Contents

1

Introduction to Biometry

Carmelo Velardo, Jean-Luc Dugelay

Lionel Daniel, Antitza Dantcheva, Nesli Erdogmus

Neslihan Kose, Rui Min, Xuran Zhao
EURECOM, 2229 Route des Crêtes, 06560 Sophia Antipolis

CONTENTS

The term *Biometric* comes from the ancient Greek $\beta\iota o\varsigma$ (bios: life) and $\mu\varepsilon\tau\rho o\nu$ (metron: to measure, to count). Both concepts indicate that there is something related to life (the human nature) that can be measured, or counted. Biometry is the science that tries to understand how to measure characteristics which can be used to distinguish individuals. Humans have developed such skills during the evolution: the brain has specialized areas to recognize faces [1] and to link identities with specific patterns (behavioral or physical [2]). Researchers in the biometry field have always tried to automatize such processes making them suitable to be run on a computer or a device.

The study of biometric patterns led to the definition of requirements which have to be respected to make a human trait feasible to be used in a recognition process. A biometric trait can be summarized as: a characteristic that each person should have (**Universality**), in which any two persons should present some differences (**Distinctiveness**), that should not drastically vary over a predefined period of time (**Permanence**), that should be quantitatively measurable (**Collectability**).

Furthermore the biometric traits can be divided into the two following classes: *physical* and *behavioral*. To the former class belongs the face appearance, the pattern of the iris and the fingerprint, the structure of the retinal veins as well as the shape of the ear. Each of these traits can be additionally subdivided into *genotypic* and *randotypic*, the former indicates a correlation with some genetic factors (like hereditary similarities in twins), the latter describes traits that develop randomly during the fetal phase. Behavioral biometrics develop as we grow older and are not a priori defined. To those traits belong the gait, or even the keystroke pattern (the way of typing on a keyboard).

In this chapter we will provide a broad view of what a biometric system is and which techniques are commonly employed to measure and compare systems' performance. An overview of the current biometric traits part of the International Civil Aviation Organization (ICAO) standard will be provided. A full presentation and comparison of biometric traits is out of the scope of this work. In Section 1.1 a general discussion will define the components of a biometric system and the tools to measure and compare systems' performance. Section 1.2 will concentrate on several biometric traits and their associated recognition techniques. Section 1.3 will present the new trends and challenges that the biometric panorama offers today, and a series of examples of working systems and applications will be presented as well. Finally, the conclusion will summarize the potential of biometrics and the challenges still opened.

1.1 Biometric for person authentication

Since the beginning of biometry's history the discriminative power of some traits (e.g. fingerprints) was used for the identification and tracking of criminals. Recently, after the attacks of the 11^{th} September 2001, a sudden urge of security promoted the boost of biometry as a tool which could ease the prevention of such events [3]. The international organizations started gathering information about all passengers crossing their borders by using biometrics. Thus, biometric authentication started being used in many airports and train stations. Biometric traits are mainly used to perform identification in order to allow/deny access to restricted areas, to index a set of pictures by person, or to enable decrypting data in biometric enabled devices. Thus, biometry is now employed in many technologies not always related with security.

Biometric-based authentication can nowadays complements or replaces both *knowledge-based* and *token-based* authentications, which require from an authenticated user to know a secret password and/or to keep a personal token like a physical key. Although a biometric traits cannot be forgotten like a password, or lost like token, they may be unconsciously disseminated like fingerprints or DNA (e.g. hair), this raises ethical concerns about users' privacy.

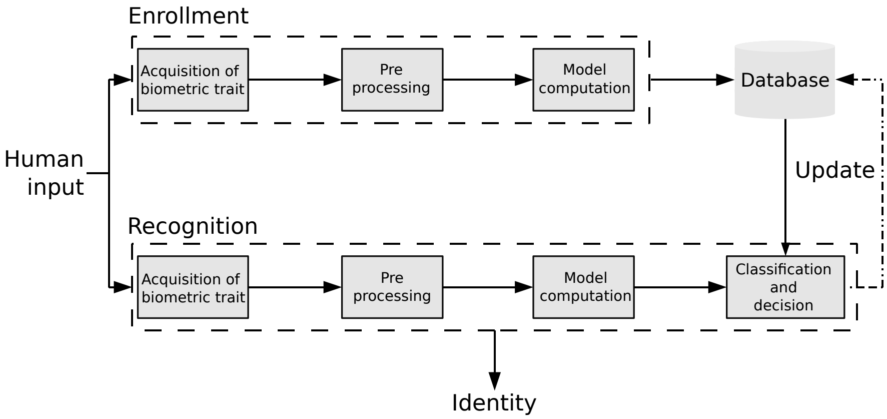


FIGURE 1.1
Scheme of a general biometric system and its modules: enrollment, recognition, and update. Typical interactions among the components are shown.

In figure 1.1 we present the typical scheme of a general biometric system, three main components can be identified: enrollment, recognition, and update. While the first two components are required, the last step is optional in an automatic application. In this section a description will be provided for each of the modules, while the last part will focus on techniques which allow performance evaluation of biometric systems.

