Emerging Biometric Technologies for Automated Border Control Gates

Ruggero Donida Labati, Angelo Genovese, Enrique Muñoz, Vincenzo Piuri, Fabio Scotti, and Gianluca Sforza [1]
1) Università degli Studi di Milano, via Bramante 65, 26013 Crema, IT;
email: name.surname@unimi.it; Web address: https://homes.di.unimi.it/surname

Abstract: *Automated Border Control (ABC) gates, or shortly e-Gates, are systems able to verify automatically the identity of the travelers through the biometric traits, and to grant passage of the border. Biometric technologies make the clearance automation possible, with a positive impact on efficiency, effectiveness, security, and usability of the process. The e-Gate compares biometric data of the traveler from an electronic document against live acquisitions, using different biometric traits. The face emerged in this area as the primary trait used by the e-Gates, with fingerprint and iris more adopted in registered traveler programs. This paper analyzes the main biometric aspects relating to both the human-machine interaction and the technologies used for ABC, and presents the emerging solutions that can produce a performance enhancement.*

***Keywords*:** ABC gates, e-Gates, biometrics, performance evaluation, usability, emerging techniques

1. INTRODUCTION

The ever-growing traffic of passengers worldwide, especially by air transportation [1], requires to strengthen the resources of the Border Crossing Points (BCP) for passenger immigration clearance. In particular, BCPs should increase their throughput in meeting the border crossing requests, while maintaining or even improving the overall security of the clearance process, typically conducted manually by the border guards. Increasing the throughput capability of a BCP would also improve the traveler experience with border check.

Automated Border Control (ABC) refers to the use of information and communication technologies able to verify the identity of travelers crossing the borders at BCPs automatically, i.e., without a constant human intervention [2]. E-Gates are those systems that perform this task in a stand-alone manner or with the support of kiosks for pre-enrolment. By exploiting the biometric traits of the travelers, e-Gates can verify their identity and grant them permission to cross the border. Biometric technologies are emerging for the automated verification of the traveler's identity, and are thus earning themselves a central role in ABC.

The deployment of e-Gates is growing in recent years, and always more countries throughout the world are adopting such systems. Moreover, research projects on ABC are running; for example, ABC4EU [3] and FastPass [4] involve industry and academy to develop a harmonized framework for ABC systems across Europe, employing state-of-the-art biometric techniques. This trend goes hand in hand with the spread of electronic travel documents, such as electronic passports and ID cards. These documents, which store biometric samples of the owner, enable the use of e-Gates without the need of pre-enrolment. Typically, a face image is saved in the document, together with the fingerprints optionally. As an alternative, travelers can enroll in a Registered Traveler Program (RTP), in which case the biometric samples are saved in central databases. Fingerprint and iris are both widely used in RTPs.

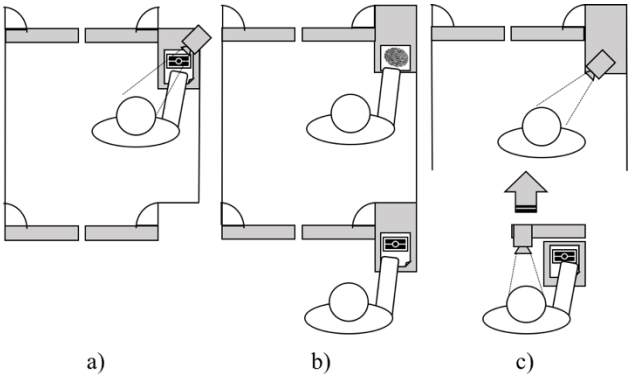

Figure 1 Different topologies of e-Gates: a) one-step; b) integrated two-step; c) segregated two-step.

This paper gives an overall view of ABC and its biometric base, and discusses the biometric technologies emerging to enhance the performance. The paper is structured as follows. Section 2 presents the typical steps performed at an e-Gate. Section 3 describes the main biometric technologies employed in ABC. Section 4 presents the characteristics of real e-Gates deployed. Section 5 discusses the techniques emerging in ABC to enhance the performance, considering both human and machine aspects. Section 6 summarizes the conclusions.

