, there are common situations where the main user needs to share a device with other people. In this case, there is the risk of loss or exposure of sensitive personal data stored in the mobile device. The authors of the study [73] conducted an interview with 12 smartphone users. On average, participants declared that they shared their device with 6.7 different guest users, including partners (11% of the 80 total subjects assessed), family members (35%), work colleagues (19%), acquaintance or strangers (19%), and friends (16%).

Cultural differences also motivate different opinions about the use of biometrics on mobile devices. In the study conducted in [74], the authors demonstrated that there are differences across countries toward smartphone unlocking behavior. The study presented the results from 8286 responses of an online survey conducted in eight countries: Australia, Canada, Germany, Italy, Japan, the Netherlands, United Kingdom, and United States. Participants were asked to give their opinion on smartphone lock mechanism and their perception of sensitivity of data stored on their devices. The non-U.S. countries were between 31% and 76% more likely than Americans to have a security mechanism on their smartphone. Japan and, to a lesser extent, Italian respondents consider the sensibility of the content in their smartphones much more than other countries. The study underlines that cultural sensitivity to perception and security mechanism adoption should be taken into consideration when designing authentication systems for smartphones.

Holz and Bentley [75] conducted an interview study about the use of on-demand biometrics authentication. They created a login system for a webpage using fingerprint recognition on smartphones. Users entered their name, received the authentication request on their smartphone, and presented their fingerprint, completing the login in the browser. To evaluate the user interaction and acceptance, the authors recruited 12 participants, with different ethnic backgrounds and occupations, all of whom had been using the fingerprint sensor on their iPhone and were regular Yahoo Mail users. At the end of the tasks, participants were interviewed about how they found the system during the experiment. Analyzing the answers, most users appreciated not having to remember a password and claimed using biometrics authentication increased their sense of security. Everyone completed the tests in a short time and satisfaction results were high. The authors point out that on-demand biometrics could be an alternative to current two-step verification systems.

D. Continuous Authentication and Wearables

Traditionally, the protection of a mobile device consists of requiring the authentication of the user only at the beginning of the interaction, and not during subsequent usage. To prevent unauthorized usage of mobile devices, the user may be continuously reauthenticated by the system, but this action needs to be unobtrusive so that the user's interaction is not interrupted. Behavioral characteristics can be used for continuous authentication. The system creates a behavior profile of the user and can detect suspicious activities when they differ from user normality.

As modern smartphones and tablets have many sensors, there are considerable amount of data that can be collected and used for continuous authentication and can also be combined with security systems conventionally used to enhance their accuracy. Different behavior characteristics can also be combined. The method proposed by authors considers a combination of behavioral features, including hand movements, orientation, and grasp. Hundred participants took part in the experiment where they were asked to answer three questions typing at least 250 characters on a smartphone. The experiment analyzed eight sessions under two different conditions: four required typing while sitting and four while walking. There was more accuracy, while the users were walking instead of standing.

The use of continuous authentication can bring many limitations: Accuracy can require high energy consumption and often a long training time. In [76], the authors analyzed the challenges of keystroke dynamics on mobile devices. The experiment required the completion of three tasks using an app during a session that lasted an hour. There were two sessions in total with a gap of at least a week in between. The results showed that the use of a probabilistic framework considering different hand postures reduced the equal error rate by 23.2% compared to the training of a single model on data from all postures, which were 1) holding the device in the right hand, touching with the right thumb, 2) holding it in both hands, touching with both thumbs, and 3) holding it in the left hand, touching with the right index finger.

Security systems conventionally use PIN or pattern, which can be considered explicit authentication methods. It is possible to combine explicit verification with implicit behavioral features, such as pressure or area of the fingertip. The study in [77] compared PIN and pattern based behavioral authentication mechanisms asking the participation of 15 volunteers. Participants were asked to use a smartphone in two sessions and a tablet in the third one. In each session, they had to perform four different types of actions: A simple pattern, a complex pattern, a simple PIN, and a complex PIN. Behavioral biometric features were extracted from each operation using two different techniques: An adapted histogram method and dynamic time warping (DTW). The results showed that PIN-based behavioral authentication can achieve the same level of accuracy of

TABLE I
STANDARDS IN BIOMETRIC INTERACTION ASSESSMENT

Standard Identifier	Title	Publication	Year
ISO 9241	Ergonomics of human-system interaction	[78]	2009
ISO 25060	The common industrial format (CIF) for usability - General framework	[80]	2010
ISO/IED 29196	Guidance for biometric enrolment	[86]	2015
ISO/IEC PDTR 30125	Biometrics used with mobile devices	[87]	2016
ISO/IEC 24714	Jurisdictional and societal considerations for commercial applications	[88]	2008
ISO/IEC 24779	Information technology - Cross-jurisdictional and societal aspects of implementation of biometric technologies - Pictograms, icons and symbols for use with biometric systems	[89]	2016
ISO/IEC 19794	Information technology - Biometric data interchange formats	[93]	2011
ISO/IEC 29156	Guidance for specifying performance requirements to meet security and usability needs in application using biometrics	[96]	2015
ISO/IEC 21472	Scenario evaluation methodology for user interaction influence in biometric system performance	[97]	2019
ISO/IEC 19795	Biometric performance testing and reporting	[98]	2006

pattern-based methods, and the proposed histogram technique produced more consistent results than the DTW.