1.1.1 Enrollment module

The enrollment module is the first important part of a biometric system. Its first step requires acquiring the biometric trait with a sensor (e.g. fingerprint scanner). Generally, a pre-processing step follows. It extracts important information from the raw representations of the data. The extracted information is then ready to be directly stored as a record in a database (usually associated with the ID of the subject), which constitutes the model of the subject.

1.1.1.1 Acquisition

For capturing biometric traits specific sensors are needed so that information can be digitized for further processing. It is clear that since each trait is different from the others, also the capturing devices need some specificities. Visual patterns like face, iris, ear, generally require cameras to record their image; for other biometrics like fingerprint, specialized scanners are needed.

Moreover, a biometric trait may bring different information, for example face can be represented with both its texture and shape, as well as with its thermal response, for this reason a variety of sensor could be used on the same biometric trait. In other cases, the biometric trait can show enhanced characteristics under different acquiring conditions; iris for example has shown better performance under infrared lighting, imposing the use of infrared light emitters and near-infrared cameras.

Strong variations can bring as well to a temporary *failure to acquire*, which forces the user to repeat the acquisition. The acquisition may also be repeated several times in order to generate a subject model that is more robust to possible variations.

Two classes of sensors exist: *contact* sensors, in which the biometric traits must touch the acquisition device surface (e.g. fingerprint scanners), or *contact-less* sensor if this requirement is not necessary (e.g. camera for face recording). For each of the two kind of sensors, a variety of technologies can be used to perform the scan. Each one could provide improvements in speed, accuracy, or even overcome adverse conditions (e.g. recording at night using infrared cameras).

The acquisition module is critical as all the following modules depends on the quality of the acquisition. Moreover the acquisition stability should hold between enrollment and recognition so that the recognition error rate remains low.

1.1.1.2 Pre-processing

After digitizing the biometric trait several pre-processing techniques might be involved to improve the quality of the recording, to reduce the dimensionality of the captured data, or to extract important features from the biometric trait.

Improving the quality of the recording may include: the restoration of corrupted image areas due to acquisition noise; the compensation of unwanted external elements, like illumination, face expression, and occlusions in face recognition; or the enhancement of some features, like binarizing the ridges in a fingerprint. Many pre-processing techniques aim at extracting some content from the given data. For example eyes detection may be useful for identifying the location of facial features for face registration, or for a successive iris detection. Another useful tool employed in biometric data pre-processing is dimensionality reduction. Mathematical tools like Principal Component Analysis (PCA) or Linear Discriminant Analysis (LDA) allow the extraction of important variations of given biometric traits by discarding redundant information, thus reducing data size.

Features extraction is part of pre-processing, it consists in the the extraction of salient information from the given trait. Such saliences should be representative enough to allow a classification of the biometric trait; transforming then the raw biometric data to a vector $V = [f_1, f_2, \dots f_n]$ where f_i represents a single feature. The concept is very close to dimensionality reduction but in this case the information is selected according to given heuristics and algorithms (like Local Binary Patterns [4] or SIFT [5] descriptors for face recognition). More detailed descriptions on how to perform such operations for several biometrics will be given in Section 1.2.

1.1.1.3 Model computation

After the acquisition and pre-processing steps, data has to be elaborated in order to create a model (also known as template) to be stored in a secured database. The model is used as reference for the identity of the user. When the user will try to access the system again, his/her scans will be matched against the template.

Directly storing raw scans in the database is a straightforward way to create user models. This brings some advantages but also some disadvantages: on one hand the system is not bounded to the use of a single matching strategy which could be changed if needed, on the other hand the amount of memory demanded to the system could be bigger and the subject privacy lower. Another approach is to save the features, previously extracted in the pre-processing step, so that the required memory is smaller, and the recognition step would not have to compute two models to perform the matching. However, using this paradigm, the system is bounded to the matching algorithm; if this has to be changed, all the system have to be restructured.

Other approaches are similar to dictionary-like systems; here a large set of features is analyzed and the discriminant ones are kept as basis (*words*). Each biometric trait can be described as a collection of such words. Descriptors like SIFT and LBP were both used successfully in dictionary-like methods [6].

1.1.2 Recognition module

The recognition module utilizes the information stored in the database during the enrollment phase. The biometric modality is sensed again using a similar (but not necessarily the same) device priorly used for the enrollment. However, because of the natural variability of the biometric trait (e.g. face expression, pupil dilatation), or because of the acquisition conditions (e.g. illumination, finger position on the scanner) some differences may arise. For this reason the elaboration of the model has to consider them and create a template robust to variations.

The recognition module has to verify an identity (*verification*) or to recognize a person in a pool of candidates (*identification*). During *verification* a subject claims his/her own identity to a system (e.g. through the use of a token) that collects the biometric trait and decides if the extracted features match the ones of the model corresponding to the claimed identity. We can summarize the process as trying to reply to the question "Is the subject identity the one he/she claims?". In a *identification* paradigm the question changes: "Who is this person?". In this case the system provides a guess on the user identity, to be chosen among all the enrolled clients. While in the first case the problem is a *one-to-one* matching (also called *open*), in the second paradigm the match is *one-to-many* (also known as *closed*).