2. ABC WORKFLOW

Typically, an e-Gate checks on the face of the travelers to grant them border crossing. This process involves three main steps: 1) Authentication of the electronic travel document; 2) Face verification of the traveler's identity against data in the document; 3) Check on central databases (e.g., watch lists) for crossing authorization. When verification is not successful and the traveler cannot pass the automated gate, the traditional manual control occurs. A border officer supervises the whole process remotely.

The automated process requires that the traveler holds an electronic Machine Readable Travel Document (e-MRTD), which contains the biometric samples. Typically, this is an electronic passport compliant to the specifications of International Civil Aviation Organization (ICAO) [5] and commonly referred to as an e-Passport, which features only the face image (the first generation), or face and fingerprint images (the second generation).

An e-Gate is made of interconnected subsystems, which make use of both hardware and software components. Every subsystem is in charge of a different task [6]: checking the validity of the travel document, verifying the identity of the traveler through a biometric comparison, interfacing with external databases and with border guards oversighting the e-Gate's functioning.

Typically, the components of an e-Gate are [2]: one or two physical barriers, an e-Passport scanner, a monitor to display instructions and feedback to the traveler, the biometric acquisition devices, and hardware and software for managing the system, including the communication with external systems with a connection to border control. The clearance process is conducted as a one-step or a two-step process, based on whether document and identity verification are separated steps or not [2]. The two steps can either be integrated into a single e-Gate, or segregated into a pre-enrollment kiosk for identity verification, and the e-Gate itself for actual border crossing (see Figure 1).

When needed, the e-Gate queries external databases to verify the eligibility of the traveler for border crossing. These databases contain information about visa, registered travelers, individuals that require close surveillance, and entry-exit events.

3. BIOMETRIC TECHNOLOGIES IN ABC

The biometric verification of identity, known also as biometric identification, is an automated process for recognizing a person by means of the measure of physiological or behavioral traits [7]. ICAO has selected the face as the primary biometric trait to include into e-Passports, and the fingerprint and iris as optional traits [8]. The face offers many advantages, for instance it is socially accepted, capture is not intrusive, and border guards are familiar with it. The standard ISO/IEC 19794-5 [9] defines the quality requirements for a face image to be recorded in travel documents, which are not always attended [10]. Often, methods for face recognition are based on distinctive facial features such as the eyes, mouth, nose, and other fiducial points, and on their geometric relations [11] [12]. Problems relative to illumination, pose and expression, as well as to the image resolution, cause a reduction of the face recognition performance.

Fingerprint is an optional biometric in e-Passports; second generation gives the possibility to store this data in addition to face. The fingerprint trait offers high recognition accuracy and good social acceptance. The standard ISO/IEC 19794-4 [9] defines quality specifications about the fingerprint data an e-Gate expects to read from an e-MRTD. Very popular in fingerprint recognition is the analysis of the discontinuities in the ridge structure of the fingertip, called minutiae points [13], particularly of their position and orientation. Problems related to ergonomics of the sensor, fingertip skin conditions (either temporary like dirt and moisture, or permanent) [14], hygiene perception, and latent fingerprints on the sensor, may decrease the performance of the biometric recognition.

Iris is also an optional data in e-Passports. It offers very high accuracy and speed of recognition, but acceptance of the people in using it decreases, as the capture is perceived as more intrusive than with other traits. Useful in countries were face can be partially covered because of traditional habits. The standard properties of an iris image to be recorded in an e-Passport are specified by ISO/IEC 19794-6 [9]. Distinctive texture features are extracted from the iris pattern and successively used for recognition [15]. Problems of illumination, involuntary eye movements, usability and confidence in the acquisition machinery may affect the iris recognition performance.