IV. Standards in Biometric Interaction Assessment

Although the biometric community has acknowledged the importance of the interaction between users and biometrics and its assessment, historically, it has not been much standardization activity with this respect. However, as it has been detailed in previous sections, the research on biometrics HCI is getting stronger and several research groups have shown interest to work on standardization in order to achieve a common ground for the biometric interaction assessment. This common ground will enable more research on this area and the possibility of reach interoperability among results.

The purpose of this section is to provide an overview of the main standards that are applied in the biometric system interaction assessment (see Table I). In the first part, we present the general standards on usability and on HCI evaluations. Finally, in the second part, we list all the biometric-specific directives provided by the current standardization.

A. General Usability Standards

Most of the research work undertaken on biometrics interaction assessment references the multipart standard ISO 9241 "Ergonomic requirements for office work with visual display terminals (VDTs)" [78]. This standard appeared in the 1980s. From 2006, the ISO 9421 family was renamed as "Ergonomics of human-system interaction" in order to reflect its bigger and broader potential use.

Within the ISO 9241, it is worth mention the part 210 "Human-centered design for interactive systems" [79]. This part is focused specifically on making systems usable: The human-centered design provides a guideline to identify and document all the relevant usability information, enabling its later evaluation.

Usability has also been defined through the ISO / IEC TR 25060 Common Industrial Format (CIF) for Usability—General Framework [80]. This is series of standards that specify the context of use (ISO/IEC 25063 [81]), the user needs (ISO/IEC 25064 [82]), and required specification (ISO / FDIS 25065 [83]), and how to report the evaluation (ISO/IEC 25066:2016 [84]). This family of standards provides useful directives to measure the time of tasks, error rates, and the user satisfaction. For this reason, they could be used in the biometric interaction evaluation as shown in [85].

B. Usability Within ISO/IEC JTC1 SC37 Biometrics

ISO/IEC JTC1 SC37 Biometrics acknowledged the need of bringing biometric usability facets to the biometric standardization community. Usability is mentioned on different ISO/IEC JTC1 SC37 biometric standards as a key factor for biometric implementations, but its analysis has not been thoroughly analyzed and standardized as yet. Most of the usability standardization work has been undertaken within SC37/Working Group (WG) 4 "Technical Implementation of Biometric Systems" and WG 6 "Cross-Jurisdictional and Societal Aspects". In SC37/WG 4, usability has been highlighted as one of the key factors to be considered while planning the implementation of biometric systems in the following standards.

The ISO/IEC Technical Report (TR) 29196:2015 "Guidance for Biometric Enrolment" [86] again points out the usability as a key factor for planning an enrolment within a biometric system implementation [79]. Within biometric enrolment processes, this technical report proposes the following:

1) the sample quality as one of the aspects of system's effectiveness;
2) enrollment time and errors to measure efficiency;
3) users' satisfaction related to "user attitudes, perceptions, feelings, and opinions regarding the system."

ISO/IEC TR 30125:2016 "Biometrics used with mobile devices" [87] provides guidelines for the correct implementation of biometric authentication mechanisms within mobile device applications. It identifies three major issues when considering mobile biometrics with commercial devices: The uncontrolled nature of the capture environment, the data security implications, and the need of ensure "best practices" and consistent "look and feel" for user among different applications and devices. Based on these ideas, it states that mobile devices can be used in a whole range of situations and positions by a wide range of possible users. This technical report provides advice for obtaining performance in usability evaluations, although it does not detail any specific methodology. At the same time, SC37 WG 6 also addresses the usability in the standard ISO/IEC TR 24714-1:2008 "Jurisdictional and societal considerations for

commercial applications—Part 1: General guidance" [88] providing guidelines for the implementation of biometric systems regarding three major areas: 1) jurisdictional issues related to user's privacy and personal data protection, 2) accessibility, and 3) health and safety issues.

Alongside these three major areas, this standard also highlights usability as a key factor for ensuring optimal biometric system performance. At the same time, it provides guidelines for usability issues related to the physical environment where the biometric system operates, such as climate, contamination, location, and position. It also stresses the importance of training and guiding the users and highlights the need of easy-to-use capture devices and processes.

1) Addressing User Feedback. Icons and Symbols: The ISO/IEC 24779 multipart standard [89] intends to provide a standard family of visual icons and/or symbols for being used at biometric systems. These icons and symbols were designed to assist and guide subjects to get prepared for a specific biometric modality, type of sensor, and guide them for present appropriately the biometric sample. In Part 1 [89], modality independent icons/symbols are provided for aiding human interaction with biometric capture devices. For specific biometric modalities, Part 5 [90] (Face applications) is under development. Part 4 [91] (fingerprint applications) and Part 9 [92] (Vascular applications) have already been published. Additional biometric modalities (following the part numbers of ISO/IEC 19794 series [93]) are expected to be developed.

Alongside SC37/WG6, NIST performed several usability studies in order to evaluate user's interpretation and comprehension of this set of symbols with cross-cultural implications [33], [94]. These studies were split in two phases. Phase 1 was based on one-by-one interview with participants collecting their interpretation of different biometric symbols. Part 2 was a participant matching exercise for meaning and symbols. Based on those studies, the most promising symbols in terms of interpretation and less cross-cultural issues were selected and included in U.S. National Body contributions to this multipart standard [95].