1.1.3 Update module

As anticipated, each scan of the same biometric may result in a different representation of the same features. Those variations may depend on the variability of conditions at sensing time, or on the intrinsic nature of biometric traits which do not always appear the same. To compensate the variability during the enrollment phase one could record many acquisitions of the same trait allowing a generalization of the client's template. Nevertheless, the time can have a critical impact on the biometric trait itself. While some biometric traits are not modified as the subject grows older (e.g. iris), some others are subjected to degradations because of aging effects (e.g. face). Some of those variabilities can be compensated by the use of an *update* module. The purpose of such a step is to tune the enrolled model to make it more robust against natural variations. Thus, when the biometric system recognizes a client within a sufficient confidence range, it can extract features from the current biometric modality, and update the corresponding database entry. Some biometric traits which are more subjected to variations because of their non-permanent nature (e.g. voice) will particularly benefit of the model update; in these cases such an element should always be part of the system.

1.1.4 Classification and fusion of multiple modalities

Classification is the problem that involves the identification of sub-populations in a set of input data. For biometrics it means finding a transformation that leads from the feature space to a class space. The purpose of a biometric authentication system is mainly to retrieve the identity of a person, or to verify that a person is who he/she claims to be. The verification problem is a binary classification (genuine versus impostor), whereas the identification problem is an n-ary classification, where $n \in \mathbb{N}$ is the number of mutually-exclusive identities. A person, represented as a feature set, is classified by measuring its similarity to the template of each class; the person is then said to belong to the class that has the most similar template(s). Classification task is to minimize the *intra-class* variations (i.e. the variations which a biometric trait experiences because of natural conditions) and maximizing the *inter-class* variations which occur between different persons. For classification a similarity measure has to be defined. Such operation measures the distance of a feature projected into the classification space against all the templates.

In a multi-modal biometric system, several different feature sets per person are usually available. In order to classify a person according to those data, one could concatenate the features to form a larger array that will be classified by a general-purpose classifier (e.g. SVM, neural network). However, the computational complexity of the classification may exponentially increases in accordance to the bigger dimensionality of the new feature set. An alternative to feature concatenation is *classification fusion*, which merges the results of several low-dimensional classifications.

Combining diverse[1] biometric systems aim at improving the characteristics of the overall system. For example, the system will be more universal: if a biometric trait is missing because of a failure at acquisition time or because of a handicap, the other modalities could compensate. Also, circumventing the system will become increasingly complex as an impostor will have to deploy several spoofing techniques. Besides being multi-modal (more than one modalities, like face, fingerprint, gait), a system can be multi-sensor (more than one sensor per modality), multi-sample (more than one acquisition per modality), and multi-algorithm (many classifiers per features, and different kind of features extracted per modality).

The information flow of a multi-modal biometric can be fused at several levels.

- Fusion at *sensor* level consolidates raw sensory data before the feature extraction; images can be fused at pixel level (stitching, mosaicking), phases of radio or sound waves can be aligned (beam-forming), and data from one sensor (e.g. 2D camera) can help to interpolate the data of another sensor (e.g. 3D camera).

- Fusion at *feature* level consolidates data either by merging them, or by concatenating them. The former strategy can be used for updating and improving the templates; this requires compatible feature spaces and data normalization. The latter method linearly increases the feature space, hence exponentially increases the enrollment and authentication computations. A solution to that could be represented by space reduction techniques like PCA and LDA, and assumptions about features independence.

- Fusion at *score* level consolidates matcher outputs. Similarly to feature

[1] Biometrics systems are *diverse* if the cause of an error in one system is unlikely to affect the other systems.

fusion, score fusion needs the scores to be compatible, which involves normalization techniques that would be discussed in the following. In case the purpose of the biometric system is to identify people, matchers may provide a ranking of the enrolled people; fusing ranks has a strong advantage over fusing scores: ranks are comparable and voting theory provides axiomatic solutions to *rank* level fusion.

- Fusion at *decision* level is similar to rank level fusion, where voting theory provides axiomatic solutions.

The role of low level fusions like sensor or feature fusions is to separate the discriminative information from the environmental noise. On the other hand the role of high level fusions like score, rank, and decision fusions is to find a consensus amongst opinions, which are possibly weighted by reliability measures induced from quality measures (e.g. blurriness of the 2D face images).

Score level fusion is common since industrial biometric system usually provides scores, and since scores is a richer information than rank or decision. However, the scores might be incompatible since they come from different sources. Contrarily to ranks and decisions, the scores are usually normalized before being fused. Near-linear normalization techniques, like minmax ($\text{Score}_{\text{Normalized}} = \frac{Score-min}{max-min}$), scale and shift the scores to map them onto a common domain. Other normalizations can be applied in order to align score distributions, but such normalizations need a deeper training step during which the score distributions are estimated.