The multibiometric approach fuses multiple biometric data, also from different modalities –e.g., face and fingerprint. Increasing the biometric evidence available offers many advantages on accuracy, usability and security of the biometric component, when compared with monomodal systems [16]. However, an increased amount of sensible information required by the e-Gate poses more privacy concerns, both in terms of data protection and in the perception of the traveler. The use of multibiometric for access control at the BCPs is favored by the growth of second generation e-Passports –containing both fingerprint and iris—in circulation today. Multibiometric e-Gates are already operative, as in some European and Asian airports [17] [18].

4. E-GATE DEPLOYMENTS

Today, e-Gates are mainly used at airports but they are starting to be present also at sea and land borders. Worldwide, more than 180 airports deployed and regularly use the automated biometric gates [19]. In particular, 45% of them implement face recognition, while the 56% use fingerprint as biometric trait, and the 12% the iris. Fingerprint and iris recognition is especially adopted to check on registered travelers. The 12% of the deployments considered by this statistic supports more than one biometric modality to process the border crossing requests. The performance requirements of the biometric recognition algorithms run by an e-Gate are quite demanding, given the security level expected. They can be measured in terms of False Accept Rate (FAR) and False Reject Rate (FRR), which represent the proportion of travelers incorrectly admitted and not admitted to cross the border, respectively [20]. A false accepted traveler means a security fall of the system and a potential threat to security. On the contrary, a false rejected traveler increases the processing time and the resources required, and causes frustration on the traveler too. For e-Gates, the foreseen FAR should be lower than 0.1%, while the FRR lower than 5% for face and lower than 3% for fingerprint [21].

It is worth noting that the performance evaluation of the biometric component of an e-Gate should not only include technical factors, related to the algorithm, but also behavioral human factors. In fact, more experienced travelers may be more successful at the e-Gate than the novices, because they learnt how to use the system properly [22]. People reluctant to use the systems, e.g., for a prior negative experience or privacy concerns, are likely to produce more errors when use the system, or even decide not to use it.

In relation to the biometric component of ABC deployments, real performance data in terms of FAR and FRR are rarely made available to the public. Also, the FAR is actually difficult to assess in a real operational scenario. However, the use of automated checks in the long-term may produce better performance, both in terms of biometric verification and of the final BCP throughput.

5. EMERGING SOLUTIONS TO CENTRAL ASPECTS OF ABC

Despite of the spreading of ABC, the actual uptake of this new technology on travelers is not yet fully satisfactory, owing to personal inclinations of the people towards technology and lack of awareness, or to the characteristics of the machines used [23]. In this section, we analyze the impact of challenging aspects, regarding both human-machine interaction (HMI) and technology, on the performance of an ABC system, presenting emerging solutions that can improve its functioning. Figure 2 groups the concepts presented in the form of a mind map.

Travelers not aware of this new technology, who are resistant or even excluded from its access, cause a lack of ABC usage. Consistency with previous processes would help the uptake, producing more confidence in the novelty and requiring less effort from the users. As time goes on and e-Gates become more advertised and visible as part of ordinary border clearance, more and more people may approach them, thus making ABC more effective. However, increased use of ABCs does not necessarily mean that the BCP throughput will increase unless travelers first gain sufficient experience on its use (learning curve). Familiarization with this new technology will be essential in order to increase the actual capacity of border clearance.

Some aspects particularly contribute to this purpose; they are usability and privacy [23] [24]. Several measures can be adopted to improve usability, which can make these systems more accepted and inclusive. These measures include an easy and more intuitive interaction with the e-Gate, particularly with the document and the biometric readers. Research is progressing on the design of less-intrusive technologies for biometric recognition, such as touchless fingerprint and palmprint recognition, and iris recognition at a distance. These technologies include the design of appropriate acquisition devices, e.g., scanners and cameras, and dedicated software. They can serve to perform biometric verification under less controlled conditions, e.g., at higher distances, with natural light, or while the traveler is moving. Touchless technologies, above touch, meet the preference of the users [25], and can be a better solution in terms of hygiene, because of the absence of contact with surfaces [26]. There is a wide literature on touchless solutions based on fingerprint [27] and palmprint [28]. Regarding the iris recognition, besides exploitation of traditional images, iris acquisition on the move was also considered [29]. However, less constrained approaches to biometric acquisition are not much deployed in ABC gates yet.