2) Metrics to Assess Usability: Finally, in WG 5 "Biometric Performance Testing and Reporting" can be found as a standard which suggests metrics to assess the human interaction influence in biometrics' performance. The ISO/IEC TR (Technical Report) 29156:2015 "Guidance for specifying performance requirements to meet security and usability needs in applications using biometrics" [96]. This TR describes security and usability tradeoffs of biometrics authentication systems compared with other common authentication mechanisms, such as those based on tokens or passwords (covering the three classes of factor authentication: knowledge, possession or personal-characteristics based). It also addresses the use of biometric authentication systems in combination with other authentication mechanisms (multi-factor authentication) to meet security and usability requirements.

In addition, the ISO/IEC 29156:2015 mentions technical, human, and procedural vulnerabilities that can undermine the integrity of the authentication result. It also describes different performance parameters for usability for the three different classes of authentications (knowledge, possession, or personal-characteristics based). Specifically, it highlights the importance of FTE which could be linked with accessibility/usability issues, FTA, which could be linked with poor performing sensors or human/procedures factors, throughout times, FRR, and ergonomic considerations. It states that all the different authentication mechanisms have their own strengths and vulnerabilities and suggests that the use of multifactor authentication mechanisms can mitigate some vulnerabilities and improve the overall solution strengths.

More recently, SC37 experts have acknowledged the lack of a standardized methodology for evaluating the effects of the user interaction in the biometric systems' performance. Thus, the project ISO/IEC 21472 "Scenario evaluation methodology for user interaction influence in biometric system performance" [97], within the ISO/IEC SC37 WG5, intends to provide a methodology to assess the impact of three kinds of factors (human, biometric systems, and their interaction) on the performance of biometric systems. ISO/IEC 21472 is based on the methodology stated within ISO/IEC 19795 [98] for biometric performance testing and reporting.

V. Conclusion and Future Challenges

Advances in biometric recognition systems, not only in terms of system performance, but also in the user interaction with the technology, involved the increase of its use. Moreover, biometrics convenient features (e.g., universality, uniqueness, or permanence) have motivated its application in several contexts and not only in forensics scenarios. In order to continue the biometrics integration smoothly, further testing must be carried out to meet user's requirements.

Many of the current works on biometrics interaction started with the NIST directives and guidelines. Furthermore, NIST contributions to standards have been very relevant from the early studies. Further researching groups also started to make significant contributions in this area, highlighting the importance of the user interaction in biometrics.

According to the variety of biometric recognition uses in mobile devices, this integration has been successful (face, voice, handwritten signature, or fingerprint recognition are some examples). Emergent modalities, *a priori* convenient for mobile scenarios (gait, mobile keystroke, gestures, etc.), are currently under early stages and may be deeply studied in user interaction terms. Then, users and developers could identify their convenience. In any case, as long as mobile devices are progressing and being improved, interaction factors change accordingly, requiring new testing methodologies. Moreover, market tendencies show a growing interest of companies in integrate biometrics in their mobile business [99], [100].

The future of the user interaction in biometrics goes along with technology trends. Biometric recognition is moving now to smart environments, where systems tend to be transparent for users. Mobile biometrics, soft biometrics, and wearables (sometimes altogether) are rising as the most promising topics in the field. With the plethora of sensors within smart devices that may be used for biometric authentication testing interaction in across

scenarios and modalities is required to make new biometrics usable and convenient for users. Experience and support from usability-related groups, such as NIST visualization and usability group will be essential to drive the future of user-system interaction research in new biometric systems.

The use of biometric recognition in the access control systems and in banking (ATM or smartphone apps) is bringing also the attention of the public. Future research in biometrics should be focused then on guaranteeing the usability in those scenarios where the security extent needs to be high and may bring usability issues.

REFERENCES

[1] C.-L. Tsai, C.-J. Chen, and D.-J. Zhuang, "Secure OTP and biometric verification scheme for mobile banking," in *Proc. 3rd FTRA Int. Conf. Mobile, Ubiquitous, Intell. Comput.*, 2012, pp. 138–141.

[2] D. Gorodnichy, S. Yanushkevich, and V. Shmerko, "Automated border control: Problem formalization," in *Proc. IEEE Symp. Comput. Intell. Biometrics Identity Manage.,* 2014, pp. 118–125.

[3] M. O. Derawi, C. Nickel, P. Bours, and C. Busch, "Unobtrusive user-authentication on mobile phones using biometric gait recognition," in *Proc. 6th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process.*, 2010, pp. 306–311.

[4] A. Kumar, "Can we use minor finger knuckle images to identify humans?," in *Proc. IEEE 5th Int. Conf. Biometrics: Theory, Appl. Syst.*, 2012, pp. 55–60.

[5] M. M. Sathik and G. Sofia, "Identification of student comprehension using forehead wrinkles," in *Proc. Int. Conf. Comput., Commun. Elect. Technol.*, 2011, pp. 66–70.

[6] A. K. Jain and B. Klare, "Matching forensic sketches and mug shots to apprehend criminals," *Computer*, vol. 44, no. 5, pp. 94–96, May 2011.

