International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Advancing Human-Computer Interaction through Biometric Authentication: Innovations, Challenges, and Future Directions

[1]Ishrat Begum, [2]Dr. Meena Chaudhary

Submitted: 07/02/2024 **Revised**: 15/03/2024 **Accepted**: 21/03/2024

Abstract: The personalized experience that people want and that organizations strive to provide relies heavily on recognizing and identifying individual users. Recent paradigm shifts in biometric system design have prompted the need for more thorough testing procedures, particularly in mobile settings where user input is less constrained by physical space, which might have a significant impact on system efficiency. In order to gather data for testing and design, testing methodologies include thinking about how user-system interaction affects system performance as a whole. In addition, we lay out the present obstacles and future directions for research on biometrics systems interface.

Keywords: *HCI, User Recognition, Behavioral Biometrics*

1. Introduction

The integration of intelligent sensors, actuators, sophisticated communications, fast computing, and AI in HCI has the potential to revolutionize our daily lives and the way we do business. Almost every industry is already using some kind of Internet of Things technology [1]. Through the use of security-sensitive services provided by Internet of Things (IoT) applications, smart, integrated systems are improving resource efficiency and quality of life in a wide range of industries, including transportation, energy, entertainment, education, food, banking, healthcare, and energy. The basic needs to prohibit real-time data access directly from IoT-enabled smart devices deployed in IoT ecosystems are user authentication, access control, key management, and intrusion detection, according to Bera et al. [2]. Research has shown that application-layer attacks on the Internet of Things are notoriously difficult to identify and counter [3, 4]. At the end of the day, customers and society stand to lose a lot if security breaches in IoT networks occur [5]. Maintaining CIA in the system requires strong and easily-understood Authentication, Authorization, and Accounting (AAA) methods for apps that connect people to IoT ecosystems, also known as IoT apps. Passwords, Personal Identification Numbers (PINs), and tokens are still used by many Internet of Things (IoT) ecosystems as user authentication methods [6]. Despite this, traditional (knowledge- and token-based) identification methods have problems with usability and security [7, 8]. Traditional authentication methods also often use a binary decision-making procedure [9]. Passwords and PINs are insecure because they are easy to guess, distribute, copy, or steal [10]. Traditional verification Dictionary, observation, and replay attacks are only a few of the many prevalent types of attacks that may compromise 24 schemes [11]. The majority of botnet-based attacks, like Mirai, that affect many IoT devices still have weak passwords as their root cause [12]. A number of usability concerns also exist with them [13], such as the fact that they impose an excessive cognitive burden on users and that, for more recent Internet of Things (IoT) end-points, they are ergonomically inefficient. Thus, re-evaluating human-to-things recognition approaches for IoT ecosystems is necessary; behavioral biometrics offers a suitable substitute for addressing the shortcomings of traditional authentication methods.

2. Literature Review

These days, biometric identification is commonplace in many places, including banking [14], ABS systems [15], home automation systems [16], and mobile device authentication. Researching biometric systems from an HCI vantage point is now pertinent due to the increasing prevalence of biometric applications. Researching human reactions to biometric technologies is essential for figuring out how these systems and gadgets interact with users. In addition, new biometric situations and devices have brought many new problems that need to be re-engineered in order to solve them. This includes the need for new or adapted authentication algorithms that work with certain devices, sensors, and modalities, among other things. There are a growing number of trustworthy alternative biometric modalities to traditional ones, such as knuckle recognition[17] or gait recognition[16] or forehead recognition[18] or facial drawings [19] among