Usability is a fundamental aspect to consider in designing the access and interaction with the e-Gates of people that have difficulties in their movements or in vision, caused for example by ageing [30]. Mobile scanners [31] and algorithms [32] [33] that can work in non-ideal conditions of the samples acquired are practical solutions that could help to reach more flexibility and robustness in biometric identification.

The introduction of biometric data, along with biographic data, in border checks, requires new measures of data protection. Biometrics are personal data that cannot be changed once stolen. Users then may need to be assured about the privacy measures adopted by the e-Gate operator

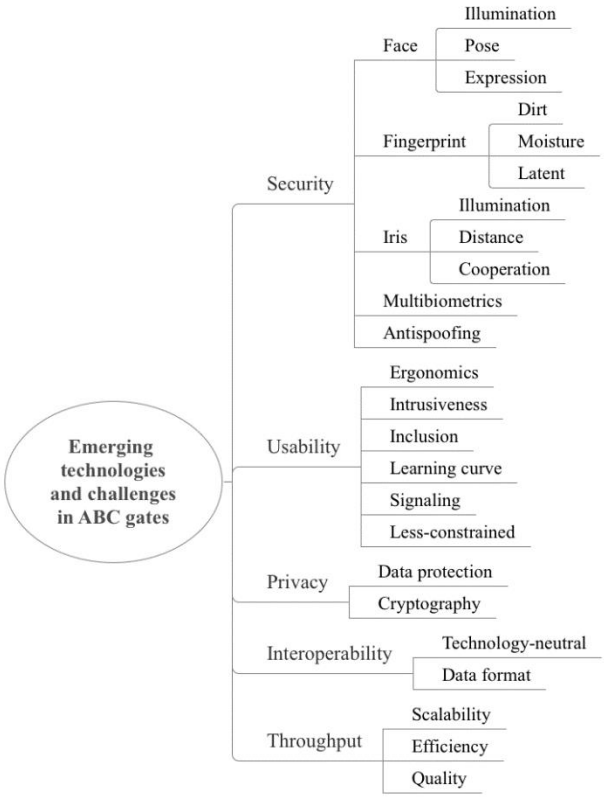

Figure 2 Main challanges and emerging technologies in current ABC systems.

and the document provider, for increasing their confidence in ABC [23]. For this reason, national legislations limit the collection of personal data strictly to the period that data is effectively used, and data logs for monitoring the quality of the system is saved after being anonymized. As concerns biometric data, the adoption of template of features extracted from the sample, rather than the original sample, and cryptographic techniques, helps to protect privacy in data storage and communication [34] [35].

From the technological point of view, the performance and capacity of e-Gates can improve by facing some challenging aspects, related to security, interoperability with different technologies, biometric performance. In particular, are important aspects the anti-spoofing techniques, the compatibility between systems, the scalability of biometric systems, the capture of higher quality face and fingerprint images, and the use of multibiometrics. [36].

The development of better anti-spoofing techniques for liveness detection is important to detect possible attacks to the biometric system while accepting legitimate verification attempts. Such kind of attacks include presentation to the biometric sensor of printed face images [37], fake fingers made of silicone [38], or synthetic irises [39].

ABC systems are made of several collaborating. subsystems [6]. To favor the exchange of biometric information, common rules will be used, regarding data format [9], type of data exchanged (whether the whole sample or the reduced template) [40], and eventually cryptography schemes [35].

ABC systems potentially operate with large

populations of users. Because the biometric component is central in ABC, the design of scalable biometric systems [41] is needed to effectively support such a requirement.

