Biometric Recognition in Automated Border Control: A Survey

RUGGERO DONIDA LABATI, ANGELO GENOVESE, ENRIQUE MUÑOZ, VINCENZO PIURI, FABIO SCOTTI and GIANLUCA SFORZA, Università degli Studi di Milano

The increasing demand for traveler clearance at international border crossing points (BCPs) has motivated research for finding more efficient solutions. Automated border control (ABC) is emerging as a solution to enhance the convenience of travelers, the throughput of BCPs, and national security. This is the first comprehensive survey on the biometric techniques and systems that enable automatic identity verification in ABC. We survey the biometric literature relevant to identity verification and summarize the best practices and biometric techniques applicable to ABC, relying on a real experience collected in the field. Furthermore, we select some of the major biometric issues raised and highlight the open research areas.

CCS Concepts:•**Security and privacy** → **Authentication;** *Biometrics;*•**Social and professional topics** → Surveillance;

Additional Key Words and Phrases: Security, Authentication, Automated Border Control, e-Gate, Biometric recognition

ACM Reference Format:
Donida Labati, R., Genovese, A., Muñoz, E., Piuri, V., Scotti, F. and Sforza, G. *ACM Comput. Surv.* V, N, Article A (January YYYY), 39 pages.
DOI: 0000001.0000001

1. INTRODUCTION

Passenger traffic is significantly increasing worldwide: the most recent forecasts for air transportation expect an annual increase of 5 percent for the next 20 years [Boeing 2015]. Thus, international border crossing points (BCPs) – particularly airports, but also seaports and land borders – must increase their processing throughput without affecting the overall security of the controls. States and border management agencies are working to increase both the integrity of the borders and the speed of the travel flows. However, for the majority of the states, increasing the number of border guards to reach these objectives may not be viable [IATA 2014a].

The continuous increase in passenger traffic has resulted in border guards having less time to make decisions. Typically, a border guard has only 12 seconds to decide whether the traveler in front of them is allowed to cross the border [Fergusson 2014]. In such little time, border guards have to make a decision that can occasionally be crucial for the passenger. Automated processing of the crossing requests is desirable to facilitate the clearance procedures for passengers while keeping security high. Such a system can guarantee the same level of efficiency at all times, without variations due to typical human factors, such as fatigue. Automating the border control process for low-risk travelers can free up border control resources to focus on higher-risk travelers. The introduction of biometric technologies in automated checks has a relevant impact

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). Authors’ addresses: Department of Computer Science, Università degli Studi di Milano, 26013 Crema, IT. emails: name.surname@unimi.it.

DOI: 0000001.0000001

on improving the efficiency and effectiveness of the checking process and the security of the travelers. Furthermore, a survey conducted by [IATA 2012b] revealed that 91% of travelers are interested in automated gates for a faster border control processing, yet the uptake of this innovation has still to grow up within the passengers. In fact, there are many categories of non-users, most of them being unaware of the existence of actual automated gates, which will need more time to get involved [Oostveen 2014]. Automating border control is part of a wider initiative of smart border, which also encompasses commercial aspects, such as security of shipments at the customs [Adam et al. 2005]. As such, several countries such as the USA, the EU, Rwanda, China, and Australia are making efforts to selectively control both the flow of persons and of goods using new information technologies, so as to help border officers and customs inspectors make better decisions.

Automated Border Control (ABC) can be defined as the use of automated or semi-automated systems that can verify the identity and authorization of travelers to cross the borders at BCPs, without the need for human intervention [Frontex 2012a]. Basically, the automated border crossing process includes three types of checks: 1) authentication of the travel document, 2) biometric verification of the traveler's identity, and 3) check of whether the traveler is authorized to cross the border. The ABC system first checks whether the traveler is carrying a genuine and valid travel document. Subsequently, it live captures a biometric sample of the traveler – typically, a face image, fingerprint, or iris image – for a one-to-one match against the image obtained from the biometric document holder. Finally, it checks whether the traveler is entitled and authorized to cross the border. The ABC system is supervised by an officer in a remote station, who can intervene in case of problems. Automated biometric gates, also known as e-Gates, automatically verify the traveler, allowing their passage in the case of success. Regular e-Gates use an electronic machine-readable travel document (e-MRTD), generally an e-Passport compliant with International Civil Aviation Organization (ICAO) specifications that contains biometric samples of the owner.

This is the first survey on the biometric techniques used in ABC, and it offers an up-to-date picture of the ABC systems that are operating all over the world. Its contributions are three-fold:

- analysis of state-of-art techniques for biometric identity verification;
- presentation of updated performance data and coverage of the features of several ABC systems operating worldwide;
- investigation of usability concerns and of emerging biometric techniques to improve the user's experience.

This article is structured as follows. Section 2 presents background information about ABC; the structure of an e-Gate including its external links; and the biometric data involved. Section 3 presents the biometric techniques currently in use and emerging in ABC systems, including multi-modality, as well as a picture of actual implementations. Finally, Section 4 discusses some of the main issues that an ABC application faces and the main challenges that are still open.

2. BACKGROUND

The main goal of implementing an ABC solution is to achieve an automated, self-service clearance process with high levels of speed and security such that increasing the passenger throughput does not compromise the reliability of the border control. Implementing the ABC process requires different technologies and the support of biometrics. The ISO/IEC TR 29195 recently provided guidelines and operational considerations for the design of automated border control systems thus addressing the needs of the business and of the traveler in automated border processing [ISO/IEC 2015c].

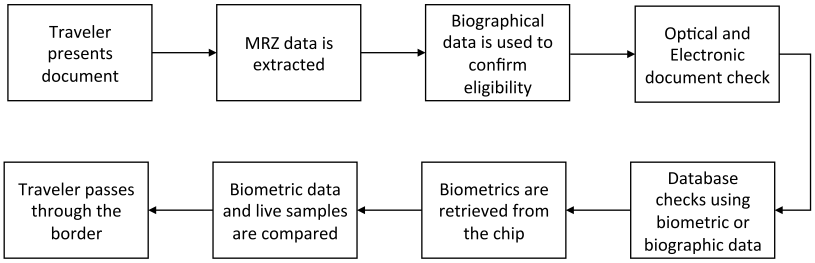

Traveler presents document
MRZ data is extracted
Biographical data is used to confirm eligibility
Optical and Electronic document check
Database checks using biometric or biographic data
Biometrics are retrieved from the chip
Biometric data and live samples are compared
Traveler passes through the border

Fig. 1. ABC process steps.

There are three generations of ABC systems beginning from the early 2000s [Gorodnichy et al. 2014]: the 1^{st} generation ABC systems only process registered travelers (e.g., Privium in The Netherlands, Global Entry in the USA, and Nexus across Canada/USA); the 2^{nd} generation systems, the e-Gates, serve travelers with an e-MRTD issued by the nation that installed the system, and possibly foreign nationals through bilateral agreements (e.g., several states in the EU and Australia); and the forthcoming 3^{rd} generation systems will be able to communicate globally, as envisaged by [IATA 2012a].

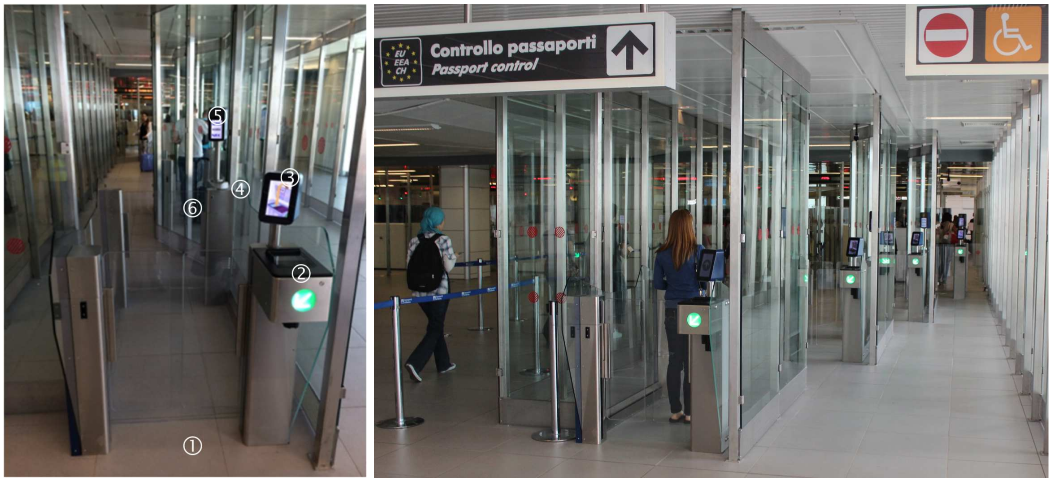
Among the several implementations of ABC systems currently available, there are three main types, with various levels of automation: the e-Gates, the ABC kiosks, and other semi-automated kiosks. An e-Gate can automatically perform both verification of the traveler and allow the traveler's secure passage through the border. A kiosk performs part of this job: it can perform biometric pre-enrollment and document checks and ultimately issue a transaction receipt. In a second step, this ticket can be double checked, either automatically by an e-Gate or manually by an officer, as performed with semi-automated automated passport control (APC) systems and similarly with the US Global Entry fidelity program. Typically, fully automated ABC systems require a biometric identity document, an e-MRTD, whereas semi-automated systems can also be used with less advanced MRTDs.

Regardless of the type of solution implemented, all of these systems share the same automation objectives. There are more than 180 air ABC deployments already operating regularly worldwide (see Table I in Section 3.5). In this article, we considered the e-Gate as a reference solution to the ABC task. This section describes the architecture of e-Gates and cooperation with external systems, and it presents an overview of the biometric document used by travelers.

2.1. The e-Gate

In general, an e-Gate performs automated traveler clearance through the following steps [Frontex 2012a] (see Figure 1): first, the traveler presents the document to the system, and the document reader extracts biographic data from the machine-readable zone (MRZ). The system double checks the e-MRTD and verifies whether the traveler is eligible to cross the border. Then, it reads the biometric data from the document's chip and compares this data to the live captured samples: if the comparison is successful, it opens the doors to allow the traveler to cross the border.

Figure 2 shows the structure and an application scenario of real e-Gates: these systems based on multiple biometric modalities, such as fingerprints, face and iris, have been deployed worldwide, and on the basis of the information gathered [Vision-box 2015; NAO 2015; The National 2015; Kephart 2015] it can be estimated that they have allowed the passage of more than one-hundred-million people per year.



(a) (b)

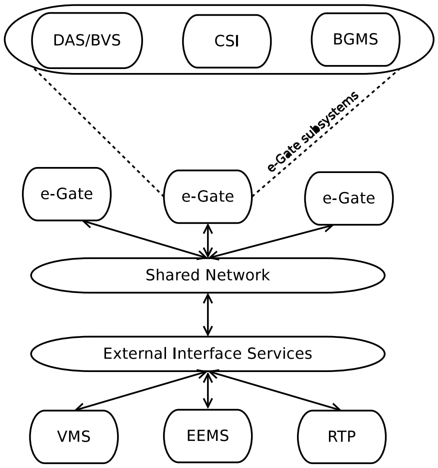
Fig. 2. Structure of an e-Gate (a) and deployment at Roma Fiumicino International Airport (b). Numbering in figure (a) mark locations of 1: entry door, 2: passport reader, 3: passport display, 4: fingerprint reader, 5: face camera and display, 6: exit door. Reproduced with permission of Polizia di Frontiera Italiana (a) and Aeroporti di Roma (b).

In the following, we present the aspects related to the logical and physical architectures of an e-Gate, as well as the external systems queried during the clearance process.

2.1.1. Logical architecture of an e-Gate. An e-Gate can be conceptually represented as a system composed of four interconnected (sub)systems, namely (see Figure 3), Document Authentication System (DAS), Biometric Verification System (BVS), Central Systems Interface (CSI) and Border Guard Maintenance System (BGMS) [Donida Labati et al. 2015b]. In this representation, the DAS is responsible for checking the validity of the document and extracting the information contained in the MRZ and in the chip. The BVS has a central role in the overall system, as it serves to verify the identity of the passenger through the biometric traits. The BGMS is assigned to the border guards' activities of monitoring and controlling the ABC system, whereas the CSI has the function of managing the interfaces with external systems. In response to a request for automated clearance, heterogeneous sources of information can indeed be queried from multiple external systems [Mitra et al. 2006]. In this case, a secure communication among the systems is relevant [Adam et al. 2006], particularly because of the exchange of personal data such as the biometrics.

The clearance process that an e-Gate performs may follow different logics based on timing in which the document authentication and the biometric system operate: one-step process and two-step process [Frontex 2012a]. In the *one-step process*, identity verification and passage through the border occur in a single process, and the traveler performs all clearance actions inside the e-Gate. The *two-step process* clearly divides the clearance process into two separate steps: during the first step, the traveler initiates the verification procedures outside the e-Gate and completes the passage in a second stage.

2.1.2. Physical architecture of an e-Gate. Typically, an e-Gate is composed of the following components associated with the previously described subsystems including one or two physical barriers, an e-Passport scanner for text recognition and chip reading, a



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. 3. Logical architecture of an e-Gate and links to external systems.

monitor that displays instructions to the traveler, biometric acquisition devices (one for each trait used) and the system management HW/SW, which are also used for communicating with external systems [Frontex 2012a].

As previously described, the clearance process follows two different logics, depending on the time at which document authentication and biometric verification occur. Three different topologies for the e-Gates (illustrated in Figure 4) correspond to these logics, with different placements of the physical components: there are double-door (*mantrap*) solutions and single-door solutions (kiosk plus e-Gate).

The one-step process is typically implemented with a double-door solution, one door at entry and one at exit, and all the components for the verification of the passenger placed inside the e-Gate. This configuration can deliver a high-speed clearance time because several actions can be performed in parallel, provided that the traveler is well trained. An example of the use of this topology can be found in the PARAFE project implemented in France [Frontex 2012b].

The two-step process can either be integrated into a single location or segregated into two different locations. The segregated two-step process is typically implemented in a pre-enrollment kiosk for traveler verification and a single-door e-Gate for border crossing. The integrated two-step process is a type of hybrid implementation, i.e., a double-door solution where the document verification component is placed outside the e-Gate while biometric match occurs inside. The Portuguese authorities chose this configuration for their RAPID initiative [IATA 2014b]. In any configuration, the first step produces a temporary token that is checked in the second step. The two-step process provides better control over the ABC process, although it slightly decreases throughput. Moreover, the flexibility and the usability are improved and the risk of user error is reduced because the traveler can easily understand which tasks to perform at each step. The SmartGate initiative of Australia and New Zealand initially employed a segregated two-step configuration [Frontex 2010]. In July 2015, the New Zealand customs ministry announced the installation of a new generation of e-Gates, SmartGate Plus, switching to a one-step solution to accelerate the clearance process.

2.1.3. Biometric system components. The BVS essentially contains the following HW/SW components, which are described for the main biometric modalities that have been implemented in ABC systems:

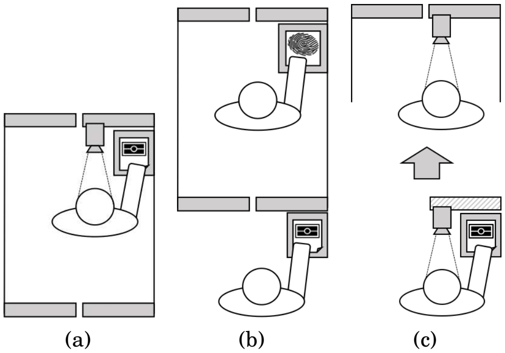


Fig. 4. Topologies of an e-Gate: mantrap for a) one-step process and b) integrated two-step process; c) segregated two-step process with kiosk plus single door e-Gate. The biometric traits depicted are given as an example of the traits potentially used at an e-Gate.

- the acquisition sensors,
- the illumination system,
- the biometric quality assessment module,
- the biometric verification module.