[1]*Research Scholar, Computer Science, Institute of Engineering and Technology, Mangalayatan University, Aligarh, UP, India*
[2]*Asst. Professor, Institute of Engineering and Technology, Mangalayatan University, Aligarh, UP, India*

many others. Biometrics on mobile platforms have spurred many of the aforementioned advances. Since smartphones, tablets, and laptops are now ubiquitous in our everyday lives, there is a greater need to secure access to these devices. This is especially true when it comes to storing sensitive data like contacts, emails, and calendars, as well as while making online purchases and bank transfers. The perfect multifunctional computer device, these gadgets are so simple to lose or have stolen because to their inherent mobility and ever-growing capabilities. The usage of biometrics to secure smartphone access has recently surpassed that of PIN and password. Users are protected from assaults like shoulder surfing and don't even need to memorize passwords with biometric systems [20]. In addition to lowering the cost of deploying authentication systems, the existence of capturing sensors incorporated on the device itself has encouraged the use of biometrics in mobile platforms [21]. In addition to being able to make phone calls, the microphone on every mobile device may also be used for speech recognition. Most of these gadgets also include a touchscreen and a camera, so you can use them to verify your signature or face. Fingerprint and iris sensors have been integrated into mobile devices recently, enabling the usage of these biometric authentication methods. Users' experiences with biometric sensors may change when new use cases and biometric modalities emerge, which might impact the system's overall effectiveness. While algorithms have long been thought to have a significant role in performance rates, several other variables, including environmental conditions, biometric sensor quality, changes in biometric sample characteristics, and user-system interaction, all play a role [22], [23].

To further understand consumers' perceptions and preferences, Zimmermann and Geber [24] examined their interaction with several authentication mechanisms in 2017. Using eight distinct technologies—a written password, a graphical password, gesture recognition, fingerprint recognition, face recognition, iris recognition, voice recognition, and ear shape recognition—35 individuals were asked to verify their identity in the experiment. A Sony VAIO laptop equipped with a fingerprint sensor, a microphone, video cameras, two displays (one for collecting biometric data via the FaceLAB system and another for providing feedback as they worked), and a connection to the system were all components of their workstation. Users were asked to rate the security of the various schemes at the conclusion of the work. The findings demonstrate that participants still favored biometrics over passwords due to its uniqueness and immutability, regardless of their familiarity with passwords.

Research out of the University of Surrey was one of the first to focus on making biometric systems more user-friendly [25], [26]. Through a series of trials, individuals who are visually impaired were able to utilize a tiny camera to snap selfies with the use of aural feedback, following pre-established instructions. In light of these results, it is clear that proper HCI design and alternate feedback design based on the auditory cue are crucial. As part of an accessibility test, NIST also looked at visual impairments to see how people with vision loss utilize fingerprint systems [27]. Ten volunteers submitted their biometric data to the sensor three times for the research. With the use of a tone and a textured surface, participants were able to find the gadget and correctly place their fingerprints on it. The research found that auditory tones helped participants locate the scanner, and with the exception of one, everyone could use the textured surface to determine their right-hand position. The first research including the elderly was published in 2013 in the book Age Factors in Biometric Processing [29] by Sasse et al., which included the chapter "Usable Biometrics for an Ageing Population" [28]. Researchers, developers, and operators of biometric systems have both possibilities and disadvantages as a result of aging, which are covered in this study. This study's key takeaway is that there's a window of opportunity for well-designed biometric recognition systems due to the existing authentication solutions' poor accessibility and usability. To help persons with disabilities use automated teller machines (ATMs) (via fingerprint and signature), Sanchez-Reillo et al. [30] released a biometric recognition prototype in 2013. The fingerprint sensor was linked to a portable device using USB, and the user interface was modified to conform to the "Accessibility requirements suitable for public procurement of ICT products and services in Europe" standard (EN 301 549). The authors assert that their method is flexible enough to accommodate the unique needs of individuals with disabilities. Additional research has assessed the usability of accessible smartphone applications for those with impairments (reviewed in [31]). As a result of low fingerprint quality (fingerprints deteriorate with time), the results demonstrate subpar fingerprint performance. Results for signature identification, however, are competitive with state-of-the-art methods. According to the authors, the majority of the participants were already acquainted with signing. The writers of these publications reach the conclusion that, given the diversity of current accessibility challenges, it is very difficult, if not impossible, to create applications that are accessible to all users. So, according to their results, specific topic features are crucial for an accessible design that is both convenient and user-friendly.

