Advanced Biometric Technologies: Emerging Scenarios and Research Trends

Angelo Genovese, Enrique Muñoz, Vincenzo Piuri, and Fabio Scotti

Università degli Studi di Milano – Department of Computer Science
via Bramante 65, I-26013 Crema (CR), Italy
firstname.lastname@unimi.it

Abstract. Biometric systems are the ensemble of devices, procedures, and algorithms for the automatic recognition of individuals by means of their physiological or behavioral characteristics. Although biometric systems are traditionally used in high-security applications, recent advancements are enabling the application of these systems in less-constrained conditions with non-ideal samples and with real-time performance. Consequently, biometric technologies are being increasingly used in a wide variety of emerging application scenarios, including public infrastructures, e-government, humanitarian services, and user-centric applications. This chapter introduces recent biometric technologies, reviews emerging scenarios for biometric recognition, and discusses research trends.

Key words: Biometrics, emerging scenarios, research trends, touchless, less-constrained applications

1 Introduction

Traditional authentication mechanisms are based on something that is known or possessed, such as keys, tokens, passwords, and codes. In these mechanisms, the information to be recalled and the objects to be stored can be stolen or spoofed. In contrast, biometric systems are based on the characteristics of individuals that cannot be stolen or forgotten and are more difficult to spoof [27].

The interest in these technologies is growing and the biometric market is expected to reach 21 billion US$ by the end of 2020 [43]. This market growth is mostly due to the increased adoption of automatic recognition systems for national biometric identification, border control, access control, and mobile phones. Biometric identification systems are also increasingly being used in forensic analyses to identify criminals and terrorists.

The increased adoption of biometric systems has been fostered by the introduction of advanced processing algorithms, high-resolution acquisition systems, and parallel architectures, which have enabled the development of highly accurate real-time biometric systems that are capable of handling less-constrained conditions and the presence of sample non-idealities, commonly defined as the possible problems affecting the quality of the biometric samples.

The innovations in recent biometric systems have led to the heightened acceptance and popularity of biometric technologies in consumer applications, in addition to governmental and forensic scenarios. Less-constrained and highly usable biometric systems are enabling technologies for creating smart applications that simplify human-machine interactions by adapting their characteristics to users' needs. Emerging application scenarios for biometric technologies include public infrastructures (e.g., automated systems for border control, surveillance, humanitarian services, e-health, and public transport), private infrastructures (e.g., e-banking, e-commerce, and private transportation), user-centric applications (e.g., home automation, user-centric entertainment, and social media), and personal devices (e.g., smartphones and laptops).

To further expand the possible applications of biometric technologies, the research community is currently studying novel hardware and software solutions by considering all the aspects that characterize biometric systems, such as usability, user acceptance, privacy, security, accuracy, execution time, and interoperability.

This chapter introduces recent advances in the main biometric technologies, reviews emerging scenarios for biometric recognition, and discusses research trends considering the different aspects of a biometric system.

The remainder of this chapter is structured as follows. Section 2 describes the main biometric traits and recent advances in each trait. Section 3 presents the emerging scenarios for biometric recognition. Section 4 analyzes the challenges and research trends of current biometric systems by analyzing biometric technologies from different perspectives. Finally, Section 5 concludes the overview.

2 Recent advances in biometric technologies

Biometric traits are physiological or behavioral characteristics that present sufficient distinctiveness and permanence to be used for recognizing individuals. Regarding physiological traits, the characteristics are related to a person's body and include the face, fingerprint, iris, and palmprint. For behavioral traits, the characteristics are related to actions performed by an individual and include their voice and gait.

Biometric traits have different characteristics that should be evaluated based on the application scenario and its requirements, with no biometric system being the perfect choice for every situation. In particular, the most important characteristics are related to the recognition accuracy that can be achieved using a specific biometric trait and the user acceptance of the corresponding acquisition procedure. The recognition accuracy measures the ability of the biometric system to discriminate between individuals based on the biometric trait, while the user acceptance refers to how the users perceive the system based on its usability, invasiveness, and perceived risks. These two aspects are strictly related and must be evaluated at the same time. In fact, biometric systems with higher recognition accuracies usually have intrusive acquisition procedures, resulting in a lower user acceptance. As a consequence, more accurate biometric systems are usually deployed when it is necessary to guarantee high security (e.g., military

Table 1. Summary of the accuracy and user acceptance of the main biometric traits

Biometric trait	Accuracy	User acceptance
Face	Medium (96% TAR at 0.1% FAR) [29]	High [28]
Fingerprint	High (99.4% TAR at 0.01% FAR) [29]	Medium [28]
Iris	Very high (99.1% TAR at 0.001% FAR) [20]	Low [28]
Voice	Medium (93% TAR at 0.1% FAR) [29]	High [28]

Notes: TAR (True Acceptance Rate) represents the probability that the system correctly grants access to an authorized person; FAR (False Acceptance Rate) represents the probability that the system incorrectly grants access to a non-authorized person

installations, border control), while biometric systems with greater user acceptance are often preferred for low-security applications (public transport, personal devices).

In contrast to biometric traits, soft biometric features are characteristics with limited distinctiveness or permanence and can be used to complement the biometric information or to classify individuals into sets of people with a common characteristic [27]. Examples of soft biometric features include age, gender, ethnicity, and height.

Every biometric technology presents a different recognition accuracy and user acceptance. These characteristics greatly influence the diffusion of each biometric technology. Table 1 summarizes the recognition accuracy and user acceptance of systems based on the mostly used physiological and behavioral biometric traits [20, 28, 29]. The accuracy is expressed using the following figures of merit: True Acceptance Rate (TAR), which represents the probability that the system correctly grants access to an authorized person; False Acceptance Rate (FAR), which represents the probability that the system incorrectly grants access to a non-authorized person. Differently, the user acceptance is expressed using qualitative values, because this characteristic of biometric systems is particularly subjective and cannot be easily described using quantitative figures of merit. Table 1 shows that the most accurate biometric systems are based on the iris and fingerprint. On the other hand, biometric systems based on the face and voice are more accepted by the users but are less accurate. In addition to the biometric traits analyzed in Table 1, palmprint, electrocardiogram, gait, and soft biometric features are obtaining increasing attention from the research community due to their favorable trade-off between accuracy and user acceptance for a wide set of application scenarios.

This section introduces the main biometric technologies based on physiological traits, behavioral traits, and soft biometric features. For each biometric trait and soft biometric feature discussed, this section presents the traditional recognition methods, followed by the recent advances and the research trends in biometrics. Finally, this section presents recent advances in multibiometric systems.

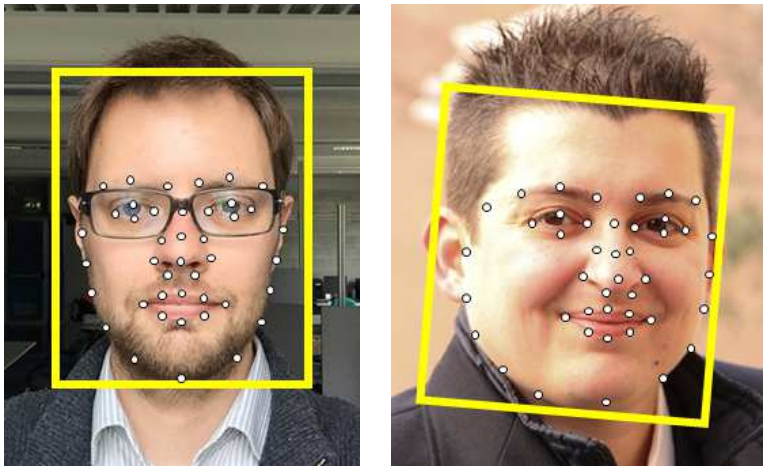

Fig. 1. Examples of face images of different individuals, along with the local features (dots) used for face recognition

2.1 Face

The face is one of the biometric traits most used for recognition because it offers the advantages of being socially accepted and having a non-intrusive acquisition process.

Methods for face recognition include approaches based on either global features or local features. The first class of methods considers the entire facial image for recognition, whereas the second class analyzes facial landmarks such as the eyes, mouth, and nose. Methods based on global features generally present higher recognition accuracy but require high-quality samples, whereas methods based on local features are more robust to non-ideal acquisitions of face images, such as the ones performed with non-uniform illumination, non-frontal pose, or different expressions. Fig. 1 shows examples of local features used for face recognition.

Traditional methods for face recognition can achieve relevant accuracy in applications characterized by cooperative users and controlled illumination conditions, in which the acquisitions are performed by illuminating uniformly the face, without occlusions caused by glasses or hair, and using steady subjects with frontal gazes and neutral expressions. However, the performance of these methods can be decreased by negative factors, such as aging of the users, uncontrolled illumination, lateral poses, expressions, and non-idealities of the face images caused by occlusions, blur, noise, and low resolution.