The acquisition sensors have to meet strong quality requirements that guarantee that the acquired samples have high image quality. In addition, they may automatically adjust to the characteristics of the traveler such that the acquisition process is simple and intuitive. The illumination system has to provide uniform and symmetric lighting, which compensates for the external lights to provide a high-quality sample. The quality assessment module checks the quality of the image, rejecting those that do not guarantee a high recognition accuracy. The verification module applies feature extraction to create a compact representation of an image known as a template and matching algorithms to verify whether the live captured image and that present in the document/database correspond to the same person. Section 3 thoroughly explores the different instruments and techniques used for each biometric trait.

The ISO/IEC 19784-1 Biometric Application Programming Interface (BioAPI) specifies a standard architecture for the communication between SW modules with biometric sensors of different vendors [ISO/IEC 2006]. The BioAPI 2.0 framework, via the so-called Biometric Service Provider (BSP) components, allows the SW modules to use any technology for which there is a BSP or it can be done.

2.1.4. External systems support to passenger clearance. ABC e-Gates are part of a larger smart border infrastructure that is being developed in many countries. When applicable, database queries are sent to external systems to verify the eligibility of the traveler to cross the border [Donida Labati et al. 2015b]. Figure 3 presents the overall schema of an e-Gate with links to the external systems. This figure illustrates three external systems: Visa Management System (VMS), Registered Traveler Program (RTP) and Entry-Exit Management System (EEMS). These systems essentially refer to central databases that collect different pieces of data related to border crossing. In particular:

- VMS stores visa application data. Additionally, it facilitates the exchange of visa application data, which may vary between states. Biometric samples of the traits captured during the visa application are stored, along with personal information, details of the travel and of previous applications [Unisys 2008].
- EEMS registers the entries and exits of travelers who cross the borders of a foreign state. EEMS is meant to replace the longstanding passport stamping procedure by

producing electronic records with the biometric data of the traveler. EEMS can help border authorities in identifying overstayers and collecting reliable statistical information on the migration flows.

- RTP is a voluntary enrollment system with the purpose of facilitate the border crossing of frequent foreign national travelers, e.g., people who travel for business or family reasons. During the enrollment in RTP, the traveler is extensively pre-screened, and biometric samples are collected and stored in a central database.
  Although RTP and EEMS are already present in some countries, other countries are conducting feasibility studies to analyze the relevant aspects of their implementation [PwC 2014].

To guarantee an appropriate level of interoperability between the e-Gate and the external systems, both parts need to rely on a standard definition of biometric data exchange formats. Several standards support the interoperability of applications and systems developed by different vendors. The Common Biometric Exchange Formats Framework (CBEFF) describes a set of data elements that can be used to exchange biometric information between systems, providing for the addition of metadata (e.g., capture device information) to a biometric data format (e.g., a fingerprint image) [ISO/IEC 2015a]. The ANSI/NIST ITL 1-2011 establishes formats for the markup and transmission of biometric data for the major biometric modalities [ANSI/NIST 2011]. Additionally, ISO addresses the interchange of biometric data via the multipart document ISO/IEC 19794 [ISO/IEC 2011]. This standard defines different acceptable formats to guarantee interoperability in biometric recognition systems, adding information about compression limits, such that conformance to this standard ensures the acquisition of sufficient quality samples. In addition to the formats used, the type of information exchanged impacts several aspects of the biometric verification process: samples, containing more information, make the system more flexible with feature extraction and matching [Donida Labati et al. 2015b]. In contrast, templates require less memory space, which reduces the required communication bandwidth, and are more privacy compliant [Donida Labati et al. 2014].

2.2. Electronic travel documents

When an e-Gate checks the identity of a traveler, it can rely on two types of travel documents: an identification MRTD, i.e., machine-readable passports, visas and ID cards, or a membership card issued to registered travelers who enroll in specific programs. Several countries have developed such registered (or trusted) traveler programs that release such cards, such as in The Netherlands and Saudi Arabia [van de Rijt and Santema 2010; Khan et al. 2010]. The use of MRTDs for checking identity facilitates travelers who do not require previous registration. The biometric passport, also referred to as an e-Passport, is currently widely used in border crossings due to their diffusion. It is estimated that more than 600 million e-Passports are in circulation today [ICAO 2015a], issued by some 120 countries [Siciliano 2014]. Some implementations additionally process national e-ID cards, as recently done in some airports in Spain [Cuesta Cantarero et al. 2013] and Portugal [IATA 2014b].

An e-MRTD is a combination of paper and electronics that contains the biometric markers of the owner. ICAO specifies in Doc 9303 the (de facto) standard guidelines for these biometric-enabled documents, to which an e-Passport should fully conform [ICAO 2015b]. An e-Passport stores the electronic information into a contactless integrated circuit (IC). The IC is composed of a microprocessor chip and a radio frequency identification (RFID) antenna embedded either into the center page, the back or the front cover of the e-Passport [Atanasiu and Mihailescu 2010]. To protect the information contained in the e-Passport, the data are protected with public-key infrastructure

(PKI) cryptographic technology, and the chip implements several security protocols [Mostowski and Poll 2010].

The ICAO specification requires that e-Passports contain the following elements:

- symbol of e-Passport;
- unified passport data page, containing the MRZ;
- personal data of the holder: name, date of birth, and other data;
- biometric samples (e.g., face image, fingerprints).

To decide among the different biometric traits available for person recognition, including the most common face, fingerprint and iris, but also signature, hand or voice, ICAO considered several features: global interoperability, uniformity, technical reliability, practicality, and durability [ICAO 2007]. For global interoperability of the recognition systems, [ICAO 2006] specifications mandate the use of facial data, and optionally, of fingerprint and iris data. While certain countries, such as the USA, the UK, Australia and New Zealand, decided to include no other biometric data in the e-Passport than a face image, others instead chose to also add fingerprints, e.g., the European countries in the Schengen area (face image and two fingerprints) and Malaysia (face image and two thumbprints) [Kwon and Moon 2008].

The inclusion of a second biometric trait inside the e-Passport can significantly improve the recognition performance of e-Gates, as the results obtained from the Spanish ABC system illustrate [Cuesta Cantarero et al. 2013]. However, because fingerprints are considered to be sensitive personal data, they are protected with an additional control mechanism. This mechanism increases the complexity of passport reading, and it requires that the countries exchange certificates to guarantee access to the fingerprint images. This additional access control to secondary biometrics is not yet specified by Doc 9303, but ICAO allows the use of national schemes to protect these data, and a specification is foreseen for future editions [ICAO 2015b].

3. BIOMETRIC TECHNIQUES FOR IDENTITY VERIFICATION IN ABC

In the context of ABC, biometric verification is the process of confirming that the person holding the e-MRTD is actually the owner of the document by using biometric technology [Frontex 2012b]. An ABC system can determine in a very short period of time and with a very high reliability whether the person attempting to cross the border is the legitimate holder of the presented travel document based on one or multiple biometrics. This section analyzes how e-Gates apply biometric identity verification, their setups, procedures and techniques employed, paying special attention to the most commonly used biometrics.

3.1. Biometric verification procedure

The most common biometric operation performed by e-Gates is identity verification, in which the e-Gate performs a comparison between live captured samples and the biometric data stored in an e-MRTD or a token. In some circumstances, the e-Gate uses biometrics to perform an identification operation, which involves a biometric search in a database. This type of operation can occur in the following situations: if the traveler is undocumented, if the system needs to check a watch list, if the ABC is based on a RTP, if the ABC includes an EEMS, or if the e-Gate uses two segregated steps.

ABC systems perform the biometric verification procedure following these steps:

- *Biometric data reading from identity document*: the e-Gate validates the authenticity of the document and reads the biometric data stored in it. This process should be quick. In particular, durations of two seconds for the optical check and of eight seconds for the chip reading are considered acceptable [Frontex 2012b].

— *Biometric sample capture*: the e-Gate informs the traveler of how to provide the biometric sample. The indications should illustrate the correct placement of the biometric trait toward the device for a better interaction. Moreover, the capture device may automatically or manually adjust to the characteristics of the traveler – e.g., height. The duration of this process is considered acceptable if it takes less than one second per frame [Frontex 2012b];
— *Quality evaluation and capture retry*: the e-Gate checks the quality of the acquired image. If it is not sufficiently high, the e-Gate could ask the traveler to retry the acquisition a specified number of times. To ensure an effective verification process, the captured biometric image must be compliant with the international standards. Only in this way will it be possible to accurately perform the matching.
— *Matching*: the e-Gate compares the live data with that stored in the travel document to check whether they correspond to the same person. The result of the verification process consists in the acceptance or rejection of the matching. It depends on a threshold defined by the border authority according to the security level, and result in values for the false acceptance rate (FAR) and false rejection rate (FRR). Therefore, the threshold value also has an impact on the performance of the system. The result of the verification process, as well as details such as the matching score or the reasons for rejection, are shown to the operator at the monitoring station. The biometric matching should not be longer than a few seconds, even in a centralized system, where the process is more complex because many distributed computing nodes are involved [Frontex 2012b].

To guarantee good service, the passage through an automated biometric gate should not take more than thirty seconds on average, from the moment the traveler scans the document to enter the e-Gate until the exit. However, analyzing the global performance of an ABC system is a complex problem, and it is further analyzed in Section 4. Many factors impact the accuracy of an algorithm and the overall performance of a system, such as the quality of data input, which depends on the sensors and feature extraction algorithms, the matching algorithms used or the population tested. Moreover, the procedure used by the e-Gate implementation, the user friendliness and, in general, usability are determining factors to the operation of an e-Gate and may affect the performance of the system [Spreeuwers et al. 2012]. This means that the performance data reported in this section are not intended to provide an absolute comparison between the different modalities, but they are valid for the specific conditions used in the cited studies.

3.2. Quality of the biometric sample

Capturing high-quality biometric samples is crucial for the performance and security of an ABC system [Donida Labati et al. 2015a]. The quality of a biometric sample represents the degree to which a biometric sample fulfills the specified requirements of an application, and the quality score is a quantitative expression of quality [ISO/IEC 2009].

There are three components that define the quality of a biometric sample: character, fidelity and utility [ISO/IEC 2009]. The character of a sample represents the inherent physical quality of the features of the subject. The fidelity indicates the degree of similarity between the acquired sample and the original source. The utility refers to the impact of the sample on the performance of a biometric system, generally in terms of matching performance. Utility depends on both the character and fidelity of a sample. It is generally accepted that the quality score should measure the predicted matching performance of the sample [Tabassi and Grother 2015].

Several factors can deteriorate the quality of a biometric sample [Alonso-Fernandez et al. 2012]. These factors are user-related factors (physical and behavioral), user-sensor interaction factors (environmental and operational), acquisition sensor factors (ease of use, maintenance, acquisition area and resolution), and processing system factors (constraints on storage, on exchange speed, government regulations and network communication). The following are more relevant in an ABC context [Donida Labati et al. 2015a]:

— *inexperienced travelers*: travelers who are not familiar with biometric recognition systems can have trouble performing biometric acquisitions;
— *stress*: the stress that many travelers suffer when they perform the border cross can make the interaction with the e-Gate difficult;
— *luggage*: many travelers carry luggage that can make the biometric acquisition uncomfortable;
— *lack of feedback*: if the ABC system does not provide proper feedback, the travelers cannot correct the problems that caused the acquisition of low-quality images;
— *lack of supervision by an operator*: the users can have problems interacting with the sensor if the system does not provide appropriate instructions. This problem can be alleviated if an operator explains the functioning of the sensor.

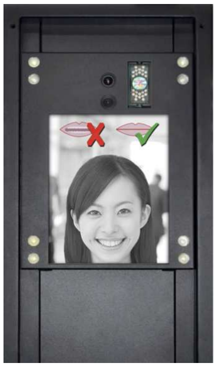
3.3. Monomodal verification

This section analyzes the recognition techniques used for biometric person verification in ABC, particularly face, fingerprint and iris. As shown in Section 3.5, these are indeed the most used biometric traits in ABC. We describe some aspects related to the quality of the acquired sample, how to assess it and the factors that influence quality. We examine the various recognition algorithms proposed in the literature for each trait, categorize the different approaches, and present the performance obtained in real ABC contexts or large-scale tests. Furthermore, we analyze the main advantages and disadvantages of these approaches in relation to the ABC context. As general criteria, the effectiveness and efficiency of an algorithm are key factors for its suitability to an ABC application, as well as exhaustive testing on large-scale populations and real operating conditions. Further discussion on the figures of merit that are more suitable for evaluating the biometric performance of an ABC system is presented in Section 4.2.

It is worth to note that government agencies do not easily release performance data in public reports because of security reasons [Bachenheimer 2014]. However, the disclosure of performance data can be useful for assessing the progress of an ABC project, to better design technology, and eventually to enhance credibility of the operator [Gelb and Clark 2013].

3.3.1. Face recognition techniques. Faces contain many stable features that guarantee high variability in facial appearance, such as the skeleton and musculature, the lips, eyes, brows or the face contour [Burrows and Cohn 2015]. The face is the primary biometric trait for e-Passports [ICAO 2006] because it offers many advantages. For instance, it is accepted from a social perspective because it is used normally by people to identify each other. Furthermore, 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, 45% of the systems explored use face recognition, either alone or combined with other modalities (See Table I in Section 3.5). Some examples of systems that use face recognition are RAPID in Portugal, SmartGate in Australia [Frontex 2010], the Spanish ABC System [Cuesta Cantarero et al. 2013] and APC in Canada and the US [Gorodnichy et al. 2014].

Current face recognition systems installed in e-Gates operate as follows. The face capture system directs the attention of the traveler to the camera, and instructional



(a)

Fig. 5. Face recognition at the e-Gate with instructional displays (reproduced with permission of Cognitec Systems GmbH).

displays help the traveler maintain a full-frontal and ICAO compliant pose, also requiring minimal effort from the traveler (see Figure 5). Moreover, many systems adjust their height to the eye height of the traveler, such as RAPID, or use more than one camera, such as SmartGate or the Spanish deployment. Other solutions include a pan-tilt camera, a movable mirror (1- and 2-axes), and a single wide-angle camera. The lighting that illuminates the face of the traveler can also be dynamically adjusted. To obtain high-quality images of the face, the illumination system has to provide uniform and symmetric illumination, which compensates the external lights and avoids blinding the traveler.

Factors that influence face image quality. Digital images acquired using cameras or scanners can be degraded by many factors. When poor quality face data are acquired at the authentication stage, face recognition becomes significantly more challenging [Jia and Gong 2015]. In an ABC context, the difficulties encountered in face recognition are due to factors related to personal characteristics (e.g., pose, facial expression, hairstyle, makeup, small occlusions, and motion blur) and to illumination conditions or device specifications (e.g., camera resolution, photo size, and image file format) [Sanchez del Rio et al. 2015; Conde et al. 2012]. In particular, the variation in the illumination conditions can cause dramatic changes in the appearance of the face [Zou et al. 2007]. Additionally, pose variation causes a significant decrease of the face recognition accuracy, particularly when large variations between enrolled and actual faces are present. For this reason, the e-Gate should guide the traveler to look straight into the camera and maintain a correct distance from the camera because the resolution decreases when the distance increases.

Other types of degradation in face images are more specific to images that are digitally acquired from the image printed in the e-MRTD. These problems include halftoning and dithering (non-idealities of the image typically deriving from the printing methods and quantization errors, respectively), and the presence of security watermarks on documents [Bourlai et al. 2011]. For example, 5% of European passports have photos of insufficient quality, which cause problems during the identity verification [Spreeuwers et al. 2012].

Quality assessment. For assessing the quality of face samples, many approaches use general image properties, including contrast, sharpness, and illumination intensity [Brauckmann and Werner 2006]. These properties are not actually specific to the face and cannot properly measure the degradation of face samples. In the literature, however, a number of works have assessed specific measures of face sample quality, such as detecting illumination, pose and facial expression changes [Abdel-Mottaleb and Mahoor 2007; Gao et al. 2007; Raghavendra et al. 2014].

The standardization of face image quality is required for the interoperability of the ABC system and reliability of the biometric verification. The following standards address this topic:

- ISO/IEC 29794, part 5 [ISO/IEC 2009]: This standard formally defines and specifies methodologies for computing quantitative quality scores for face images with the relative interpretation.
- ISO/IEC 19794, part 5 [ISO/IEC 2011]: This standard defines the acceptable formats for the storage of face images. It specifies scene constraints, photographic properties and digital image attributes of the face images. Moreover, it describes the full frontal face image and token face image as two suitable formats for verification processes. The face images contained in e-Passports have to be compliant with this standard [ICAO 2006]. Hence, it provides a description of the prototypical images with which ABC systems will have to operate.