1.1.5 Performance evaluation: robustness and security

A practical way to categorize a biometric system is to analyze it under the three following aspects. The first one considers the *performance* of such a system, like the achievable recognition accuracy, speed, and throughput. User *acceptability* is another important parameter as it gives a measure of how many people are willing to use that biometric system in their life. This could be influenced by benefits, like the access to fast lanes in airports, as well as from cultural factors. A third parameter is the *circumvention* which represents how easily the system can be compromised and spoofed by subjects with malicious intent. Hereafter we will focus on how to quantitatively measure system's performance.

1.1.5.1 Evaluation database

In order to simulate system behavior under normal usage conditions, a set of labeled data are used. These labeled acquisitions allow for measuring the system performance in presence of simulated clients and impostors. The use of such database guarantees scientific repeatability since data does not vary from one test to the other. Usually a dataset is associated with one or many protocols, that are defined rules establishing how to perform the experiments. Databases and protocols are used as testbeds for algorithms and as common platform for the comparison of different systems.

Existing datasets for face recognition are: FERET, the first one to include big temporal variations, and FRGC which includes both 2D and 3D scans of participants faces. Other databases exist for other biometric traits like iris (UBIRIS and CASIA). Fingerprint databases can be synthesized with the SFINGE toolbox [7].

Multiple modalities require large databases containing several traits per user. MBGC, for example, is a multi-modal database as it contains both irides and face scans. When multi-modal datasets do not exist it is common practice to mix biometric traits from different databases to create synthetic (*chimeric*) users. Each of these identities will be valid from the experimental point of view, even if it is the result of a mix of different persons samples.

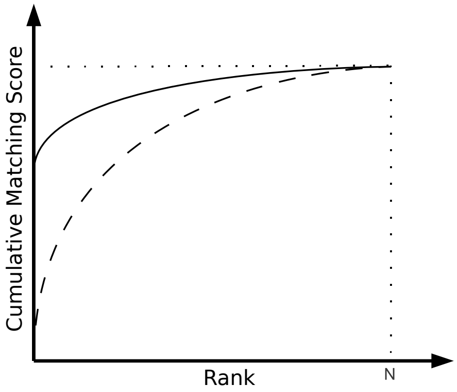


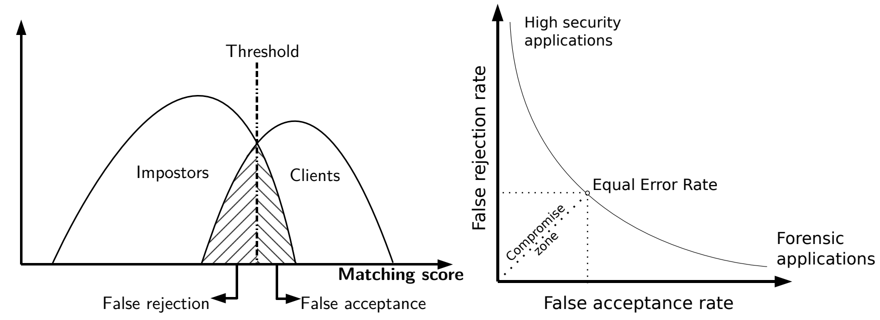
FIGURE 1.2
The lines represent two examples of cumulative matching characteristic curve plots for two different systems. The solid line represent the system that performs better. N is the number of subjects in the database.

The research community developed a set of mathematical tools which allow to measure the recognition performance of a biometric system [8]. Here we focus on how to measure recognition performance, while intentionally omit speed and bandwidth measures which can be tuned by simply investing more resources to the system.

The recognition rate is the most used performance measure, but it alone does not provide information on the system's behavior. Indeed, while testing a biometric system, also the position of the true positive is important, we refer to this as the *rank* of the true positive. The higher the test rank, the better the system recognized that user. Thus, a better biometric system always ranks higher the person's identity. The most common and compact representation of the biometric system's performance is represented by the Cumulative Matching Score (see figure 1.2), which shows the recognition rate as a function of the rank given to the person's identity by the biometric system.

For what concerns the verification mode two errors are relevant: *false acceptance*, and *false rejection* error. In the first case the system accepts an impostor as a client, while in the second case it wrongly rejects a client considering it as an impostor. In both cases two error rates can be computed over all the system. We can refer then to *False Acceptance Rate* and *False Rejection Rate*, or *FAR* and *FRR*.

The distributions of the scores for both impostors and clients are represented in figure 1.3.a as well as *FAR* and *FRR*. Intuitively, by modifying the defined threshold, we vary the performance of our system, making it more or less restrictive. Each threshold define a different *operating point* of the system. Then, testing all the operating points means varying the threshold and recording different values of *FAR* and *FRR*: by plotting those pairs of rates we obtain the *Receiver Operating Characteristic* curve (or simply *ROC* curve). An example can be found in figure 1.3.b. The *equal error rate* (or *EER*) corresponds to the point where the FAR is equal to the FRR, it is one operating point particularly relevant as it is used to compare systems' performance. *Security* is another important aspect of a biometric system performance and it should not be confused with *Robustness*, which is the recognition capability of the system. Still explored by the research community, security is a key point for the development of commercial applications as it deals with many different aspects and working conditions of the biometric system itself. For this reason



(a)

(b)

FIGURE 1.3
Typical examples of biometric system graphs, the two distributions (a) represent the client/impostor scores; by varying the threshold different values of FAR and FRR can be computed. A ROC curve (b) is used to summarize the operating points of a biometric system, for each different application different performances are required to the system.

here we will focus principally on what concerns the security of a system from the biometric point of view: spoofing.