Research trends aim to increase the biometric recognition accuracy and the possible applications of face recognition methods. In particular, the research community is currently studying several approaches, such as techniques based on three-dimensional models; hybrid methods that combine global and local information; algorithms to compensate rotations, facial expressions and aging;

Fig. 2. Examples of fingerprint images of different individuals with respective minutiae points

and methods based on global features using recent machine learning techniques, such as Deep Learning (DL) and Convolutional Neural Networks (CNNs) [6].

2.2 Fingerprint

The fingerprint is one of the biometric traits most widely used because, even though its acquisition can be considered as more intrusive than the acquisition of facial images, it offers a good trade-off between accuracy and user acceptance.

Fingerprint recognition systems typically require the user to touch a surface to perform a biometric acquisition. The acquired sample consists of a greyscale image representing the pattern of the ridges and valleys of the fingertip. The majority of fingerprint recognition algorithms exploit information related to discontinuities in the ridges, called minutiae points. The patterns of minutiae points are highly distinctive, are unique for every person, and do not change throughout life. The biometric algorithms typically perform the recognition by enhancing the image, extracting the minutiae points, and then comparing the relative coordinates of the minutiae in the samples using non-exact graph matching techniques [27]. Fig. 2 shows examples of fingerprints of different individuals with the corresponding minutiae points.

One of the main drawbacks of traditional fingerprint recognition systems lies in the acquisition process. The contact with a sensor surface can be considered by the users as being uncomfortable or privacy-invasive, introduces non-linear distortions in the ridge pattern, and can be inaccurate in the case of dirty fingers. Fingerprint sensors are also prone to presentation attacks that are performed

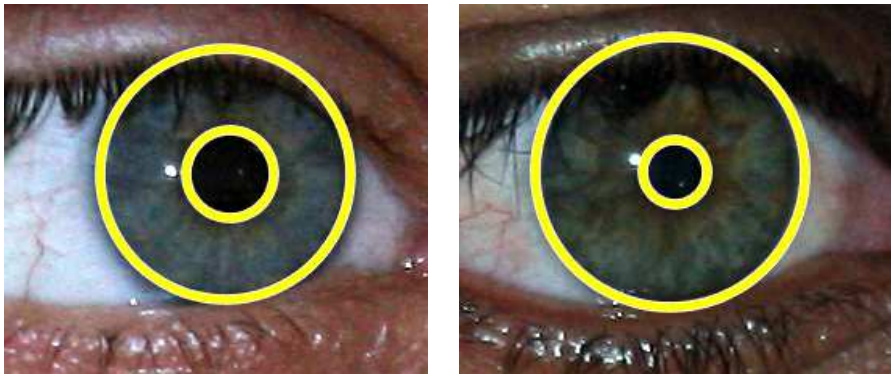

Fig. 3. Examples of images of the eyes of different individuals and their corresponding iris regions

using fake fingerprints. Furthermore, fingerprint recognition algorithms generally perform identity verifications by comparing two samples per time. Therefore, an identification query needs to compare a fingerprint sample with all the identities stored in a biometric database, which requires hours or days of computation in the case of governmental databases containing millions of identities.

One of the main research trends in fingerprint recognition aims to overcome the limitations of traditional touch-based acquisitions by focusing on touchless acquisition systems using two-dimensional images or three-dimensional models [16]. Other research trends focus on improving the robustness and accuracy of traditional touch-based fingerprint recognition for low-quality samples, detecting fake samples, and reducing the computational time needed for identification queries [34].

2.3 Iris

The iris is a ring-shaped membrane on the frontal part of the eye that, together with the pupil, controls the amount of light that a person perceives. Iris recognition systems offer very high accuracy and low matching times. Iris recognition is particularly useful in countries where the face may be partially covered due to traditional habits or in the case of worn fingerprints (e.g., manual workers or elderly people).

The acquisition process consists of capturing an ocular image with an iris scanner, which is a digital camera capable of capturing near-infrared images at a distance of approximately 30 centimeters. The biometric recognition process includes three main steps: segmentation, feature extraction, and matching. The majority of the methods in the literature segment the iris by approximating its shape to a ring delimited by two concentric circles, extracting biometric templates consisting of binary strings, and using a fast matching algorithm based on the computation of the Hamming distance between two templates [27]. Fig. 3

shows examples of images of the eyes of different individuals and their corresponding iris regions.

The main limitation of iris recognition systems consists of the used acquisition procedure, which requires high cooperation from the users to avoid possible problems due to a non-frontal gaze and occlusions caused by eyelids, eyelashes, and glasses. Furthermore, the acquisition procedure can be negatively influenced by environmental light conditions, which can introduce reflections, reduce the contrast of the iris pattern and modify the size of the pupil. The acquisition procedure also presents low user acceptance and can erroneously be considered as dangerous to health due to the use of near-infrared illuminators.

The main research trend consists of reducing the constraints of the acquisition process by studying methods working at distances greater than 30 centimeters from the sensor in natural light conditions and with non-cooperative users [15]. To achieve this goal, researchers are studying novel techniques to increase the robustness of the overall biometric recognition process. Specifically, the research community is working in the following directions: designing less-constrained acquisition setups and hardware, studying algorithms for segmenting the iris region as a non-circular shape from noisy ocular images affected by occlusions and poor illumination, implementing techniques for compensating pupil dilations and gaze deviations, and realizing feature extraction and matching techniques based on recent machine learning techniques, such as DL and CNNs.

2.4 Palmprint

The palmprint is the region of the hand from the wrist to the base of the fingers. The skin in this area is of the same type as that covering the fingertips and contains highly distinct features. The advantages of palmprint recognition systems with respect to other biometric technologies reside mainly in the fact that they can use low-cost acquisition devices, achieve high recognition accuracy, and are generally well-accepted by users.

Palmprint recognition systems can perform touch-based and touchless acquisitions. Based on the acquisition device used, biometric matching algorithms can use ad hoc segmentation algorithms and feature extraction approaches based on the principal lines of the palm, local texture descriptors, or coding-based algorithms that output a binary image of the palm [17]. Fig. 4 shows examples of segmented regions of interest considered by palmprint recognition systems.

One of the main limitations of palmprint recognition systems is that they need high-quality acquisitions to achieve satisfactory accuracy. Therefore, palmprint acquisition systems require training the users to properly place their hand in front of the camera or adopting physical guides to direct hand positioning.

The main research trend consists of studying techniques for achieving highly accurate recognitions while reducing the acquisition constraints. In particular, the research community is studying methods based on three-dimensional models to compensate possible problems due to unconstrained hand positions in touchless acquisitions and novel feature extraction and matching techniques based on local texture descriptors, coding methods, or CNNs [49].

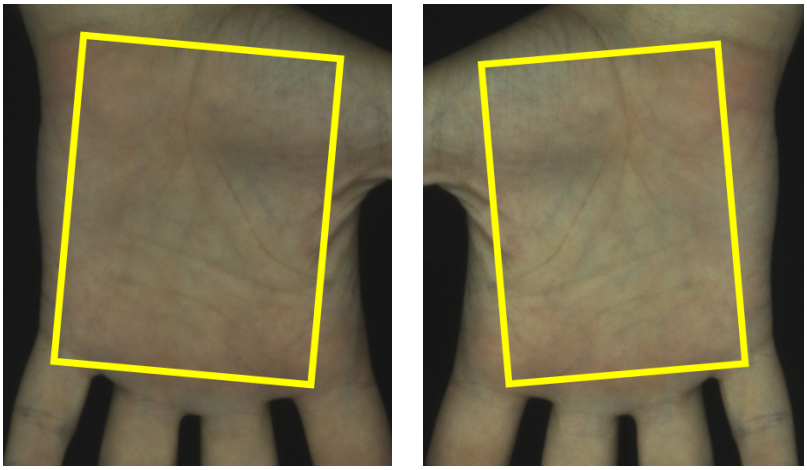

Fig. 4. Examples of regions of interest considered by palmprint recognition systems, which correspond to the region of the hand covering from the wrist to the base of the fingers

2.5 Electrocardiogram

The electrocardiogram (ECG) is a set of physiological signals representing the electrical activity of the heart over a period of time and collected using electrodes placed on the skin. ECG signals are generally collected for medical purposes, but studies in the literature have proven that they present sufficient discriminability to also be used for biometric recognition. With respect to other biometric traits, the ECG presents the advantages of being more difficult to counterfeit and acquirable for longer periods of time without requiring specific actions from the user.

In the literature, there are different methods for ECG recognition, which can be based on signals acquired using one or more electrodes. The biometric recognition approaches can use fiducial or non-fiducial features. Methods based on fiducial features extract points of interest within the heartbeat wave, called fiducial points. Systems based on non-fiducial features do not consider fiducial points and generally extract features in a transformed domain (frequency or wavelet) [40]. Fig. 5 shows the fiducial points commonly extracted from a heartbeat wave.

