Advanced design of Automated Border Control gates: biometric system techniques and research trends

Ruggero Donida Labati, Angelo Genovese, Enrique Muñoz, Vincenzo Piuri, Fabio Scotti, Gianluca Sforza
Department of Computer Science, Università degli Studi di Milano, Italy.
Email: {ruggero.donida, angelo.genovese, enrique.munoz, vincenzo.piuri, fabio.scotti, gianluca.sforza}@unimi.it

***Abstract*—Last few years have witnessed an ever-increasing demand of border crossing, whose processing introduces the need to speed-up the clearance process at the Border Crossing Points (BCP). Automated Border Control (ABC) gates, or shortly e-Gates, can verify the identity of the travelers crossing the borders by exploiting their biometric traits, without the need of a constant human intervention. Biometric technologies have a relevant impact on the improvement of efficiency, effectiveness and security of the checking processes. Automated biometric recognition can increase the border processing throughput of the BCP, as well as facilitate the clearance procedures. To grant the passage of the border, the e-Gate compares the biometric samples of the traveler stored into the electronic document with live acquisitions. This paper presents the latest substantial advances in the design of e-Gates. In particular, it presents the Biometric Verification System in detail, including its hardware and software components, as well as the procedures followed during the biometric verification of the traveler's identity. We address the complex issue of measuring the performance of an ABC system, considering the real applicability of the figures of merit usually adopted in biometric system's evaluation. To complete the view of the current e-Gates, we highlight the main challenges and the research trends relating to the biometric systems currently used in e-Gates.**

I. Introduction

The global passenger traffic is constantly growing. The last forecasts, particularly for air transportation, expect a positive and constant increment in the next years [1]. International Border Crossing Points (BCP) should then increase their border processing throughput, without affecting the overall security of the border controls. The traditional identity verification process conducted by the border guards is subject to limitations of the security personnel, who may have problems dealing with time pressure and attacks to security (e.g., forged documents or the use of aliases) [2].The installation of Automated Border Control (ABC) systems that employ biometrics for identity recognition, constitutes an integral part of the solution [2], along with surveillance systems for monitoring [3].

Frontex, the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union, defines Automated Border Control (ABC) as "the use of automated or semi-automated systems which can verify the identity of travelers crossing the borders at BCPs, without the need for human intervention" [4]. These systems commonly referred to as ABC gates, or shortly e-Gates, basically perform three types of checks: 1) Authentication of the travel document; 2) Biometric verification of the traveler's identity; 3) Check on the traveler authorization to cross the border. Typically, the system captures live a facial image of the traveler, for a biometric 1:1 verification against the image stored on the e-Passport's chip. In some implementations, the system may check fingerprint or iris samples as additional biometric traits. If the recognition is successful then the gate opens, letting the traveler go through, otherwise the traveler is redirected to manual control. An officer in a remote station supervises the e-Gate during the whole process.

Regular e-Gates use an electronic machine readable travel document (e-MRTD), usually an ICAO compliant e-Passport, containing the biometric samples of the owner. First generation e-Passports features only the facial image, whereas the second generation supports two biometric modalities, face and fingerprint. The number of second generation e-Passports in circulation is continuously growing. This means that it will be possible to further increase the recognition accuracy thanks to the use of multiple biometric modalities [5]. At the present time, some multi-biometric systems are already operative, e.g., in Spanish and Italian airports [6], [7].

In Europe, passengers that are eligible for using the e-Gates are citizens of the European Union (EU) and other States taking part to the Schengen cooperation, who hold an e-Passport or a biometric e-ID card, and Third-Country Nationals (TCN) previously registered as Registered Traveller Programme (RTP) members [4], [8]. EU recommends the use of ABC systems to facilitate the control at borders of TCN who travel frequently in the Schengen area and to speed-up the external border crossing of European citizens with an e-Passport [9].

This paper focuses on the design of the Biometric Verification System (BVS), which occupies a central role in the overall ABC system: it is responsible for the traveler clearance through the verification of biometric traits. The paper is organized as follows: Section II presents the architectural design of the whole ABC system. Section III describes the components employed for processing the biometric data. Section IV discusses the techniques for evaluating the BVS performance and the related figures of merit. Section V presents the main challenges and research trends emerging in biometric systems for ABC. Section VI reports our main conclusions.

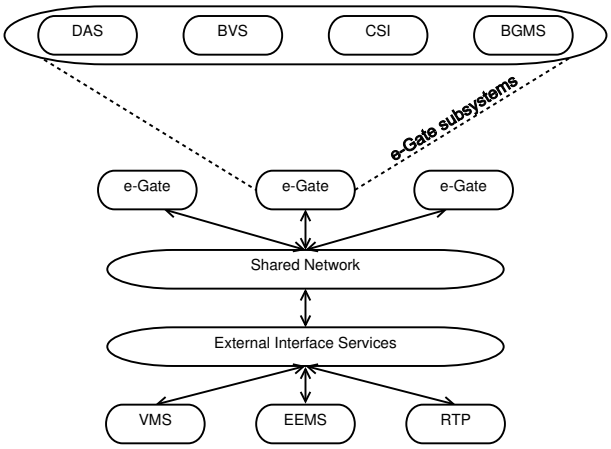

Fig. 1. Structure of an e-Gate and links to external systems. Abbreviations – BVS: Biometric Verification System, CSI: Central Systems Interface, DAS: Document Authentication System, BGMS: Border Guard Maintenance System, VMS: Visa Management System, EEMS: Entry-Exit Management System, RTP: Registered Traveler Program.