[7] E. Von Zezschwitz, A. De Luca, P. Janssen, and H. Hussmann, "Easy to draw, but hard to trace? On of the observability of grid-based (Un)lock patterns," in *Proc. 33rd Annu. ACM Conf. Human Factors Comput. Syst.*, 2015, pp. 2339–2342.

[8] A. S. Patrick, "Usability and acceptability of biometric security systems," in *Proc. Financial Cryptography Conf.*, 2004, pp. 105–107.

[9] M. F. Theofanos, R. J. Micheals, and B. C. Stanton, "Biometrics systems include users," *IEEE Syst. J.*, vol. 3, no. 4, pp. 461–468, Dec. 2009.

[10] M. Theofanos, B. Stanton, R. Micheals, and S. Orandi, "Biometric systematic uncertainty and the user," in *Proc. 1st IEEE Int. Conf. Biometrics: Theory, Appl., Syst.*, 2007, pp. 1–6.

[11] *Ergonomic Requirements for Office Work With Visual Display Terminals (VDTs)—Part 11: GUIDANCE on Usability*, ISO 9241-11:1998. [Online]. Available: https://www.iso.org/standard/16883.html

[12] R. R. Heckle, A. S. Patrick, and A. Ozok, "Perception and acceptance of fingerprint biometric technology," in *Proc. 3rd Symp. Usable Privacy Secur.*, 2007, pp. 153–154.

[13] Visualization and usability group | NIST.[Online]. Available: https://www.nist.gov/itl/iad/visualization-and-usability-group

[14] M. Theofanos, R. Micheals, J. Scholtz, E. Morse, and P. May, "Does habituation affect fingerprint quality?," in *CHI Extended Abstracts on Human Factors in Computing Systems*. New York, NY, USA: ACM, 2006, 1427–1432.

[15] B. Stanton, M. Theofanos, S. Orandi, R. Micheals, and N.-F. Zhang, "Effects of scanner height on fingerprint capture," in *Proc. Human. Factors Ergon. Soc. Annu. Meet.*, Oct. 2007, vol. 51, no. 10, pp. 592–596.

[16] M. Theofanos *et al.*, *Usability Testing of Height and Angles of Ten-Print Fingerprint Capture*. Scotts Valley, CA, USA: CreateSpace Independent Publishing Platform, 2008.

[17] B. C. Stanton, M. F. Theofanos, S. Orandi, R. J. Micheals, and N. F. Zhang, *Usability Testing of Ten-Print Fingerprint Capture*. Scotts Valley, CA, USA: Createspace Independent Pub, 2007.

[18] B. Fernandez-Saavedra, R. Alonso-Moreno, A. Mendaza-Ormaza, and R. Sanchez-Reillo, "Usability evaluation of fingerprint based access control systems," in *Proc. 6th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process.*, 2010, pp. 333–336.

[19] E. Kukula and S. Elliott, "Implementing ergonomic principles in a biometric system: A look at the human biometric sensor interaction (HBSI)," in *Proc. 40th Annu. Int. Carnahan Conf. Secur. Technol.*, 2006, pp. 86–91.

[20] E. P. Kukula, M. J. Sutton, and S. J. Elliott, "The human–biometric-sensor interaction evaluation method: Biometric performance and usability measurements," *IEEE Trans. Instrum. Meas.*, vol. 59, no. 4, pp. 784–791, Apr. 2010.

[21] B. C. Stanton, M. F. Theofanos, S. M. Furman, J. M. Libert, S. Orandi, and J. D. Grantham, "Usability testing of a contactless fingerprint device: Part 1," NIST, Gaithersburg, MD, USA, Rep. NISTIR 8158, Dec. 2016.

[22] B. Stanton, M. Theofanos, S. Furman, P. J. Grother, P. Grother, and P. Pritzker, "Usability testing of a contactless fingerprint device: Part 2," NIST, Gaithersburg, MD, USA, Rep. NISTIR 8159, 2016.

[23] S. M. Furman, B. C. Stanton, M. F. Theofanos, J. M. Libert, and J. D. Grantham, "Contactless fingerprint devices usability test," NIST, Gaithersburg, MD, USA, Rep. NISTIR 8171, Mar. 2017.

[24] M. F. Theofanos, B. Stanton, C. Sheppard, and R. Micheals, "Usability testing of face image capture for us ports of entry," in *Proc. IEEE 2nd Int. Conf. Biometrics: Theory, Appl. Syst.*, 2008, pp. 1–6.

[25] M. F. Theofanos, B. Stanton, Y.-Y. Choong, and R. Micheals, "Usability testing of an overlay to improve face capture," in *Proc. IEEE 3rd Int. Conf. Biometrics: Theory, Appl., Syst.,* 2009, pp. 1–6.

[26] M. Brockly, R. Guest, S. Elliott, and J. Scott, "Dynamic signature verification and the human biometric sensor interaction model," in *Proc. Carnahan Conf. Secur. Technol.,* 2011, pp. 1–6.

[27] M. Brockly, S. Elliott, J. Burdine, M. Frost, M. Riedle, and R. Guest, "An investigation into biometric signature capture device performance and user acceptance," in *Proc. Int. Carnahan Conf. Security Technol.*, 2014, pp. 1–5.

