User Interaction in Mobile Biometrics

Barbara Corsetti, Ramon Blanco-Gonzalo, Raul Sanchez-Reillo
University Group for Identification Technologies (GUTI),
University Carlos III of Madrid
Leganes (Madrid), Spain
{bcorsett, rbgonzal, rsreillo}@ing.uc3m.es

***Abstract*— Current trends in smartphone authentication have brought new kinds of user interactions which may affect biometric recognition performance severely. This paper brings a snapshot of the current state of the art and validates the recent ISO/IEC 21472 user-biometric system interaction evaluation methodology. Our goal in this work is to evaluate the accessibility of an entrance control system by means of biometric recognition. By studying how the users interact with a system (especially developed for people with accessibility concerns), the final purpose is to derive improvements to future mobile applications in terms of accessibility and universality.**

Keywords— Biometrics; Mobile Biometrics, Face recognition, Fingerprint recognition; User interaction; Accessibility.

I. INTRODUCTION

In recent years, biometrics had eased people lives in many contexts. For instance, biometrics is deeply used in security contexts such as banking, or forensics and it is considered as a user-friendly authentication mode.

Today, the market offers thousands of mobile devices with sensors that can be used for biometric recognition. Modern smartphones have cameras, microphones and touch-screens. This allows quick authentication by means of face, voice or fingers among others. Thus, the more smartphone demand increases, the more biometrics becomes a widespread technology among people. It is estimated that the number of smartphones in the world will pass the 5 billion in 2019 [1]. Acuity Market Intelligence foresees that in 2019 all the smartphones will have at least a kind of biometric technology [2], and by 2020 the same will happen for wearable and tablet devices.

Hence, in the last decade it became necessary studying how people interact with mobile biometrics, and how that interaction could affect the biometrics performance on smartphones. In this way, it is possible to establish guidelines for developing high-performance and easy to use mobile systems.Studies in this area are commonly focused on the error rates such as FTE (Failure-To-Enroll), FTA (Failure-To- Acquire) [3] FNMR (False-No-Match-Rate) and FMR (False-Match-Rate) [4].

Further works studied the user-biometric system interaction through the usability (*"the extent to which a product can be used by specific users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use"* [5]). Usability analysis allows to understand how to design systems in such a way that users could be able to complete their tasks without too much effort (effectiveness), in a reasonable time (efficiency) and being satisfied with the system.

Even when biometrics in mobile devices may be considered as user friendly in previous studies, a significative percentage of the population may find several barriers. That is why assessing accessibility is necessary and why we carry out this work. Accessibility is defined by ISO 26800:2011 [6] as "*the extent to which products, systems, services, environments and facilities can be used by people from a population with the widest range of characteristics and capabilities, to achieve a specific goal in a specific context of use".* Accessibility evaluation in biometrics is necessary to better understand why people have difficulties to interact with biometric applications and how to prevent them.

Taking all these considerations into account, we are developing a biometrics-based access control as a meaningful example of the daily use of biometric recognition. During our experiment, participants will interact with an access control system allowing people to open a door using fingerprint and face recognition. We will evaluate the system following the directives coming from the recent standard ISO/IEC 21472 [7]. Our final discussion will allow us to analyse which factors are the most influent in the biometric performance. To obtain results as much realistic as possible we will enroll participants with mobility issues (sitting on a wheelchair). This group of people represents a high percentage of the global population that every day must face several barriers.

The rest of the paper is organized as follows: Section II presents the literature review on user interaction and accessibility in mobile biometrics. The methodology to

ISBN 978-90-827970-1-5

validate by our experiment is presented in Section III; Section IV describes the evaluation set up, and finally, Section V presents a discussion about the work.

I. Previous Works

The user interaction with biometric systems has been deeply observed in the last years. The aim had been to gain a better knowledge about which factors may influence the relationship between user and biometric system and how much the user interaction could affect the biometric system performance. Works carried out in this field analysed the user acceptance, the usability and the accessibility related to the biometric application on mobile devices.

In the last decade, several studies were focused on the people' opinion about biometrics and mobile biometrics. So many surveys were conducted on the user acceptance regarding biometric application in mobile environments. In 2014 Karthikeyan et al. [8] carried out a comparison between the Apple's Touch ID and the PINs. During the experiment, participants were required to unlock an iPhone 5S once by PIN and by fingerprint identification. Users were video-recorded during the whole process in order to catch their reaction and feelings interacting with the system. At the end of the experiment they were asked about their experience. Results showed that the 60% of the users preferred the use of Touch ID, considering it as more secure than PINs.