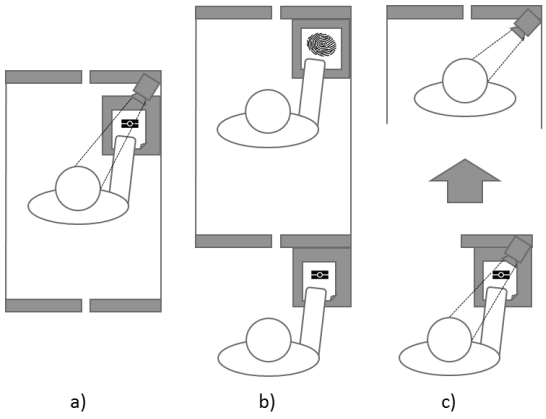

Fig. 2. Topologies of an e-Gate: a) one-step process; b) integrated two-step process; c) segregated two-step process. The depicted biometric traits represent examples of the traits potentially used at an e-Gate.

II. Architecture of the ABC system

An e-Gate deals with granting travelers entry to a country. The system receives in input the electronic travel document, the biometric samples of the traveler, and additional data from external systems (e.g., watch lists, visa or RTP information). The output of the system consists in granting or denying the border crossing to the passenger. The design of an e-Gate includes mainly four interconnected subsystems: Document Authentication System (DAS), Biometric Verification System (BVS), Central Systems Interface (CSI) and Border guard Maintenance system (BGMS). The DAS is in charge of checking the validity of the document and extracting the information contained in it, including information displayed in the Machine Readable Zone (MRZ) and stored in the chip. The BVS is responsible of verifying the identity of the traveler through the comparison of live images acquired at the e-Gate and information contained in the document. The CSI manages the interfaces with external systems (introduced in subsection II-A). The border-guards use the BGMS to monitor and control the ABC system. Fig. 1 presents the overall schema of an e-Gate.

A normal border crossing check is usually performed through the following steps:

1) e-Gate entry,
2) passport scanning & authentication,
3) extraction of data from the chip,
4) biometric identity verification,
5) request of data from external systems,
6) e-Gate exit.

Depending on their features, three generations of e-Gates arise in the current landscape [10]: the 1^{st} generation processes only registered travelers (e.g., PREVIUM in Netherlands, NEXUS in Canada); the 2^{nd} generation serves travelers with biometric eID / ePassports (e.g., several ABC systems in EU, Australia); and the 3^{rd} generation will be working in future (2020).

Typically, an e-Gate is made of these components associated to the clearance steps listed above [4]: one or two physical barriers, an e-Passport scanner for text recognition and chip reading, a monitor displaying instructions to the traveler, the biometric acquisition devices (one for each trait used) and the system management hardware and software, also for the communication with external systems. The clearance process may follow different logics, based on timing and location in which the document authentication and the BVS operate. To these logics there correspond different patterns of topological design for the e-Gates (illustrated in Fig. 2): one-step process, integrated/segregated two-step process [4].

In the *one-step process*, document and identity verifications happen in one single process, and the traveler performs all required actions inside the e-Gate. This configuration of the e-Gate can deliver a high speed clearance time, since the traveler can perform several actions in parallel. For example the e-Gate can capture the biometric samples while it authenticates the travel document. As a consequence, the e-Gate can deliver a higher throughput, provided that the traveler is well trained.

The *two-step process* clearly divides the ABC process into two distinct steps. During the first step, the DAS extracts the biometric information about the passenger from the electronic travel document. After that, the BVS checks this information against the live biometric data captured in the second step. The ABC system can integrate the two steps into a single e-Gate, or segregate them into a pre-enrollment kiosk for traveler verification and the e-Gate itself for border crossing. In any configuration, the first step produces a temporary token, which the second step uses to check the identity of the traveler. The two-step process provides a better control over the ABC process, even if slightly diminishing its throughput. It also improves the usability and reduces the risk of user errors, because it is easier to understand which tasks to perform at each time. This configuration can improve the security by pre-screening the passengers travel documents before they enter the e-Gate. The segregated two-step process, in particular, may be more flexible in how to occupy the floor space, whereas it permits to split the queues between the e-Gate and pre-enrollment kiosks. However, such an articulated process may be confusing for inexperienced travelers, who may not understand that they have to perform a clearance process divided into two linked sub-

processes. Initial costs of a segregated solution may be cheaper than fully-fledged integrated e-Gates, but they require more maintenance during their life cycle since they are composed by more machines.

A. External systems with an interface to the ABC system

E-Gates are part of a larger smart border infrastructure that many countries are developing. When applicable, the ABC system has to send database queries to external systems to verify the eligibility for border crossing of the traveler. These systems are: Visa Management System (VMS), Registered Traveler Program (RTP) and Entry-Exit Management System (EEMS). Fig. 1 shows the connections of an e-Gate to the external systems.

VMS refers basically to a central database that stores visa application data. These data include the biometric samples captured during the visa application, as well as personal information, details of the travel, and a track record of the previous visa applications. The European VMS database stores ten fingerprints and the facial image of the traveler, and keeps the visa application data for a maximum period of five years [11]. The ABC system usually performs a search in the VMS using the number of the visa sticker together with the fingerprints of the visa holder.