In ABC systems, the use of quality assessment algorithms is of considerable importance. In most cases, deployed systems rely on commercial algorithms, whose implementation details are unknown. SmartGate, for instance, uses the technology provided by Cognitec [Jenkins and Burton 2008], the American APC employs technology provided by Vision-Box, and the Japanese deployment uses NEC's solutions. However, the lack of standardized approaches for calculating face quality is accompanied by some attempts. For instance, the Biometrics Identity Management Agency at the United States Department of Defense developed image quality measurement algorithms using the features identified in ISO/IEC standards to determine the quality characteristics of biometric images [Yen et al. 2013].

Feature extraction and matching. Once the e-Gate has obtained a high-quality face image, the recognition process can begin. Face recognition algorithms for ABC systems should be invariant to large variations in external variables such as illumination, pose and expression, as well as robust to noise. In an ABC scenario, the biometric acquisition is controlled, thus facilitating the recognition. As in the case of face quality estimation, ABC deployments use commercial face recognition algorithms, whose details are not public. Nonetheless, these algorithms share some common methods and characteristics that are analyzed below.

The typical pipeline followed by a face recognition system is: face detection, face image normalization, feature extraction and matching. After detecting the face from the image, it follows a normalization step, usually geometric and photometric. Geometric normalization serves to align the reference faces or a predefined face model using some landmarks, such as the eye centers. This step is very important because inaccurate landmark positions can reduce recognition performance. Hence, it is necessary to use misalignment-robust algorithms [Shan et al. 2015].

The following step is feature extraction. Combining the feature extraction methods, which are global and local, face recognition algorithms can be grouped into three main categories – global, local, and hybrid –, depending on how they analyze and represent the face image [Zhao et al. 2003]. Given the relevance of this step, many methods have been developed [Sanchez del Rio et al. 2015; Patil and Deore 2013], some of them being also used for detection. In the following, representative works and reviews are recalled.

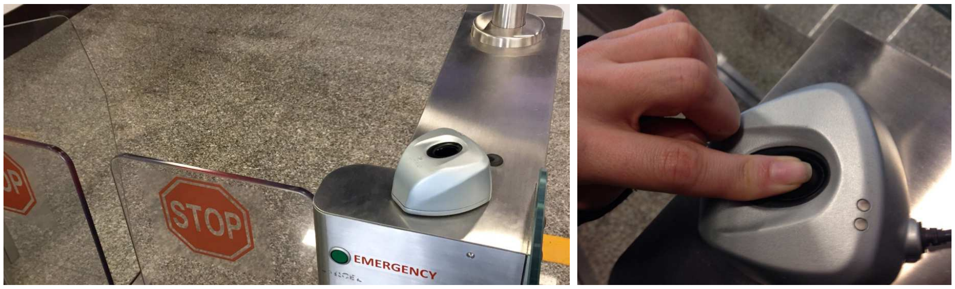
- *Global approaches for feature extraction.* Global (or holistic) approaches generally consider the entire face region for the recognition. Different feature extraction techniques are used to represent the entire face, including eigenface based on principal component analysis [Turk and Pentland 1991], Fisherface based on linear discriminant analysis [Belhumeur et al. 1997], Laplacianface using locality preserving projections [He et al. 2005], frequency domain based approaches [McCool and Marcel 2009], and methods based on sparse representation, such as the sparse representation classifier [Wright et al. 2009]. Recently, deep neural networks have been also used to learn face features, as in DeepID [Sun et al. 2014] and DeepFace [Taigman et al. 2014]. An advantage of the holistic approach is that all of the information in the image is considered, not limited to regions or points of interest. However, it is assumed that all pixels in the image are equally important. Hence, these techniques are computationally expensive and require a high degree of correlation between the compared images. Moreover, their effectiveness decreases under large variations in pose, scale and illumination. Regarding e-Gates, for high image qualities that do not require any particular enhancement, the holistic approach may be preferable. As an example, it is claimed that the Cognitec Systems company, which participates in the EasyPASS ABC project at major German airports, uses a global approach based on linear discriminant analysis for feature extraction in some commercial products [Huang et al. 2011].

—*Local approaches for feature extraction.* Local (or feature-based) approaches reduce the input face image to a vector of geometric features. They first process the input image to identify and measure distinctive facial features such as the eyes, mouth, and other landmarks, and then they compute the geometric relationships among those points. Local feature extraction techniques include Gabor wavelet-based techniques [Serrano et al. 2010], local feature analysis [Penev and Atick 1996], the *fiducial points* extracted in the elastic bunch graph matching [Wiskott et al. 1997], active appearance models [Cootes et al. 2001], local binary patterns [Ahonen et al. 2006]; scalar image feature transform [Bicego et al. 2006], histograms of oriented gradients [Dalal and Triggs 2005]. The main advantage offered by the feature-based techniques is that they are relatively robust to pose variations and can be invariant to scale and lighting. Moreover, these schemes offer a compact representation of the face images and high-speed matching. Their major disadvantages instead are the difficulty of automatic feature detection and the fact that the implementer has to select which features are more important than others. This could lead to non-harmonization of different automatic ABC systems. If the acquired image is not high quality, the local approach could be a better solution to account with imperfect face areas that would not be useful for matching, such as occlusions or areas with bad illumination.

After feature extraction, the last step the e-Gate applies is matching. For face verification, techniques based on supervised learning for binary classification, e.g., linear discriminant analysis or support vector machines [Guo et al. 2000], are commonly employed. Also, the simple Euclidean distance [Bicego et al. 2006], and neural networks [Lin et al. 1997] have been used. Finally, the deep neural networks used to learn face features [Sun et al. 2014; Taigman et al. 2014], are significantly improving state-of-the-art face recognition performance. The ABC scenario may benefit of this promising technique in future, but taking into account the need of increased computing resources.

Performance. Current face recognition algorithms can be more accurate than humans. In particular, many commercial algorithms have been tested in an independent performance evaluation, and the best performing algorithms can obtain results with very high accuracy, with a fixed FAR of 0.1% and FRRs of 0.3% [Quinn and Grother 2011]. These results represent the maximum performance of face recognition systems in a controlled environment.

Face recognition algorithms deployed in e-Gates should provide high recognition performance. In particular, the FAR should be less than 0.1% and the FRR less than 5%



(a) (b)

Fig. 6. Fingerprint recognition at the e-Gate: fingerprint sensor installed at the e-Gate (a), and particular of the in-use sensor (b). Reproduced with permission of Polizia di Frontiera Italiana.

to be considered acceptable [Frontex 2012b], but a FAR up to 1% was sometimes found to be set in real e-Gates [eu-LISA 2015b]. Using images acquired from a real ABC environment, various commercial algorithms have demonstrated that it is possible to obtain acceptable performance for an operational ABC application [Spreeuwers et al. 2012]. In particular, the best algorithm obtained a FAR of 0.1% and FRR on the order of 2%. Face verification in the EasyPASS project reached a 0.1% FAR and 5% FRR [Nuppeney 2012]. In a different setup that used real ABC images from the RAPID project, the algorithm provided by the supplier could achieve a FAR of 0.03% and a FRR of 4.25%. If the database contains only people that look alike (e.g., parents and their children or twins), the performance can decrease to a FRR of 5.2% [Frontex 2010]. However, in the same study 17% of the false rejections can be attributed to the use of glasses; other factors include wearing hats or occluding the face with hair.

3.3.2. Fingerprint recognition techniques. Fingerprints present a unique pattern of alternating ridges and valleys on the surface of each fingertip [Maltoni 2015]. This pattern is highly distinctive and unique for each individual. Moreover, their structure does not change during the individual's lifetime. Fingerprint recognition is currently the most mature biometric technology, with a great trade-off between performance and social acceptance [Maltoni et al. 2009].

Although fingerprints are optional in e-Passports [ICAO 2006], many ABC systems have employed them for traveler recognition. In fact, 56% of the ABC systems explored include fingerprint recognition systems, either alone or combined with other modalities (see Table I in Section 3.5). Some examples of systems that use fingerprint recognition are Global Entry [Pogoda 2011] in the US, PARAFE in France [Tsormpatzoudi et al. 2014], e-Channel in Hong Kong [Xiong et al. 2011] and the Spanish ABC system [Cuesta Cantarero et al. 2013].

Current fingerprint recognition e-Gates rely on optical acquisition devices, which are currently the most accurate [Maltoni et al. 2009] and require pressing the fingertip onto the acquisition surface. The e-Gate instructs the traveler on which finger to place on the sensor plate and how to do it by displaying appropriate instructions and illumination schemes (see Figure 6). Both one-finger and four-finger devices have been commercialized, compliant to international quality specifications [FBI 2013; BSI 2007]. These specifications include requirements on minimum capture size, resolution or spatial frequency response, and maximum distortion of the image. Recently, four-finger devices have been increasingly used across the world [Department of Homeland Security 2009].

Factors that influence fingerprint image quality. Acquired fingerprint images can be degraded by many factors. In particular, low-quality samples can result from physical aspects, such as poor skin conditions (e.g., skin being too dry or moist), dirty fingers, or latent fingerprints remaining on the sensor surface. Behavioral aspects can also influence the quality if the user is not familiar with the technology: for example, too low or too high pressure on the sensor will result in lower quality fingerprints [Maltoni et al. 2009]. Moreover, ergonomic aspects can also influence the quality, for example, when the sensor is placed at a non-comfortable height and inclination [Theofanos et al. 2008], as described in Section 4.1. Other aspects that are more specific to ABC environments include the presence of dust or grease on the fingertip and the difficulties imposed by luggage [Donida Labati et al. 2015a].

Quality assessment. In the literature, quality assessment algorithms for fingerprints can be divided into global, local and classifier-based methods [Alonso-Fernandez et al. 2007]. Global methods examine the image in a holistic manner, extracting global features such as the direction field, the uniformity of ridge-to-valley ratio or the clarity of the ridge pattern. Local methods divide the image into non-overlapping blocks and analyze features such as the orientation of the ridges and valleys, their structure or the power spectrum. Classifier-based methods use supervised learning techniques to combine local and global features to predict the matching performance. NIST Fingerprint Image Quality (NFIQ) [Tabassi et al. 2004; Merkle et al. 2010] is a widely used classifier-based method that has become the de facto standard for fingerprint quality assessment. In particular, the NFIQ algorithm measures features such as the orientation field and pixel intensity and assigns a quality value to each of the minutiae extracted from the image. Then, a neural network classifier analyzes the features and assigns the final quality value. Currently, a new version of this standard, NFIQ 2.0, is under development [Olsen et al. 2013].

To guarantee the interoperability of the ABC system, it is necessary to analyze the standards that address fingerprint image quality:

— ISO/IEC 29794, part 4 [ISO/IEC 2009]: This standard formally defines and specifies methodologies for computing quantitative quality scores for fingerprint images with the relative interpretation.
— ISO/IEC 19794, part 4 [ISO/IEC 2011]: This standard defines different acceptable formats to store fingerprint images, and it is the standard used for e-Passports [ICAO 2006]. The encoded information includes scanning parameters, compressed or uncompressed images and vendor-specific information, as well as the image format (WSQ, JPEG, and JPEG2000).

In ABC systems, the analysis of fingerprint image quality is also very important. In some cases, the system requires the use of standard algorithms, such as NFIQ or a compliant implementation, as in APC kiosks [Sava 2014]. In other cases, deployed systems rely on commercial algorithms, whose implementation details are not public. For instance, the Italian deployment in the Fiumicino airport uses the algorithm provided by Lumidigm, and PARAFE utilizes Morpho's technology.

Feature extraction and matching. Many ABC deployments use commercial fingerprint recognition algorithms, whose details are unknown. Nonetheless, these algorithms share some common methods and characteristics, which are analyzed below.

Fingerprint recognition techniques can be based on three different levels of analysis: Level 1 analysis is the coarsest one and considers the global ridge flow; Level 2 analysis is based on the extraction of the distinctive points caused by the discontinuities in the ridge structure, called minutiae points; and Level 3 analysis is the most detailed and is based on fine details, such as skin pores and inter-ridge information. Level 1 features are usually adopted to support the methods based on minutiae, while Level 3 analysis is not commonly adopted because it requires acquisition sensors with higher resolution than the ones currently used in ABC systems. Level 2 analysis is the most commonly used method in fingerprint recognition systems [Donida Labati and Scotti 2011]. It requires images captured with a resolution of at least 500 dpi and usually evaluate local characteristics of terminations and the bifurcations of the ridges.

In fingerprint recognition, the conventional pipeline based on Level 2 features consists of four steps: segmentation, image enhancement, feature extraction, and matching. The segmentation step is usually based on algorithms that perform local statistical analyses [Maltoni et al. 2009]. The second step is the enhancement, which aims to reduce noise and increase the contrast between ridges and valleys. There are different approaches in the literature. One of the mostly used techniques is based on a contextual filtering algorithm that applies Gabor filters tuned according to the local ridge characteristics to the input sample [Hong et al. 1998].

The most commonly used characteristics by feature extraction methods are the spatial coordinates and the orientation of the minutiae points [Bansal et al. 2012]. These methods estimate the minutiae coordinates from a binary image of the ridge pattern [Gamassi et al. 2005b] or extract the minutiae directly in gray-scale images [Maio and Maltoni 1997]. Moreover, methods that compute binary images can extract the feature points from thinned images representing the skeleton of the ridges [Arcelli and Sanniti Di Baja 1985], or directly search the minutiae in the binary images [Watson et al. 2007]. Usually, refinement method for removing erroneously estimated minutiae are also applied [Zhao and Tang 2007].

The extracted features are then used to compute the match score. In particular, global matching methods and local matching methods can be used [Maltoni et al. 2009]. Global methods compute the match score considering the whole set of minutiae extracted, and using different alignment strategies based on geometrical transformations to find the greatest number of matching minutiae [Watson et al. 2007]. In contrast, local techniques consider the minutiae extracted only in sub-regions of the fingerprint image, for example by adopting auxiliary graph structures [Liang et al. 2007].

Performance. Current fingerprint recognition systems offer a high recognition accuracy. They can obtain performance values on the order of $FAR \leq 0.01\%$, $FRR = 0.2\% - 0.3\%$ and $FAR = 0.1\%$, $FRR = 0.1\%$ in independent technology evaluations [Dorizzi et al. 2009]. However, technology evaluations are generally performed in controlled scenarios and may not consider poor quality samples, such as those that can be acquired in e-Gates due to the typical skin conditions of travelers or due to inexperienced users [Donida Labati et al. 2015a]. In real scenarios that use large databases, the performance can decrease to $FAR \leq 0.01\%$ and $FRRs = 3.5\%$ even if the recognition system uses the best finger enrolled [UIDAI 2012].

Fingerprint recognition algorithms deployed in e-Gates should provide high recognition performance, with at least $FAR \leq 0.1\%$ and $FRR \leq 3\%$ [Frontex 2012b]. The analysis of commercial algorithms in a real ABC deployment, PEGASE, has demonstrated that this performance can be achieved, obtaining a FRR of 1.6% [Frontex 2007] (FAR value not available).

3.3.3. Iris recognition techniques. The iris is the ring-shaped colored diaphragm that provides color to the eye and controls the amount of light that enters the interior of the eye. The iris typically has a rich pattern of furrows, ridges, and pigment spots [Bowyer et al. 2008], and it is very stable and presents a very high statistical variability among different individuals. These characteristics make the iris a very successful biometric trait.

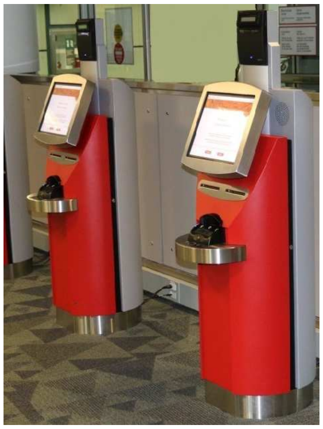


Fig. 7. Iris recognition kiosks of the NEXUS program (reproduced with permission of Canada Border Services Agency).