[28] J. Young and J. Scholtz, "Portable biometrics workstation: Session interface," NIST, Gaithersburg, MD, USA, 2005. [Online]. Available: https://www.nist.gov/sites/default/files/sessionuiprototypecif.pdf

[29] "UKPS biometric enrolment trial," *Biometric Technology Today*, vol. 13, no. 7, pp. 6–7, 2005.

[30] M. A. Sasse, "Red-eye blink, bendy shuffle, and the yuck factor: A user experience of biometric airport systems," *IEEE Secur. Priv. Mag.*, vol. 5, no. 3, pp. 78–81, May 2007.

[31] Y.-Y. Choong, M. Theofanos, B. Stanton, and P. Hofman, "Symbols representing biometrics in use," National Institute of Science and Technology (NIST) Gaithersburg, MD, USA, 2008. Internal Report NISTIR 7645 [Online]. Available: https://www.nist.gov/sites/default/files/nistir7645_symbols-representing-biometrics-in-use.pdf

[32] Y.-Y. Choong, B. Stanton, and M. Theofanos, "Biometric symbol design for the public-case studies in the United States and four Asian countries," in *Proc. 3rd Int. Conf. Appl. Human Factors Ergonom.*, 2010.

[33] L. A. Jones, A. I. Antón, and J. B. Earp, "Towards understanding user perceptions of authentication technologies," in *Proc. ACM Workshop Privacy Electron. Soc.*, 2007, pp. 91–98.

[34] S. J. Elliott, S. A. Massie, and M. J. Sutton, "The perception of biometric technology: A survey," in *Proc. IEEE Workshop Autom. Identification Adv. Technol.*, 2007, pp. 259–264.

[35] R. Tassabehji and M. A. Kamala, "Improving E-banking security with biometrics: Modelling user attitudes and acceptance," in *Proc. 3rd Int. Conf. New Technol., Mobility Secur.*, 2009, pp. 1–6.

[36] N. Gunson, D. Marshall, F. McInnes, and M. Jack, "Usability evaluation of voiceprint authentication in automated telephone banking: Sentences versus digits," *Interact. Comput.*, vol. 23, no. 1, pp. 57–69, Jan. 2011.

[37] N. Gunson, D. Marshall, H. Morton, and M. Jack, "User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking," *Comput. Secur.*, vol. 30, no. 4, pp. 208–220, Jun. 2011.

[38] L. Coventry, "Biometrics, self-service and the user," *Biometric Technol. Today*, vol. 12, no. 10, pp. 7–9, Nov. 2004.

[39] B. R. Barricelli, "Human work interaction design: Designing engaging automation," in *Proc. 5th IFIP 13.6 Working Conf., HWID*, Espoo, Finland, 2018.

[40] R. Blanco-Gonzalo, R. Sanchez-Reillo, R. Ros-Gomez, and B. Fernandez-Saavedra, "User acceptance of planar semiconductor fingerprint sensors," in *Proc. Int. Carnahan Conf. Security Technol.*, 2015, pp. 31–36.

[41] K. Krol, S. Parkin, and M. A. Sasse, ""I don't like putting my face on the Internet!": An acceptance study of face biometrics as a CAPTCHA replacement," in *Proc. IEEE Int. Conf. Identity, Secur. Behav. Anal.*, 2016, pp. 1–7.

[42] V. Zimmermann and N. Gerber, "If it wasn't secure, they would not use it in the movies—security perceptions and user acceptance of authentication technologies," in *Human Aspects of Information Security, Privacy and Trust*. Cham, Switzerland: *Springer*, 2017, pp. 265–283.

[43] J. Gill and M. Rejman-Greene, *Conference on Accessible Biometrics*. 2005. [Online]. Available: http://johngilltech.com/publications/phoneability/accessible_biometrics/

[44] R. Wong, N. Poh, J. Kittler, and D. Frohlich, "Towards inclusive design in mobile biometry," in *Proc. 3rd Int. Conf. Human Syst. Interact.*, 2010, pp. 267–274.

[45] N. Poh, R. Blanco-Gonzalo, R. Wong, and R. Sanchez-Reillo, "Blind subjects faces database," *IET Biometrics*, vol. 5, no. 1, pp. 20–27, Mar. 2016.

[46] B. Stanton, M. Theofanos, and C. Sheppard, "A study of users with visual disabilities and a fingerprint process," NIST, Gaithersburg, MD, USA, *Rep. NISTIR 7484*, 2008.

[47] M. A. Sasse and K. Krol, "Usable biometrics for an ageing population," in *Age Factors in Biometric Processing*. Stevenage, U.K.: IET, 2013.

[48] M. Fairhurst, *Age Factors in Biometric Processing*. Stevenage, U.K.: IET. 2013. [Online]. Available: https://www.theiet.org/resources/books/security/age_factors.cfm

[49] R. Sanchez-Reillo, R. Blanco-Gonzalo, J. Liu-Jimenez, M. Lopez, and E. Canto, "Universal access through biometrics in mobile scenarios," in *Proc. 47th Int. Carnahan Conf. Secur. Technol.*, 2013, pp. 1–6.

[50] R. Blanco-Gonzalo, C. Lunerti, R. Sanchez-Reillo, and R. M. Guest, "Biometrics: Accessibility challenge or opportunity?" *PLoS One*, vol. 13, no. 3, p. e0194111, Mar. 2018.