EEMS is a centralized database that registers the entry and exit of foreign nationals crossing the borders of a State. EEMS is meant to replace the current passport stamping procedure by electronic records, which include biometric data of the traveler. EEMS helps the border authorities to identify overstayers, and to collect reliable statistical information on the migration flows and overstaying patterns of foreign nationals, which is valuable to adjust immigration policies.

RTP is a voluntary enrollment system aimed at facilitating the border crossing of foreign national frequent travelers, e.g., travelers for business or family reasons. During the enrollment in RTP, the traveler is subject to an extensive pre-screening process. In addition, the system collects and stores the traveler's biometric samples in a central database. EU is discussing about the adoption of EES and RTP [12], [13], as illustrates the ongoing EU 7FP-funded projects ABC4EU (Automated Border Control Gates for Europe) and FastPass. These actions are investigating the necessary biometric data. One option is the use of the facial image and four fingerprints, which has a beneficial impact on verification in terms of speed and security.

Compatibility between systems is a key factor for their integration, which reflects on interfaces and data structures that the e-Gate and the external systems should use. In order to guarantee interoperability between systems, it is necessary to rely on a formal standard that defines an appropriate biometric data exchange format [14]–[16]. In addition, the type of information exchanged makes the difference: samples contain more information, and make the system more flexible with regard to feature extraction and matching algorithms. On the other hand, templates need less memory space, reduce the required communication bandwidth, and are more privacy compliant [17]–[23].

B. Development methodology of the BVS

The development of a BVS and its interactions with other systems is a very complex task [24]. Thus, designers generally adopt various development methods frequently used in systems engineering, e.g., sequential or incremental development methods [25]. In this section, we detail some of the techniques associated to the development process of a BVS, inspired by the techniques adopted within the project ABC4EU.

1) Analysis: This phase requires the definition of a domain conceptual model and of a business conceptual model. We propose to use Unified Modeling Language (UML) to create them. The domain conceptual model has to capture the significant entities within the BVS. The business conceptual model has to identify the high level business processes and to illustrate the processes that use the biometric dataset. Successively, it is necessary to extract a full set of requirements that include functional and non-functional requirements. The functional requirements should cover aspects like the configuration, and maintenance of the BVS, the user interface, or the ergonomics. The non-functional requirements should analyze aspects like the hardware equipment, the compliance with standards or the performance.

2) Design: This phase requires the definition of mainly four UML models: the use case model, the data model, the class model and the interface model. The use case model identifies the main actors and the biometric use cases. The data model describes the information that the BVS needs to store and retrieve. The class model introduces the classes that make up the final system. The user interface model presents a description of the graphic user interfaces and the signaling that the e-Gates will use to communicate with the users.

3) Implementation: This phase requires the use of an architectural pattern that permits to deal with the complexity of the BVS. The use of Service Oriented Architecture (SOA) [26] together with open standards provides many advantages since it permits to deploy services incrementally while simplifying the developing process. In particular, BioAPI (Biometric Application Programming Interface) [27] is a standard defined by ISO to support SOA systems that use biometric technology. This standard is the most commonly used for the development of BVSs.

4) Test: The performance analysis of a BVS is particularly challenging. Many issues can affect this phase, as privacy-protection laws or lack of information. In Section IV, we provide a thorough discussion about these issues and present the techniques typically used for performance estimation.

III. Components and procedures for acquisition and verification of the different biometric traits

ICAO defines three possible biometric traits, which are the most commonly used: face, fingerprint and iris. This section analyzes the most common setups and procedures designed for ABC systems for these biometric traits.

A. Face recognition in e-Gates

ICAO has chosen face recognition as the primary biometric trait for e-Passports, since it offers many advantages [33], for instance: it is accepted from a social point of view, its capture

is not intrusive, and human border guards are familiar with it. For this reason, many ABC systems rely on face recognition. In particular, among the systems studied by the EU project ABC4EU, 60% used face recognition.

An e-Gate that implements facial recognition generally employs four components: the acquisition cameras, the illumination system, the face quality assessment module and the facial verification module. To cover diverse traveler's heights, the e-Gate can use more than one camera or it can automatically adjust the camera's height. In order to obtain high quality images, the illumination system has to provide a uniform and symmetric illumination, which compensates the external lights, and which avoids blinding the traveler. In addition, the face quality assessment module should check the quality of the image, rejecting those images that do not guarantee high recognition accuracy. This module has to take into account the recommendations provided by ISO/IEC [14] and ICAO [33]. The Facial verification module has to verify if the live captured image and that present in the document/database correspond to the same person.

The e-Gate performs face recognition applying the following steps: i) Once the traveler is inside the e-Gate, the e-Gate chooses the right camera or automatically adjusts camera's height. ii) A display indicates the traveler how to look at the camera. iii) The illumination system corrects lighting problems. iv) If the quality assessment software considers that the quality of the facial image is not sufficient, the e-Gate can retry the acquisition a specified number of times. v) Once the e-Gate has acquired a high quality image, it perfoms a matching between the live image and that stored in the travel document.

B. Fingerprint recognition in e-Gates

ICAO describes fingerprint recognition as an optional biometric for e-Passports [33]. Therefore, not all travel documents include fingerprint samples. However, due to its high recognition accuracy and social acceptance, many ABC systems have used and continue to use it. In particular, among the systems studied by the EU project ABC4EU, 61% used fingerprint recognition to identify travelers.