Iris recognition has frequently been used at border controls [Daugman 2015]. Its main advantages are its extraordinary resistance against false matches, as well as its substantial matching speed [Burge and Bowyer 2013]. These characteristics favored its application in the first deployments of e-Gates, which generally relied on RTPs and biometric identification rather than verification. Some examples of these first deployments include IRIS in the UK [Palmer and Hurrey 2012], Privium in The Netherlands [van de Rijt and Santema 2010], NEXUS and CANPASS Air in Canada [Acharya and Kasprzycki 2010], ABG in Germany [Koslowski 2003] and the system deployed in the UAE [Daugman 2004].

One of the main drawbacks of iris recognition when it is used in ABC systems is that none of the e-Passports currently in circulation include the iris as a biometric trait [Palmer and Hurrey 2012], although it is an optional biometric for e-Passports [ICAO 2006]. This means that the ABC systems that use iris recognition need to create extra back-end systems that contain iris information. For this reason, they tend to be less flexible and cost-effective than systems that rely on e-Passports [Palmer and Hurrey 2012]. Nonetheless, 12% of the systems studied in this document use iris technology, either alone or in combination with other modalities (See Table I in Section 3.5).

Current iris recognition systems installed in e-Gates rely on short-range digital cameras, which typically operate at a distance of approximately 25 cm when one eye needs to be scanned and approximately 100 cm when both eyes are necessary [Donida Labati et al. 2015b] (see Figure 7). The acquisition system displays directions that instruct the traveler to correctly look at the camera. Then, the system illuminates the face of the traveler with near-infrared illumination (in the 700-900 nm range) that allows a visible texture for both light and dark irises [Burge and Bowyer 2013]. By using this procedure, the system guarantees that the iris images are of high quality, which facilitates recognition and improves the overall experience of the traveler.

Factors that influence iris image quality. The analysis of iris image quality is also a major concern in ABC systems, which perform quality assessments to detect and discard images with common quality problems such as extremely dilated pupils or unreasonably closed eyelids [Daugman 2015]. In particular, the factors that affect iris image quality are divided into two main groups [Schmid et al. 2013]: unconstrained presentation of the subject (e.g., off-angle presentation, heavy occlusion) and environmental and camera effects (e.g., insufficient lighting, defocus blur). These types of problems have a negative impact on the recognition accuracy [Abhyankar and Schuckers 2009].

Quality assessment. The taxonomies of iris image quality algorithms generally divide them into two classes: local and global analyses [Schmid et al. 2013]. Global methods analyze the entire image to detect aspects that can reduce recognition performance. Local methods study different regions of the image based on the assumption that iris texture is very localized, which changes the quality from region to region [Chen et al. 2006]. However, most recent approaches fuse both local and global information, using each approach to detect different acquisition problems. Indeed, comprehensively assessing iris image quality is a challenging problem because it is influenced by multiple factors, whose contributions to the quality are not fully understood [Li et al. 2011]. These approaches can detect many problems that can become important in an ABC context, such as out-of-focus or motion blur, occlusions, off-angle gaze, poor illumination, specular reflections, excessive pupil dilation, uneven lighting or poor quality of the segmentation.

To ensure the interoperability of the ABC implementations, it is necessary to rely on standards for iris image quality. This topic has been addressed by the following standards:

- ISO/IEC 29794, part 6 [ISO/IEC 2009]: This standard formally defines a set of quality components that quantitatively measure image-specific or subject-specific factors. This standard also considers compression algorithms that can be used to reduce storage space, which can become important given the storage space constraints imposed by the chips installed in e-Passports. Indeed, different studies have demonstrated that iris images can be compressed to as small as 2 kB with little impact on accuracy if the system is properly configured [Rakshit and Monro 2007].
- ISO/IEC 19794, part 6 [ISO/IEC 2011]: This standard defines different acceptable storage formats for iris images and has to be used for the images in e-Passports [ICAO 2006]. However, the number of systems that use this standard is limited [Quinn et al. 2013]. In many cases, the ABC system directly relies on the iris template, though this approach is not interoperable. This is the case of systems based on RTPs, such as the IRIS project or the UAE's system [Daugman 2015].

Feature extraction and matching. Once the e-Gate has obtained a high-quality iris image, the proper recognition process can begin. The first step is iris segmentation. The special characteristics of the iris make this process particularly difficult because the iris is a relatively small area of the eye, wet and in constant motion caused by involuntary movements. An incorrect segmentation can lead to a reduction in the final accuracy of the ABC system [Donida Labati et al. 2012].

Most ABC systems based on iris recognition use the algorithm proposed by Daugman, which approximates the iris using two concentric circumferences [Daugman 2004]. However, in some cases, this approach is not the best solution. Indeed, the human iris is not perfectly circular. Some methods address this problem using more complex approximations, such as ellipses, active contours, the analysis of local characteristics, or hybrid methods [Donida Labati and Scotti 2010; Donida Labati et al. 2012].

The next step in iris recognition analyzes the segmented iris image to extract distinctive features from the iris pattern. Using these features, the recognition system computes the iris template. One of the most commonly used templates in ABC systems is IrisCode [Daugman 2004], which has been used in IRIS, the UAE [Daugman 2015] and Privium [Shoniregun and Crosier 2008], for example. In particular, IrisCode uses a pseudo polar coordinate system that is invariant with regard to factors such as the size of the pupil, the distance from the eye to the camera or the angle and orientation of the iris. The patterns are then encoded using a 2D Gabor wavelet transform that extracts the phase structure of the iris and produces a template of 512 or 1,024 bytes. However, algorithms based on other technologies are gaining acceptance. Among them, we can highlight the following [Bowyer et al. 2013]: the adaptation of eigenfaces from face recognition; the use of alternative filters to analyze the iris texture, such as local intensity variations; the use of alternative methods to represent textures, such as edge maps; or the analysis of the iris in parts and the combination of the results.

Once the template is calculated, the final step computes a matching distance between the templates to determine whether they are from the same person. In most systems, the matching score is calculated using the Hamming distance [Daugman 2004]. In the border controls that operate on large databases, such as the one installed in the UAE, it might be necessary to use optimized algorithms that can reduce the search time [Hao et al. 2008]. Machine learning techniques have also been applied to iris recognition [Marsico et al. 2016]. Very recently, deep learning was used to tackle the problem of heterogeneous iris verification that typically arises in large-scale identification applications, where different sensors are likely to be used [Liu et al. 2015].

Performance. Iris recognition systems offer a high recognition accuracy. The best performing algorithms can obtain results of $FRR = 0.28\%$ and $FAR = 0.001\%$ when tested by independent agencies [Grother et al. 2009]. These results represent the maximum performance of iris recognition systems in a controlled environment.

When tested using images from an ABC environment, iris recognition algorithms have also exhibited a high recognition performance. For instance, using images from the UAE ABC system, it was possible to obtain a FRR of 0.32% with $FAR = 0\%$ [Hao et al. 2008]. Additionally, considering problems such as smartcard reading or iris acquisition errors, the performance may decrease. Even if the FAR has been reported as very low [Frontex 2007], FRR increases, as in the case of the Privium project, with a FRR of approximately 1.5%, and IRIS project, with a FRR of less than 2% and $FAR = 0\%$ [Frontex 2007].

3.4. Multimodal verification

Multimodal biometric systems utilize more than one physiological or behavioral characteristic for enrollment, verification, or identification. These systems have the potential to conduct more reliable verifications of the traveler's identity because of the increase in information available for recognition [Jain and Ross 2004]. In particular, automatic identity verification of a passport holder using the face may not be effective against identity theft unless multimodality is adopted [Kosmerlj et al. 2005]. Furthermore, an improvement in the matching performance would result in a better experience for the user and in an increase in the traveler flow efficiency.

The multimodal approach to identity verification is increasingly finding consensus in ABC systems, as illustrated by the increasing number of deployments that have started using this technology. The choice of biometric traits, however, is still not standard. For example, the ABC systems deployed in Beijing Airport and Shenzhen Bay Port in China or the project J-BIS in Japan combine face and fingerprint; Friendship Gate in Pakistan uses face, fingerprint and/or iris; and Israel-Palestine land border control utilizes face and hand geometry [Nanavati 2011].

Multimodal biometric systems contribute to reducing several problems of monomodal systems [Jain and Ross 2004; Gamassi et al. 2004; Cimato et al. 2006], including non-universality, which is relevant in a large-scale context with a large variety of users such as ABC systems, accuracy of the sensor, noisy data, intra-class variability, limited discriminability and limited spoofing robustness, which is an essential feature for border check applications (further discussion in Section 4.3). However, multimodal systems present costs, acquisition times and computational times that are higher than those of the traditional monomodal systems [Ross et al. 2006], and user perception may be of larger invasiveness for their privacy.

Multimodal biometrics can use data obtained from multiple sensors, multiple modalities, multiple instances, multiple samples and multiple algorithms [Ross et al. 2006]. In addition, the system can acquire the biometric data both simultaneously and sequentially [ISO/IEC 2007]. In a simultaneous presentation, the system acquires biometric samples from multiple modalities in a single event, e.g., a face and iris of the traveler taken from the same camera. Using this type of biometrics presentation, systems are able to provide higher throughput, but the complexity of the overall functioning may increase. In a sequential presentation, the system acquires biometric samples from one or multiple modalities in separate events.

In particular, the information coming from each monomodal component can be integrated at four different levels depending on the module of the biometric system at which they are fused [Ross et al. 2006]: 1) sensor level, immediately after the samples have been acquired; 2) feature set level, once the features from each sample have been extracted; 3) matching score level, after the matching score for each sample has been calculated; and 4) decision level, once a decision has been obtained for each sample.

Fusion at the sensor level is normally performed using a concatenation of the data collected from different sensors. This type of method is the least commonly used, and its application in ABC systems is still complex. Fusion at the feature set level is normally performed by merging the extracted feature vectors and then performing the matching on the combined feature vector. In principle, possible dependencies between the multiple biometrics can be exploited more with such a fusion approach than by using a score-level fusion [ISO/IEC 2007], obtaining a greater improvement in performance. However, its application is more difficult. The application of this type of technique to ABC systems is a promising trend currently under study, for instance, in the ABC4EU project [ABC4EU 2014].

Fusion at levels 3) and 4) occurs after the matching module is invoked and is closer to the characteristic of "neutrality" with respect to the technology producer, which is useful for the integration of different software modules for biometric identity verification. Fusion at the matching score level is performed by aggregating the scores of the different matching methods. A single decision module is then used to determine whether the comparison is genuine or an impostor. This fusion level is the most used technique in real applications because it can greatly increase the accuracy of a biometric system while being simpler to implement than fusion at a lower level. These types of methods have great potential to be used in ABC systems. Decision-level fusion is performed by aggregating the decisions of the different decision modules. It has the great advantage of being applicable to all existing biometric systems because it exploits only the final binary output of the system. However, it generally provides less accuracy and flexibility on the system's design compared with other fusion techniques. This type of method has already been deployed in ABC.

It has frequently been observed that fusion at the early stages can favor the accuracy of the system more than if integration occurs at later stages [Rattani et al. 2007]. However, the application of fusion at the sensor and feature levels in ABC gates is difficult because the raw data of the traits embedded in the sensors are typically not available for other manipulations. Nevertheless, fusion at higher levels, namely, at the matching or decision level, still offers a significant increase in accuracy to the overall biometric system [Raghavendra and Busch 2015].

Technical details about ABC systems deployed are limited, making it difficult to classify them according to the fusion approach adopted. Nonetheless, in the context of the ABC4EU project, we had access to the details of the Spanish and Italian systems, which use face and fingerprint with a cascaded decision-level procedure. The Spanish ABC system uses the face as the primary biometric modality, whereas fingerprints are used in uncertain situations. In particular, two thresholds (lower and upper) are selected for face verification: with a value under the lower limit, the traveler is surely rejected, whereas they are safely admitted when the score is greater than the upper limit. Fingerprints are then used only when the verification score falls between the upper and lower limits and additional evidence is required [Cuesta Cantarero et al. 2013]. Using this approach, the system could reduce the FRR from 12.23% to 3.72%. The Italian ABC also uses the face as the primary biometric. If the face verification fails, the traveler proceeds with fingerprint verification, independently of the obtained matching score. The Italian border authority has not reported an improvement in recognition performance.

3.5. Deployments

ABC is gaining ground worldwide, currently being present in 48 countries. The number of ABC systems is expected to increase as some pilot deployments – such as Smart Borders [eu-LISA 2015b], FastPass [FastPass 2013], and ABC4EU [ABC4EU 2014] – have a full-scale roll out, particularly at land borders and seaports. Today, the majority of e-Gates are used at airports, whereas land and seaports represent only 4.7% and 22%, respectively, of all e-Gates deployed [Acuity Market Intelligence 2014].

Many ABC systems deployed chose the face as the biometric trait for person verification. This is the case in Portugal, Australia, and the US, among others. Nevertheless, fingerprint recognition systems are often employed in automatic border control. There are systems installed in France and the USA, as well as in Rwanda, Venezuela, Qatar and other nations. The deployments in Venezuela, Colombia and Estonia, for example, perform a combination of face and fingerprint biometric verification. The map in Figure 8 presents an overview of the systems deployed worldwide marked per biometric trait, and Table I presents the number of deployments per trait.

At the top level, ABC systems can be divided into two different types, depending on whether registration is required for their use: the regular systems, designed for travelers holding an e-MRTD, and RTP systems, which may require a membership card from travelers who have been pre-screened in that registered traveler program. Given the increasing number of e-Passport issued, many countries have invested in the deployment of ABC systems based on e-Passport for traveler clearance [IATA 2014a]. Other countries, such as those in the EU, are developing novel systems that integrate both the regular and registered features [EC 2011], and pilots are also currently in support of automated border control at sea and land ports [eu-LISA 2015a]. The US Global Entry scheme is the largest system to use registration. Table II lists the number of ABC systems using a certain biometric trait, both for registered and non-registered travelers. This table clearly shows that fingerprints and face are the biometric traits most used in the registered and non-registered cases, respectively.

Different types of travel documents can be used for eligibility, including e-MRTDs, permanent resident cards or registered traveler cards. The data collected in our study indicates that within the systems allowing the use of e-MRTDs, the face is the most used trait if registration is not required. In the case of registration, a biometric document may not be required by the system because it can retrieve the biometric data of passengers from a database. For example, the U.S. Global Entry allows travelers to use a machine-readable passport or, alternatively, a permanent resident card. With the exception of the EU, whose e-Passport includes fingerprint, only in the 35% of the cases are biometric traits other than the face used without a previous registration. Typically,

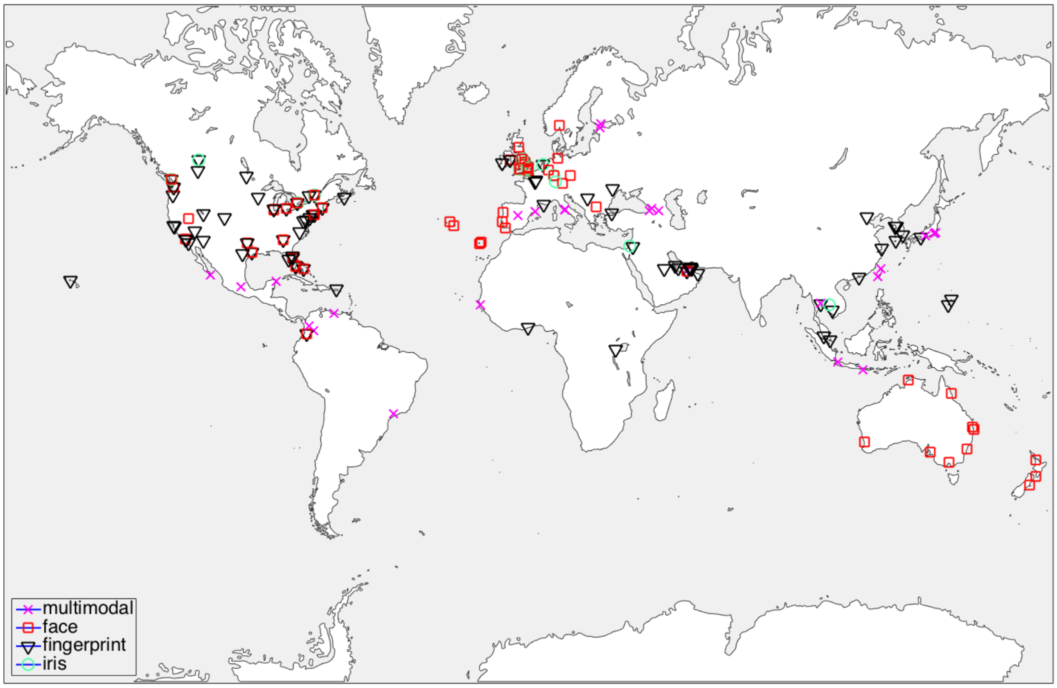


Fig. 8. Biometric traits used at ABC systems deployed worldwide. Data source: http://www.iata.org/.