[51] E. Kukula, "Design and evaluation of the human-biometric sensor evaluation method," Ph.D. dissertation, Dept. Industrial Eng., Purdue Univ., West Lafayette. IN, USA, 2008.

[52] S. J. Elliott, B. Senjaya, E. P. Kukula, J. M. Werner, and M. Wade, "An evaluation of the human biometric sensor interaction using hand geometry," in *Proc. 44th Annu. IEEE Int. Carnahan Conf. Secur. Technol.*, 2010, pp. 259–265.

[53] J. J. Robertson, R. M. Guest, S. J. Elliott, and K. O'Connor, "A framework for biometric and interaction performance assessment of automated border control processes," *IEEE Trans. Human-Machine Syst.*, vol. 47, no. 6, pp. 983–993, Dec. 2017.

[54] BODEGA Project—PROACTIVE Enhancement of Human Performance in Border Control. [Online]. Available: https://bodega-project.eu/

[55] FastPass—A Harmonized, Modular Reference System for All European Automated Border Crossing Points. [Online]. Available: https://www.fastpass-project.eu/

[56] FIDELITY Project—About FIDELITY. [Online]. Available: http://www.fidelity-project.eu/

[57] SMart mobILity at the European land borders—SMILE. [Online]. Available: http://smile-h2020.eu/smile/

[58] D. Petcu and D. A. Stoichescu, "A hybrid mobile biometric-based e-voting system," in *Proc. 9th Int. Symp. Adv. Topics Elect. Eng.*, 2015, pp. 37–42.

[59] A. E. Flores Zuniga, K. T. Win, and W. Susilo, "Biometrics for electronic health records," *J. Med. Syst.*, vol. 34, no. 5, pp. 975–983, Oct. 2010.

[60] M. Tistarelli and B. Schouten, "Biometrics in ambient intelligence," *J Ambient Intell. Human Comput.*, vol. 2, pp. 113–126, 2011.

[61] R. Wang and B. Fang, "Affective computing and biometrics based HCI surveillance system," in *Proc. Int. Symp. Inf. Sci. Eng.*, vol. 1, 2008, pp. 192–195.

[62] R. Sanchez-Reillo, D. Sierra-Ramos, R. Estrada-Casarrubios, and J. A. Amores-Duran, "Strengths, weaknesses and recommendations in implementing biometrics in mobile devices," in *Proc. Int. Carnahan Conf. Secur. Technol.*, 2014, pp. 1–6.

[63] R. Blanco-Gonzalo, R. Sanchez-Reillo, O. Miguel-Hurtado, and J. Liu-Jimenez, "Usability analysis of dynamic signature verification in mobile environments," in *Proc. Int. Conf. BIOSIG Special Interest Group*, 2013, pp. 1–9.

[64] R. Blanco-Gonzalo, O. Miguel-Hurtado, R. Sanchez-Reillo, and A. Gonzalez-Ramirez, "Usability analysis of a handwritten signature recognition system applied to mobile scenarios," in *Proc. 47th Int. Carnahan Conf. Secur. Technol.* , 2013, pp. 1–6.

[65] B. Fernandez-Saavedra, J. Liu-Jimenez, R. Ros-Gomez, and R. Sanchez-Reillo, "Small fingerprint scanners used in mobile devices: The impact on biometric performance," in *IET Biometrics*, vol. 5, no. 1, pp. 28–36, Mar. 2016.

[66] PIDaaS—Private ID as a Service. [Online]. Available: http://www.pidaas.eu/cms/

[67] O. Miguel-Hurtado, R. Blanco-Gonzalo, R. Guest, and C. Lunerti, "Interaction evaluation of a mobile voice authentication system," in *Proc. IEEE Int. Carnahan Conf. Secur. Technol.*, 2016, pp. 1–8.

[68] O. Miguel-Hurtado, R. Guest, and C. Lunerti, "Voice and face interaction evaluation of a mobile authentication platform," in *Proc. Int. Carnahan Conf. Secur. Technol.*, 2017, pp. 1–6.

[69] S. Trewin, C. Swart, L. Koved, J. Martino, K. Singh, and S. Ben-David, "Biometric authentication on a mobile device: A study of user effort, error and task disruption," in *Proc. 28th Annu. Comput. Secur. Appl. Conf.*, Orlanco, FL, USA, 2012, pp. 159–168.

[70] C. Bhagavatula *et al.*, "Biometric authentication on iPhone and Android: Usability, perceptions, and influences on adoption," in *Workshop Usable Secur.*, San Diego, CA, USA, 2015, pp. 1–2.

[71] A. De Luca, A. Hang, E. Von Zezschwitz, and H. Hussmann, "I feel like I'm taking selfies all day! Towards understanding biometric authentication on smartphones," in *Proc. 33rd Annu. ACM Conf. Human Factors Computing*, Seoul, South Korea, 2015, pp. 1411–1414.

[72] M. Harbach, E. Von Zezschwitz, A. Fichtner, A. De Luca, and M. Smith, "It's a hard lock life: A field study of smartphone (un)locking behavior and risk perception," in *Proc. 10th USENIX Conf. Usable Privacy Secur.*, Menlo Park, CA, USA, 2014, pp. 213–230.