In general, the e-Gates that perform fingerprint recognition use three components: The fingerprint scanner, the fingerprint quality assessment module and the fingerprint verification module. Depending on the number of fingerprints that the ABC system needs to acquire, the fingerprint scanner can be a 4-finger or single-finger sensor. It should comply with the quality specifications defined by the ISO/IEC standard [15]. The capture technology is generally optical [34]. The fingerprint quality verification module has to check if the fingerprint image has sufficient information to guarantee a correct verification performance. The NIST Fingerprint Image Quality (NFIQ) [35] indicator is the most common standard, but many deployments use proprietary software. The fingerprint verification module has to compare the fingerprint live-image with that stored in the document/database. The most commonly used technique is minutiae comparison [28], [32], [34], [36].

The e-Gate performs fingerprint recognition applying the following steps: i) The e-Gate automatically adjusts the height and inclination of the sensor, if it is capable of doing so. ii) A display indicates to the traveler which finger has to place on the sensor and the correct way to place it. iii) If the image does not fulfill the quality standard, the e-Gate can retry the acquisition a specified number of times. iv) If the verification needs more than one fingerprint, the e-Gate acquires it following steps ii and iii. v) The e-Gate performs the matching between the live image and that stored in the travel document/database.

C. Iris recognition in e-Gates

The inclusion of iris biometrics in e-Passports is optional, according to ICAO [33]. This fact, together with other challenges introduced in Section V, have hindered the development of e-Gates based on iris recognition. Among the systems studied by the EU project ABC4EU, 8% used iris technology.

The e-Gates that perform iris recognition, generally employ three components: The acquisition camera, the illumination system, and the iris verification module. The acquisition camera is a short range camera, operating at a distance of around 25 cm for scanning a single eye, and around 100 cm when both eyes are necessary. The illumination system uses a near-infrared setup that eliminates the problems posed by dark irises, permitting to scan both light and dark irises. With this illumination all irises have a readily visible texture [37]. The iris verification module applies the template extraction and matching algorithms verifying if the live captured image and that present in the document/database correspond to the same person [29]–[31]. The most commonly used algorithm is the one developed by Daugman [38].

The e-Gate carries out iris recognition applying the following steps: i) A display indicates the traveler how to place himself and to look at the camera, so that the e-Gate can acquire the irises. ii) The illumination system performs a pulse of near-infrared light that allows the camera to control the iris position and pupil dilation. iii) The matching between the live image and that stored in the document/database is performed.

IV. Measuring ABC system's effectiveness

The performance evaluation of e-Gates is a particularly challenging task. It includes the computation and aggregation of heterogeneous figures of merit designed to evaluate all the systems involved in the identity recognition process. In this context, the evaluation of the accuracy of the BVS needs particular attention, since it determines to what extent the ABC system can guarantee that an individual is really who he/she claims to be.

The operational evaluation [39] of the BVS requires specifically designed strategies since many of the figures of merit commonly employed for testing biometric systems are not directly applicable in an ABC context. This kind of evaluation has to consider different aspects of the system [40]: technical performance of the physical components of the system; matching performance; process timings of users of the system; observations of the interaction between the users and the system; and travelers' perceptions of the system.

In this context, the matching performance evaluation is a particularly important aspect since it determines the expected level of accuracy in matching decisions performed by the

biometric system [41], [42]. However, this evaluation can be particularly challenging in real application scenarios. Indeed, different legislation across different countries may interfere in the calculation of the most commonly used figures of merit in the literature, such as, false acceptance rate (FAR), and false rejection rate (FRR), equal error rate (EER), receiver operating characteristic (ROC), and detection error trade-off (DET) curves. For instance: many countries include privacy laws that limit the collection and storage of biometric data; matching scores and decision thresholds are not public; in most of the cases, it is not possible to assess if travelers that were granted access were effectively who they claimed to be. In many scenarios, the matching performance evaluation of the BVS has therefore to rely on a subset of the figures of merit, without providing a complete picture of the system accuracy.

V. Challenges and research trends

In this section, we study the most challenging problems that biometric recognition systems have to face in ABC systems, and the research trends that we expect will lead future research and innovations in e-Gates. We first introduce the general challenges valid for all ABC systems. After that, we analyze the particular challenges and future trends for the most frequently used biometric technologies. Then, we present new approaches that can improve ABC systems' performance.

One of the major issues that compromises the security of ABC systems is liveness detection using anti-spoofing systems. Impostors can use several techniques to fool biometric recognition systems. For instance: face impressions, fake fingers made of gelatin or silicone [43], synthetic iris textures [37] and other techniques. It is important to develop techniques for detecting these attacks, to ensure the security of border controls. Unfortunately, data of impostors that attempted to fraud the biometric checks at the e-Gates are not publicly available. Nevertheless, there are several studies that show the vulnerability of biometric systems to spoof attacks and provide different detection solutions [44]. The EU 7FP-funded project TABULA RASA (Trusted Biometrics under Spoof Attacks) further emphasizes the importance of spoof detection. This research project aims at developing effective countermeasures to spoof attacks for increasing the robustness of biometric systems.