The main problem with using ECG signals for biometric recognition is that the research community has not yet proven the stability of the trait over long periods of time and in heterogeneous emotional and physiological conditions. Furthermore, the interoperability between acquisition devices has not been sufficiently analyzed.

An important research trend in ECG-based biometric recognition consists of studying techniques to guarantee the stability and interoperability of ECG signals. Other trends consists of adapting ECG recognition methods for signals

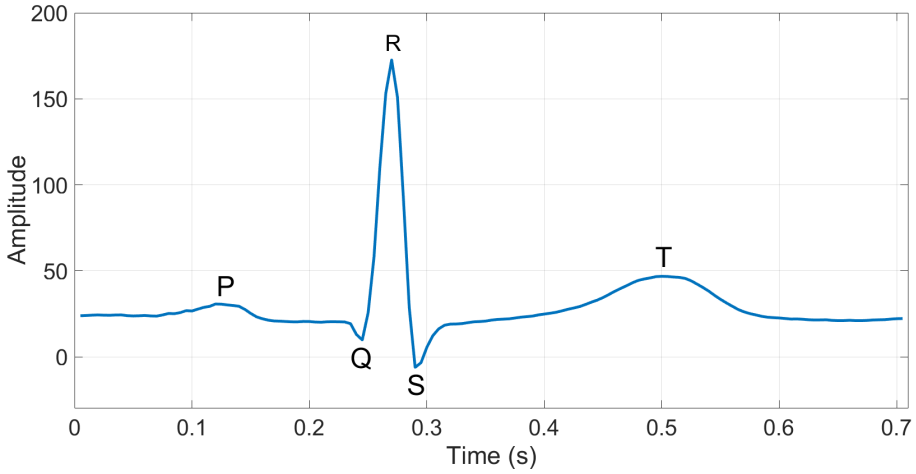

Fig. 5. Example of a heartbeat wave in an ECG signal, with the fiducial points used for recognition

acquired from wearable devices (e.g., from smartwatches or hardware for continuous health monitoring) and in designing continuous authentication techniques based on ECG signals [44].

2.6 Voice

The voice is one of the most widespread behavioral traits used for biometric recognition since the acquisition of voice signals requires only a microphone and in most cases does not require additional devices [27]. It is possible to divide voice recognition systems into speaker recognition and speech recognition systems. Whereas the former is aimed at recognizing the identity of the speaker, the latter is mostly used in human-computer interaction to transcribe spoken words into a digital format; therefore, it will not be discussed here.

Speaker recognition can be conducted with either text-dependent or text-independent verification techniques, based on whether the words spoken by the individual need to be identical to a text. In both text-dependent and text-independent verification, the majority of voice recognition methods use the mel-frequency cepstral coefficients, which are features designed to resemble the frequency characteristics perceived by humans.

Although a satisfactory recognition performance can be achieved using high-quality signals, state-of-the-art voice recognition systems have the main drawback of having a significant decrease in accuracy when low-quality or noisy signals are used.

The main research trend consists of designing biometric recognition methods that are robust to poor-quality signals, and the research community is mainly focused on DL techniques, which learn the discriminative representation of an individual directly from the raw input signal [18].

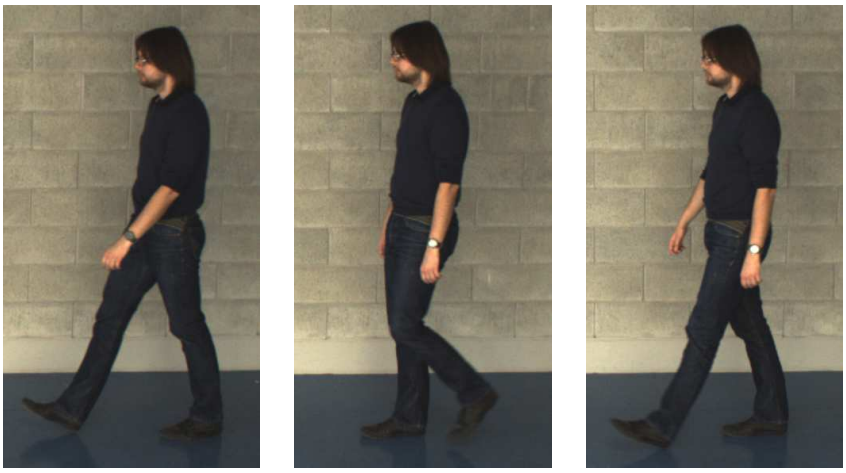

Fig. 6. Examples of images used to perform gait recognition

2.7 Gait

The gait is a behavioral biometric trait that is especially used for recognition when the traditional biometric traits cannot be easily observed, for example, when the individual is distant or presents a non-frontal pose. Biometric systems based on gait consider the distinctive characteristics of the way an individual walks to perform the recognition.

The distinctive pattern of the gait can be extracted from frame sequences acquired at long distances and with low-quality cameras. For each frame, the recognition methods extract the silhouette of the individual. The silhouettes are processed to extract motion features, which are the inputs of machine learning techniques used to recognize the individual. Fig. 6 shows examples of images used to perform gait recognition.

Although they exhibit satisfactory performance under partially constrained situations (e.g., constant direction with respect to the camera and uniform walking speed), the current methods for gait recognition are less reliable for recognition in the presence of non-ideal acquisitions, such as those performed at long distances, with different points of view, non-frontal poses, uncontrolled backgrounds, blur, or occlusions.

One of the main research trends consists of studying novel approaches capable of handling samples acquired in unconstrained scenarios. In particular, the research community is working on innovative techniques based on three-dimensional models and CNNs [50] and on using gait features to perform unobtrusive continuous authentication [47].

2.8 Soft biometric features: age and gender

Age and gender are two of the most used soft biometric features due to the possibility of estimating them from face images to complement the biometric

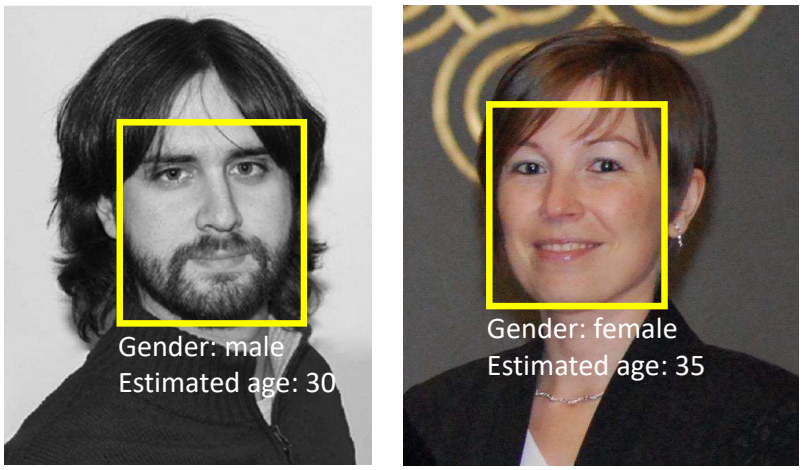

Fig. 7. Examples of age and gender estimation from facial images of different individuals

information used in face recognition systems. Age and gender estimation is performed in different scenarios, including face recognition systems, surveillance, and ambient intelligence applications.

Age and gender estimation techniques typically extract features from the images and then use machine learning approaches to perform the estimation. Examples of features include Gabor features, local binary patterns, and ad hoc features [52]. Fig. 7 shows examples of age and gender estimation from facial images of different individuals.

The performance of age and gender estimation methods are satisfactory for face images acquired in controlled conditions and from cooperative users. However, state-of-the-art methods suffer from decreasing performance in the presence of samples affected by rotations, non-neutral facial expressions, poor illumination, and occlusions.

The research trends in age and gender estimation are increasingly considering DL and CNNs to achieve high accuracy and to estimate a person's age and gender directly from images acquired in uncontrolled conditions [22].

2.9 Multibiometrics

Multibiometric systems fuse biometric data from multiple sources, for example, different biometric traits or different biometric algorithms. The goal of multibiometric systems is to overcome some of the problems of systems based on a single biometric trait, such as non-universality of the trait, limited distinctiveness, noisy data, or variability in different biometric acquisitions of the same individual. Furthermore, the use of multiple biometric traits improves the recognition accuracy and the resistance to spoofing attacks with respect to systems based on a single biometric trait.

Typically, biometric systems consider data originated from a single source (e.g., a single biometric trait). They can be divided into four main components: *i)* the sensor module, which acquires the biometric sample; *ii)* the feature extraction module, which extracts an abstract and discriminative representation from the sample, called biometric template; *iii)* the matching module, which compares the biometric templates and outputs a match score representing the degree of similarity or dissimilarity between the templates; *iv)* the decision module, which compares the match score against a threshold and returns a Boolean (yes/no) decision indicating whether the the considered biometric templates belong to the same person or not.