Table I. Modalities used at 181 air automated border control deployments worldwide. Data source: http://www.iata.org/.

	Face	Fingerprint	Iris	Other[a]	Multimodal
Number of systems	81	102	22	1	22

[a]Hand geometry

Table II. Modalities most used at air automated border control deployments with or without traveler registration. Data source: http://www.iata.org/.

	Registered	Not Registered (MRTD/e-MRTD)
Face systems	8	73
Fingerprint systems	75	27
Iris systems	19	3
Multimodal	11	11

these systems work for national citizens only, or for countries with which there is an agreement.

4. BIOMETRIC CHALLENGES AND RESEARCH TRENDS IN ABC SYSTEMS

This section analyzes the major issues, challenges, and research trends related to biometric recognition in ABC systems. In particular, we introduce some design considerations related to the usability and ergonomics of the biometric devices, as well as in the case of passengers with special needs, and present the issues in the evaluation of biometric systems in the context of ABC systems. We describe vulnerabilities and possible attacks on biometric systems, along with anti-spoofing methods. Additionally, the section includes considerations regarding privacy protection of the biometric data.

4.1. Usability and ergonomics

In order for ABC systems to be successful, they not only have to support security, but they also need to guarantee that the travelers can interact with the e-Gate, and make the user experience acceptable [Sasse 2007]. To do that, the system has to consider aspects as usability and ergonomics. These terms are often intertwined in the design and implementation of a system featuring human-machine interactions. In particular, these terms refer to different aspects:

- *Usability* refers to the extent to which specified users can use a product to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use [ISO 1998]. Particularly, the effectiveness can be measured by the number of errors in using the ABC system and by the rate at which the users complete the border crossing, whereas the efficiency can be measured by the time spent using the ABC system. Finally, user satisfaction considers the way the system is perceived by the users, if people like to use it, and if they can successfully use it to cross the border.
- *Ergonomics* refers to the design principles used to arrange the components of the system that require interaction with the user such that the people can use the system easily and safely.

Usability and ergonomics are strongly dependent on each other, and the design of a usable system must consider ergonomic principles, and vice versa. In ABC systems, usability is primarily related to the user interface used to instruct and guide the travelers [Oostveen et al. 2014], whereas ergonomics is primarily related to the position of the biometric devices inside the e-Gate.

The user interface and the instructions shown during the border crossing procedure are designed to be clear to understand by people of different nationalities and cultures, to reduce the amount of time required to use the system (increasing the efficiency), the errors due to unclear procedures, and the difficulty in learning them (increasing the effectiveness). In fact, instructions rely on symbols, rather than text, and tell the traveler where to place their feet to have their face captured and where to look, where to place their finger during the fingerprint acquisition step, and which finger to use. Similarly, instructions guide the traveler to place their eye on the iris scanner. For this purpose, illuminations are used in some cases to direct the user toward the appropriate sensor at the right time: for example, the optical fingerprint scanners used in ABC systems emit a light when they are active, and the cameras used to capture the face images, as well as the iris scanners, use a led when they are turned on. Instructions often also clearly instruct the user about the outcome of the recognition procedure (positive or negative).

The position of the biometric acquisition devices is chosen to be the most natural possible by considering the average height and size of a person passing through the e-Gate and adapting the position of the sensors accordingly. The camera used to capture the face images may be capable of adjusting its height to capture a frontal acquisition [Frontex 2010]. Moreover, by designing a fingerprint scanner that is capable of automatically moving up or down according to the height of the user, the usability and ergonomics of the biometric recognition process would be improved because the height and inclination of the fingerprint scanner, in relation to the height of the people using it, influence the quality of the captured samples [Theofanos et al. 2008]. Similarly, adjustable iris scanners with automatic tilt features have been implemented [M2Sys 2015].

4.1.1. Challenges and design considerations for passengers with limited mobility. Currently, ABC systems seldom adopt usability and ergonomics design principles for accommodating people with limited mobility, and biometric recognition procedures can present several obstacles for people in such situations. In some countries, specific laws specify equal rights for air transportation [EC 2006]. For these reasons, innovative ABC systems shall be designed by also considering the limitations of these categories of people.

In particular, it is possible to consider four categories of travelers with limited mobility:

- *Injured travelers* can have problems providing a high-quality biometric sample. For instance, an injured face, finger, or iris may not be usable for recognition. In addition, an injured traveler may encounter difficulties in placing their finger on the sensor. In cases where the injury causes the recognition step to not be sufficiently reliable, the passenger needs to be redirected to a manual check, where the help of a trained operator and the use of a mobile scanning unit [MobilePass 2014] could perform the acquisition in a greater number of situations.
- *Travelers with walking aids (e.g., crutches)* could have problems in placing their finger on the sensor while using the walking aid (e.g., the hand is the same) or if the e-Gate is too narrow and is not easily accessible while holding the walking aid. In this situation, a chair or a support could help people in performing the biometric recognition with more comfort.
- *Travelers in wheelchairs* could encounter difficulties in passing through the e-Gate if it is too narrow and in reaching the biometric sensors if they are placed too high. Larger gates and biometric devices with automatic height and tilt adjustment could help in these situations.
- *Travelers not able to freely move their limbs (e.g., with arthritis or muscle damage)* may have problems in moving their head to capture a frontal acquisition. Similarly, they may lack the ability to place the required finger on the surface, keep it steady for a sufficient time, or exert the necessary pressure. Moreover, they may encounter difficulties in correctly placing their face near the iris scanning device. In these situations, face recognition algorithms able to detect non-frontal acquisitions [Abiantun et al. 2014], fingerprint scanners with pressure sensors, or iris recognition systems with automatic tilting systems or able to work with off-axis acquisitions [Chou et al. 2010] could help in promptly detecting the problem.

4.1.2. Challenges and design considerations for passengers with visual impairments. Several aspects of e-Gates could present problems for people with colorblindness, poor eyesight, or with total visual impairments. In the design of innovative ABC systems to accommodate people with visual impairments, we can consider three categories of people:

- *Colorblind people* have problems in distinguishing some colors, and they may face difficulties if such colors are used in the interface to instruct them during the biometric recognition process. In this case, safe and pleasant combinations of colors could be used to avoid problems for colorblind people and to increase user satisfaction.
- *People with poor eyesight*, for example, elderly people, can move in confined spaces and interact with most objects, but they may have problems in reading text or in precise positioning (e.g., placing the passport in the slit or placing the finger onto a small surface). In these situations, larger symbols and illuminations could be used to guide the traveler. Sounds could also be used in conjunction with illumination or with the appearance of graphical instructions to help guide such people.

—*People with total visual impairment* cannot see the graphical instructions given, the physical structure of the e-Gate, or the placement of the biometric sensor inside it. In these situations, unless the traveler is familiar with a particular place, e.g., a person who often travels in the same airport (in which case auxiliary annotations in an adequate language (e.g., Braille) could be provided), an operator shall be alerted on time to help him or direct him to a manual check.

4.1.3. Challenges and design considerations for aging passengers. The aging process can have implications for the usability of the e-Gate because it can change physical and cognitive characteristics. In addition, if elder users have difficulties to present their biometrics, this can lead to their exclusion [Sasse and Krol 2013]. Although some of these problems have been contemplated in Sections 4.1.1 and 4.1.2, the design of ABC systems should take into account other aspects, such as the impact of cognitive aging on the use of technology.

In this context, the main difficulties are the deterioration of cognitive capabilities (e.g., memory decline or longer reaction times), the lack of knowledge and mental models and the variations in cultural and social values [Sasse and Krol 2013]. These difficulties can be addressed in the following ways: providing appropriate training and feedback, designing the interface paying attention to elder's needs, and taking into consideration that practice and a higher degree of exposure will improve performance and increase acceptance.

4.1.4. Research trends. Currently, several projects involving producers, research institutions and governmental authorities are active in the design and development of innovative and more usable ABC systems. For example, the research projects ABC4EU [ABC4EU 2014], FastPass [FastPass 2013], and MobilePass [MobilePass 2014] have the purpose of harmonizing the functionalities of different e-Gate implementations and enhancing the workflow of the border crossing process through introducing a series of design recommendations regarding usability and ergonomics.

Some published research results, which address the typical issues of each biometric trait, can improve the overall usability of an ABC system. Regarding face recognition, novel matching algorithms capable of working with non-frontal acquisitions, degraded images, or variations in illumination, expression and pose have been researched [Sanchez del Rio et al. 2015]. In particular, 3D face recognition can provide more robustness in the case of variations in pose and illumination conditions [Lei et al. 2014].

From the research activities performed under the ABC4EU project, we obtained original results regarding the quality estimation of fingerprint images. We proposed an advanced method for detecting the type of dirt that could be present on the finger of the traveler (e.g., flour or cream) or which action resulted in the temporary modification of finger features (e.g., hand swollen due to carrying a heavy bag) [Donida Labati et al. 2015a], and we used this information to suggest corrective actions to the traveler. Moreover, innovative algorithms have also been proposed to match low-quality fingerprints [Yang et al. 2013]. For iris recognition, innovative algorithms have also been proposed for non-frontal (off-axis) acquisitions [Chou et al. 2010].

Finally, innovative touchless and less-constrained biometric acquisition systems have recently been proposed to lower capture times and increase the usability and user acceptance of the recognition using the iris [Matey et al. 2006; Nguyen et al. 2011; Donida Labati and Scotti 2010], the palm [Genovese et al. 2014; Kanhangad et al. 2011], and the fingerprint [Genovese et al. 2016; Donida Labati et al. 2016; Donida Labati et al. 2015b; Donida Labati et al. 2015; Donida Labati et al. 2014].

4.2. Evaluation of the biometric recognition

The evaluation of a biometric recognition system must take several aspects into consideration [Genovese et al. 2014]:

- *accuracy* refers to the ability of the biometric system to correctly match the live sample against the sample contained in the e-Passport or to correctly identify the individual in a database (e.g., an RTP or watch list), and it is generally measured in terms of equal error rate (EER), FAR, and FRR;
- *speed* refers to the time required to perform the recognition, and it is an important factor, particularly when performing identification (e.g., in the case of RTPs or watch lists);
- *scalability* refers to the ability of the biometric system to function efficiently when the number of travelers and enrolled users increases;
- *interoperability* is related to the use of common standards for exchanging biometric data (e.g., same template format) and results (e.g., same match score range) and to the use of the same biometric device, which is important for the adoption of a common ABC infrastructure;
- *usability* regards the ease of use of the system and the ease with which the people learn to use it, as described in Section 4.1;
- *social acceptance* refers to the way the system is perceived, and it is influenced by the usability, invasiveness, risks (real and perceived), and personal opinions;
- *security* refers to anti-spoofing measures and to methods for defending the software and hardware architecture against attacks, as described in Section 4.3;
- *privacy* refers to the techniques used for avoiding theft or misuse of the biometric data, as described in Section 4.4.

In the context of ABC systems, the evaluation of the BVS is a particularly complex task because it requires the consideration of several systems and procedures involved in verifying the identity of travelers. In fact, it is necessary to consider possible differences in the physical media (e.g., passports issued by different countries), the biometric devices (quality and type of cameras, iris, and fingerprint scanners may vary considerably), the e-Gate implementations (with potentially different sizes and crossing times), the interaction with external systems and databases (VMS, EEMS, and RTP), and variations in the biometric recognition procedures (devices cleaned less or more frequently and variable number of possible biometric acquisition retries).

In particular, the operational evaluation of the BVS focuses on aspects such as accuracy of recognition, traveler throughput, and usability, as well as analyzing how these factors influence each other [MacLeod and McLindin 2011]. However, although most aspects can be accurately evaluated in ABC systems, the accuracy evaluation faces some challenges because too few impostor attempts are present [MacLeod and McLindin 2011] and collected biometric data are not readily made public for privacy reasons. In fact, the legislation of some countries does not allow the public dissemination of biometric data (particularly regarding the fingerprint and iris traits), match scores, and decision thresholds obtained and used by the biometric systems installed for government activities [Sprokkereef 2008; Iglezakis 2013]. Therefore, it is not possible to compute the typical figures of merit used in the accuracy evaluation of biometric systems, such as the FAR, FRR, and receiver operating characteristic (ROC) [Gamassi et al. 2005a; Mansfield and Wayman 2002], and the evaluation of the accuracy primarily relies on figures of merit computed using technology evaluations performed on public datasets or using internal testing procedures [MacLeod and McLindin 2011]. However, data collection procedures can be performed on a subset of the transactions processed by ABC systems to verify its correct functioning [Frontex 2012a] (e.g., match scores or error messages), as long as data protection techniques are used [EC 2009].

4.3. Vulnerabilities and attacks

In the literature, the attacks on biometric systems are grouped in eight types [Ratha et al. 2001]. Figure 9 illustrates the adaptation of these attacks to the ABC system scenario, while Table III presents a brief overview. Attacks can be further divided in two main classes [Galbally et al. 2010]: Types 2 to 8 of indirect attacks, which perform actions against the communication channels and the software modules of the biometric system, and Type 1 of direct attacks, which consist of submitting a fake biometric to the sensor. In the following, we describe and discuss the two classes.

Type 2 attacks consist of intercepting the channel that connects the sensor with the feature extractor to replay a sample previously acquired. This type of attack can affect the RTP or EEMS, which can require the submission of the sample to a central repository. Type 3 attacks force the feature extractor to produce a template chosen by the attacker rather than that obtained from the real sample. This type of attack is difficult to perform [Faúndez-Zanuy 2004] and could probably require the use of a Trojan horse that bypasses the feature extractor [Galbally et al. 2010]. Type 4 attacks are similar to Type 2 attacks but intercept the channel between the feature extractor and the matcher. Again, RTP or EEMS systems are more vulnerable to this type of attack. Type 5 attacks make the matcher produce lower or higher scores, independently of the template, similar to Type 3 attacks. Type 6 attacks alter the database that stores the sample or the template that is compared with the input sample by substituting it with an impostor template. In an ABC environment, this database can be the RTP or EEMS systems or the e-MRTD. If this attack is successful, the e-Gate will be permanently fooled into considering the corresponding impostor comparison as genuine. This attack is particularly feasible if the traveler carries a fake e-MRTD. To avoid this type of attack, most e-MRTD include optical security features that permit identifying whether tampering with the e-MRTD has occurred. Moreover, they also implement security measures to preserve the data stored in the passport. In general, the data are digitally signed by the issuing institution, and the access to the data stored in the chip is protected by secure protocols, such as basic access control (BAC) [Frontex 2007] or extended access control (EAC) [Frontex 2010]. Type 7 attacks intercept the channel between the database (the RTP or EEMS database or the e-MRTD) and substitute the data stored there in an analogous way as in Types 2 and 4. This attack can affect the RTP or EEMS scenarios as in Type 2 and 4 attacks. In a system that uses e-MRTDs, this attack can be particularly relevant because the communication between the reader and the document is wireless in many cases. In particular, e-Passports use RFID chips to communicate with the reader. The design of these chips assumes a communication range between 0 and 10 cm. However, it is possible to design devices that operate at longer distances [Frontex 2007], which can permit the communication channel to be attacked. Type 8 attacks skip the entire biometric verification process and overwrite its decision. This attack intercepts the communication channel between the matcher and the mechanism that controls the e-Gate. Indirect attacks require knowledge of the internal working of the recognition system and, in most cases, physical access to its software components [Galbally et al. 2010]. For this reason, this type of attack is more complex to perform.