The current generation of ABC systems in general, and the biometric system in particular, rarely implement measures to support travelers that are not fully able to use the e-Gate, i.e., people with reduced mobility or visual impairment. People with reduced mobility may have problems dealing with the biometric acquisition sensor. For instance, people using a wheelchair could have problems using an iris sensor, people with muscular dystrophy may not be able to adopt the correct pose for face acquisition, or people using walking aids may not be able to correctly interact with a fingerprint scanner. On the other hand, visually impaired people may not be able to follow the instructions displayed on a screen, or may have problems locating the acquisition sensor. For these reasons, the design of the e-Gate's biometric system should take into account these types of travelers, providing solutions that permit travelers with special needs to use the system. This aspect is particularly important in those countries that have legislated to regulate these aspects, as in the case of the EU.

A. Face recognition challenges

With regard to face recognition, the capture of ICAO compliant face images is of major importance in order to guarantee a high recognition accuracy in ABC systems [45]. However, many aspects make difficult the acquisition of high quality face images, for instance user inexperience or difficulties in capturing the user's attention. To reduce this problem it is necessary to create systems that instruct the users and guide them through the acquisition process. To guarantee high quality it is also important to take into account the traveler's height and pose. The acquired images should be full-frontal, with the face in the center of the image, and the traveler directly looking at the camera. The system should be able to detect when the image fulfills these requirements, to capture it. Moreover, in general the illumination of the places where the authorities deploy the ABC systems is not ideal. Hence, the biometric system has to deal with illumination changes, which can damage image quality. It is important to develop illumination systems that can counteract these changes.

B. Fingerprint recognition challenges

With respect to fingerprint recognition, to guarantee sufficient image quality, it is very important to improve the usability of the system. The development of quality analysis algorithms that identify acquisition problems, and propose corrective actions is an important aspect that can increase the usability and performance of the system [46], [47].

Another major issue in fingerprint recognition in ABC systems is the lack of cryptographic interoperability between countries. In many cases, the authorities use cryptographic algorithms to protect the chip of the electronic document, making more difficult the access to the stored fingerprints. The definition of standards that guarantee the interoperability of the systems could permit an easy access to the fingerprints. At the same time, they can protect fingerprints' integrity and prevent illegal access.

Another challenge is fingerprint acquisition speed, which, in some cases, can be slow. A correct acquisition needs that the user places the finger on the sensor in a correct way. To avoid this problem, many sensors require that the user moves the finger over the acquisition surface for some seconds, waiting until a frame has sufficient quality. It is important to develop fingerprint sensors and protocols that permit to reduce the acquisition time.

C. Iris recognition challenges

Regarding iris recognition, one of the main challenges that ABC systems need to face is cost. Iris capture systems are expensive, compared with face or fingerprint recognition sensors. In addition, iris is not included in any passport currently in circulation [48]. Hence, the ABC systems that use iris recognition need to create extra back-end systems that contain iris information.

Most of the users perceive iris scanners users as highly intrusive and difficult to use. The development of new approaches that alleviate this problem will surely improve the acceptability of the ABC systems that employ iris recognition.

D. Multibiometrics

As future trend and to improve security, a promising development is the use of multibiometrics. These systems, which fuse multiple sources of biometric data, will increasingly impact identity management in the 21st century [5]. This approach offers many advantages, improving accuracy, usability and security if compared with monomodal systems that rely on the evidence of a single biometric trait. Notably, multibiometric systems if properly designed, permit to overcome several drawbacks associated to monomodal systems, including [49]–[51]: non-universality, accuracy limitations of the sensor, noisy data, limited ability to discriminate the biometric trait and limited robustness against spoofing. A recent publication [52] suggested that multibiometrics is the most significant trend against spoofing attacks.

The work in [53], testing the combination of face and fingerprint biometric with a population of about $1,000$ subjects, revealed significant performance improvement over monomodal biometric systems. Likewise, actual ABC deployments showed the benefits of multibiometrics. In two Spanish international airports for example, using multiple biometric traits led to a sensible increase of the performance of the ABC system: fingerprint fusion improved facial verification result from 12.23% to 3.72% FRR for a population of $13,478$ subjects [6]. The considered subjects were Spanish nationals holding a second generation e-Passport. The Spanish ABC uses face as the main biometric modality, and follows a cascaded decision-level fusion of the fingerprint image [54].

However, multibiometrics can also present some drawbacks in an automated border context. The use of multiple biometric sensors renders the system more complex, adding points of failure, which may cause that inexperienced users get confused. In addition, an unsuitable deployment of multiple biometrics can hinder the optimization of the travelers flow. While improving the security of the system, an increased amount of sensible information can threaten the users' privacy. Several studies proposed different solutions for protecting the multiple biometric information from malicious attempts to break the privacy [55], [56].

E. Unconstrained biometrics

The ease of use of a biometric trait is also particularly important in an automated border context, since one of the main objectives of ABC systems is to reduce traveler's processing time. In particular, the constraints that the biometric system imposes on the traveler limit its ease of use [57]. The reduction of these constraints is one of the research trends that will have a greater impact in the development of e-Gates.

Unconstrained biometrics aim at facilitating the capture of the biometric sample. For instance: They do not require the contact of the traveler, i.e., are contactless; permit the acquisition at higher distances or while the traveler is moving; or allow the system to use natural light conditions. Some of the most promising techniques with regard to e-Gates are contactless fingerprint recognition [58]–[66], contactless palm recognition [67] and iris recognition at a distance [57], [68].