In 2015, Bhagavatula et al. investigated the user acceptance of two biometric authentication modalities: the Android Face ID and the iPhone fingerprint recognition [9]. Authors recruited 198 users, half owners of an Android phone and half owners of an iPhone 5S (not all of them were used to biometric recognition thought their smartphone). Participants were asked to complete an online survey. Among the former user of fingerprint recognition more than the 70% evaluated the biometric recognition more secure than the traditional PIN. While, among former user of face recognition the 40% rated it as the securest recognition.

Von Zezschwitz et al. in [10] carried out another online survey in 8 different countries (Australia, Canada, Germany, Italy, Japan, the Netherlands, United Kingdom and United States). Authors' aim was studying how the cultural differences can affect the use of mobile biometric applications. Results, demonstrated that people coming from different countries have different opinions about smartphone lock mechanisms. The non-U.S.A. countries are more willing to use security mechanisms on their phone. Thus, authors argue to consider cultural differences as an influence factor during the development of authentication schemes for mobile devices.

Naturally, users' opinion could also be influenced by external factors, or factors related to the environment. For example, time and stress could affect the perception that people have of mobile biometrics, changing their grade of trust. Authors in [11] tested the dynamic handwritten signature on mobile devices. The results pointed out that the performance of the system decreased under stressful scenarios. Collota et al. [12] assessed the usability of a fingerprint sensor on Android smartphones. They also found out that time is important on user interaction. Satisfaction results showed that users sometimes had the feeling that the process is too slow and feel annoyed, causing negative consequences on the system performance.

Another influential factor in mobile biometrics is ergonomics. Actually, the shape of the devices, the size of biometric sensors and even the posture of the user could influence the user interaction. A study about this subject was carried out in [13] by Blanco-Gonzalo et al., where authors tested the usability of the DSV (Dynamic Signature Verification) in mobile environments analysing different scenarios (Figure 1).

Figure 1. Users interacting with biometrics in different scenarios during ergonomics experiments [13].

During this evaluation, three different experiments were carried out, each one testing different combinations of influential factors (visual feedback, stress, posture, devices and stylus). Results showed that providing visual feedback helps the participants completing their tasks, while stressful scenarios affect the user attention and decrease the performance. As regard the ergonomics, the best system performance score was reached when the users handled the device. Finally, this study also suggests that the performance could be influenced by other ergonomic factors, such as the shape of the styluses or the mobile devices' size and shape. The best performance score was obtained with the stylus-based devices.

Later on, the same authors in [14] carried out another usability and accessibility evaluation of DSV. 21 participants joined the assessment and were asked to sign on an iPad. The experiment was split in three different sessions (one week apart), and three different scenarios were tested (Figure 2).

Figure 2. Scenarios tested in the experiment [14].

ISBN 978-90-827970-1-5 © EURASIP 2018

In the first scenario participants signed sitting with the iPad on a table; in the second scenario user remained seated holding the device; in last scenario user stand with the device over a slope surface. Three styluses with different shape, length and diameter were tested in all scenarios. Usability metrics improved during the sessions, meaning that users got used to the system during the evaluation. Moreover, the analysis of performance showed that different postures implicate different results.

Kukula and Elliott in [15] combined several factors that may influence the relationship between user and the biometric system in a single model. The aim was to use common biometric measurements (e.g. sample quality and system performance), ergonomics (physical and cognitive), and usability (efficiency, effectiveness, and satisfaction). This framework is known as Human Biometric-System Interaction (HBSI).

In 2016 Miquel-Hurtado et al. [3] carried out an user interaction evaluation of a mobile voice authentication system. They applied the HBSI model to the PIDaaS Mobile Application (PMA) [16], an European project to store biometric data safely. They evaluated this application in a working desk. 27 participants participated in this experiment, testing the PMA in two different sessions one week apart. Results show an improvement of efficiency and effectiveness between the first and the second session. During the last visit users completed the task faster, with less errors than the first visit. In addition, most of the participants evaluated positively the voice recognition process through PMA.

One year later, the same authors updated their work including also the face recognition in the PMA [17]. They planned three different sessions split in different weeks. At the end of the whole evaluation people filled a questionnaire about their interaction with the mobile app. Participants declared that face recognition is more user-friendly than voice (this could be clarified by the daily use that people have in taking photo). During the last sessions users completed the tasks quickly and with less errors that the first visit. Authors argued that the user experience with the biometric application is important to obtain better performance.