By contrast, direct attacks (Type 1 in Figure 9) consist of submitting a fake biometric to the sensor, e.g., a fake finger, a face photograph or a contact lens with a printed iris pattern. Several researchers have demonstrated the success of this type of attack. Its main advantage, from the attacker's perspective, is that it only requires a fake biometric trait. Hence, its feasibility can be high compared with indirect attacks [Uludag

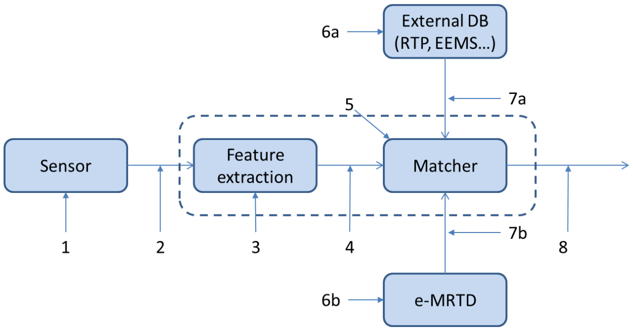


Fig. 9. Vulnerabilities of the biometric system of an e-Gate and corresponding points of attack.

Table III. Overview of the vulnerabilities of the biometric system of an e-Gate

Attack point	Description	Class	Type
Sensor	Spoofing attacks, i.e., submission of a fake biometric to the sensor	Direct	Type 1
Channel between sensor and feature extractor	Resubmission of a stored biometric that replaces the live one	Indirect	Type 2
Feature extractor	Forcing the feature extractor to produce a template chosen by the attacker	Indirect	Type 3
Channel between feature extractor and matcher	Resubmission of a stored template	Indirect	Type 4
Matcher	Forcing the matcher to produce a higher or lower score	Indirect	Type 5
Database of external systems, such as EEMS or RTP	Altering the biometric information stored in external databases	Indirect	Type 6a
Chip in the e-MRTD	Altering the biometric information stored in the e-MRTD	Indirect	Type 6b
Channel between an external database and the ABC system	Substitution of the biometric data stored in the database by data chosen by the attacker	Indirect	Type 7a
Channel between e-MRTD and document reader	Substitution of the biometric data stored in the e-MRTD by data chosen by the attacker	Indirect	Type 7b
Channel between the matcher and the mechanism that controls the e-Gate	Overwriting the final decision of the biometric verification	Indirect	Type 8

and Jain 2004]. For this reason, the implementation of anti-spoofing tests that detect the liveness of the biometric is an important measure to guarantee the security of the border controls performed by e-Gates [Donida Labati et al. 2015b; Rattani et al. 2013]. The ISO/IEC 30107 multi-part standard, which is in preparation, will provide specifications for detecting this type of attack [ISO/IEC 2015b]. The guidelines for deploying ABC systems illustrate the importance of these controls and request the implementation of such checks for face and fingerprint recognition [Frontex 2012b; 2012a]. Currently, there are no public statistical data regarding the incidence of direct attacks on ABC systems, although some cases have been reported. For instance, in 2008, Japanese border guards reported that they had detected a woman who used a special tape over her fingers in an attempt to spoof the fingerprint recognition sensor. They also believe that many more illegal travelers have used the same technique [Erdogmus and Marcel 2014].

The majority of spoof detection techniques follow one of these approaches [Nixon et al. 2008]:

- *different sensors:* use of different sensors to detect multiple signals to have higher discriminative power than a single biometric trait (e.g., face and iris captured at the same time);
- *additional data:* acquisition of additional information using the same sensor (e.g., acquisition of multiple face images to detect movement or blood flow);
- *sample processing:* use the data collected for biometric purposes to search for the inherent characteristics of the biometric trait (e.g., searching for evidence of printed patterns on face images).

Every biometric trait uses different techniques to counteract specific attacks. The most common ABC face recognition deployments operate on 2D images. In this type of system, there are three main possible attacks: i) photo attacks, ii) video attacks and iii) makeup, mask, or mannequin head attacks, for which there are three types of spoof detection methods based on i) motion analysis, ii) texture analysis, or iii) liveness detection [Kahm and Damer 2012]. Moreover, while 3D face recognition systems are more robust against spoofing [Kahm and Damer 2012], they are vulnerable to attacks based on 3D masks or on photographic masks [De Marsico et al. 2012].

Fingerprint recognition systems deployed in e-Gates can be attacked using fake fingers created using gelatin, silicone or other materials, as well as with dead fingers [Marasco and Ross 2014]. The techniques to detect fingerprint spoofing attempts use approaches based on vitality analysis, dynamic behavior analysis, or static characteristic analysis [Marasco and Ross 2014].

Iris recognition systems can be deceived using methods such as artificial eyes, printed iris images, cosmetic contact lenses with a printed iris pattern or displays [Wei et al. 2013]. The techniques for detecting iris spoofing attempts use approaches based on the analysis of physiological characteristics (e.g., eye motion) or on the analysis of optical characteristics (e.g., reflectance) [Sun and Tan 2014].

Although the literature describes many approaches for addressing spoofing, this area of research is still considered to be in its early stages. In particular, anti-spoofing techniques tend to have a limited validity period because the spoofing methods continue to be perfected. For this reason, joint efforts between industry and academia have been made. Recently, the research project TABULA RASA had the purpose of defining standard procedures for assessing the vulnerability of biometric systems to spoofing attacks, as well as innovative anti-spoofing methods that include the use of novel biometrics and the adoption of multibiometric systems [TABULA RASA 2010]. Furthermore, the Biometrics Institute formed the Biometrics Vulnerability Assessment Expert Group with the mission of reducing vulnerabilities in biometrics and encouraging vendors to develop efficient solutions to address these attacks.

4.4. Privacy evaluation and protection

The development of ABC systems poses also some ethical dilemmas, particularly concerning normative assumptions and privacy protection. Biometrics, being based on the differences of bodily features, can be used to categorize people in ways that can have considerable ethical, legal or political significance, such as gender, age, ethnic or weight categories. In addition, concepts like usability, accessibility or failure to use the biometric system, can invoke considerations about what is normal and what is not, formally known as “normalization”, which can lead to social exclusion [van der Ploeg 2011]. Moreover, the problem of privacy protection in ABC systems is particularly relevant in regard to the biometric data used. Indeed, biometric information can be used to recognize individuals automatically and with greater accuracy than traditional methods based on smartcards or passwords, and a misuse of such biometric information can have dangerous consequences. In fact, it is not possible to change biometric traits when a user does not want to be recognized anymore, and the association of a biometric trait to a particular context (e.g., a fingerprint or iris sample incorrectly placed in a watch list) may not be removed easily. Moreover, the theft of biometric data is not always detected (e.g., a fake fingerprint), and the thief may be able to impersonate the victim for an indefinite amount of time [Donida Labati et al. 2012]. This may pose security problems while such a traveler goes unnoticed when crossing the border of a country.

This problem is often feared by the general population, who fear that their biometric data will be used to place them on watch lists or to track their activities because they are not always made aware of the purposes that their biometric data will be used for [Cimato et al. 2008].

It is thus necessary to consider several factors in the design of privacy-compliant biometric systems, related to both technological and sociological aspects [Ciriani et al. 2007; De Capitani di Vimercati et al. 2012], such as real and perceived risks, the context of application, and the employed biometric trait. In particular, perceived risks are related to how people view the biometric technology, whether they trust it, and whether they like to use it. This aspect can be influenced by factors such as usability, type of biometric trait, incidents involving the related biometric data, and associations with criminal activities. Moreover, real risks are influenced by the context in which the biometric system operates: for example, covert systems operating without the user's knowledge (e.g., surveillance systems) pose more privacy risks than overt systems, and government applications can be more privacy invasive that private applications because the user may fear the misuse of data from the authorities. For these reasons, in some countries, laws prohibit surveillance without the user's awareness or uses of biometric data different from the scope of the system. For example, biometric data stored in e-Passports can only be used for issuing electronic documents [EC 2009]. Points of view regarding privacy compliance in ABC are very different between states. The Australian SmartGate system archives MRZ data and images for as long as seven years in a central database, as in the report [Frontex 2010]. However, EU systems should conform to a more restrictive treatment of personal data [EC 1995], and such data must be anonymized prior to storage. Finally, the accuracy of the biometric trait also influences the risks associated with it. Biometric traits capable of 1:N identification – face, fingerprint, and iris – used in most of the ABC systems pose more privacy risks than less accurate traits (e.g., hand shape, voice, and signature) because the first can be associated to the individual also outside the scope of the application.

Based on the above considerations, it is necessary to consider four aspects when implementing methods and procedures for protecting the privacy of biometric data in ABC systems [Donida Labati et al. 2012]:

- *The scope of the system* has to be communicated to the users, it should not change, and biometric data should not be used outside the defined scope of the system. In fact, the perceived risks do also strongly depends on the level of trust that people have in the institutions or the organisations operating the technology. The biometric data contained in e-Passports and the live samples captured by e-Gates are used only for the purpose of verifying the identity of the individual during the border crossing procedure [EC 2009] and are not stored longer than necessary. The procedures used for handling biometric data should also be disclosed. The importance of this measure is confirmed by research in the FastPass project, which has shown that travelers assume the e-Gate stores their biometric data for an unknown period and used by all sorts of security agencies, not only national.
- *User control of personal data* must always be possible such that the users can decide when to no longer be recognized using the specified biometric modality. In particular,

it is the right of the individual to ask for removal or erasure of biometric data in electronic documents [EC 2009; Tsormpatzoudi et al. 2014].

— *Disclosure* to the users about the purpose of the system, the enrollment and matching modalities, and the methods used for data protection should be present [Tsormpatzoudi et al. 2014].
— *Data protection techniques* should be deployed to avoid theft of biometric information by adopting cryptographic representation of the biometric data [EC 2009; Ciriani et al. 2010; Acquisti et al. 2007] and secure access control techniques to e-Passports [Ardagna et al. 2010; Kundra et al. 2014].

Further recommendations related to privacy can be found in ISO/IEC TR 24714-1 [ISO/IEC 2008]. However, while cryptographic methods based on public key infrastructure (PKI) have been proposed for regulating secure access to the data contained in e-Passports [Kundra et al. 2014; Peeters et al. 2014], methods for protecting the privacy of biometric data through cryptographic techniques have not been extensively used, and actual samples are generally stored in e-Passports [Schouten and Jacobs 2009].

In fact, traditional cryptographic methods (e.g., AES and RSA) cannot be applied on biometric data because the intra-class variability present in the captured samples would result in differences in the cryptographic representation of samples of the same individual. For example, encrypted images of multiple face or fingerprint acquisitions, captured from the same individuals, would be significantly different from one another. It is thus necessary to investigate ad hoc methods for protecting biometric templates [Jain et al. 2008; Adler and Schuckers 2015] based on cancelable biometrics [Rathgeb and Uhl 2011], biometric cryptosystems [Cimato et al. 2009], or cryptographically secure techniques [Bianchi et al. 2010].

Recently, the FIDELITY project has been directed toward studying the current vulnerabilities and shortcoming of e-Passports to design and develop innovative, more secure, and more privacy-compliant e-Passports [FIDELITY 2012].

5. CONCLUSIONS

Automated Border Control is emerging as a great innovation in modern passenger transportation. Automating the border control process for which hundreds of thousands of people are subjected to daily has a strong relationship with biometrics. ABC systems are increasingly studied, both in commercial and academic research. In this article, we presented the architecture of e-Gates and the procedures adopted for identity verification based on the biometric traits most used today. We reviewed the main recognition techniques described in the literature and discussed their features with respect to an ABC scenario. Finally, we discussed the major problems that affect biometric systems in ABC and the challenges that they pose to the research community. We collected several experiences, best practices and results already in the literature, attempting to provide both a detailed current overview of automated border control and its biometric background to whoever wants to approach this area.

REFERENCES

ABC4EU. 2014. EU FP7 Project. (2014). http://abc4eu.com/

M. Abdel-Mottaleb and M.H. Mahoor. 2007. Application notes - Algorithms for assessing the quality of facial images. *IEEE Computational Intelligence Magazine* 2, 2 (2007), 10–17.

A. Abhyankar and S. Schuckers. 2009. Iris quality assessment and bi-orthogonal wavelet based encoding for recognition. *Pattern Recognition* 42, 9 (2009), 1878–1894.

R. Abiantun, U. Prabhu, and M. Savvides. 2014. Sparse feature extraction for pose-tolerant face recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 36, 10 (2014), 2061–2073.

L. Acharya and T. Kasprzycki. 2010. *Biometrics and government.* Library of Parliament, Ottawa, Canada.

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

Acuity Market Intelligence. 2014. Automated Border Control (ABC) eGate deployments - market research. http://www.acuity-mi.com/eGatedep.php. (2014).

N. R. Adam, V. Atluri, R. Koslowski, R. Grossman, V. P. Janeja, and J. Warner. 2006. Secure interoperation for effective data mining in border control and homeland security applications. In *Proceedings of the International Conference on Digital Government Research*. 124–125.

N. R. Adam, V. Atluri, R. Koslowski, V. P. Janeja, J. Warner, and A. Paliwal. 2005. Agency interoperation for effective data mining in border control and homeland security applications. In *Proceedings of the National Conference on Digital Government Research*. 285–286.

A. Adler and S. A. C. Schuckers. 2015. Security and liveness, overview. In *Encyclopedia of Biometrics*, S.Z. Li and A.K. Jain (Eds.). Springer, 1335–1342.

T. Ahonen, A. Hadid, and M. Pietikainen. 2006. Face Description with Local Binary Patterns: Application to Face Recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 28, 12 (2006), 2037–2041.

F. Alonso-Fernandez, J. Fierrez, and J. Ortega-Garcia. 2012. Quality measures in biometric systems. *IEEE Security and Privacy Magazine* 10, 6 (2012), 52–62.

F. Alonso-Fernandez, J. Fierrez, J. Ortega-Garcia, J. Gonzalez-Rodriguez, H. Fronthaler, K. Kollreider, and J. Bigun. 2007. A comparative study of fingerprint image-quality estimation methods. *IEEE Transactions on Information Forensics and Security* 2, 4 (2007), 734–743.

ANSI/NIST. 2011. ANSI/NIST-ITL 1-2011: Data format for the interchange of fingerprint, facial & other biometric information, part 1. NIST Special Publication 500-290. (2011).

C. Arcelli and G. Sanniti Di Baja. 1985. A Width-Independent Fast Thinning Algorithm. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 7, 4 (1985), 463 – 474.

C. A. Ardagna, J. Camenisch, M. Kohlweiss, R. Leenes, G. Neven, B. Priem, P. Samarati, D. Sommer, and M. Verdicchio. 2010. Exploiting Cryptography for Privacy-enhanced Access Control: A Result of the PRIME Project. *J. Comput. Secur.* 18, 1 (2010), 123–160.

A. Atanasiu and M. I. Mihailescu. 2010. Biometric passports (ePassports). In *Proceedings of the IEEE International Conference on Communications*. 443–446.

D. Bachenheimer. 2014. Performance Measurement in ABC and Surveillance Scenarios. International Biometric Performance Testing Conference. (2014).

R. Bansal, P. Sehgal, and P. Bedi. 2012. Minutiae Extraction from Fingerprint Images - a Review. *International Journal of Computer Science Issues* 8, 5 (2012), 929–940.

P. N. Belhumeur, J. P. Hespanha, and D. J. Kriegman. 1997. Eigenfaces vs. Fisherfaces: Recognition Using Class Specific Linear Projection. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 19, 7 (1997), 711–720.

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

M. Bicego, A. Lagorio, E. Grosso, and M. Tistarelli. 2006. On the Use of SIFT Features for Face Authentication. In *Proceedings of the Computer Vision and Pattern Recognition Workshop*. 35–41.