By reducing or eliminating the peculiar contact-based acquisition constraints, unconstrained biometrics may improve acquisition quality, usability and user acceptability of the biometric system. The design of biometric systems of this kind could lead to a greater confidence in biometric recognition and to a broader adoption of biometric technologies [69], [70]. The results of a survey on user acceptability presented in [59], report that 96.7% of the volunteers prefer the touchless fingerprint system to an equivalent touch-based, and 100% of the volunteers consider it more hygienic. Moreover, users perceive the touchless system as more privacy compliant, possibly because no latent fingerprint can be left.

VI. Conclusions

Within an e-Gate there are mainly four subsystems, cooperating to the traveler clearance process by: biometric verification, document authentication, border guard maintenance and interface to external systems. The BVS holds a central role, being responsible for the biometric verification of the traveler's identity. The paper describes the design of the BVS components for acquiring and processing the biometric samples, and the procedures adopted at the e-Gate for the verification of the biometric traits most accepted today.

The analysis of the figure of merits typically used for the evaluation of biometric systems suggested that only some of them are actually applicable to the operative scenarios of BCPs, because of the privacy concerns [71]–[73] that may impede the collection of passengers' personal data. Considering the challenges inherent to every biometric trait, usability of the biometric systems arouse as critical. Therefore, we presented important research trends to improve usability, with particular attention to multibiometrics and unconstrained biometric technologies.

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); and the Italian Ministry of Research within the project "GenData 2020" (2010RTFWBH).

References

[1] Boeing, "Current market outlook: 2014-2033," Seattle, 2014. [Online]. Available: http://www.boeing.com/

[2] Frontex Agency, "Best practice technical guidelines for automated border control (ABC) systems," European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union, Tech. Rep., 2012. [Online]. Available: http://frontex.europa.eu/

[3] A. Amato, V. Di Lecce, and V. Piuri, *Semantic Analysis and Understanding of Human Behavior in Video Streaming*. Springer, 2013.

[4] Frontex Agency, "Best practice operational guidelines for automated border control (ABC) systems," European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union, Tech. Rep., 2012. [Online]. Available: http://frontex.europa.eu/

[5] A. Ross, K. Nandakumar, and A. Jain, *Handbook of Multibiometrics*, ser. International Series on Biometrics. Springer, 2006, vol. 6.

[6] D. Cuesta Cantarero, D. Perez Herrero, and F. Martin Mendez, "A multimodal biometric fusion implementation for abc systems," in *Proc. of the IEEE Intelligence and Security Informatics Conf.*, 2013, pp. 277–280.

[7] Aeroporti di Roma, "Fiumicino is the first airport in Italy to automate border controls," 2014. [Online]. Available: https://www.adr.it/

[8] PricewaterhouseCoopers, "Technical study on smart borders (final report)," European Commission, Tech. Rep., 2014. [Online]. Available: http://www.europarl.europa.eu/

[9] European Commission Directorate-General for Justice, Freedom and Security, "Preparing the next steps in border management in the European Union," Tech. Rep., 2008. [Online]. Available: http://ec.europa.eu/

[10] D. Gorodnichy, S. Yanushkevich, and V. Shmerko, "Automated border control: Problem formalization," in *Proc. of the IEEE Symposium on Computational Intelligence in Biometrics and Identity Management*, 2014, pp. 118–125.

[11] European Parliament, "Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas," 2008.

[12] European Commission, "Proposal for a regulation of the European Parliament and of the Council establishing a Registered Traveller Programme," 2013. [Online]. Available: http://ec.europa.eu/

[13] European Commission, "Proposal for a regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the external borders of the Member States of the European Union," 2013.

[14] International Organization for Standardization, "ISO/IEC 19794-5:2011, Information technology – Biometric data interchange formats – part 5: Face image data," 2011.

[15] International Organization for Standardization, "ISO/IEC 19794-4:2011, Information technology – Biometric data interchange formats – part 4: Finger image data," 2011.

[16] International Organization for Standardization, "ISO/IEC 19794-6:2011, Information technology – Biometric data interchange formats – part 6: Iris image data," 2011.

[17] Unisys, "Entry-exit feasibility study - final report," European Commission, Tech. Rep., 2008. [Online]. Available: http://www.europarl.europa.eu/

[18] R. Donida Labati, V. Piuri, and F. Scotti, *Biometric privacy protection: guidelines and technologies*, M. S. Obaidat, J. Sevillano, and F. Joaquim, Eds. Springer, 2012, vol. 314.

[19] S. Cimato, M. Gamassi, V. Piuri, R. Sassi, and F. Scotti, *Privacy in biometrics*, ser. Computational Intelligence, N. Boulgouris, K. Plataniotis, and E. Micheli-Tzanakou, Eds. Wiley-IEEE Press, 2009.

[20] M. Barni, T. Bianchi, D. Catalano, M. D. Raimondo, R. Donida Labati, P. Failla, D. Fiore, R. Lazzeretti, V. Piuri, F. Scotti, and A. Piva, "A privacy-compliant fingerprint recognition system based on homomorphic encryption and fingercode templates," in *Proc. of the IEEE Int. Conf. on Biometrics: Theory Applications and Systems*, 2010, pp. 1–7.

[21] T. Bianchi, R. Donida Labati, V. Piuri, A. Piva, F. Scotti, and S. Turchi, "Implementing fingercode-based identity matching in the encrypted domain," in *Proc. of the IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications*, 2010, pp. 15–21.