1.1.5.2 Spoofing

It has been shown that conventional biometric techniques, like fingerprint or face recognition, are vulnerable to attacks. One of the most important vulnerabilities is *spoofing* attacks, where a person tries to masquerade as another one by falsifying data and thereby gaining an illegitimate access to the system. Spoofing can be defined as a class of attacks on a biometric security system where a malicious individual attempts to circumvent, at the acquisition phase, the correspondence between the biometric data acquired from an individual and his/her identity. In other words, the malicious individual tries to introduce fake biometric data into a system that does not belong to that individual, either at enrollment and/or recognition [9].

Currently there is a strong need for efficient and reliable solutions for detecting and circumventing such kind of attacks. The exact techniques for spoofing vary depending on the particular type of biometric trait involved [9]. For example a prosthetic fake finger can be used for fingerprint spoofing. Early works on the field showed that gelatin and conductive silicon rubber may be used for that purpose [10, 11]. On the other hand, for iris spoofing, a high resolution image of an iris can be used to pass the security check. Also face appearance based systems suffer from similar vulnerabilities as a masked fake face, a video of the user or even a photo of the client can be used for spoofing purposes.

The typical countermeasure to a spoofing attack is liveness detection. The aim of liveness testing is to determine if the biometric data is being captured from a live user who is physically present at the point of acquisition [12]. In [13], liveness detection is grouped in four different ways. First way is to use available sensors to detect in the signal a pattern characteristic of liveness/spoofing (*Software-based*). Second method is to use dedicated sensors to detect an evidence of liveness (*Hardware-based*), which is not always possible to deploy. Liveness detection can also exploit *Challenge-response* methods by asking the user to interact with the system. Another way is to use recognition methods intrinsically robust against attacks (*Recognition-based*). Along those direct methods for liveness detection also multiple modalities could be exploited (e.g. voice could be jointly used with face recognition in video based solutions). [13] present some examples of countermeasures for face recognition systems that involve for the first group skin reflectance/texture/spectroscopy analysis as well as the use of 3D shape of the head as way to measure the liveness of a system's user. In the second group we can mention active lighting, multi-camera face analysis, and detection of temperature. The third group involves challenge-response approach, synchronized lip movement, and speech for liveness detection. For the last group multi-spectral scanning of the face may be useful to distinguish live/spoofed face.

1.2 ICAO biometrics

In this section we will provide a brief overview of several biometric traits: face, iris, and fingerprint. We selected those because they are included in the open standard of biometric passport created by ICAO (International Civil Aviation Organization). For each biometrics we will refer to the scheme in figure 1.1 using the keywords: ***acquisition***, ***pre-processing***, ***model computation***, and ***classification***.

1.2.1 Face

The human face is a fundamental element in our social lives because it provides a variety of important signals: for example, it carries information about identity, gender, age, and emotion. For this reason, human face recognition has been a central topic [14, 15] in the field of person identification.

Acquisition Face is one of the easiest biometrics to digitize as a normal camera is usually enough. Nevertheless, a camera can only extract the texture information, thus incurring a series of problematics like pose and illumination variations. For this reason several methods are nowadays explored which make use of innovative sensors like 3D scanners or thermal cameras to extract many other information from a face.

Capturing face from a distance makes such a biometric trait non-intrusive, easy to collect, and in general well-accepted by the public. However, it is still a very challenging task, as faces of different persons share global shape characteristics, while face images of the same person are subject to considerable variability. This is due to a long list of factors including facial expressions, illumination conditions, pose, facial hair, occlusions, and aging. Although much progress has been made over the past three decades, Automatic Face Recognition (AFR) is largely considered as an open problem.

In this section, we present two widely adopted approaches to AFR from still intensity images, one deals with face as a whole, the other one is a local feature based approach. An exhaustive review is out of the scope of this chapter due to the large body of existing work. On the other hand, a brief summary on the recent technologies in AFR and several novel techniques is given at the end of the section.

1.2.1.1 Eigenfaces

Pre-processing Kirby and Sirovich first outlined that the dimensionality of the face space, i.e. the space of variation between images of human faces, is much smaller than the dimensionality of a single face considered as an arbitrary image [16]; later on, Turk and Pentland applied those considerations into practice to the problem of AFR [17]. As a useful approximation, one may consider an individual face image to be a linear combination of a small number of face components. Such components are called *eigenfaces* and can be derived from a set of reference face images.

The name eigenfaces comes directly from the use of eigenvector and eigenvalues decomposition (also known as eigen-decomposition process) used in *Principal Component Analysis*. PCA, (cf. [16]), describes how to deduce from a set of data a decreased number of components. Thanks to PCA for each given set of faces we can deduce a subspace that discards redundant information of the original space. In other words we obtain from the face space, a set of orthogonal vectors (eigenfaces) that represents the main variations of the original input.