3. Method And Results

A software framework that incorporates biometric input (like fingerprint data) while prioritizing usability, accessibility, and user experience design is the essence of the strategy. This framework should also aim to make the software easy to use for all users.

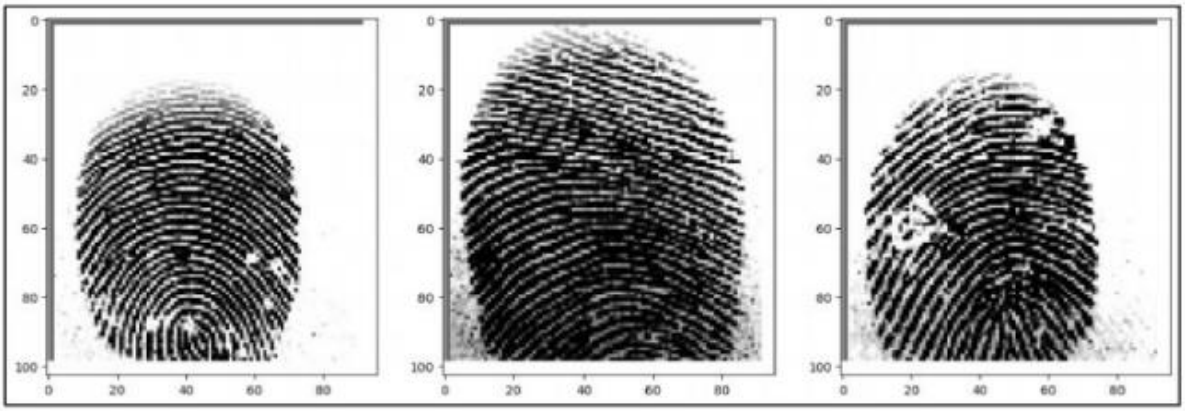

Fig 1 : Input Image used in this study

Feature Shape for Convolutional Neural Networks

CNNs specifically depend on the input form and structure to address the characteristics of the received information. There is a hint on the aspect of the data supplied to the network. For image data, this data set can include the dimensions and the breadth of the image together with the quantity of the colour channels like RGB for coloured pictures. It is necessary that the architecture of the communication network should be designed to accommodate different forms of data, depending of the input form of data affects the handling and processing of the data within the network.

How Input Shape Matters

CNNs are very much affected by the input shape while processing the data. These formats of data are created to simulate all significant aspects of data in more than one dimension and the format of the input influences how the learning in the CNN occurs. For instance, if the input pictures are three color channels with a size of 224 x 224, then the network needs to be designed in a format of tensors, which are of the form (224,224,3). To feed the network and have it work to extract features and perform tasks such as picture categorization or even identification of an object in the picture, the input shape has to be well defined.

Topology for Convolutional Neural Networks

A layered architecture that follows a linear pattern is the most common CNN arrangement and design with layers that follow the sequence of the data flow. This structure generalized all layers and the input tensor is the same with all layers as the output tensor. This sequential architecture helps in the design and the implementation of the network as well. The frequently used CNN layers are; the fully connected layer, the pooling layer as well as the convolutional layer; various layers undertake different transformation and analysis of the data.

Coupled Tensors for Input and Output

Layers of a sequential convolutional neural network (CNN) architecture take in tensors as inputs and produce tensors as outputs. Because the roles and contributions of each layer are obvious, this simple method facilitates network management and troubleshooting. While the network's lower levels are responsible for extracting simple properties like edges and textures, the higher layers combine these information to identify objects and patterns with more intricate details. One of the main reasons why CNNs are very good at image processing is because of this hierarchical feature extraction.