Multibiometric systems can integrate biometric information at four levels, corresponding to every module of typical biometric systems: *i)* at the sensor level, they combine raw biometric samples to obtain a more complete representation; *ii)* at the feature level, it is possible to concatenate the features obtained using different feature extraction algorithms to obtain a single template; *iii)* at the match score level, multibiometric systems can merge the scores resulting from different matching algorithms; *iv)* at the decision level, they combine the Boolean decisions of the single biometric systems.

The majority of multibiometric systems perform the fusion at the match score level, which enables them to fuse information from heterogeneous biometric sources with significant increases in accuracy and in a technology-independent manner [27]. Fig. 8 presents an outline of the match score-level fusion of face and fingerprint biometrics.

Although it is almost always possible to improve the recognition accuracy by fusing biometric information originating from different sources, multibiometric systems presents different drawbacks based on the fusion level considered. At the sensor level, it is necessary to combine samples captured with compatible devices and in similar conditions. As a consequence, the diffusion of heterogeneous sensors increases the complexity of sensor-level fusion methods. At the feature level, it is not always possible to concatenate features obtained using heterogeneous feature extraction algorithms, since they might use a different representation. At the match score level, fusion algorithms are dependent on the distribution of the scores in the considered application scenario, which might not be available in every situation. In some cases (e.g., commercial biometric systems already deployed), it might not be possible at all to access information at intermediate levels such as sensor, feature, or match score level.

An important research trend in multibiometric systems consists of designing an advanced feature-level fusion of heterogeneous biometric sources, which can improve the accuracy and robustness of the state-of-the-art multibiometric systems [24]. The research community is also working on machine learning techniques to perform an adaptive fusion at the match score level [2] and on multibiometric fusion strategies for ambient intelligence applications.

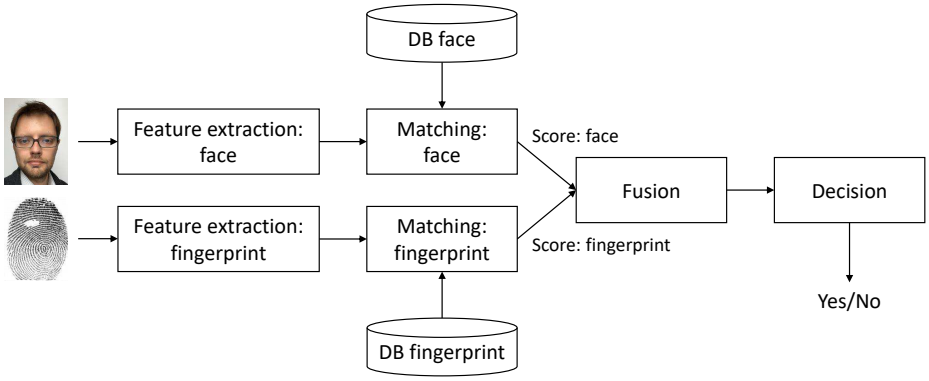

Fig. 8. Outline of the match score-level fusion of face and fingerprint biometrics

3 Emerging scenarios for biometric recognition

Biometric systems have gained increasing user acceptance and popularity and are now also being applied to novel scenarios beyond the traditional security and forensic applications. This section reviews the main emerging scenarios in which biometric systems are becoming more widespread, considering four main areas: *i)* public infrastructures, *ii)* private infrastructures, *iii)* user-centric applications, and *iv)* personal devices.

3.1 Public infrastructures

For infrastructures owned by public institutions or destined for public use (e.g., trains or buses), the main emerging scenarios include automated systems for border control, surveillance, humanitarian services, e-health, and public transport.

Automated Border Controls The term Automated Border Control (ABC) refers to an ensemble of technologies that enable automatic verification of the identities of travelers at border crossing points (i.e., without requiring constant human intervention). In particular, ABC gates (or e-Gates) use biometrics to perform a fast, reliable, and accurate verification of a traveler's identity. The deployment of e-Gates has been growing in recent years and has been increasingly adopted worldwide, with 48 countries currently using ABC systems in airports, land borders, and seaports. Therefore, the problem of developing a harmonized global framework for ABC systems is receiving increasing attention from the academic and industrial communities.

The diffusion of machine-readable travel documents such as electronic passports (or e-Passports) and electronic ID cards is also increasing. These documents store biometric samples of the owner and enable the use of e-Gates without needing the users to be enrolled in dedicated databases. Typically, the documents store a face image and, optionally, fingerprint and/or iris samples.

With the increased adoption of ABC systems and e-Passports, and therefore, the greater flow of passengers using such systems that is expected in the near future, it is necessary to design biometric systems with high usability, accuracy, and speed. Biometric systems for e-Gates should be easy to use by the majority of the population; able to guarantee an accurate biometric recognition, with sufficiently low execution times to enable a high throughput of passengers; and resistant to spoofing attacks. In particular, to improve the usability of ABC systems, research trends are considering advanced quality assessment algorithms that are able to detect and identify specific acquisition problems in fingerprint and face biometric modalities. To increase the recognition accuracy, other research trends are focusing on novel privacy-compliant multibiometric fusion techniques that can be tuned to operate in ABC systems [14].

Surveillance Biometric recognition in surveillance applications consists of recognizing individuals from samples captured at long distances, on the move, with non-frontal poses, and from uncooperative subjects. In surveillance scenarios, the most useful biometric traits are those that can be acquired at a distance, such as face or gait, but soft biometric features can also be extracted from face or body images. However, biometric recognition in surveillance systems faces problems caused by low-resolution images and poor-quality samples, making the use of such traits complex. To overcome the problem of low-resolution images, academic and industrial communities are considering the use of pan-tilt-zoom cameras, which enable acquiring high-resolution biometric data even at high distances. Other research trends are focusing on surveillance applications based on gait and soft biometrics, which are showing encouraging results for biometric recognition under unconstrained conditions. Gait information and soft biometric features can also be used together with other biometric traits in multimodal systems to achieve higher accuracy [38].

Humanitarian services Humanitarian services consists of the ensemble of aid given by a government to those who need help (e.g., due to war, famine, or natural disasters). The success of humanitarian actions depends to a significant degree on being able to identify people in need of essential goods and services. For this purpose, biometrics can act as enabling technologies that allow enrolling and identifying aid recipients and helps to reduce fraud. Recently, biometric technologies have been receiving increasing attention as useful tools for emergency support and refugee management. In fact, the United Nations High Commissioner for Refugees considers the adoption of biometric technologies to be strategic [26]. However, biometric systems used for the recognition of individuals in the context of humanitarian services face problems such as a high risk of spoofing attempts performed to receive goods and services allocated to other individuals and the impossibility to enroll a part of the population when using a particular biometric trait (e.g., fingerprints worn or damaged). To overcome these problems, iris recognition systems are being studied to identify refugees in Afghan regions [25].

Fig. 9. Examples of images used to count pedestrians in public transportation

E-health Electronic healthcare (or e-health) consists of the ensemble of hardware and software architectures that permit access to healthcare services through information and communication technologies. In e-health applications, the major issue is represented by the low confidence of people toward the exchange of health information, considered as private and sensitive information, over communication networks. Biometric technologies are therefore emerging in this field to provide greater security with respect to traditional authentication mechanisms and to increase the confidence of the users toward the use of healthcare services. In this case, biometrics can be used to protect and manage sensitive information, verify the identities of patients, improve security in medical facilities, restrict access, and reduce fraud. Thanks to these advantages, research trends are considering the application of fingerprint recognition in e-health to control access to medical resources and encrypt personal medical data [1].

Public transport Public transport refers to the means and technologies used to transport groups of passengers, which are available to the general public and often operating on fixed schedules. In public transport applications, biometrics offer many possibilities for authorities to monitor and secure the infrastructures. In fact, biometrics can verify the identities of driver's license holders or travel documents when they include biometric data such as face, fingerprint or iris. Other possible applications include securing access to traffic management centers and providing accurate estimates of the number of pedestrians [23]. Fig. 9 shows examples of images used to count pedestrians in public transport.

Since public transport applications typically represent low-security applications that need to guarantee a high throughput of passengers, biometric recognition technologies should perform a fast and highly usable recognition. Recent trends in public transport are therefore focusing on technologies based on uncontrolled face recognition or touchless fingerprint acquisition [36].

3.2 Private infrastructures

Private infrastructures consist of the structures that are owned by private companies and are not necessarily available for public use. Among the numerous applications of biometric systems in this area, the main emerging scenarios include e-commerce, e-banking, and private transport.