[73] A. K. Karlson, A. J. B. Brush, and S. Schechter, "Can i borrow your phone? understanding concerns when sharing mobile phones," in *Proc. SIGCHI Conf. Human Factors Computing Syst.*, Boston, MA, USA, 2009.

[74] M. Harbach, A. De Luca, N. Malkin, and S. Egelman, "Keep on lockin' in the free world: A multi-national comparison of smartphone locking," in *Proc. CHI Conf. Human Factors Computing Syst.*, 2016, pp. 4823–4827.

[75] C. Holz and F. R. Bentley, "On-demand biometrics: Fast cross-device authentication," in *Proc. CHI Conf. Human Factors Computing Syst.*, San Jose, CA, USA, 2016, pp. 3761–3766.

[76] D. Buschek, A. De Luca, and F. Alt, "Improving accuracy, applicability and usability of keystroke biometrics on mobile touchscreen devices," in *Proc. 33rd Annu. ACM Conf. Human Factors Computing Syst.*, Seoul, South Korea, 2015, pp. 1393–1402.

[77] Y. Li, J. Yang, M. Xie, D. Carlson, H. G. Jang, and J. Bian, "Comparison of PIN- and pattern-based behavioral biometric authentication on mobile devices," in *Proc. IEEE Military Commun. Conf.*, Tampa, FL, USA, 2015, pp. 1317–1322.

[78] *Ergonomic Requirements for Office Work With Visual Display Terminals (VDTs)—Part 1: General Introduction*, ISO 9241-1:1997. [Online]. Available: https://www.iso.org/standard/21922.html

[79] *Ergonomics of Human-System Interaction—Part 210: Human-Centred Design for Interactive Systems*, ISO 9241-210:2010. [Online]. Available: https://www.iso.org/standard/52075.html

[80] *Systems and Software Engineering—Systems and Software Product Quality Requirements and Evaluation (SQuaRE)—Common Industry Format (CIF) for Usability: General Framework for Usability-Related Information*, ISO/IEC TR 25060:2010. [Online]. Available: https://www.iso.org/standard/35786.html

[81] *Systems and Software Engineering—Systems and Software Product Quality Requirements and Evaluation (SQuaRE)—Common Industry Format (CIF) for Usability: CONTEXT of Use Description*, ISO/IEC 25063:2014. [Online]. Available: https://www.iso.org/standard/35789.html

[82] *Systems and Software Engineering—Software Product Quality Requirements and Evaluation (SQuaRE)—Common Industry Format (CIF) for Usability: User Needs Report*, ISO/IEC 25064:2013. [Online]. Available: https://www.iso.org/standard/35790.html

[83] *Systems and Software Engineering—Software Product Quality Requirements and Evaluation (SQuaRE)—Common Industry Format (CIF) for Usability: User Requirements Specification*, ISO/FDIS 25065. [Online]. Available: https://www.iso.org/standard/72189.html

[84] *Systems and Software Engineering—Systems and Software Quality Requirements and Evaluation (SQuaRE)—Common Industry Format (CIF) for Usability—Evaluation Report*, ISO/IEC 25066:2016. [Online]. Available: https://www.iso.org/standard/63831.html

[85] M. F. Theofanos, B. C. Stanton, and C. Wolfson, Usability and biometrics ensuring successful biometric systems. NIST, Gaithersburg, MD, USA, 2008. [Online]. Available: https://www.nist.gov/sites/default/files/usability_and_biometrics_final2.pdf

[86] *Guidance for Biometric Enrolment*, ISO/IEC TR 29196:2015(en). [Online]. Available: https://www.iso.org/obp/ui/fr/#iso:std:iso-iec:tr:29196:ed-1:v1:en

[87] *Information Technology—Biometrics Used With Mobile Devices*, ISO/IEC TR 30125:2016. [Online]. Available: https://www.iso.org/standard/53245.html

[88] *Information Technology—Biometrics—Jurisdictional and Societal Considerations for Commercial Applications—Part 1: General Guidance*, ISO/IEC TR 24714-1:2008(en). [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:24714:-1:ed-1:v1:en

[89] *Information Technology—Cross-Jurisdictional and Societal Aspects of Implementation of Biometric Technologies—Pictograms, Icons and symbols for Use With Biometric Systems—Part 1: General Principles*, ISO/IEC 24779-1:2016(en). [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:24779:-1:ed-1:v1:en

[90] *Information Technology—Cross-Jurisdictional and Societal Aspects of Implementation of Biometric Technologies—Pictograms, Icons and Symbols for Use With Biometric Systems—Part 5: Face Applications*, ISO/IEC DIS 24779-5. [Online]. Available: https://www.iso.org/standard/70909.html

[91] *Information Technology—Cross-Jurisdictional and Societal Aspects of Implementation of Biometric Technologies—Pictograms, Icons and Symbols for Use With Biometric Systems—Part 4: Fingerprint Applications*, ISO/IEC 24779-4:2017. [Online]. Available: https://www.iso.org/standard/60477.html

[92] *Information Technology—Cross-Jurisdictional and Societal Aspects of Implementation of Biometric Technologies—Pictograms, Icons and Symbols for Use With Biometric Systems—Part 9: Vascular Applications*, ISO/IEC 24779-9:2015. [Online]. Available: https://www.iso.org/standard/58100.html

[93] *Information Technology—Biometric Data Interchange Formats—Part 1: Framework*,. ISO/IEC 19794-1:2011. [Online]. Available: https://www.iso.org/standard/50862.html

[94] Y.-B. Kwon, Y. Lee, and Y.-Y. Choong, "An empirical study of Korean culture effects on the usability of biometric symbols," in *Proc. 3rd Int. Conf. Appl. Human Factors Ergonom.*, 2010. [Online]. Available: https://www.nist.gov/publications/empirical-study-korean-cultural-effects-usability-biometric-symbols

[95] *Information Technology—Cross-Jurisdictional and Societal Aspects of Implementation of Biometric Technologies—Pictograms, Icons and Symbols for Use With Biometric Systems— Part 1: General Principles*, ISO/IEC 24779-1:2016. [Online]. Available: https://www.iso.org/standard/57379.html.