A successful biometric recognition depends to a great extent from the quality of the sample acquired. Enhancing the features of the acquisition devices (e.g., camera resolution) and their ergonomics (e.g., presence of multiple cameras for face, placement of fingerprint readers at the right height), creating the best environmental conditions (e.g., uniform illumination and background for face, or air sufficiently humid for fingerprint), instructing the user to an effective interaction with the sensors by proper signaling (e.g., about pose and facial expression, or pressure of the finger), and designing algorithms that are effective to evaluate the quality of the samples acquired, all contribute to reach this objective [10] [14].

To further increase the matching performance of a biometric system, a well-known approach is using multiple biometrics [42] [43]. Some ABC deployments already use this approach, obtaining significant improvements of the accuracy of recognition [18]. Using multiple biometric sources has positive effects also on usability and resistance to attacks of the system [44], as well as to compensate non-universality of the biometric trait employed, and low discriminability of some traits [45]. There are different ways of performing multibiometric recognition, exploiting either information from different modalities (i.e., fingerprint and face), from multiple samples of the same trait, or from multiple features of the same sample. For example, the fingerprint images contain information at three levels, namely, Level 1 (pattern), Level 2 (minutiae points) and Level 3 (pores and ridge shape), which can be combined to enhance recognition [46]. In ABC, the use of a second modality can be a backup solution, in case the first modality is difficult to capture, or fused, following different schemes [47]. Given the characteristics of e-Gates, fusing the matching scores obtained by the comparison of every biometric allows fusion to be independent from the technology installed. Because of the many positive effects previously illustrated, multibiometrics is slowly emerging also in ABC. However, the added complexity of multiple biometrics could render the systems costly and difficult to maintain, while the privacy concerns of the users might increase [48].

Having ABC systems more performant, easy to use, and privacy respectful would be of stimulus on the travelers to use the e-Gates instead of the manual clearance.

6. CONCLUSION

The paper gives a brief overview of ABC to the reader, describing the biometric aspects on which it is based, and discussing the values that brought some technologies to emerge in current deployments, as well as their intrinsic drawbacks. The paper presents also the emerging solutions in biometrics for improving the current performance of the e-Gates both from the HMI and the technological side.

7. ACKNOWLEDGMENT

This work was supported in part by: the EC within the 7FP under grant agreement 312797 (ABC4EU); the EC within the H2020 program under grant agreement 644597 (ESCUDO-CLOUD).

8. REFERENCES

[1] Boeing, *Current market outlook: 2014-2033*, 2014.

[2] Frontex Agency, "Best practice operational guidelines for automated border control (ABC) systems," 2012.

[3] "ABC4EU - EU FP7 Project," 2014. [Online]. Available: http://abc4eu.com/.

[4] "FastPass - EU FP7 Project," 2013. [Online]. Available: https://www.fastpass-project.eu/.

[5] ICAO, "Doc 9303, machine readable travel documents (7th ed.), part 9," 2015.

[6] R. Donida Labati, A. Genovese, E. Muñoz, V. Piuri, G. Sforza and F. Scotti, "Advanced design of automated border control gates: biometric system techniques and research trends," in *Proc. of the IEEE Int. Symp. on Systems Engineering*, 2015.

[7] S. Z. Li and A. K. Jain, Eds., Encyclopedia of Biometrics, Springer, 2015.

[8] International Civil Aviation Organization (ICAO), "Doc 9303, machine readable travel documents, part 1, vol. 2," 2006.

[9] ISO/IEC, *ISO/IEC 19794 (all parts): Biometric data interchange formats*, 2011.

[10] L. J. Spreeuwers, A. J. Hendrikse and K. J. Gerritsen, "Evaluation of automatic face recognition for automatic border control on actual data recorded of travellers at Schiphol airport," in *Proc. of the Int. Conf. of the Biometrics Special Interest Group*, 2012.

[11] R. Jafri and H. R. Arabnia, "A Survey of Face Recognition Techniques," *Journal of Information Processing Systems*, vol. 5, no. 2, pp. 41-68, 2009.