Boeing. 2015. Current Market Outlook: 2015-2034. http://www.boeing.com/commercial/market/long-term-market/traffic-and-market-outlook/. (2015).

T. Bourlai, A. Ross, and A.K. Jain. 2011. Restoring degraded face Images: a case study in matching faxed, printed, and scanned photos. *IEEE Transactions on Information Forensics and Security* 6, 2 (2011), 371–384.

K. W. Bowyer, K. Hollingsworth, and P. J. Flynn. 2008. Image understanding for iris biometrics: A survey. *Computer Vision and Image Understanding* 110, 2 (2008), 281–307.

K. W. Bowyer, K. Hollingsworth, and P. J. Flynn. 2013. A survey of iris biometrics research: 2008-2010. In *Handbook of Iris Recognition*, Mark J. Burge and Kevin W. Bowyer (Eds.). Springer, 15–54.

M. Brauckmann and M. Werner. 2006. *Proceedings of NIST Biometric Quality Workshop*. Technical Report. NIST.

BSI. 2007. *BSI-TR 03104: Technical Guideline for production, data acquisition, quality testing and transmission for passports - Annex 2 - Quality requirements for the acquisition and transmission of the fingerprint image data as biometric feature for electronic identification documents*. Technical Report. Bundesamt für Sicherheit in der Informationstechnik.

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

A. M. Burrows and J. F. Cohn. 2015. Comparative anatomy of the face. In *Encyclopedia of Biometrics*, S.Z. Li and A.K. Jain (Eds.). Springer, 313–321.

Y. Chen, S. C. Dass, and A. K. Jain. 2006. Localized iris image quality using 2-D wavelets. In *Advances in Biometrics*, David Zhang and Anil K. Jain (Eds.). Springer, 373–381.

C.-T. Chou, S.-W. Shih, W.-S. Chen, V. W. Cheng, and D.-Y. Chen. 2010. Non-orthogonal view iris recognition system. *IEEE Transactions on Circuits and Systems for Video Technology* 20, 3 (2010), 417–430.

S. Cimato, M. Gamassi, V. Piuri, D. Sana, R. Sassi, and F. Scotti. 2006. Personal identification and verification using multimodal biometric data. In *Proceedings of the IEEE International Conference on Computational Intelligence for Homeland Security and Personal Safety*. 41–45.

S. Cimato, M. Gamassi, V. Piuri, R. Sassi, and F. Scotti. 2009. A multi-biometric verification system for the privacy protection of iris templates. In *Proceedings of the International Workshop on Computational Intelligence in Security for Information Systems*, E. Corchado, R. Zunino, P. Gastaldo, and Á. Herrero (Eds.). Advances in Soft Computing, Vol. 53. Springer, 227–234.

S. Cimato, R. Sassi, and F. Scotti. 2008. Biometrics and privacy. *Recent Patents on Computer Science* 1 (2008), 98–109.

V. Ciriani, S. De Capitani Di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati. 2010. Combining fragmentation and encryption to protect privacy in data storage. *ACM Transactions on Information and System Security* 13, 3 (2010), 22:1–22:33.

V. Ciriani, S. De Capitani di Vimercati, S. Foresti, and P. Samarati. 2007. Microdata Protection. In *Secure Data Management in Decentralized Systems*, T. Yu and S. Jajodia (Eds.). Springer-Verlag, 291–321.

C. Conde, I. M. de Diego, and E. Cabello. 2012. Face Recognition in Uncontrolled Environments, Experiments in an Airport. In *E-Business and Telecommunications*, M.S. Obaidat, J. L. Sevillano, and J. Filipe (Eds.). Communications in Computer and Information Science, Vol. 314. Springer, 20–32.

T. F. Cootes, G. J. Edwards, and C. J. Taylor. 2001. Active Appearance Models. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 23, 6 (2001), 681–685.

D. Cuesta Cantarero, D.A. Perez Herrero, and F. Martin Mendez. 2013. A multi-modal biometric fusion implementation for ABC systems. In *Proceedings of the European Intelligence and Security Informatics Conference*. 277–280.

N. Dalal and B. Triggs. 2005. Histograms of oriented gradients for human detection. In *Proceedings of the Conference on Computer Vision and Pattern Recognition*, Vol. 1. 886–893.

J. Daugman. 2004. How iris recognition works. *IEEE Transactions on Circuits and Systems for Video Technology* 14, 1 (2004), 21–30.

J. Daugman. 2015. Iris recognition at airports and border crossings. In *Encyclopedia of Biometrics*, S.Z. Li and A.K. Jain (Eds.). Springer, 998–1004.

S. De Capitani di Vimercati, S. Foresti, G. Livraga, and P. Samarati. 2012. Data privacy: definitions and techniques. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems* 20, 6 (2012), 793–817.

M. De Marsico, M. Nappi, D. Riccio, and J. Dugelay. 2012. Moving face spoofing detection via 3D projective invariants. In *Proceedings of the IAPR International Conference on Biometrics*. 73–78.

Department of Homeland Security. 2009. New biometric technology improves security and facilitates U.S. entry process for international travelers. (2009).

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

R. Donida Labati, A. Genovese, E. Muñoz, V. Piuri, G. Sforza, and F. Scotti. 2015b. Advanced design of automated border control gates: biometric system techniques and research trends. In *Proceedings of the IEEE International Symposium on Systems Engineering*. 1–8.

R. Donida Labati, A. Genovese, V. Piuri, and F. Scotti. 2012. Iris segmentation: state of the art and innovative methods. In *Cross Disciplinary Biometric Systems*. Springer, 151–182.

R. Donida Labati, A. Genovese, V. Piuri, and F. Scotti. 2014. Touchless fingerprint biometrics: a survey on 2D and 3D technologies. *Journal of Internet Technology* 15, 3 (2014), 325–332.

R. Donida Labati, A. Genovese, V. Piuri, and F. Scotti. 2016. Toward unconstrained fingerprint recognition: a fully-touchless 3-D system based on two views on the move. *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 46, 2 (2016), 202–219.

R. Donida Labati, V. Piuri, R. Sassi, and F. Scotti. 2014. HeartCode: a novel binary ECG-based template. In *Proceedings of the IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications*. 86–91.

R. Donida Labati, V. Piuri, and F. Scotti. 2012. Biometric privacy protection: guidelines and technologies. In *E-Business and Telecommunications*. Springer, 3–19.

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

R. Donida Labati and F. Scotti. 2010. Noisy iris segmentation with boundary regularization and reflections removal. *Image and Vision Computing - Iris Images Segmentation Special Issue* 28, 2 (2010), 270–277.

R. Donida Labati and F. Scotti. 2011. Fingerprint. In *Encyclopedia of Cryptography and Security (2nd ed.)*, H.C.A. van Tilborg and S. Jajodia (Eds.). Springer, 460 – 465.

B. Dorizzi, R. Cappelli, M. Ferrara, D. Maio, D. Maltoni, N. Houmani, S. Garcia-Salicetti, and A. Mayoue. 2009. Fingerprint and on-line signature verification competitions at ICB 2009. In *Advances in Biometrics*, M. Tistarelli and M. S. Nixon (Eds.). Lecture Notes in Computer Science, Vol. 5558. Springer, 725–732.

EC. 1995. Protection of individuals with regard to the processing of personal data and free movement of such data. Directive 95/46/EC. (1995). EU Commission.

EC. 2006. Rights of people with reduced mobility in air transport. Regulation No 1107/2006. (2006). EU Commission.

EC. 2009. Standards for security features and biometrics in passports and travel documents issued by Member States. Regulation No 444/2009 amending Regulation No 2252/2004. (2009). EU Commission.

EC. 2011. Smart borders - options and the way ahead, COM(2011) 680 final. Communication. (2011). EU Commission.

N. Erdogmus and S. Marcel. 2014. Introduction. In *Handbook of biometric anti-spoofing*, S. Marcel, M. Nixon, and S.Z. Li (Eds.). Springer, 1–11.

eu-LISA. 2015a. Delegation Agreement on Smart Borders Pilot. (2015). European Agency for the Operational Management of large-scale IT Systems in the area of Freedom, Security and Justice (eu-LISA).

eu-LISA. 2015b. *Smart Borders Pilot Project - Report on the technical conclusions of the Pilot*. Technical Report.

FastPass. 2013. EU FP7 Project. (2013). https://www.fastpass-project.eu/

M. Faúndez-Zanuy. 2004. On the vulnerability of biometric security systems. *IEEE Aerospace and Electronic Systems Magazine* 19, 6 (2004), 3–8.

FBI. 2013. Electronic Biometric Transmission Specification - Appendix F. (2013).

J. Fergusson. 2014. Twelve seconds to decide: Frontex and the principle of best practice. (2014).

FIDELITY. 2012. EU FP7 Project. (2012). http://www.fidelity-project.eu/

Frontex. 2007. *BIOPASS - Study on automated biometric border crossing systems for registered passengers at four European airports*. Technical Report.

Frontex. 2010. *BIOPASS II - Automated biometric border crossing systems based on electronic passports and facial recognition: RAPID and SmartGate*. Technical Report.

Frontex. 2012a. Best practice operational guidelines for Automated Border Control (ABC) systems. (2012).

Frontex. 2012b. Best practice technical guidelines for Automated Border Control (ABC) systems. (2012).

J. Galbally, C. McCool, J. Fierrez, S. Marcel, and J. Ortega-Garcia. 2010. On the vulnerability of face verification systems to hill-climbing attacks. *Pattern Recognition* 43, 3 (2010), 1027–1038.

M. Gamassi, M. Lazzaroni, M. Misino, V. Piuri, D. Sana, and F. Scotti. 2005a. Quality assessment of biometric systems: a comprehensive perspective based on accuracy and performance measurement. *IEEE Transactions on Instrumentation and Measurement* 54, 4 (2005), 1489–1496.

M. Gamassi, V. Piuri, D. Sana, and F. Scotti. 2004. A high-level optimum design methodology for multimodal biometric systems. In *Proceedings of the IEEE International Conference on Computational Intelligence for Homeland Security and Personal Safety*. 117–124.

M. Gamassi, V. Piuri, and F. Scotti. 2005b. Fingerprint local analysis for high-performance minutiae extraction. In *Proceedings of the IEEE International Conference on Image Processing*, Vol. 3. 265 – 268.

X. Gao, S. Z. Li, R. Liu, and P. Zhang. 2007. Standardization of face image sample quality. In *Proceedings of the International Conference on Advances in Biometrics*. 242–251.

A. Gelb and J. Clark. 2013. Performance Lessons from India's Universal Identification Program. (2013).

A. Genovese, E. Muñoz, V. Piuri, F. Scotti, and G. Sforza. 2016. Towards touchless pore fingerprint biometrics: a neural approach. In *Proceedings of the International Joint Conference on Neural Networks*. –. Accepted.

A. Genovese, V. Piuri, and F. Scotti. 2014. *Touchless Palmprint Recognition Systems*. Advances in Information Security, Vol. 60. Springer.

D. Gorodnichy, S. Yanushkevich, and V. Shmerko. 2014. Automated border control: problem formalization. In *Proceedings of the IEEE Symposium on Computational Intelligence in Biometrics and Identity Management*. 118–125.

P. Grother, E. Tabassi, G. W. Quinn, and W. Salamon. 2009. *IREX I performance of iris recognition algorithms on standard images*. Technical Report NISTIR 7629.

G. Guo, S. Z. Li, and K. Chan. 2000. Face recognition by support vector machines. In *Proceedings of the IEEE International Conference on Automatic Face and Gesture Recognition*. 196–201.

F. Hao, J. Daugman, and P. Zielinski. 2008. A fast search algorithm for a large fuzzy database. *IEEE Transactions on Information Forensics and Security* 3, 2 (2008), 203–212.

X. He, S. Yan, Y. Hu, P. Niyogi, and H.-J. Zhang. 2005. Face recognition using Laplacianfaces. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 27, 3 (2005), 328–340.

L. Hong, Y. Wan, and A. Jain. 1998. Fingerprint image enhancement: algorithm and performance evaluation. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 20, 8 (1998), 777–789.

T. Huang, Z. Xiong, and Z. Zhang. 2011. Face Recognition Applications. In *Handbook of Face Recognition*, Z. S. Li and A. K. Jain (Eds.). Springer, 617–638.

IATA. 2012a. Checkpoint of the future concept. (2012).

IATA. 2012b. Global passenger survey highlights. (2012).

IATA. 2014a. ABC implementation guide. (2014).

IATA. 2014b. Portuguese immigration & border service. Case Study. (2014).

ICAO. 2006. ICAO Doc 9303, machine readable travel documents. Part 1, Volume 2. (2006).

ICAO. 2007. The biometric identification for use with ICAO-compliant machine readable travel documents. *ICAO MRTD Report* 2, 1 (2007), 18–21.

ICAO. 2015a. The history of the chip inside symbol. *ICAO MRTD Report* 10, 2 (2015), 18–19.

ICAO. 2015b. ICAO Doc 9303: machine readable travel documents (seventh Edition) - Part 9: Deployment of biometric identification and electronic storage of data in eMRTDs. (2015).

I. Iglezakis. 2013. EU data protection legislation and case-law with regard to biometric applications. *Social Science Research Network* (2013).

ISO. 1998. ISO 9241: Ergonomic requirements for office work with visual display terminals - Part 11: Guidance on usability. (1998).

ISO/IEC. 2006. ISO/IEC 19784, Biometric application programming interface - Part 1: BioAPI specification. (2006).

ISO/IEC. 2007. *ISO/IEC TR 24722: Multimodal and other multibiometric fusion*. Technical Report.

ISO/IEC. 2008. *ISO/IEC TR 24714: Jurisdictional and societal considerations for commercial applications - Part 1: General guidance*. Technical Report.

ISO/IEC. 2009. ISO/IEC 29794 (all parts): Biometric sample quality. (2009).

ISO/IEC. 2011. ISO/IEC 19794 (all parts): Biometric data interchange formats. (2011).

ISO/IEC. 2015a. ISO/IEC 19785: Common Biometric Exchange Formats Framework - Part 1: Data element specification. (2015).

ISO/IEC. 2015b. ISO/IEC PRF 30107: Biometric presentation attack detection - Part 1: Framework. (2015).

ISO/IEC. 2015c. *ISO/IEC TR 29195: Traveller processes for biometric recognition in automated border*. Technical Report.

A. K. Jain, K. Nandakumar, and A. Nagar. 2008. Biometric template security. *EURASIP Journal on Advances in Signal Processing* 2008 (2008), 113:1–113:17.

A. K. Jain and A. Ross. 2004. Multibiometric Systems. *Commun. ACM* 47, 1 (2004), 34–40.

R. Jenkins and A. M. Burton. 2008. 100% Accuracy in automatic face recognition. *Science* 319, 5862 (2008), 435–435.

K. Jia and S. Gong. 2015. Face sample quality. In *Encyclopedia of Biometrics*, S.Z. Li and A.K. Jain (Eds.). Springer, 522–526.

O. Kahm and N. Damer. 2012. 2D Face liveness detection: an overview. In *Proceedings of the International Conference of the Biometrics Special Interest Group*. 1–12.

V. Kanhangad, A. Kumar, and D. Zhang. 2011. Contactless and pose invariant biometric identification using hand surface. *IEEE Transactions on Image Processing* 20, 5 (2011), 1415–1424.

J. Kephart. 2015. *Securing our border: Biometric Entry and Exit at our Ports of Entry*. Technical Report. Secure Identity & Biometrics Association.

B. Khan, M. Khurram Khan, and K. S. Alghathbar. 2010. Biometrics and identity management for homeland security applications in Saudi Arabia. *African Journal of Business Management* 4, 15 (2010), 3296–3306.

R. Koslowski. 2003. Information technology and integrated border management. In *Proceedings of the Workshop on Managing International and Inter-Agency Cooperation at the Border*. 293–296.

M. Kosmerlj, T. Fladsrud, E. Hjelms, and E. Snekkenes. 2005. Face recognition issues in a border control environment. In *Advances in Biometrics*, D. Zhang and A. K. Jain (Eds.). Lecture Notes in Computer Science, Vol. 3832. Springer, 33–39.