[96] *Information Technology—Guidance for Specifying Performance Requirements to Meet Security and Usability Needs in Applications Using Biometrics*, ISO/IEC TR 29156:2015. [Online]. Available: https://www.iso.org/standard/45235.html

[97] *Information Technology—Scenario Evaluation Methodology for User Interaction Influence in Biometric System Performance*, ISO/IEC CD 21472. [Online]. Available: https://www.iso.org/standard/70950.html

[98] *Information Technology—Biometric Performance Testing and Reporting—Part 1: Principles and Framework*, ISO/IEC 19795-1:2006. [Online]. Available: https://www.iso.org/standard/41447.html

[99] *Google's Creepy Plan to Kill the Password*, Engadget.com. [Online]. Available: https://www.engadget.com/2016/01/15/googles-creepy-plan-to-kill-the-password/

[100] *Google to Launch Facial Recognition on Phones*, |PYMNTS.com. [Online]. Available: https://www.pymnts.com/news/biometrics/2016/googles-next-play-facial-recognition-smartphones/

Ramon Blanco-Gonzalo received the Ph.D. degree in electrical and electronic engineering from Universidad Carlos III de Madrid, Spain, in 2016, where he was involved in analyzing and improving the usability in biometric systems.

He works with the University Group of Identification Technologies (GUTI) in University Carlos III of Madrid, Madrid, Spain, as a Postdoc Researcher.

Dr. Blanco-Gonzalo has been a member of the Spanish Standardization Subcommittee UNE/CTN71/SC37 Biometrics since 2013. Furthermore, he is part of the ISO/IEC JTC1/SC37 "Biometric Identification."

Oscar Miguel-Hurtado received the Ph.D. degree in electrical, electronic and automatic engineering from Universidad Carlos III de Madrid, Spain, in 2011, where he was involved in signature verification and biometric international standards.

He works with Callsign, London, U.K., as a Research Scientist working on behavioral biometric recognition systems and biometric evaluation.

Dr. Miguel-Hurtado has been taking part in ISO/IEC JTC1/SC37 since 2008.

Chiara Lunerti received the B.Eng. degree in electronic engineering from the University of Roma Tre, Rome, Italy, in 2014, and the M.Sc. degree in information security and biometrics from the University of Kent, Canterbury, U.K., in 2015. She is currently working toward the Ph.D. degree in mobile biometric facial quality at the University of Kent.

Her research interests include the users' interaction with mobile biometric platforms to maximize the performance of the system and the users' acceptance and experience.

Richard M. Guest received the Ph.D. degree in electronic engineering from University of Kent, U.K., in 2000.

He is currently Reader with Biometric Systems Engineering and the Deputy Head of the School of Engineering and Digital Arts at University of Kent, Canterbury, U.K. His research interests include image processing and pattern recognition, specializing in biometric and forensic systems, particularly in the areas of image and behavioral information analysis, standardization, and mobile systems.

Barbara Corsetti received the Bachelor's degree in clinical engineering and the Master's degree in biomedical engineering, from Sapienza Università di Roma, Italy, in 2014 and 2016, respectively. She is currently working toward the Ph.D. degree in usability aspects of mobile biometric systems.

In September 2017, she joined the University Group for Identification Technology (GUTI) at University Carlos III of Madrid, Madrid, Spain, where she is currently working as Early Stage Researcher within the Marie Skłodowska-Curie Innovative Training Network AMBER.

Elakkiya Ellavarason received the B.E. degree in computer science and engineering from Karunya University, Coimbatore, India, in 2009. She received the M.Sc. degree in computer science and engineering from Denmark Technical University, Lyngby, Denmark, in 2013. Her Ph.D. degree is based on the topic "Usability Performance Assessment of Mobile Touch-Screen Behavioral Biometrics" from the University of Kent.

She is currently working as a Marie Sklodowska-Curie Early Stage Researcher with enhAnced Mobile BiomEtRics (AMBER) at University of Kent, Cantebury, U.K.

Raul Sanchez-Reillo received the Ph.D. degree in telecommunication engineering from Universidad Politécnica de Madrid, Spain, in 2000.

He is a Professor with University Carlos III of Madrid, Madrid, Spain, and the Head of the University Group for Identification Technologies (GUTI), involved in project development and management concerning a broad range of applications, from social security services till financial payment methods. He is also an expert in Security and Biometrics.

Dr. Sanchez-Reillo is a member of SC17, SC27, and SC37 Standardization Committees, holding the Spanish Chair in SC17 and the Secretariat in SC37.