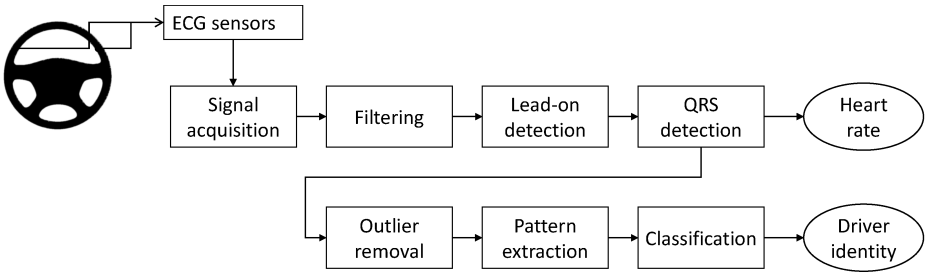

Fig. 10. Architecture of a biometric and health monitoring system for cars based on ECG signals. The system processes the ECG signal to detect heart rate anomalies and to perform continuous driver authentication.

E-commerce and e-banking E-commerce is increasingly used on the Internet to perform online transactions such as payments and e-banking operations. Although online payments are only a small proportion of total transactions, they represent a major source of losses for financial institutions due to fraud. Another major issue faced by e-commerce and e-banking applications is the possible lack of confidence of people toward performing online transactions that may involve considerable amounts of money. In online transactions, many of the security challenges involve user authentication because the service provider and the user are not in the same location. To address these issues and minimize losses in e-commerce and e-banking, novel techniques based on biometric systems are increasingly being studied to improve the security of identification and authentication tasks. In particular, biometric traits such as palmprint and fingerprint are being studied to enhance the security of one-time passwords for e-commerce and e-banking transactions [42].

Private transport Private transport refers to the means and technologies for transportation that are not available to the general public. In private transport applications, biometrics are receiving increasing interest due to the recent possibility of using portable devices with embedded biometric sensors that can also monitor the health status of the driver in real time. Biometric technologies, such as fingerprint readers, can be used to prevent thefts. A promising research trend consists of using portable devices with biometric capabilities to capture ECG signals, which can then be used to detect important factors that affect safe driving behavior, such as distractions, drowsiness, and drunkenness [33]. Fig. 10 shows an example of an architecture of a biometric and health monitoring system for cars based on ECG signals.

A different area of private transport that can benefit from biometrics is car sharing since the service supports short-term car rentals, typically for a duration of minutes or hours, requesting a fast recognition of the authorized users. The market for this type of service is evolving quickly, although the security part is evolving more slowly. To use car-sharing services, users simply need to log in with a password; then, they receive a smart key that they can use to unlock the car and drive. In car-sharing applications, biometric authentication mechanisms are

being increasingly studied to increase the security of the driver authentication and guarantee a more reliable service for both users and the service provider [41].

3.3 User-centric applications

User-centric applications represent ensembles of systems and technologies that facilitate individuals' interactions with the environment by providing adaptive services tailored to their preferences and activity patterns. Some of the emerging scenarios that apply biometric systems to user-centric applications include home automation, user-centric entertainment, and social media.

Home automation Home automation refers to the technologies used to facilitate human-computer interactions in ambient intelligence scenarios, with a specific focus on home environments. In these scenarios, a growing area of research considers the application of biometric technologies to facilitate a transparent human-computer interaction and support individuals in their everyday life tasks and activities. The biometric technologies required for ambient intelligence should be less constrained than those in traditional biometric systems. In addition, given the limited computational resources available for ambient intelligence devices, ambient intelligence and home automation applications should use low-complexity and optimized algorithms. In particular, fingerprint recognition systems are being increasingly studied in home automation scenarios, for example, by using mobile applications on smartphones to restrict access to appliances after the user performs a user-friendly authentication via the integrated fingerprint reader [10]. Similarly, voice recognition systems are being studied to identify users independently of their position in home environments, with the purpose of personalizing the user experience in home control applications [7].

User-centric entertainment User-centric entertainment refers to the technologies used to provide amusement to a single individual. Electronic games are the most common form of user-centric entertainment and are being increasingly studied as a test field for biometric technologies. In fact, computer games are virtual environments that allow researchers to evaluate biometric and physiological sensors in simulated applications without causing harm to the individuals [35]. Entertainment devices used in electronic games are evolving to integrate an increasing number of smart functionalities. In these devices, biometric recognition technologies can be used to automatically recognize users and tailor the entertainment content according to their preferences or to estimate the user's age to limit access to mature content [5]. In particular, research trends are attempting to use off-the-shelf depth sensors designed for games to perform in-game face recognition or age estimation [8]. Fig. 11 shows an example of age and gender estimation using three-dimensional body metrics obtained with a depth sensor.

Social media Social media refers to the computer technologies used to create virtual communities where individuals can exchange information and ideas. In this field, impersonation attacks represent a serious issue because they are

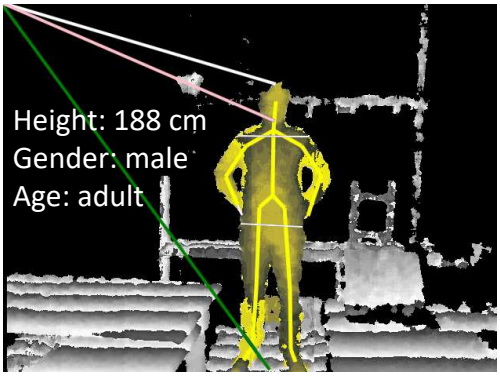

Fig. 11. Example of age and gender estimation using three-dimensional body metrics obtained with the Kinect sensor

difficult to discover and relatively easy to perform. Biometric technologies, as user-friendly approaches that can authenticate users both at the beginning of the session and then continuously, are emerging in social media applications as useful tools for preventing impersonation attacks. In addition, social media service providers can use biometrics to build user profiles for targeted marketing [31].

Another emerging topic in social media is the definition of distinctive features based on social network activities, called social behavioral biometrics. These biometric features are increasingly being used to verify a user's identity in virtual domains, perform continuous authentication in cyberspace, or obtain forensic information for cybercrimes. These biometric features can be used alone and in combination with other biometric traits [48].

3.4 Personal devices

Personal (or mobile) devices are computing devices that are small enough to be held and operated with one hand, such as smartphones or personal digital assistants (PDAs). Today, many such devices are equipped with biometric capabilities, and many users prefer their use over traditional passwords or personal identification numbers. However, biometric systems deployed on personal devices must address several issues, such as limited computational capabilities, limited size of the sensors, use in uncontrolled conditions, and spoofing attacks.

To overcome these issues and the specific drawbacks of biometric recognition using personal devices, research trends are considering different biometric traits. In particular, fingerprint recognition has been increasingly adopted due to the decreasing size of touch-based capacitive sensors, which are currently integrated in many mobile devices. Touchless fingerprint recognition algorithms for personal devices are also being studied since they can perform the recognition without requiring dedicated sensors but using only the integrated camera. However, touchless acquisitions of fingerprint images are more sensitive to vari-

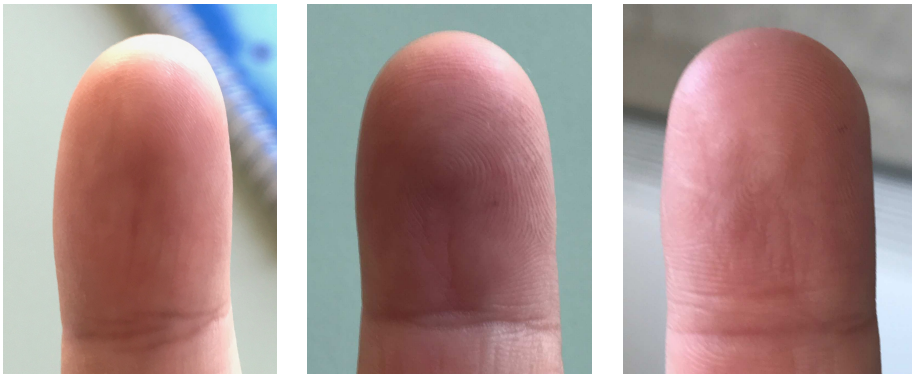

Fig. 12. Examples of fingerprint images acquired with a smartphone under different environmental illumination and background conditions

ations in illumination and background with respect to touch-based acquisitions. Therefore, research trends are considering robust processing algorithms able to extract the pattern of minutiae points in touchless acquisitions performed using personal devices. Fig. 12 shows examples of fingerprint images captured by the camera of a smartphone under different environmental illumination and background conditions.

Facial recognition is also a popular trait in mobile devices. However, personal devices capture face samples under uncontrolled conditions, with the consequence that the acquisitions present uncontrolled backgrounds, non-uniform illumination, and differences in pose and expression. For these reasons, research trends are focusing on dedicated sensors that can capture the three-dimensional model of the face in real time, thereby increasing the robustness to differences in background, illumination, and pose variations.

The use of iris recognition is also gradually becoming popular for personal devices, and research trends are studying recognition algorithms using uncontrolled acquisitions performed using visible light, with non-frontal gaze and with a non-constant distance from the sensor. Furthermore, studies are focusing on optimizing the iris processing algorithms due to the limited computational capabilities of personal devices.