[22] M. Barni, T. Bianchi, D. Catalano, M. D. 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, pp. 231–240.

[23] S. Cimato, M. Gamassi, V. Piuri, R. Sassi, and F. Scotti, "A biometric verification system addressing privacy concerns," in *Proc. of the Int. Conf. on Computational Intelligence and Security*, 2007, pp. 594–598.

[24] M. Gamassi, V. Piuri, D. Sana, O. Scotti, and F. Scotti, "A multi-modal multi-paradigm agent-based approach to design scalable distributed biometric systems," in *Proc. of the IEEE Int. Conf. on Computational Intelligence for Homeland Security and Personal Safety*, 2005, pp. 65–70.

[25] L. D. Bentley, J. L. Whitten, and K. Dittman, *Systems analysis and design methods*. McGraw Hill, 2007.

[26] R. Perrey and M. Lycett, "Service-oriented architecture," in *Proc. of the Symposium on Applications and the Internet Workshops*, 2003, pp. 116–119.

[27] R. Sanchez-Reillo and M. Niesing, "Bioapi, standardization," in *Encyclopedia of Biometrics*, S. Z. Li and A. K. Jain, Eds. Springer US, 2014, pp. 1–6.

[28] V. Piuri and F. Scotti, "Fingerprint biometrics via low-cost sensors and webcams," in *Proc. of the IEEE Int. Conf. on Biometrics: Theory, Applications and Systems*, 2008, pp. 1–6.

[29] R. Donida Labati, V. Piuri, and F. Scotti, "Agent-based image iris segmentation and multiple views boundary refining," in *Proc. of the IEEE Int. Conf. on Biometrics: Theory, Applications and Systems*, 2009, pp. 1–7.

[30] F. Scotti and V. Piuri, "Adaptive reflection detection and location in iris biometric images by using computational intelligence techniques," *IEEE Trans. on Instrumentation and Measurement*, vol. 59, no. 7, pp. 1825–1833, 2010.

[31] R. Donida Labati, V. Piuri, and F. Scotti, "Neural-based iterative approach for iris detection in iris recognition systems," in *Proc. of the IEEE Symp. on Computational Intelligence for Security and Defence Applications*, 2009, pp. 1–6.

[32] M. Gamassi, V. Piuri, and F. Scotti, "Fingerprint local analysis for high-performance minutiae extraction," in *Proc. of the IEEE Int. Conf. on Image Processing*, vol. 3, 2005, pp. 265–268.

[33] International Civil Aviation Organization, "Doc 9303, machine readable travel documents. Part 1, vol. 2," 2006. [Online]. Available: http://www.icao.int/

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

[35] E. Tabassi, C. Wilson, and C. Watson, "Fingerprint image quality," National Institute of Standards and Technology (NIST), NISTIR 7151, Tech. Rep., 2004. [Online]. Available: http://www.nist.gov/

[36] M. Gamassi, V. Piuri, D. Sana, and F. Scotti, "Robust fingerprint detection for access control," in *Proc. of the Workshop RoboCare*, 2005.

[37] M. J. Burge and K. Bowyer, *Handbook of iris recognition*. Springer Science & Business Media, 2013.

[38] J. Daugman, "How iris recognition works," *IEEE Trans. on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 21–30, 2004.

[39] National Science & Technology Council Subcommittee on Biometrics, "Biometric testing and statistics," Tech. Rep., 2006. [Online]. Available: http://www.biometrics.gov

[40] 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. Jain, E. Aidman, and C. Abeynayake, Eds. Springer, 2011, vol. 338, pp. 115–145.

[41] M. Gamassi, M. Lazzaroni, M. Misino, V. Piuri, D. Sana, and F. Scotti, "Quality assessment of biometric systems: a comprehensive perspective based on accuracy and performance measurement," *IEEE Trans. on Instrumentation and Measurement*, vol. 54, no. 4, pp. 1489–1496, 2005.

[42] R. Donida Labati, A. Genovese, V. Piuri, and F. Scotti, "Accurate 3D fingerprint virtual environment for biometric technology evaluations and experiment design," in *Proc. of the IEEE Int. Conf. on Computational Intelligence and Virtual Environments for Measurement Systems and Applications*, 2013, pp. 43–48.

[43] 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.

[44] S. Marcel, M. S. Nixon, and S. Z. Li, Eds., *Handbook of Biometric Anti-spoofing: Trusted Biometrics under Spoofing Attacks*. Springer, 2014.

[45] L. J. Spreeuwers, A. Hendrikse, and K. Gerritsen, "Evaluation of automatic face recognition for automatic border control on actual data recorded of travellers at Schiphol Airport," in *Proc. of the IEEE Int. Conference of the Biometrics Special Interest Group*, 2012, pp. 1–6.

[46] R. Donida Labati, A. Genovese, V. Piuri, and F. Scotti, "Quality measurement of unwrapped three-dimensional fingerprints: a neural networks approach," in *Proc. of the IEEE-INNS Int. Joint Conf. on Neural Networks*, 2012, pp. 1123–1130.

[47] R. Donida Labati, V. Piuri, and F. Scotti, "Neural-based quality measurement of fingerprint images in contactless biometric systems," in *Proc. of the IEEE-INNS Int. Joint Conf. on Neural Networks*, 2010, pp. 1–8.

[48] A. J. Palmer and C. Hurrey, "Ten reasons why iris needed 20:20 foresight: some lessons for introducing biometric border control systems," in *Proc. of the IEEE Intelligence and Security Informatics Conf.*, 2012, pp. 311–316.