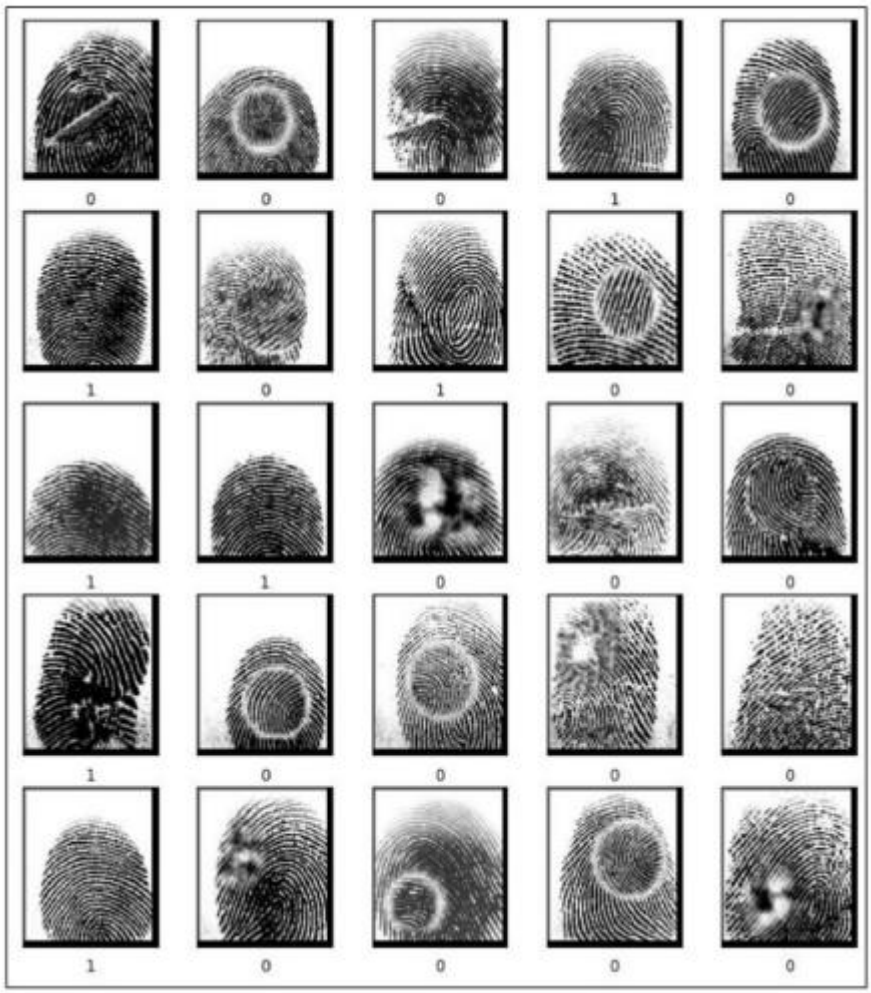

Fig 2: Final representation of this study

Table 1: Sequential Model

Layer (type)	Output Shape	Param #
conv2d (Conv2D)	(None, 101, 94, 32)	896
(None, 101, 94, 32)	(None, 50, 47, 32)	0 D)
conv2d_1 (Conv2D)	(None, 48, 45, 64)	18496
max_pooling2d_1 (MaxPooling)	(None, 24, 22, 64)	0 g2D)
conv2d_2 (Conv2D)	(None, 22, 20, 64)	36928
Total params	56320 (220.00 KB)	
Trainable params	56320 (220.00 KB)	
Non-trainable params	0 (0.00 Byte)	

Level One Convolutional Layer

This first layer of the network where a Conv2D implementation is used forms this layer. Dominantly, this first convolutional layer is utilized in the process of feature extraction from the input picture. In this layer the 32 3x3 pixel convolutional filters operated on the input picture. With this setup, the network can start learning and identifying the basic picture elements.

Feature and Shape Maps for Output

The sizes of the output feature maps differ with the input picture sizes after the convolution operations are carried

out. Specifically, the feature maps was resized from the input dimension of 199?94 pixels down to 101?94. The convolutional method usually leads to such decrease which may be due to padding schemes or filters involved in it. However, the depth which is proportional to the quantity of feature channels is higher and goes up to 32. By getting 32 different feature maps out, it is seen that the dimension has improved to contain the input image edges, textures, and other peculiarities.