In 2013 Sanchez-Reillo et al. carried out one of the first studies on accessibility in biometrics [18]. In this work different kinds of physical and cognitive issues are discussed in order to give directives to build an authentication system accessible to every kind of user.

Starting from the previous work [18] Blanco-Gonzalo et al. [19] assessed a mobile app for making payment using biometrics recognition. The app was evaluated by means of the standard EN 301 549 *"Accessibility requirements suitable for public procurement of ICT products and services in Europe"* [20] by the same authors. During this evaluation, users were instructed to approach the smartphone to PoS (Point of Sales: contactless smartcard for the financial transactions) to make a payment and authenticate themselves by fingerprint or signature recognition. 21 participants with accessibility concerns completed the entire evaluation, split in two different sessions at least one week apart. At the end of the experiment, all the users were interviewed. By the results obtained, authors concluded that accessibility reached higher score than expected, as the app was not specifically designed for users with accessibility concerns.

All the studies presented in this section are an excellent starting point for our study. We will implement our access control process in which the influence of several factors related with the user interaction could be observed. The results from the analysis will help us to understand how to avoid the influence of the user interaction on the system's performance. The intention is to provide guidelines in terms of accessibility for the future biometric applications.

III. METHODOLOGY

In order to evaluate the influence of the user interaction on the performance of the biometric system, we have applied the methodology developed by Blanco-Gonzalo et al. in 2016 [21]. This methodology is described as a "*functional test in which data subjects interact with the system with the aim to calculate the accuracy and the speed of the recognition algorithm when one of more the following situations occur*:

- *Certain characteristics related to the biometric capture device have been changed,*
- *Users or their biometric features have certain attributes,*
- *Other factors related to the user interaction process itself have been modified."*

According to the ISO/IEC 21472 [7], to carry out this work, we shall perform a scenario evaluation. The complete description of a scenario evaluation is within the ISO/IEC 19795-2:2006 [22]. Testing the user influence on the performance of a biometric system means to perform two (at least) scenario evaluations: one under Reference Evaluation Conditions (REC) and others under the Target Evaluation Conditions (TEC). *"REC and TEC are the identical (i.e., both shall have identical test specification and test procedures) except for the user interaction factor to study"*. Each evaluation condition is specified to assess different combinations of user interaction factors. These combinations

ISBN 978-90-827970-1-5 © EURASIP 2018

are decided based on the objectives of the evaluation. The main aim of this work is to find out which are the most influential factors in the performance. Factors to be analysed in this work are those related to an access control scenario for people having accessibility concerns.

During the evaluation data subjects will pass the access control using biometric authentication in a mobile device and/or embedded in the access control. Biometric samples and performance (in terms of FMR, FNMR and EER) will be recorded as well as further information regarding the interaction (e.g., possible inconveniences or errors) according to ISO/IEC 21472. As long as there are not standardised metrics to measure the accessibility in this specific context, it will be evaluated on the basis of the following rates:

- Number of people who cannot start the experiment (or any part).
- Number of people who cannot complete the experiment (or any part).
- Number of people who do not want to start the experiment (or any part). This factor is not considered as an accessibility metric. Nevertheless, we decide to keep it as acceptability and trust index.

Furthermore, the comparison between results from REC and TEC (performances) allows knowing the influence of the factors.

VI. Evaluation Set up

The experiment is divided into two sessions at least one week apart in order to not make people used to the system. The first session consists of two parts: enrolment and verification. Prior to start the evaluation users will receive instruction about the evaluation characteristics (e.g., timing, sessions or biometrics). During the enrolment we will collect participants' personal data and biometric references on a database through an Android app specifically developed for this experiment. At the end, users may complete the verification, presenting their biometric traits (voice and fingerprint) to the system which will compare them with the references previously stored. We will prepare five scenarios with the purpose of recreate a realistic environment in which our system is supposed to be used: the homes' door point.

In the baseline scenario, a user arrives at the door point and present her finger to a biometric sensor embedded on the door lock (Figure 3).

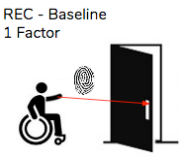

Figure 3. Scenario under Reference Evaluation Condition (REC).