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

[50] M. Gamassi, V. Piuri, D. Sana, and F. Scotti, "A high-level optimum design methodology for multimodal biometric systems," in *Proc. of the IEEE Int. Conf. on Computational Intelligence for Homeland Security and Personal Safety*, 2004, pp. 117–124.

[51] S. Cimato, M. Gamassi, V. Piuri, D. Sana, R. Sassi, and F. Scotti, "Personal identification and verification using multimodal biometric data," in *Proc. of the IEEE Int. Conf. on Computational Intelligence for Homeland Security and Personal Safety*, 2006, pp. 41–45.

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

[53] R. Snelick, M. Indovina, J. Yen, and A. Mink, "Multimodal biometrics: Issues in design and testing," in *Proc. of the ACM International Conference on Multimodal Interfaces*, 2003, pp. 68–72.

[54] International Organization for Standardization, "ISO/IEC 24722:2007, Information technology – Biometrics – Multimodal and other multibiometric fusion," 2007.

[55] S. Cimato and M. Gamassi and V. Piuri and R. Sassi and F. Scotti, "Privacy-aware biometrics: design and implementation of a multimodal verification system," in *Proc. of the Annual Computer Security Applications Conf.*, 2008, pp. 130–139.

[56] S. Cimato, M. Gamassi, V. Piuri, R. Sassi, and F. Scotti, "A multi-biometric verification system for the privacy protection of iris templates," in *Proc. of the Int. Workshop on Computational Intelligence in Security for Information Systems*, ser. Advances in Soft Computing, E. Corchado, R. Zunino, P. Gastaldo, and . Herrero, Eds. Springer Berlin Heidelberg, 2009, vol. 53, pp. 227–234.

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

[58] R. Donida Labati, A. Genovese, V. Piuri, and F. Scotti, "Touchless fingerprint biometrics: a survey on 2D and 3D technologies," *Journal of Internet Technology*, vol. 15, no. 3, pp. 325–332, 2014.

[59] 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*, 2015.

[60] R. Donida Labati, V. Piuri, and F. Scotti, *Touchless Fingerprint Biometrics*, ser. Security, Privacy and Trust. CRC Press, 2015.

[61] R. Donida Labati, A. Genovese, V. Piuri, and F. Scotti, "Contactless fingerprint recognition: a neural approach for perspective and rotation effects reduction," in *Proc. of the IEEE Workshop on Computational Intelligence in Biometrics and Identity Management*, 2013, pp. 22–30.

[62] R. Donida Labati and A. Genovese and V. Piuri and F. Scotti, "Virtual environment for 3-D synthetic fingerprints," in *Proc. of the IEEE Int. Conf. on Virtual Environments, Human-Computer Interfaces and Measurement Systems*, 2012, pp. 48–53.

[63] R. Donida Labati, A. Genovese, V. Piuri, and F. Scotti, "Two-view contactless fingerprint acquisition systems: a case study for clay artworks," in *Proc. of the IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications*, 2012, pp. 1–8.

[64] R. Donida Labati and A. Genovese and V. Piuri and F. Scotti, "Fast 3-D fingertip reconstruction using a single two-view structured light acquisition," in *Proc. of the IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications*, 2011, pp. 1–8.

[65] R. Donida Labati, V. Piuri, and F. Scotti, "A neural-based minutiae pair identification method for touchless fingeprint images," in *Proc. of the IEEE Workshop on Computational Intelligence in Biometrics and Identity Management*, 2011, pp. 96–102.

[66] R. Donida Labati, A. Genovese, V. Piuri, and F. Scotti, "Measurement of the principal singular point in contact and contactless fingerprint images by using computational intelligence techniques," in *Proc. of the IEEE Int. Conf. on Computational Intelligence for Measurement Systems and Applications*, 2010, pp. 18–23.

[67] A. Genovese, V. Piuri, and F. Scotti, *Touchless Palmprint Recognition Systems*, ser. Advances in Information Security. Springer, 2014, vol. 60.

[68] R. Donida Labati and F. Scotti, "Noisy iris segmentation with boundary regularization and reflections removal," *Image and Vision Computing, Special Issue on Iris Images Segmentation*, vol. 28, no. 2, pp. 270–277, 2010.

[69] M. Theofanos, B. Stanton, C. Sheppard, R. Micheals, W. Zhang, N. Wydler, N. L., and R. Rubin, "Usability testing of height and angles of ten-print fingerprint capture," National Institute of Standards and Technology (NIST), NISTIR 7504, Tech. Rep., 2008. [Online]. Available: http://www.nist.gov/

[70] 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, pp. 170–178.

[71] A. Acquisti, S. Gritzalis, C. Lambrinoudakis, and S. De Capitani di Vimercati, Eds., *Digital Privacy: Theory, Technologies, and Practices*. CRC Press, 2007.

[72] V. Ciriani, S. De Capitani di Vimercati, S. Foresti, and P. Samarati, "Microdata protection," in *Secure Data Management in Decentralized Systems*, T. Yu and S. Jajodia, Eds. Springer-Verlag, 2007.

[73] S. De Capitani di Vimercati, S. Foresti, G. Livraga, and P. Samarati, "Data privacy: Definitions and techniques," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 20, no. 6, pp. 793–817, 2012.