[12] J. Sanchez del Rio, C. Conde, A. Tsitiridis, J. R. Gomez, I. M. de Diego and E. Cabello, "Face- based recognition systems in the ABC e-gates," in *Proc. of the Annual IEEE Int. Systems Conference*, 2015.

[13] D. Maltoni, D. Maio, A. K. Jain and S. Prabhakar, Handbook of fingerprint recognition (2nd ed.), Springer, 2009.

[14] R. Donida Labati, A. Genovese, E. Muñoz, V. Piuri, F. Scotti and G. Sforza, "Automatic classification of acquisition problems affecting fingerprint images in automated border controls," in *Proc. of the IEEE Workshop on Computational Intelligence in Biometrics and Identity Management*, 2015.

[15] J. Daugman, "Iris recognition at airports and border crossings," in *Encyclopedia of Biometrics*, S. Li and A. Jain, Eds., Springer, 2015, p. 998–1004.

[16] A. Ross, K. Nandakumar and A. Jain, Handbook of Multibiometrics, Springer, 2006.

[17] R. Donida Labati, A. Genovese, E. Muñoz, F. Scotti, V. Piuri and G. Sforza, "Biometric recognition in automated border control: a survey," *ACM Computing Surveys. To appear*, 2016.

[18] D. Cuesta Cantarero, D. Perez Herrero and F. Martin Mendez, "A multi-modal biometric fusion implementation for ABC systems," in *Proc. of the IEEE Intelligence and Security Informatics Conference*, 2013.

[19] IATA, "Automated Border Control," 2016. [Online]. Available: http://www.iata.org/whatwedo/stb/maps/Pages/automated-border-control.aspx.

[20] National Science & Technology Council - Subcommittee on Biometrics, "Biometric testing and statistics," 2006.

[21] Frontex Agency, "Best practice technical guidelines for automated border control (ABC) systems," 2012.

[22] V. MacLeod and B. McLindin, "Methodology for the Evaluation of an International Airport Automated Border Control Processing System," in *Innovations in Defence Support Systems - 2*, L. C. Jain, E. V. Aidman and C. Abeynayake, Eds., 2011, p. 115–145.

[23] A.-M. Oostveen, "Non-use of Automated Border Control Systems: Identifying Reasons and Solutions," in *Proc. of the Int. British Human Computer Interaction Conference*, 2014.

[24] M. A. Sasse, "Red-eye blink, bendy shuffle, and the yuck factor: A user experience of biometric airport systems," *IEEE Security & Privacy*, vol. 5, no. 3, p. 78–81, 2007.

[25] R. Donida Labati, A. Genovese, V. Piuri and F. Scotti, "Toward unconstrained fingerprint recognition: a fully-touchless 3-D system based on two views on the move," *IEEE Trans. on Systems, Man, and Cybernetics: Systems*, vol. 46, no. 2, pp. 202-219, 2016.

[26] M. El-Abed, R. Giot, B. Hemery and C. Rosenberger, "A study of users' acceptance and satisfaction of biometric systems," in *Proc. of the IEEE Int. Carnahan Conf. on Security Technology*, 2010.

[27] R. Donida Labati, V. Piuri and F. Scotti, Touchless Fingerprint Biometrics, CRC Press, 2015.

[28] A. Genovese, V. Piuri and F. Scotti, Touchless Palmprint Recognition Systems, Springer, 2014.

[29] J. Matey, O. Naroditsky, K. Hanna, R. Kolczynski, D. LoIacono, S. Mangru, M. Tinker, T. Zappia and W. Zhao, "Iris on the move: acquisition of images for iris recognition in less constrained environments," *Proc. of IEEE*, vol. 94, no. 11, p. 1936–1947, 2006.

[30] M. A. Sasse and K. Krol, "Usable biometrics for an ageing population," in *Age Factors in Biometric Processing*, M. Fairhurst, Ed., Institution of Engineering and Technology, 2013, p. 303–320.