S. Kundra, A. Dureja, and R. Bhatnagar. 2014. The study of recent technologies used in e-passport system. In *Proceedings of the IEEE Global Humanitarian Technology Conference*. 141–146.

T. Kwon and H. Moon. 2008. Biometric authentication for border control applications. *IEEE Transactions on Knowledge and Data Engineering* 20, 8 (2008), 1091–1096.

Y. Lei, M. Bennamoun, M. Hayat, and Y. Guo. 2014. An efficient 3D face recognition approach using local geometrical signatures. *Pattern Recognition* 47, 2 (2014), 509–524.

X. Li, Z. Sun, and T. Tan. 2011. Comprehensive assessment of iris image quality. In *Proceedings of the IEEE International Conference on Image Processing*. 3117–3120.

X. Liang, A. Bishnu, and T. Asano. 2007. A Robust Fingerprint Indexing Scheme Using Minutia Neighborhood Structure and Low-Order Delaunay Triangles. *IEEE Transactions on Information Forensics and Security* 2, 4 (2007), 721 – 733.

S.-H. Lin, S.-Y. Kung, and L.-J. Lin. 1997. Face recognition/detection by probabilistic decision-based neural network. *IEEE Transactions on Neural Networks* 8, 1 (1997), 114–132.

N. Liu, M. Zhang, H. Li, Z. Sun, and T. Tan. 2015. DeepIris: Learning pairwise filter bank for heterogeneous iris verification. *Pattern Recognition Letters* (2015), –. DOI: http://dx.doi.org/10.1016/j.patrec.2015.09.016 In Press.

M2Sys. 2015. M2-AutoTilt^{TM} Iris recognition camera. (2015).

V. MacLeod and B. McLindin. 2011. 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.). Studies in Computational Intelligence, Vol. 338. Springer, 115–145.

D. Maio and D. Maltoni. 1997. Direct Gray-Scale Minutiae Detection In Fingerprints. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 19 (1997), 27–40. Issue 1.

D. Maltoni. 2015. Fingerprint recognition, overview. In *Encyclopedia of Biometrics*, S. Z. Li and A. K. Jain (Eds.). Springer, 664–668.

D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar. 2009. *Handbook of fingerprint recognition* (second ed.). Springer.

A. J. Mansfield and J. L. Wayman. 2002. *Best practices in testing and reporting performance of biometric devices (version 2.01)*. Technical Report. Centre for Mathematics and Scientific Computing - National Physical Laboratory.

E. Marasco and A. Ross. 2014. A survey on antispoofing schemes for fingerprint recognition systems. *Comput. Surveys* 47, 2 (2014), 28:1–28:36.

M. De Marsico, A. Petrosino, and S. Ricciardi. 2016. Iris Recognition through Machine Learning Techniques: a Survey. *Pattern Recognition Letters* (2016), –. DOI: http://dx.doi.org/10.1016/j.patrec.2016.02.001 In Press.

J. R. Matey, O. Naroditsky, K. Hanna, R. Kolczynski, D. J. LoIacono, S. Mangru, M. Tinker, T. M. Zappia, and W. Y. Zhao. 2006. Iris on the move: acquisition of images for iris recognition in less constrained environments. *Proc. IEEE* 94, 11 (2006), 1936–1947.

C. McCool and S. Marcel. 2009. Parts-Based Face Verification Using Local Frequency Bands. In *Advances in Biometrics*, M. Tistarelli and M.S. Nixon (Eds.). Springer, 259–268.

J. Merkle, M. Schwaiger, O. Bausinger, M. Breitenstein, K. Elwart, and M. Nuppeney. 2010. Towards improving the NIST fingerprint image quality (NFIQ) algorithm. In *Proceedings of the Special Interest Group on Biometrics and Electronic Signatures*. 29–44.

P. Mitra, C.-C. Pan, P. Liu, and V. Atluri. 2006. Privacy-preserving semantic interoperation and access control of heterogeneous databases. In *Proceedings of the ACM Symposium on Information, Computer and Communications Security*. 66–77.

MobilePass. 2014. EU FP7 Project. (2014). http://mobilepass-project.eu/

W. Mostowski and E. Poll. 2010. *Electronic passports in a nutshell*. Technical Report ICIS-R10004. Radboud University.

R. Nanavati. 2011. *Biometric border security evaluation framework*. Technical Report DRDC CSS CR 2011-16. Defence R&D Canada.

NAO. 2015. *E-borders and successor programmes*. Technical Report. The UK National Audit Office.

K. Nguyen, C. Fookes, S. Sridharan, and S. Denman. 2011. Quality-driven super-resolution for less constrained iris recognition at a distance and on the move. *IEEE Transactions on Information Forensics and Security* 6, 4 (2011), 1248–1258.

K. A. Nixon, V. Aimale, and R. K. Rowe. 2008. Spoof detection schemes. In *Handbook of biometrics*, A.K. Jain, P. Flynn, and A. Ross (Eds.). Springer, 403–423.

M. Nuppeney. 2012. Automated Border Control based on (ICAO compliant) eMRTDs. (2012).

M.A. Olsen, E. Tabassi, A. Makarov, and C. Busch. 2013. Self-organizing maps for fingerprint image quality assessment. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops*. 138–145.

A.-M. Oostveen. 2014. Non-use of Automated Border Control Systems: Identifying Reasons and Solutions. In *Proceedings of the International British Human Computer Interaction Conference*. 228–233.

A.-M. Oostveen, M. Kaufmann, E. Krempel, and G. Grasemann. 2014. Automated border control: a comparative study at two European airports. In *Proceedings of the International Conference on Interfaces and Human Computer Interaction*.

A. J. Palmer and C. Hurrey. 2012. Ten reasons why IRIS needed 20:20 foresight: some lessons for introducing biometric border control systems. In *Proceedings of the European Intelligence and Security Informatics Conferennce*. 311–316.

S. A. Patil and P. J. Deore. 2013. Face Recognition: A Survey. *Informatics Engineering, an International Journal* 1, 1 (2013), 31–41.

R. Peeters, J. Hermans, and B. Mennink. 2014. Speedup for European epassport authentication. In *Proceedings of the International Conference of the Biometrics Special Interest Group*. 1–6.

P. Penev and J. Atick. 1996. Local feature analysis: a general statistical theory for object representation. *Network: Computation in Neural Systems* 7, 3 (1996), 477–500.

M. Pogoda. 2011. The changing face of electronic ID. *Biometric Technology Today* 2011, 1 (2011), 7–9.

PwC. 2014. *Technical study on smart borders (final report)*. Technical Report. European Commission.

G. Quinn, P. Grother, and E. Tabassi. 2013. Standard iris storage formats. In *Handbook of Iris Recognition*, M. J. Burge and K. W. Bowyer (Eds.). Springer, 55–66.

G. W. Quinn and P. J. Grother. 2011. *Performance of face recognition algorithms on compressed images*. Technical Report NISTIR 7830.

R. Raghavendra and C. Busch. 2015. Improved face recognition by combining information from multiple cameras in automatic border control system. In *Proceedings of the IEEE International Conference on Advanced Video and Signal Based Surveillance*. 1–6.

R. Raghavendra, K. B. Raja, B. Yang, and C. Busch. 2014. Automatic face quality assessment from video using gray level co-occurrence matrix: an empirical study on automatic border control system. In *Proceedings of the International Conference on Pattern Recognition*. 438–443.

S. Rakshit and D. M. Monro. 2007. An evaluation of image sampling and compression for human iris recognition. *IEEE Transactions on Information Forensics and Security* 2, 3 (2007), 605–612.

N. K. Ratha, J. H. Connell, and R. M. Bolle. 2001. An analysis of minutiae matching strength. In *Audio- and Video-Based Biometric Person Authentication*, J. Bigun and F. Smeraldi (Eds.). Number 2091 in Lecture Notes in Computer Science. Springer, 223–228.

C. Rathgeb and A. Uhl. 2011. A survey on biometric cryptosystems and cancelable biometrics. *EURASIP Journal on Information Security* 2011, 1 (2011).

A. Rattani, D.R. Kisku, M. Bicego, and M. Tistarelli. 2007. Feature level fusion of face and fingerprint biometrics. In *Proceedings of the IEEE International Conference on Biometrics: Theory, Applications, and Systems*. 1–6.

A. Rattani, N. Poh, and A. Ross. 2013. A Bayesian approach for modeling sensor influence on quality, liveness and match score values in fingerprint verification. In *Proceedings of the IEEE International Workshop on Information Forensics and Security*. 37–42.

A. Ross, K. Nandakumar, and A. K. Jain. 2006. *Handbook of Multibiometrics*. International Series on Biometrics, Vol. 6. Springer.

J. Sanchez del Rio, C. Conde, A. Tsitiridis, J. R. Gomez, I. Martin de Diego, and E. Cabello. 2015. Face-based recognition systems in the ABC e-gates. In *Proceedings of the Annual IEEE International Systems Conference*. 340–346.

M. A. Sasse. 2007. Red-eye blink, bendy shuffle, and the yuck factor: A user experience of biometric airport systems. *IEEE Security & Privacy* 5, 3 (2007), 78–81.

M. A. Sasse and K. Krol. 2013. *Age factors in biometric processing*. Institution of Engineering and Technology, Chapter Usable biometrics for an ageing population, 303–320.

K. Sava. 2014. *Automated passport control: business requirements*. Technical Report. US Customs and Border Protection.

N. A. Schmid, J. Zuo, F. Nicolo, and H. Wechsler. 2013. Iris quality metrics for adaptive authentication. In *Handbook of Iris Recognition*, M. J. Burge and K. W. Bowyer (Eds.). Springer, 67–84.

B. Schouten and B. Jacobs. 2009. Biometrics and their use in e-passports. *Image and Vision Computing* 27, 3 (2009), 305–312.

A. Serrano, I. Martin de Diego, C. Conde, and E. Cabello. 2010. Recent advances in face biometrics with Gabor wavelets: a review. *Pattern Recognition Letters* 31, 5 (2010), 372–381.

S. Shan, X. Chen, and W. Gao. 2015. Face misalignment problem. In *Encyclopedia of Biometrics*, S. Z. Li and A. K. Jain (Eds.). Springer, 459–462.

C. A. Shoniregun and S. Crosier. 2008. *Securing biometrics applications*. Springer.

M. Siciliano. 2014. Message from the editor-in-chief. *ICAO MRTD Report* 9, 2 (2014), 3.

L. J. Spreeuwers, A. J. Hendrikse, and K. J. Gerritsen. 2012. Evaluation of automatic face recognition for automatic border control on actual data recorded of travellers at Schiphol airport. In *Proceedings of the International Conference of the Biometrics Special Interest Group*. 1–6.

A. Sprokkereef. 2008. Data protection and the use of biometric data in the EU. In *The Future of Identity in the Information Society*, S. Fischer-Hubner, P. Duquenoy, A. Zuccato, and L. Martucci (Eds.). IFIP Advances in Information and Communication Technology, Vol. 262. Springer, 277–284.

Y. Sun, X. Wang, and X. Tang. 2014. Deep Learning Face Representation from Predicting 10,000 Classes. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*. 1891–1898.

Z. Sun and T. Tan. 2014. Iris anti-spoofing. In *Handbook of biometric anti-spoofing*, S. Marcel, M. Nixon, and S.Z. Li (Eds.). Springer, 103–123.

E. Tabassi and P. Grother. 2015. Fingerprint image quality. In *Encyclopedia of Biometrics*, S.Z. Li and A.K. Jain (Eds.). Springer, 635–643.

E. Tabassi, C. Wilson, and C. Watson. 2004. *NIST Fingerprint image quality*. Technical Report NISTIR 7151.

TABULA RASA. 2010. EU FP7 Project. (2010). https://www.tabularasa-euproject.org/

Y. Taigman, M. Yang, M. Ranzato, and L. Wolf. 2014. DeepFace: Closing the Gap to Human-Level Performance in Face Verification. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*. 1701–1708.

The National. 2015. More than 6.8 million people used smart gates at Dubai airport in 2014. (2015). http://www.thenational.ae/uae/government/

M. Theofanos, B. Stanton, C. Sheppard, R. Micheals, N.-F. Zhang, J. Wydler, Nadel L., and W. Rubin. 2008. *Usability Testing of Height and Angles of Ten-Print Fingerprint Capture*. Technical Report NISTIR 7504. National Institute of Standards and Technology.

P. Tsormpatzoudi, D. Dimitrova, J. Schroers, and E. Kindt. 2014. Privacy by design: the case of automated border control. In *Privacy and Identity Management for the Future Internet in the Age of Globalisation*, J. Camenisch, S. Fischer-Hubner, and M. Hansen (Eds.). Number 457 in IFIP Advances in Information and Communication Technology. Springer, 139–152.

M. Turk and A. Pentland. 1991. Eigenfaces for Recognition. *Journal of Cognitive Neuroscience* 3, 1 (1991), 71–86.

UIDAI. 2012. *Role of Biometric Technology in Aadhaar Authentication. Authentication Accuracy*. Technical Report. Unique Identification Authority of India (UIDAI).

U. Uludag and A. K. Jain. 2004. Attacks on biometric systems: a case study in fingerprints. In *Security, Steganography, and Watermarking of Multimedia Contents VI (SPIE Conference Series)*, E. J. Delp, III and P. W. Wong (Eds.), Vol. 5306. 622–633.

Unisys. 2008. *Entry-exit feasibility study - final report*. Technical Report.

A. van de Rijt and S. C. Santema. 2010. The passenger process at Schiphol and the promise of biometrics. In *Proceedings of the International Air Transport and Operations Symposium*. 76–86.

I. van der Ploeg. 2011. *Innovating Government: Normative, Policy and Technological Dimensions of Modern Government*. T. M. C. Asser Press, Chapter Normative Assumptions in Biometrics: On Bodily Differences and Automated Classifications, 29–40.

Vision-box. 2015. Border control & airports. (2015). http://www.vision-box.com/solutions/bordercontrol/

C. I. Watson, M. D. Garris, E. Tabassi, C. L. Wilson, R. M. Mccabe, S. Janet, and K. Ko. 2007. User's Guide to NIST Biometric Image Software (NBIS). (2007).

H. Wei, L. Chen, and J.A. Ferryman. 2013. Biometrics in ABC: counter-spoofing research. In *Proceedings of the Frontex Global Conference on Future Developments of Automated Border Control*.

L. Wiskott, J.-M. Fellous, N. Krüger, and C. von der Malsburg. 1997. Face Recognition by Elastic Bunch Graph Matching. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 19, 7 (1997), 775–779.

J. Wright, A. Y. Yang, A. Ganesh, S. S. Sastry, and Y. Ma. 2009. Robust Face Recognition via Sparse Representation. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 31, 2 (2009), 210–227.

M. Xiong, W. Yang, and C. Sun. 2011. Finger-knuckle-print recognition using LGBP. In *Advances in Neural Networks*, D. Liu, H. Zhang, M. Polycarpou, C. Alippi, and H. He (Eds.). Number 6676 in Lecture Notes in Computer Science. Springer, 270–277.

J. Yang, N. Xiong, and A. V. Vasilakos. 2013. Two-stage enhancement scheme for low-quality fingerprint images by learning from the images. *IEEE Transactions on Human-Machine Systems* 43, 2 (2013), 235–248.

R. Yen, A. Yoo, L. Pfaff, and G. Zektser. 2013. Measuring quality of biometric images. *Defence Standardization Program Journal* (2013).

F. Zhao and X. Tang. 2007. Preprocessing and postprocessing for skeleton-based fingerprint minutiae extraction. *Pattern Recognition* 40, 4 (04 2007), 1270 – 1281.

W. Zhao, R. Chellappa, P. J. Phillips, and A. Rosenfeld. 2003. Face recognition: a literature survey. *Comput. Surveys* 35, 4 (2003), 399–458.

X. Zou, J. Kittler, and K. Messer. 2007. Illumination invariant face recognition: a survey. In *Proceedings of the IEEE International Conference on Biometrics: Theory, Applications, and Systems*. 1–8.