Other biometric traits that are being considered for mobile devices include the voice, which can be captured using the microphone integrated in all personal devices, and the palmprint, whose recognition can be performed even with low-resolution images captured using an integrated camera. In addition, other research trends are studying biometric features specific to personal devices, such as touch screen dynamics [37].

Because almost all mobile devices integrate biometric sensors such as cameras, microphones or fingerprint scanners, the next natural step is to fuse their information using multimodal biometrics, which can provide higher accuracy and increase the difficulty of spoofing attacks [19].

4 Challenges and research trends of current biometric systems

In this section, we present challenging aspects and emerging solutions in current biometric systems by analyzing their main characteristics from different perspectives.

To incentivize more people to adopt and correctly use biometric systems in a growing number of scenarios, it is necessary to consider and improve different aspects of the biometric recognition process. The methods used to evaluate these aspects belong to different fields, ranging from engineering and computer science to social sciences and economics. In particular, the aspects to consider are the following (Fig. 13):

- *Usability* refers to how user friendly a system is to use and the time required for people to learn how to use it. Its measurement is related to the acquisition time and to the number of acquired samples of insufficient quality, as well as to the overall experience.
- *User acceptance* is based on how users perceive the system. It is related to the system's invasiveness and usability, as well as to personal inclinations or perceived privacy risks.
- *Privacy* considers the degree to which a biometric system protects the users' personal data and avoids data theft or misuse.
- *Security* refers to the robustness of the system against attacks made using fake biometric traits or malicious software.
- *Accuracy* is measured as the capability of the biometric system to effectively discriminate between users.
- *Execution time* is the amount of time required to perform the recognition, including the enrollment and matching procedures. This aspect is important because it influences the usability of the system. In fact, people can become frustrated when they feel that the recognition process takes too long.
- *Interoperability* considers the degree of compatibility between different systems. Interoperability is influenced by both the type of device (e.g., touch-based or touchless) and the data format used to store the biometric information. Biometric standards are used to partially mitigate interoperability issues.
- *Scalability* refers to the way in which the performance is affected when the number of users enrolled in the system increases or when the computer and network architecture face a greater number of requests. This aspect is related to both architectural aspects (e.g., CPU/GPU performance, hard disk throughput, and network bandwidth) and software aspects (e.g., the algorithmic complexity of the software implementation).

4.1 Usability and user acceptance

To improve the usability and user acceptance of biometric systems, research trends are currently focusing on aspects such as enhancing the characteristics of

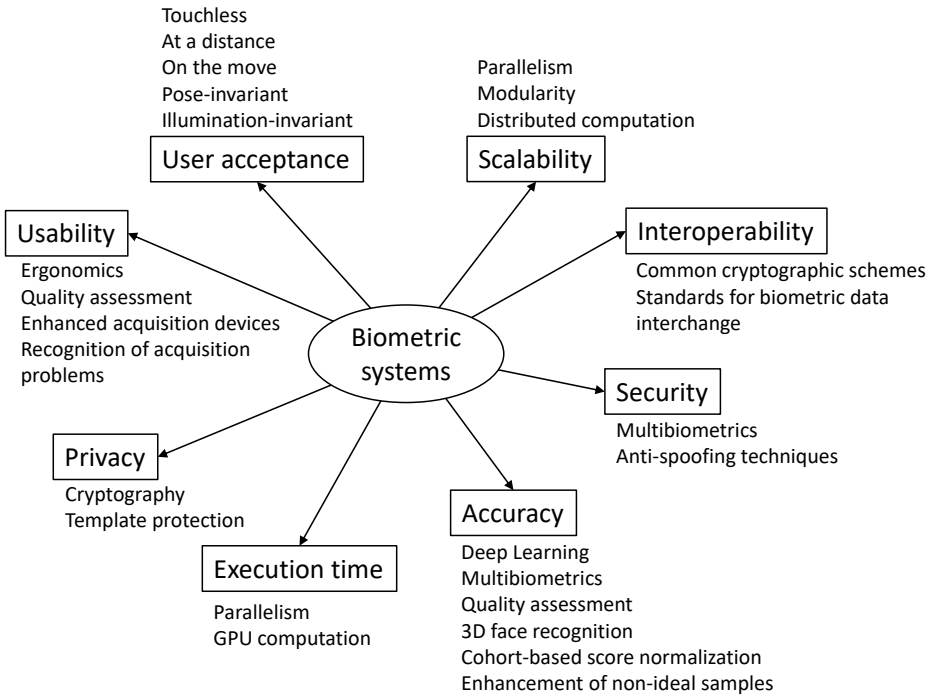

Fig. 13. Different aspects and emerging technologies in biometric systems

acquisition devices and their ergonomics, improving the robustness of the recognition algorithms to sample non-idealities, and using proper feedback techniques to achieve effective human-machine interactions.

To enhance the characteristics of acquisition devices, the research community is designing less-constrained and less-intrusive technologies for biometric recognition, such as touchless fingerprint/palmprint recognition [17], uncontrolled face recognition [6], iris recognition at a distance [39], and voice recognition in ambient intelligence scenarios [4]. Research on less-intrusive technologies includes the design of appropriate acquisition devices (e.g., scanners and cameras) and dedicated software. These technologies should be able to perform biometric verifications under less-controlled conditions compared to current biometric systems, for instance, at higher distances, in natural light, while a person is moving, or by using mobile devices. Touchless technologies are better accepted by users than touch-based biometric systems, and they can provide a better solution in terms of hygiene because they require no contact with any surface.

To achieve more robustness and flexibility in biometric identification, research trends are considering matching algorithms that can work with samples captured in non-ideal conditions [46]. For this purpose, DL and CNNs are also being increasingly studied for face [6] and gait [50] recognition systems to compensate for different non-idealities, such as acquisitions performed at high distances,

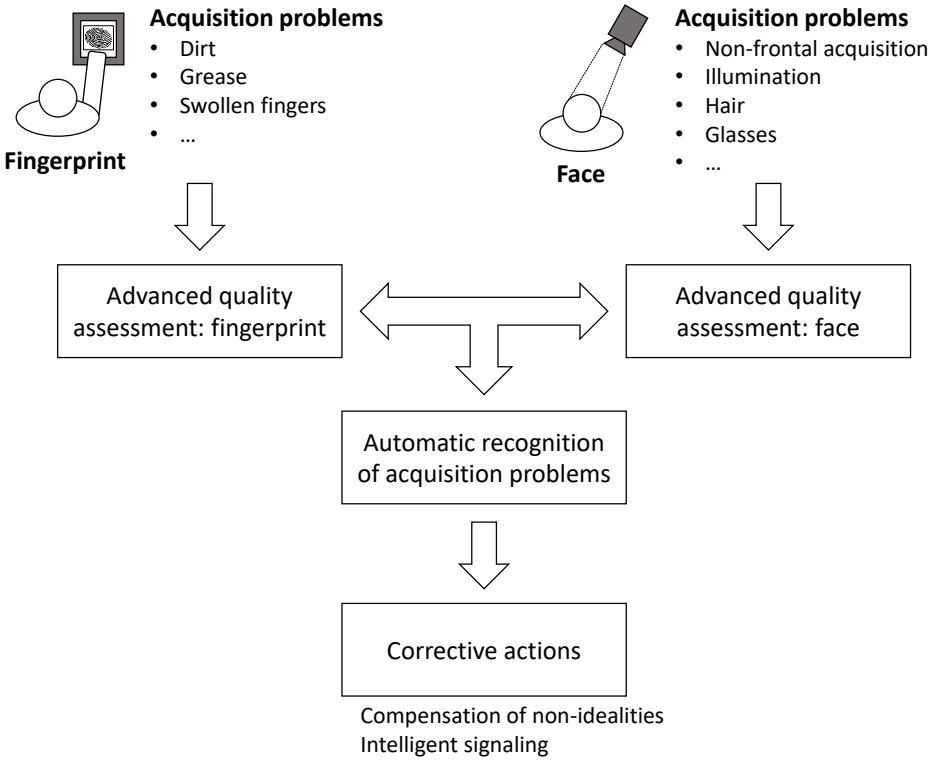

Fig. 14. Automatically detecting and correcting biometric acquisition problems in the ABC case

from different points of view, and with differences in illumination, pose, and expression.

To achieve an effective human-machine interaction, the algorithms that evaluate the quality of the acquired samples are particularly important. When people are tired, stressed, or inexperienced, such conditions can result in the capture of poor-quality samples, which can negatively affect the overall recognition accuracy. Research trends are therefore addressing advanced quality assessment algorithms for face, fingerprint [13], and iris samples [45] that can detect the different acquisition problems and improve the signaling by providing users with more precise feedback about which corrective action to perform. Fig. 14 shows an example of how advanced quality assessment algorithms for face and fingerprint acquisitions can be used in ABC systems to perform corrective actions tailored to the situation, such as compensating for non-idealities or using intelligent signaling.