[31] "MobilePass - EU FP7 Project," 2014. [Online]. Available: http://mobilepass-project.eu/.

[32] R. Abiantun, U. Prabhu and M. Savvides, "Sparse feature extraction for pose-tolerant face recognition," *IEEE Trans. on Pattern Analysis and Machine Intelligence*, vol. 36, no. 10, p. 2061–2073, 2014.

[33] C.-T. Chou, S.-W. Shih, W.-S. Chen, V. W. Cheng and D.-Y. Chen, "Non-orthogonal view iris recognition system," *IEEE Trans. on Circuits and Systems for Video Technology*, vol. 20, no. 3, p. 417–430, 2010.

[34] M. Barni, T. Bianchi, D. Catalano, M. Di Raimondo, R. Donida Labati, P. Failla, D. Fiore, R. Lazzeretti, V. Piuri, F. Scotti and A. Piva, "Privacy-preserving fingercode authentication," in *Proc. of the ACM Workshop on Multimedia and Security*, 2010.

[35] R. Donida Labati, V. Piuri and F. Scotti, "Biometric privacy protection: guidelines and technologies," in *Proc. of the Int. Joint Conf. on E-Business and Telecommunications*, vol. 314, M. Obaidat, J. Sevillano and J. Filipe, Eds., Springer, 2012, p. 3–19.

[36] R. Donida Labati, A. Genovese, E. Muñoz, V. Piuri, F. Scotti and G. Sforza, "Automated Border Control Systems: Biometric Challenges and Research Trends," in *Proc. of the Int. Conf. on Information Systems Security*, 2015.

[37] S. Marcel, M. Nixon and S. Li, Handbook of Biometric Anti-spoofing: Trusted Biometrics Under Spoofing Attacks, Springer, 2014.

[38] E. Marasco and A. Ross, "A survey on antispoofing schemes for fingerprint recognition systems," *ACM Computing Surveys*, vol. 47, no. 2, pp. 1-36, 2014.

[39] M. Burge and K. Bowyer, Handbook of Iris Recognition, Springer, 2013.

[40] Unisys, "Entry-exit feasibility study," 2008.

[41] M. Gamassi, V. Piuri, D. Sana, F. Scotti and O. Scotti, "Scalable distributed biometric systems - advanced techniques for security and safety," *IEEE Trans. Instrumentaion and Measurement*, vol. 9, no. 2, pp. 21-28, 2006.

[42] R. Snelick, M. Indovina, J. Yen and A. Mink, "Multimodal biometrics: issues in design and testing," in *Proc. of the ACM Int. Conf. on Multimodal Interfaces*, 2003.

[43] A. Ross, K. Nandakumar and A. Jain, Handbook of Multibiometrics, vol. 6, Springer, 2006.

[44] H. Wei, L. Chen and J. Ferryman, "Biometrics in ABC: counter-spoofing research," in *Proc. of the Frontex Global Conf. on Future Developments of Automated Border Control*, 2013.

[45] A. Jain and A. Ross, "Multibiometric systems," *Communications of the ACM*, vol. 47, no. 1, p. 34–40, 2004.

[46] A. Jain, Y. Chen and M. Demirkus, "Pores and Ridges: Fingerprint Matching Using Level 3 Features," in *Proc. of the Int. Conf. on Pattern Recognition*, 2006.

[47] ISO, "ISO/IEC TR 24722:2007, Multimodal and other multibiometric fusion," 2007.

[48] S. Cimato, M. Gamassi, V. Piuri, R. Sassi and F. Scotti, "Privacy-aware biometrics: design and implementation of a multimodal verification system," in *Proc. of the Annual Computer Security Applications Conference*, 2008.

[49] A. Genovese, E. Muñoz, V. Piuri, F. Scotti and G. Sforza, "Towards Touchless Pore Fingerprint Biometrics: A Neural Approach," in *Proc. of the Int. Joint Conf. on Neural Networks (accepted)*, 2016.