To formally describe the PCA process let $\{x_1, ..., x_N\}$ be a set of reference or training faces and $\overline{x}$ be the average face. Then we can obtain the centered version of our faces set by computing $d_i = x_i - \overline{x}_i$. Finally, if $\Delta = [d_1, ..., d_N]$, the *scatter* matrix S is defined as:

$$S = \sum_{i=1}^{N} \delta_i \delta_i^T = \Delta\Delta^T. \tag{1.1}$$

The optimal subspace P_{PCA} is the one that maximizes the scatter of the projected faces:

$$P_{PCA} = \arg\max |PSP^T|, \tag{1.2}$$

where $|.|$ is the determinant operator. The solution to equation 1.2 is the subspace spanned by the eigenvectors (also eigenfaces) $[e_1, e_2, ...e_K]$ corresponding to the K largest eigenvalues (λ_k) of the scatter matrix S:

$$Se_k = \lambda_k e_k. \tag{1.3}$$

As the number of images in the training set is generally lower than the dimension of the image space, i.e. the number of pixels in an image, the number of non-zero eigenvalues is $N - 1$ (cf. [14]). We remind that, since the data are normalized to be zero-mean, one of the eigenvectors and the corresponding eigenvalue are zero-valued.

Due to the size of the scatter matrix S, the direct estimation of its eigenvalues and eigenvectors is difficult. They are generally estimated either through a SVD of the matrix Δ or by computing the eigenvalues and eigenvectors of $\Delta^T\Delta$. It should be underlined that eigenfaces are not themselves usually plausible faces but only directions of variation between face images.

Model computation Each face image x_i is represented by a point w_i in the K-dimensional space: $w_i = [w_i^1, w_i^2, ...w_i^K]^T = P_{PCA} \times \delta_i$. Each coefficient w_i^k is the projection of the face image on the k-th eigenface e_k and represents the contribution of e_k in reconstructing the input face image. In other words by using the eigenfaces we are able to reconstruct the original appearance of the faces that we used to build the space. Additionally, PCA guarantees that, for the set of training images, the mean-square error introduced by truncating the expansion after the K-th eigenvector is minimized.

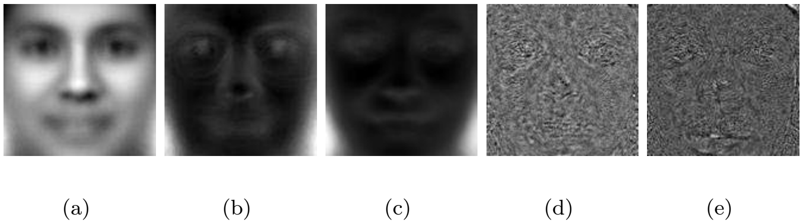


FIGURE 1.4
(a) Average face and (b)-(c) EigenFaces 1 to 2, (d)-(e) Eigenfaces 998-999 as estimated on a subset of 1,000 images of the FERET face database.

Classification To find the best match for an image of a person's face in a set of stored facial images, one may calculate the distances between the vector representing the new face and each of the vectors representing the stored faces, and then choose the image yielding the smallest distance. The distance between faces in the face subspace is generally based on simple metrics such as L1 (city-block), L2 (Euclidean), cosine and Mahalanobis distances (see [18]).

1.2.1.2 Local Binary Patterns

In order to provide a broad view on the two main approaches which are usually used in pattern recognition tasks we just discussed a *holistic* approach that treat the signal in its entirety. In this part we will present a typical *local* approach based on the extraction of local features from the original signal.

Pre-processing The Local Binary Pattern (LBP) [19] operator originally forms labels for the image pixels by thresholding the 3×3 neighborhood of each pixel with the center value and considering the result as a binary number. A histogram of these 2^8 labels, is created as the texture descriptor, by collecting the occurrences. Due to its computational simplicity and its invariance against monotonic gray level changes. LBP algorithm rapidly gained popularity among researchers and numerous extensions have been proposed which prove LBP to be a powerful measure of image texture [20, 21]. The LBP method is used in many kinds of applications, including image retrieval, motion analysis, biomedical image analysis and also face image analysis. The calculation of the LBP codes can be easily done in a single scan through the image. The value of the LBP code of a pixel (x_c, y_c) is given by:

$$LBP_{P,R} = \sum_{p=0}^{P} s(g_p - g_c)2^P \tag{1.4}$$

where g_c corresponds to the gray value of the center pixel (x_c, y_c), g_p refers to gray values of P equally spaced pixels on a circle of radius R, and s defines a Heaviside step function.

Model computation Successively, the histograms that contain data about the distributions of different patterns such as edges, spots and plain regions are built, the classification is performed by computing their similarities.

Classification Several measures have been proposed for histograms [4] such as Histogram intersection, Log-likelihood statistic. One of the most successful in the case of LBP is Chi-square statistic here defined as:

$$\chi^2(V', V'') = \sum_{i}^{n} \frac{(V_i' - V_i'')^2}{V_i' + V_i''} \tag{1.5}$$

where V' and V'' are feature histograms and the special case $\frac{0}{0} = 0$.