4.2 Privacy and security

Biometric samples are personal and sensitive data that cannot be changed and that are unequivocally related to their owner. Therefore, protecting privacy and security is of paramount importance. In fact, if a person's biometric information is stolen, the thief could potentially use the stolen biometric data to impersonate the victim for an indefinite amount of time because it is not possible for people to change their biometric traits as they can with traditional authentication mechanisms (e.g., a password or a token) [27].

To increase people's confidence in biometric systems, users may need assurance about the privacy measures that such systems adopt. Therefore, international restrictions limit the retention of sensitive personal data strictly to the period during which they are effectively used and use logs for monitoring system quality that store data in an anonymized format [12]. To ensure the privacy of biometric data, some systems store templates rather than the original samples and use cryptographic techniques that were specifically developed for biometric systems [6]. Other methods use privacy-compliant and adaptive match-score normalization and fusion approaches [3].

Regarding the security of biometric verification, researchers are studying innovative antispoofing techniques, such as liveness detection methods able to detect a greater number of fake biometrics traits, including printed face images, fake fingers made of silicone, or synthetic irises [6]. Antispoofing techniques for multibiometric systems are also being studied [53].

4.3 Accuracy and execution time

The execution time is also a decisive factor for biometric recognition because lower biometric matching times decrease the time required for authentication and enable more transparent user interactions. At the same time, lower matching times could enable the real-time identification of individuals on blacklists or in large-scale automated fingerprint identification systems.

Recently, biometric systems based on DL techniques and CNNs have been gaining popularity and have achieved accuracy improvements for face, fingerprint [30], iris [6], palm [49], ECG [44], voice [18], and gait [50] recognition, as well as for age and gender estimation. DL techniques are also being used in multibiometric systems to increase accuracy [2] or to learn multiple representations from the same biometric sample [22]. However, the main drawbacks of methods based on DL techniques are the need for large amounts of training data, which can be difficult to collect, and the potentially large number of features to be stored in the template, which can cause storage problems when high numbers of users are present in the system [4]. Furthermore, these methods could require too much computational time for some live applications. To reduce the execution time in biometric systems, recent techniques have considered optimized implementations using parallel and general-purpose computing on graphics processing units, allowing performance gains of up to 14 times compared to sequential CPU-based implementations [21].

4.4 Interoperability

At present, biometric systems are composed of several collaborating subsystems and use common rules to favor the exchange of biometric information [14]. These rules specify the data format, the type of data exchanged, and the cryptographic schemes. However, even if standards for biometric data interchange exist, interoperability problems between different biometric systems can arise when, for example, different sensors are used to collect the samples [32].

Recent methods to improve the interoperability use cross-database evaluation techniques to increase the matching accuracy between different databases captured with different sensors. The current research trends focus on fingerprints [32], irises [11], and online signatures [51].

Biometric algorithms are also using machine learning approaches to perform matching among heterogeneous databases. In fact, recent methods are able to train and test models on samples captured with different modalities, with only limited performance decreases [3].

4.5 Scalability

The scalability of a biometric system is measured as the amount that the performance of the system is negatively affected in terms of both accuracy and execution time when the size of biometric databases enlarges or when the hardware and network infrastructure must handle a greater number of requests. A scalable biometric is able to perform an accurate biometric match and respond within an acceptable time window when both the number of enrolled users and the number of requests increase, without requiring significant changes in the software, hardware, and network architectures.

Scalability is particularly important in biometric systems working in the identification modality when it is necessary to match a biometric sample against many other samples to determine the identity of the individual (e.g., in national law enforcement databases composed of millions of biometric records) or operating with large populations of users (e.g., border control applications with thousands of passengers per day).

Recent trends are considering the use of techniques based on distributed computation, parallelism, and modularity. For example, some approaches have studied the adoption of biometric recognition as a service using cloud computing architectures [9].

5 Conclusions

This chapter provided an overview on recent technologies, emerging scenarios, and research trends in biometric recognition.

One of the main goals of the research community is to increase the robustness of state-of-the-art biometric systems to samples acquired in uncontrolled conditions. Important research trends consist of studying novel and robust methods to

perform the recognition in unconstrained conditions using physiological traits, behavioral traits, soft biometric features, and multibiometric systems. For this purpose, recent machine learning approaches based on DL and CNNs showed particularly promising results in terms of accuracy and robustness to poor-quality acquisitions. The improve robustness of biometric recognition methods to poor-quality samples acquired in uncontrolled conditions is enabling a diffusion of biometric technologies in a wider set of application scenarios. Emerging scenarios include public infrastructures, where it is necessary to perform accurate biometric recognitions using databases of millions of identities, such as border control, surveillance, and humanitarian services. Other emerging scenarios include private infrastructures, where it is necessary to guarantee a correct recognition to avoid fraud, such as e-commerce and e-banking. Furthermore, emerging scenarios include user-centric applications where biometrics can facilitate the interaction of the person with the environment, such as home automation, user-centric entertainment, and personal devices.

Although the diffusion of biometric technologies is increasing in heterogeneous application scenarios, academic and industrial communities are still studying new methods to improve the different aspects of biometric technologies, making them more usable, socially acceptable, privacy compliant, and secure, as well as with higher accuracy, faster execution, and improved interoperability. However, although the research community is proposing important novelties, further studies should be performed to design biometric systems that are deployable in completely unconstrained conditions, thus permitting their diffusion in further application scenarios and making them enable technologies for new types of human-centric personalized services.

Acknowledgments

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 PRIN 2015 project COSMOS (201548C5NT).

References

1. Abbas, A., Khan, S.U.: A review on the state-of-the-art privacy-preserving approaches in the e-health clouds. IEEE Journal of Biomedical and Health Informatics 18(4), 1431–1441 (2014)
2. Al-Waisy, A.S., Qahwaji, R., Ipson, S., Al-Fahdawi, S., Nagem, T.A.M.: A multi-biometric iris recognition system based on a deep learning approach. Pattern Analysis and Applications (October 2017)
3. Anand, A., Donida Labati, R., Genovese, A., Muñoz, E., Piuri, V., Scotti, F., Sforza, G.: Enhancing the performance of multimodal Automated Border Control systems. In: Proc. of the 15th Int. Conf. of the Biometrics Special Interest Group (BIOSIG). pp. 1–5. Darmstadt, Germany (September 2016)

4. Anand, A., Donida Labati, R., Hanmandlu, M., Piuri, V., Scotti, F.: Text-independent speaker recognition for ambient intelligence applications by using information set features. In: Proc. of the 2017 IEEE Int. Conf. on Computational Intelligence and Virtual Environments for Measurement Systems and Applications (CIVEMSA). pp. 30–35. Annecy, France (July 2017)
5. Antipov, G., Baccouche, M., Berrani, S.A., Dugelay, J.L.: Apparent age estimation from face images combining general and children-specialized Deep Learning models. In: Proc. of the 2016 IEEE Conf. on Computer Vision and Pattern Recognition Workshops (CVPRW). pp. 801–809 (June 2016)
6. Bhanu, B., Kumar, A. (eds.): Deep Learning for Biometrics. Springer (2017)
7. Biagetti, G., Crippa, P., Falaschetti, L., Orcioni, S., Turchetti, C.: Distributed speech and speaker identification system for personalized domotic control. In: Conti, M., Martínez Madrid, N., Seepold, R., Orcioni, S. (eds.) Mobile Networks for Biometric Data Analysis, pp. 159–170. Springer Int. Publishing (2016)
8. Boutellaa, E., Bengherabi, M., Ait-Aoudia, S., Hadid, A.: How much information Kinect facial depth data can reveal about identity, gender and ethnicity? In: Agapito, L., Bronstein, M.M., Rother, C. (eds.) Proc. of the 2014 European Conf. on Computer Vision Workshops. pp. 725–736. Springer International Publishing, Cham (2015)
9. Castiglione, A., Choo, K.K.R., Nappi, M., Narducci, F.: Biometrics in the cloud: Challenges and research opportunities. IEEE Cloud Computing 4(4), 12–17 (July 2017)
10. Chantal, M., Lee, S.W., Kim, K.H.: A security analysis and reinforcement design adopting fingerprints over drawbacks of passwords based authentication in remote home automation control system. In: Proc. of the 6th Int. Conf. on Informatics, Environment, Energy and Applications (IEEA). pp. 71–75 (2017)
11. Connaughton, R., Sgroi, A., Bowyer, K., Flynn, P.J.: A multialgorithm analysis of three iris biometric sensors. IEEE Trans. on Information Forensics and Security 7(3), 919–931 (June 2012)
12. De Capitani di Vimercati, S., Foresti, S., Livraga, G., Samarati, P.: Data privacy: definitions and techniques. Int. Journal of Uncertainty, Fuzziness and Knowledge-Based Systems 20(06), 793–817 (2012)
13. Donida Labati, R., Genovese, A., Muñoz, E., Piuri, V., Scotti, F., Sforza, G.: Automatic classification of acquisition problems affecting fingerprint images in Automated Border Controls. In: Proc. of the 2015 IEEE Symp. on Computational Intelligence in Biometrics and Identity Management (CIBIM). pp. 354–361. Cape Town, South Africa (2015)
14. Donida Labati, R., Genovese, A., Muñoz, E., Piuri, V., Scotti, F., Sforza, G.: Biometric recognition in Automated Border Control: a survey. ACM Computing Surveys 49(2), 24:1–24:39 (November 2016)
15. Donida Labati, R., Scotti, F.: Noisy iris segmentation with boundary regularization and reflections removal. Image and Vision Computing 28(2), 270–277 (2010)
16. Donida Labati, R., Piuri, V., Scotti, F.: Touchless Fingerprint Biometrics. CRC Press (2015)
17. Genovese, A., Piuri, V., Scotti, F.: Touchless palmprint recognition systems, Advances in Information Security, vol. 60. Springer (2014)
18. Ghahabi, O., Hernando, J.: Deep Learning backend for single and multisession i-Vector speaker recognition. IEEE/ACM Trans. on Audio, Speech, and Language Processing 25(4), 807–817 (April 2017)
19. Gofman, M.I., Mitra, S., Cheng, T.H.K., Smith, N.T.: Multimodal biometrics for enhanced mobile device security. Communications of the ACM 59(4), 58–65 (2016)