In this case the authentication occurs through a one-factor recognition. The other four scenarios are carried out under different target evaluation conditions: TEC 1, TEC 2, TEC 3, TEC 4 which are shown in Figure 4. The logic of the TECs' sequence is the following:

We will start testing just one recognition factor and then we will move on testing more recognition factors. Adding recognition factors may change the way the user approaches (and interact with) the system. Many aspects related to the users' accessibility problems could be observed in each scenario. Additionally, we can also analyse the changes in term of users' trust (two-factor recognition could be considered more secure than one-factor recognition process). In the Figure 4 is a picture of the TEC's feature.

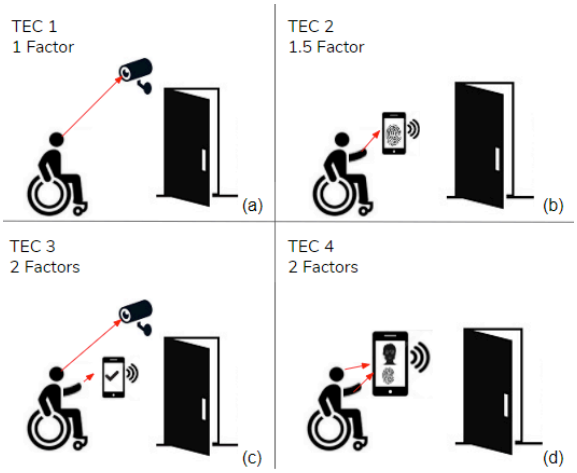

Figure 4. Scenario evaluations under Target Evaluation Conditions (TEC).

TEC 1: this scenario is similar to the baseline. It is a one-factor recognition where the user is authenticated by her face instead of her fingerprint. In this case, the user arrives at the door point and presents her face to an IP camera located above door lock (Figure 4 (a)). Once the user is authenticated, the camera communicates with the lock via Bluetooth to open the door.

TEC 2: in this scenario, users arrive at the door point and present their fingerprint to the mobile device using the App. As the previous scenario, once the user is authenticated, the smartphone sends a Bluetooth signal to the door lock to open it. (Figure 4 (b)). This is a 1.5 authentication factor scenario because the biometric recognition is made through a device that user owns.

TEC 3: this is the first scenario with 2 authentication factors. User arrives at the entrance and her face is detected by an IP camera, that recognizes send a message to the App. The user must accept the notification to open the door (Figure 4 (c)). Communications will be via Bluetooth as the previous scenarios.

ISBN 978-90-827970-1-5 © EURASIP 2018

TEC 4: in this scenario, participants use just the smartphone to self-authenticate by face and fingerprint recognition. Once this task is completed, the door will be open. This is also a two-factor authentication process (Figure 4 (d)).

V. Discussion

This work is the first published validation of the **ISO/IEC 21472, currently under WD (Working Draft) within the ISO/IEC/JTC1/SC37 – Biometrics**.

In this paper we present a current snapshot of the literature of user interaction with mobile biometrics. Most of the works discussed in Section II show that people are reacting positively to the biometric recognition by their smartphones. Although several factors may affect the relationship between user and biometric systems causing repercussions on the system performance. These factors must be taken into account during the development of biometric applications. At the same time, also the parameters related to the accessibility of biometric devices must be considered. Nowadays many applications are still difficult to use (for people with mobility concerns and for everyone).

The scenarios proposed during our experiment will allow us to observe different types of interaction between the user and the biometric system. For example, in the first scenario user must approach the biometric sensor on the door, while in the second scenario user does not even interact directly with the system (just present his face to a camera). Finally, in TEC 2, TEC 3 and TEC 4 user must complete the recognition processes through the smartphone. Studying different scenarios, it will be possibile to measure several factors that may influence the system' performance.

VI. ACKNOWLEDGEMENT

This work has been supported by Marie Skłodowska-Curie EU Framework for Research and Innovation Horizon 2020, under the Grant Agreement No. 675087 within AMBER (enhanced Mobile BiomEtRics). Authors thank Elakkiya Ellavarason for her contribution to this work.

REFERENCES

[1] Statista, "Number of smartphone users worldwide 2014-2020 | Statista," *Statista*. pp. 2019–2021, 2017.

[2] "Chart: The Future of Mobile Biometrics | Statista." [Online]. Available: https://www.statista.com/chart/11122/the-future-of-mobile-biometrics/. [Accessed: 15-Jan-2018].

[3] O. Miguel-Hurtado, R. Blanco-Gonzalo, R. Guest, and C. Lunerti, "Interaction evaluation of a mobile voice authentication system," in *2016 IEEE International Carnahan Conference on Security Technology (ICCST)*, 2016, pp. 1–8.