1.2.1.3 New Technologies and Recent Studies

Most algorithms have been proposed to deal with individual images, where usually both the enrollment and testing sets consist of a collection of facial pictures. Image-based recognition strategies have been exploiting only the physiological information of the face; in particular its appearance encoded in the pixel values of the images. However, the recognition performances of these approaches [22] have been severely affected by different kinds of variations, like pose, illumination and expression changes.

For automatic face recognition, various new algorithms and systems are still frequently proposed, targeting one of these different challenges. One of these methods is proposed by Wright et al. [23] for robust face recognition via sparse representation. In this framework, face recognition is casted as penalizing the L1-norm of the coefficients in the linear combination of an over complete face dictionary. *Sparse representation* based classification has been demonstrated to be superior to the common classifiers such as *nearest neighbor* and *nearest subspace* in various subspaces like Eigenfaces and Fisherfaces.

Some others of these emerging techniques exploit both static and dynamic information from video sequences. There exist approaches that adopt still-image based techniques to video frames, as well as ones that introduce spatio-temporal representation, in which dynamic cue of the human face contributes to recognition [24, 25].

On the other hand, as the 3D capturing process becomes faster and cheaper, 3D face models are also utilized to solve the recognition problem, especially under pose, illumination and expression variations where 2D face recognition methods still encounter difficulties. Numerous methods have been presented, which treat the 3D facial surface data as 2.5D depth maps, point clouds or meshes. Even though 3D face recognition is expected to be robust to variations in illumination, pose, and scale, it does not achieve perfect success and additionally introduces some critical problems like 3D mesh alignment [26]. Moreover, intra-class variations related to facial expressions, which cause non-rigid deformations on the facial surface still need to be dealt with.

1.2.2 Iris

The iris is the colored circular region around the pupil, the small dark hole of the eye through which the light passes to focus on the retina. What makes this part of the eye so peculiar for biometry is the presence of a particular pattern which is determined in a random manner during the fetal life phase. Even though the presence of pigments can increase during childhood, the pattern of the eye does not vary during the lifespan of a person; along with the strong randomness of the pattern those characteristics make iris a suitable biometric trait. The first automatic iris recognition system is due to the early work of Daugman [27] which first described and introduced algorithms to exploit iris random pattern for people recognition.

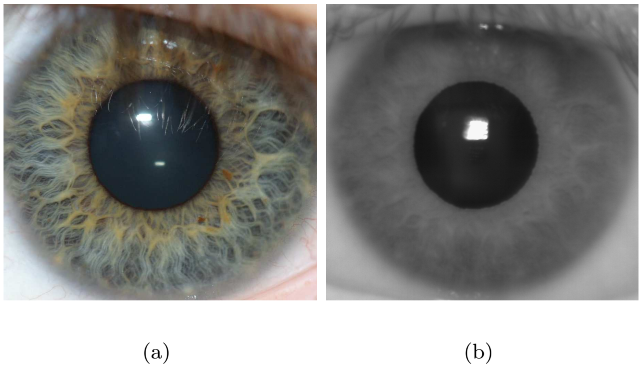

(a) (b)

FIGURE 1.5
A colored (a) and a near-infrared (b) version of the same iris.

An example of iris pattern is shown in figure 1.5, both a colored version and a near-infrared version are provided. Following the first early works on iris recognition we can distinguish two main methodologies that are nowadays used to perform the iris matching. The former technique refers to the Daugman method, the latter to the work of Wildes.

1.2.2.1 Daugman's approach

Pre-processing An overview of the methodology can be found in figure 1.6. The system requires that the eye of the subject is in the field of view of the camera. An automatic mechanism improves the sharpness of the iris image by maximizing the middle and high energy bands of the Fourier spectrum, by modifying the focus parameter of the camera, or providing information to the user which will move his/her head accordingly. A deformable template [28] is then used to seek for the position of the eye. The iris can be then described by three parameters: radius r and center position coordinates of the circle: x_0 and y_0. This kind of approximation, at first accepted for iris recognition systems, nowadays is no more considered valid. The latest works [29] deal with the non uniformity due of deformations caused by the inner nature of the iris pattern or due to partial occlusion (caused by eyelashes and eyelid).

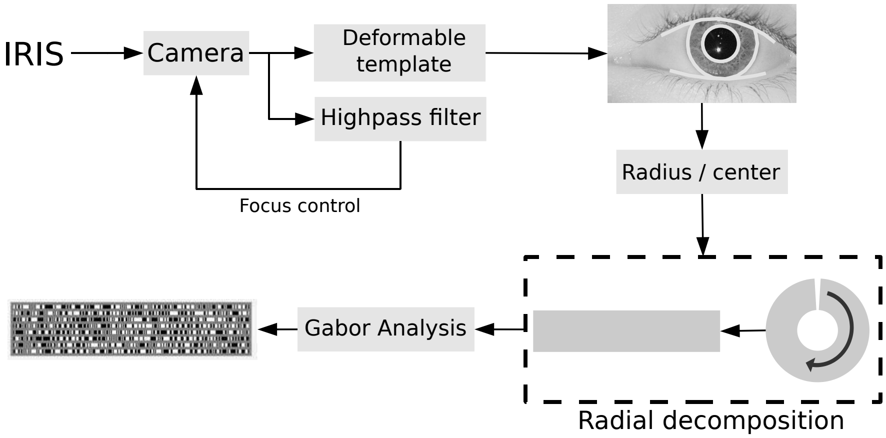


FIGURE 1.6
A scheme that summarizes the steps performed during Daugman approach.