20. Grother, P.: IREX I - performance of iris recognition algorithms on standard images. Tech. Rep. Interagency Report 7629 Supplement One, NIST (2010)
21. Gutiérrez, P.D., Lastra, M., Herrera, F., Benítez, J.M.: A high performance fingerprint matching system for large databases based on GPU. IEEE Trans. on Information Forensics and Security 9(1), 62–71 (January 2014)
22. Han, H., Jain, A.K., Shan, S., Chen, X.: Heterogeneous face attribute estimation: A deep multi-task learning approach. IEEE Trans. on Pattern Analysis and Machine Intelligence (2018)
23. Hernandez, D., Castrillon, M., Lorenzo, J.: People counting with re-identification using depth cameras. IET Conf. Proc. pp. 16–16(1) (2011)
24. Hezil, N., Boukrouche, A.: Multimodal biometric recognition using human ear and palmprint. IET Biometrics 6(5), 351–359 (2017)
25. Jacobsen, K.L.: Experimentation in humanitarian locations: UNHCR and biometric registration of afghan refugees. Security Dialogue 46(2), 144–164 (2015)
26. Jacobsen, K.L.: On Humanitarian Refugee Biometrics and New Forms of Intervention. Journal of Intervention and Statebuilding 11(4) (2017)
27. Jain, A.K., Flynn, P., Ross, A. (eds.): Handbook of biometrics. Springer (2008)
28. Jain, A.K., Ross, A., Prabhakar, S.: An introduction to biometric recognition. IEEE Trans. on Circuits and Systems for Video Technology 14(1), 4–20 (January 2004)
29. Jain, A.K., Nandakumar, K., Ross, A.: 50 years of biometric research: Accomplishments, challenges, and opportunities. Pattern Recognition Letters 79, 80–105 (2016)
30. Jang, H.U., Kim, D., Mun, S.M., Choi, S., Lee, H.K.: Deeppore: Fingerprint pore extraction using Deep Convolutional Neural Networks. IEEE Signal Processing Letters 24(12), 1808–1812 (December 2017)
31. Li, C.: Biometrics in social media applications. Biometrics in a Data Driven World: Trends, Technologies, and Challenges p. 147 (2016)
32. Lin, C., Kumar, A.: Matching contactless and contact-based conventional fingerprint images for biometrics identification. IEEE Trans. on Image Processing (2018)
33. Lourenço, A., Alves, A.P., Carreiras, C., Duarte, R.P., Fred, A.: CardioWheel: ECG biometrics on the steering wheel. In: Bifet, A., May, M., Zadrozny, B., Gavalda, R., Pedreschi, D., Bonchi, F., Cardoso, J., Spiliopoulou, M. (eds.) Machine Learning and Knowledge Discovery in Databases. pp. 267–270. Springer Int. Publishing (2015)
34. Maltoni, D., Maio, D., Jain, A.K., Prabhakar, S.: Handbook of fingerprint recognition. Springer, 2nd edn. (2009)
35. Mandryk, R.L., Nacke, L.E.: Biometrics in Gaming and Entertainment Technologies, p. 191–224. CRC Press (2016)
36. Mears, J.: Lift-off: can biometrics bring secure and streamlined air travel? Biometric Technology Today 2017(2), 10–11 (2017)
37. Meng, W., Wong, D.S., Furnell, S., Zhou, J.: Surveying the development of biometric user authentication on mobile phones. IEEE Communications Surveys Tutorials 17(3), 1268–1293 (2015)
38. Neves, J., Narducci, F., Barra, S., Proença, H.: Biometric recognition in surveillance scenarios: a survey. Artificial Intelligence Review 46(4), 515–541 (2016)
39. Nguyen, K., Fookes, C., Sridharan, S., Denman, S.: Quality-driven super-resolution for less constrained iris recognition at a distance and on the move. IEEE Trans. on Information Forensics and Security 6(4), 1248–1258 (December 2011)

40. Odinaka, I., Lai, P.H., Kaplan, A.D., O'Sullivan, J.A., Sirevaag, E.J., Rohrbaugh, J.W.: ECG biometric recognition: A comparative analysis. IEEE Trans. on Information Forensics and Security 7(6), 1812–1824 (December 2012)
41. Park, S.H., Kim, J.H., Jun, M.S.: A design of secure authentication method with bio-information in the car sharing environment. In: Park, J.J.J.H., Pan, Y., Yi, G., Loia, V. (eds.) Advances in Computer Science and Ubiquitous Computing: CSA-CUTE 2016, pp. 205–210. Springer Singapore (2017)
42. Plateaux, A., Lacharme, P., Jøsang, A., Rosenberger, C.: One-time biometrics for online banking and electronic payment authentication. In: Teufel, S., Min, T.A., You, I., Weippl, E. (eds.) Availability, Reliability, and Security in Information Systems. pp. 179–193. Springer Int. Publishing (2014)
43. PR Newswire: Market forecast by technologies, applications, end use, regions and countries (2015), https://www.prnewswire.com/news-releases/global-biometrics-market-2014-2020-market-forecast-by-technologies-applications-end-use-regions-and-countries-300095676.html
44. Ŝarlija, M., Jurîšić, F., Popović, S.: A convolutional neural network based approach to QRS detection. In: Proc. of the 10th Int. Symp. on Image and Signal Processing and Analysis. pp. 121–125 (September 2017)
45. Schmid, N.A., Zuo, J., Nicolo, F., Wechsler, H.: Iris quality metrics for adaptive authentication. In: Burge, M.J., Bowyer, K.W. (eds.) Handbook of Iris Recognition, pp. 67–84. Springer London, London (2013)
46. Si, X., Feng, J., Zhou, J., Luo, Y.: Detection and rectification of distorted fingerprints. IEEE Trans. on Pattern Analysis and Machine Intelligence 37(3), 555–568 (March 2015)
47. Stone, E.E., Skubic, M.: Unobtrusive, continuous, in-home gait measurement using the microsoft kinect. IEEE Trans. on Biomedical Engineering 60(10), 2925–2932 (October 2013)
48. Sultana, M., Paul, P.P., Gavrilova, M.: Social behavioral biometrics: An emerging trend. Int. Journal of Pattern Recognition and Artificial Intelligence 29(08), 1556013 (2015)
49. Svoboda, J., Masci, J., Bronstein, M.M.: Palmprint recognition via discriminative index learning. In: Proc. of the 2016 23rd Int. Conf. on Pattern Recognition (ICPR). pp. 4232–4237 (December 2016)
50. Takemura, N., Makihara, Y., Muramatsu, D., Echigo, T., Yagi, Y.: On input/output architectures for Convolutional Neural Network-based cross-view gait recognition. IEEE Trans. on Circuits and Systems for Video Technology (2017)
51. Tolosana, R., Vera-Rodriguez, R., Ortega-Garcia, J., Fierrez, J.: Preprocessing and feature selection for improved sensor interoperability in online biometric signature verification. IEEE Access 3, 478–489 (2015)
52. Tome, P., Fierrez, J., Vera-Rodriguez, R., Nixon, M.S.: Soft biometrics and their application in person recognition at a distance. IEEE Trans. on Information Forensics and Security 9(3), 464–475 (March 2014)
53. Wild, P., Radu, P., Chen, L., Ferryman, J.: Robust multimodal face and fingerprint fusion in the presence of spoofing attacks. Pattern Recognition 50, 17–25 (2016)