[4] R. Blanco-Gonzalo, L. Diaz-Fernandez, O. Miguel-Hurtado, and R. Sanchez-Reillo, "Usability evaluation of biometrics in mobile environments," in *2013 6th International Conference on Human System Interactions (HSI)*, 2013, pp. 123–128.

[5] "ISO 9241-11:1998 - Ergonomic requirements for office work with visual display terminals (VDTs) -- Part 11: Guidance on usability." [Online]. Available: https://www.iso.org/standard/16883.html. [Accessed: 31-Jan-2018].

[6] "ISO 26800:2011 - Ergonomics -- General approach, principles and concepts." [Online]. Available: https://www.iso.org/standard/42885.html. [Accessed: 07-Feb-2018].

[7] "ISO/IEC AWI 21472 - Information technology -- Scenario evaluation methodology for user interaction influence in biometric system performance." [Online]. Available: https://www.iso.org/standard/70950.html. [Accessed: 31-Jan-2018].

[8] S. Karthikeyan, S. Feng, A. Rao, and N. Sadeh, "Smartphone Fingerprint Authentication versus PINs: A Usability Study," 2014.

[9] C. Bhagavatula, B. Ur, K. Iacovino, S. M. Kywe, L. F. Cranor, and M. Savvides, "Biometric Authentication on iPhone and Android: Usability, Perceptions, and Influences on Adoption," *2015 Netw. Distrib. Syst. Secur. Symp.*, 2015.

[10] E. von Zezschwitz, A. De Luca, P. Janssen, and H. Hussmann, "Easy to Draw, but Hard to Trace?," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems - CHI '15*, 2015, pp. 2339–2342.

[11] R. Blanco-Gonzalo, R. Sanchez-Reillo, O. Miguel-Hurtado, and E. Bella-Pulgarin, "Automatic usability and stress analysis in mobile biometrics," *Image Vis. Comput.*, vol. 32, no. 12, pp. 1173–1180, Dec. 2014.

[12] M. Collotta, V. Conti, M. Collotta, G. Pau, and S. Vitabile, "Usability Analysis of a Novel Biometric Authentication Approach for Android-based Mobile Devices," *J. Telecommun. Inf. Technol.*, vol. 4, no. October 2015, 2014.

[13] 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 *2013 47th International Carnahan Conference on Security Technology (ICCST)*, 2013, pp. 1–6.

[14] R. Blanco-Gonzalo, L. Diaz-Fernandez, O. Miguel Hurtado, and R. Sanchez-Reillo, "Usability Evaluation of Biometrics in Mobile Environments," Springer, Cham, 2014, pp. 289–300.

[15] 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.

[16] "Home." [Online]. Available: http://www.pidaas.eu/cms/. [Accessed: 18-Oct-2017].

[17] O. Miguel-Hurtado, R. Guest, and C. Lunerti, "Kent Academic Repository Versions of research Citation for published version Voice and face interaction evaluation of a mobile authentication platform," 2017.

[18] R. Sanchez-Reillo, R. Blanco-Gonzalo, J. Liu-Jimenez, M. Lopez, and E. Canto, "Universal access through biometrics in mobile scenarios," in *2013 47th International Carnahan Conference on Security Technology (ICCST)*, 2013, pp. 1–6.

[19] R. Blanco-Gonzalo, R. Sanchez-Reillo, C. Sanchez-Redondo, and J. L. Alonso-Aguilera, "Accessibility evaluation of a mobile biometric recognition system," in *2016 IEEE International Conference on Identity, Security and Behavior Analysis (ISBA)*, 2016, pp. 1–6.

[20] Cen, Cenelec, and Etsi, "En 301549 - Accessibility requirements suitable for public procurement of ICT products and services in Europe," *Etsi.Org*, vol. 1, pp. 1–138, 2014.

[21] R. Blanco-Gonzalo, R. Sanchez-Reillo, J. Liu-Jimenez, and C. Sanchez-Redondo, "How to assess user interaction effects in Biometric performance," *2017 IEEE Int. Conf. Identity, Secur. Behav. Anal. ISBA 2017*, no. section 2, 2017.

[22] I. Jtc, "ISO/IEC JTC 1/SC 37 N 1768 Text of FDIS 19795-2, Information technology – Biometric performance testing and reporting – Part 2: Testing methodologies for technology and scenario evaluation," 2006.