Opt for Convolutional

First, 32 filters move over the fragments of the input picture while calculating dot products additionally during the process of convolution. Feature maps that distinguish different parts of the picture with certain features are produced by this method. The filters are thus aimed at selecting diverse aspects for features like texture, pattern, and edge that are further useful in understanding the images.

Learned Parameters

The layer is composed of 896 parameters, all of which correspond to weights and biases for the convolutional filters. All of these are learned by the network while being trained. It is actually through these weights that the filters are defined to respond to different visual features, while the output from the convolutional operation is further fine-tuned using the biases. Training the network to optimize these parameters enhances its performance, making it better at extracting useful characteristics from input photos.

Key Performance Metrics Overview of

The attached metrics for your study show that the recommended system is excellent in performance. There are four vital metrics when it comes to comprehending and making an evaluation on a classification system or a machine learning model; the F1-score, recall, accuracy, and precision.

Accuracy

Accuracy An important validation set of the model. With 99.22%, the model is also very close to the system that classifies the huge input numbers correctly, which will in effect make results from the system trustable and will contribute positively regarding user satisfaction. Precision

Precision

Precision measures how accurate the model's positive predictions are. It is just amazing how this system can differentiate between what is to be expected as a positive and what is actually positive, as it holds a 98.24% precision level. This means the model is very sure to be correct in making a positive prediction for any use cases that pose high negativity on false positives.

Bring to mind

Recall would explain how the model performs on finding all real occurrences because it is sensitive to the true positive. The model would have good effectiveness if it has an approximate 98.87% recall rate of capturing the real major positive instances. High recall in applications where it needs comprehensive detection would ensure that the system captures all major positive instances.

First-Level Scoring

The F1-score is then the harmonic mean of the two values and thus gives a balance between recall and accuracy to evaluate two measures. An F1-score of 98.56% would mean the system maintains a balance between the two measures without letting any one of them be too high or too low. Any application where both recall and accuracy affect the net performance must ensure this balance.

Relationship to human-computer interaction and product design

These metrics shed light on performance of the system in real-world scenarios, which is a property important for HCI and design methods. High system accuracy and balanced precision and recall can be interpreted as suggesting reliability and that user demands are effectively met. A system that classifies its input correctly and makes fewer mistakes is likely to please consumers. On that basis, the system may gain users' trust and confidence, proving to be a robust and user-friendly solution.

Conclusion The design, functionalities and user experiences of the software systems can further branch out with the amalgamation of the HCI concepts, very well imbibed programming tools and state-of-the-art considerate graphical design techniques. Developers, however, can derive high-end feature creation, system acceleration, and faster iterations and refinements—all these are very well possible with the modern frameworks, libraries, and technologies that developers can use.

It's interesting, easy, and provocative to use interfaces following HCI principles. Impressive metrics of your research demonstrate how vital such evidence is for high-performance results in the area of study. These metrics answer how proficient the system is in fulfilling the user requirements and enhancing their software usage.

Even at the very frontiers of technological advance, developing new, user-centered software solutions will always require the wedding of HCI with complicated programming tools. This way, systems can be developed that meet, but also help in the prognosis of continuously changing needs of stakeholders and users, ensuring efficiency and relevance in this dynamic environment.

4. Conclusion

The research is focused on the construction of a more advanced framework in order to improve interactions between users and digital systems. One will show in this research that good performance of the system can be achieved using pre-trained state-of-the-art convolutional neural networks with near-perfect metrics in recall, accuracy, and precision. These results make the framework more generalizable and resilient compared to the most conventional bimodal fingerprint recognition methods.

It is important to apply advanced machine learning methods while making a trustworthy, easy-to-use computer interface. Showing how the framework can improve interaction efficiency and user experience, this article calls for the adoption of cutting-edge technologies that would propel future developments in the industry. The methodology is an integral part of making efficient systems that could adjust to the evolving demands of its users.

References

Primary sources:

"Design and development of software framework to improve-Human Computer interaction". Thesis submitted by ISHRAT BEGUM". Mangalayatan University, Beswan, Aligarh, 2024. Unpublished thesis.

Secondary sources:

[1] Harvard University. (n.d.). *Technology factsheet series: Internet of things*. Belfer Center for Science and International Affairs. https://www.belfercenter.org/sites/default/files/2019-06/TechFactSheet/iot%20-%205.pdf (Accessed on June 30, 2021).

[2] Bera, B., Das, A. K., Balzano, W., & Medaglia, C. M. (2020). On the design of biometric-based user authentication protocol in smart city environment. *Pattern Recognition Letters, 138*, 439–446. https://doi.org/10.1016/j.patrec.2020.08.004

[3] Swamy, S. N., Jadhav, D., & Kulkarni, N. (2017). Security threats in the application layer in IoT applications. In *Proceedings of the International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)* (I-SMAC) (pp. 477–480). IEEE. https://doi.org/10.1109/I-SMAC.2017.8058300

[4] Trnka, M., Cerny, T., & Stickney, N. (2018). Survey of authentication and authorization for the Internet of Things. *Security and Communication Networks*. https://doi.org/10.1155/2018/4829042

[5] Verizon. (n.d.). *Data breach investigations report*. Verizon Enterprise. https://enterprise.verizon.com/resources/reports/dbir/ (Accessed on June 30, 2021).

[6] Fernandes, E., Rahmati, A., Eykholt, K., & Prakash, A. (2017). Internet of things security research: A rehash of old ideas or new intellectual challenges? *IEEE Security & Privacy, 15*(4), 79–84. https://doi.org/10.1109/MSP.2017.3151330

[7] Lin, H., & Bergmann, N. W. (2016). IoT privacy and security challenges for smart home environments. *Information, 7*(3), 44. https://doi.org/10.3390/info7030044

[8] Ometov, A., Petrov, V., Bezzateev, S., Andreev, S., Koucheryavy, Y., & Gerla, M. (2019). Challenges of multi-factor authentication for securing advanced IoT applications. *IEEE Network, 33*(2), 82–88. https://doi.org/10.1109/MNET.2019.1800271

[9] Gupta, S., Buriro, A., & Crispo, B. (2018). Demystifying authentication concepts in smartphones: Ways and types to secure access. *Mobile Information Systems*. https://doi.org/10.1155/2018/7363294

[10] Bonneau, J., Herley, C., Van Oorschot, P. C., & Stajano, F. (2012). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *Proceedings of the Symposium on Security and Privacy* (pp. 553–567). IEEE. https://doi.org/10.1109/SP.2012.44

[11] Gamundani, A. M., Phillips, A., & Muyingi, H. N. (2018). An overview of potential authentication threats and attacks on Internet of Things (IoT): A focus on smart home applications. In *Proceedings of the International Conference on Internet of Things (iThings)* (pp. 50–57). IEEE. https://doi.org/10.1109/iThings/GreenCom/CPSCom/SmartData.2018.00025

[12] Antonakakis, M. (2017). Understanding the Mirai botnet. In *Proceedings of the 26th USENIX Security Symposium* (pp. 1093–1110). https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis

[13] Katsini, C., Belk, M., Fidas, C., Avouris, N., & Samaras, G. (2016). Security and usability in knowledge-based user authentication: A review. In *Proceedings of the 20th Pan-Hellenic Conference on Informatics* (pp. 1–6). IEEE. https://doi.org/10.1109/PCI.2016.7740607

[14] Tsai, C.-L., Chen, C.-J., & Zhuang, D.-J. (2012). Secure OTP and biometric verification scheme for mobile banking. In *Proceedings of the 3rd FTRA*

International Conference on Mobile, Ubiquitous, and Intelligent Computing (pp. 138–141). https://doi.org/10.1109/MUIC.2012.61

[15] Gorodnichy, D., Yanushkevich, S., & Shmerko, V. (2014). Automated border control: Problem formalization. In *Proceedings of the IEEE Symposium on Computational Intelligence in Biometrics and Identity Management* (pp. 118–125). IEEE. https://doi.org/10.1109/CIBIM.2014.7015445

[16] Derawi, M. O., Nickel, C., Bours, P., & Busch, C. (2010). Unobtrusive user authentication on mobile phones using biometric gait recognition. In *Proceedings of the 6th International Conference on Intelligent Information Hiding and Multimedia Signal Processing* (pp. 306–311). https://doi.org/10.1109/IIH-MSP.2010.88

[17] Kumar, A. (2012). Can we use minor finger knuckle images to identify humans? In *Proceedings of the IEEE 5th International Conference on Biometrics: Theory, Applications and Systems* (pp. 55–60). https://doi.org/10.1109/BTAS.2012.6374566

[18] Sathik, M. M., & Sofia, G. (2011). Identification of student comprehension using forehead wrinkles. In *Proceedings of the International Conference on Computer, Communication and Electrical Technology* (pp. 66–70). https://doi.org/10.1109/ICCCET.2011.5762451

[19] Jain, A. K., & Klare, B. (2011). Matching forensic sketches and mug shots to apprehend criminals. *Computer, 44*(5), 94–96. https://doi.org/10.1109/MC.2011.147

[20] Von Zezschwitz, E., De Luca, A., Janssen, P., & Hussmann, H. (2015). Easy to draw, but hard to trace? On the observability of grid-based (Un)lock patterns. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (pp. 2339–2342). https://doi.org/10.1145/2702123.2702202

[21] Patrick, A. S. (2004). Usability and acceptability of biometric security systems. In *Proceedings of the Financial Cryptography Conference* (pp. 105–107). https://doi.org/10.1007/978-3-540-27809-2_11

[22] Theofanos, M. F., Micheals, R. J., & Stanton, B. C. (2009). Biometric systems include users. *IEEE Systems Journal, 3*(4), 461–468. https://doi.org/10.1109/JSYST.2009.2039074

[23] Theofanos, M., Stanton, B., Micheals, R., & Orandi, S. (2007). Biometric systematic uncertainty and the user. In *Proceedings of the 1st IEEE International Conference on Biometrics: Theory, Applications, and Systems* (pp. 1–6). https://doi.org/10.1109/BTAS.2007.4401920

[24] Zimmermann, V., & Gerber, N. (2017). 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* (pp. 265–283). Springer, Cham. https://doi.org/10.1007/978-3-319-58460-7_19

[25] Wong, R., Poh, N., Kittler, J., & Frohlich, D. (2010). Towards inclusive design in mobile biometry. In *Proceedings of the 3rd International Conference on Human System Interaction* (pp. 267–274). https://doi.org/10.1109/HSI.2010.5514537

[26] Poh, N., Blanco-Gonzalo, R., Wong, R., & Sanchez-Reillo, R. (2016). Blind subjects faces database. *IET Biometrics, 5*(1), 20–27. https://doi.org/10.1049/iet-bmt.2015.0037

[27] Stanton, B., Theofanos, M., & Sheppard, C. (2008). A study of users with visual disabilities and a fingerprint process. NIST, Gaithersburg, MD, USA. *NISTIR 7484*. https://doi.org/10.6028/NIST.IR.7484

[28] Sasse, M. A., & Krol, K. (2013). Usable biometrics for an ageing population. In *Age Factors in Biometric Processing*. Stevenage, U.K.: IET. https://doi.org/10.1049/PBSE003E

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

[30] Sanchez-Reillo, R., Blanco-Gonzalo, R., Liu-Jimenez, J., Lopez, M., & Canto, E. (2013). Universal access through biometrics in mobile scenarios. In *Proceedings of the 47th International Carnahan Conference on Security Technology* (pp. 1–6). IEEE. https://doi.org/10.1109/CCST.2013.6922038

[31] Blanco-Gonzalo, R., Lunerti, C., Sanchez-Reillo, R., & Guest, R. M. (2018). Biometrics: Accessibility challenge or opportunity? *PLoS One, 13*(3), e0194111. https://doi.org/10.1371/journal.pone.0194111