After its detection, a normalization of the iris image is needed to compensate other effects that might influence the scale of the iris. An example could be different acquisition distance; or variable light conditions, which make the pupil muscles dilate or shrink the iris pattern. The normalization of Daugman's scheme makes use of polar coordinates to identify each location of the circular pattern. The angular and radial position are then normalized respectively between 0 and 360 degrees and 0 and 1. The latter normalization assumes that the iris is modified linearly in its contractions; also this technique was questioned and explored in a later work [30].

Model computation After the extraction of the iris boundaries a technique is needed to encode the information carried by the pattern. Daugman uses convolution of the image with a set of bi-dimensional Gabor filters.

Classification The result of such convolution is then quantized and represented as a binary vector which encode the sign of real and imaginary part of the filter response. A total of 256 bytes is used to represent the signatures. The comparison of two signatures can be made using different distance measures, the one Daugman originally proposed was based on a XOR operation which simply measure the quantity of different symbols for two given signatures.

1.2.2.2 Wildes' approach

Pre-processing Wildes presents a different methodology to the iris recognition task. His approach consists of a binary thresholding of the eye image to perform the localization and segmentation of the iris. Contrary to Daugman scheme, this solution allows to be more robust to noise perturbations while detecting the iris, but in the meanwhile makes the segmentation less sensitive to finer variations.

Classification The differences between the two approaches continues also in the matching of the extracted signatures. Wildes method uses the Laplacian of Gaussian filter at multiple scales in order to derive a model of the pattern, and a correlation measure to compute the matching score.

The main differences between the two systems can be summarized as follows. Daugman's method is simpler than the latter; on the other hand Wildes's method allows for a higher information payload as it does not quantize the filter response. This allows better discriminatory power at the cost of a less compact representation of the iris pattern, and a higher computational complexity.

1.2.3 Fingerprint

Every time we touch something we release information about our identity involuntarily. This information is encoded in the small crests and valleys that draw lines on our fingertips. Those lines are called ridges and all together form the complex pattern of the fingerprints. Fingerprints are a random disposition of human skin cells that develops as the fetus grows on the mother's womb during the pregnancy. The randomness makes even the fingerprints of monozygotic twins completely different.

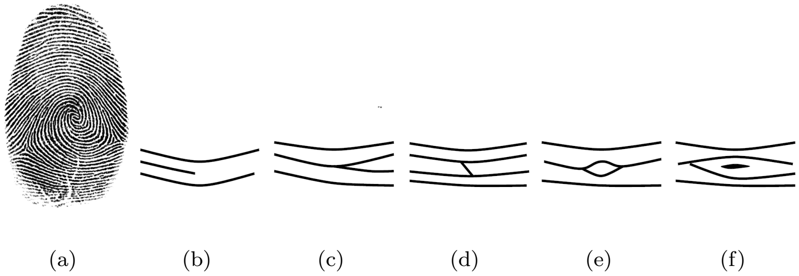


FIGURE 1.7
Example of a fingerprint (a), and of the minutiae: (b) termination, (c) bifurcation, (d) crossover, (e) lake, (f) point or island.

The fingerprint lines pattern creates several types of configurations which allow to differentiate global features, if the fingerprint is considered in its whole appearance; or local features as those lines joint or bifurcate. In the figure 1.7 a fingerprint is shown together with some of the peculiar local features called *minutiae*.

Acquisition The oldest method to acquire a fingerprint is to cover the surface of the fingertips with a layer of ink, then press the finger against a piece of paper. Nowadays scanners exist that use several techniques (optic, thermal, electromagnetic, or ultrasounds) to digitize the structure of the fingerprint [31]. The surface of the scanner can be of different size, from very small (as in the case of swiping sensors), to very big (as for full hand fingerprint systems). In the first case the finger is swiped over the sensor that reconstructs the fingerprint by stitching together the single slices sensed at time, in the second case all fingerprints of both hands can be digitized together.

Pre-processing Several methods exist in literature about evaluation of similarities between two fingerprints. Very few algorithms operate directly on the gray scale image, in general, each matching algorithm is performed only after a preprocessing of the fingerprint image [31]. During this phase, several steps can be performed to enhance the pattern formed by the ridges, or to extract information regarding the global and the local structure of the pattern.

Classification We can identify three main classes for these matching algorithm: correlation-based, minutiae-based, and ridge feature-based. In the first case two fingerprint representations are superimposed and a correlation is computed pixel by pixel while varying the rotation and translation of one image over the other, the correlation measures the similarity between the two. The minutiae-based approach is the method applied by human experts, and so far largely popular as automatic system. It is based on the extraction of minutiae configuration, in both the template and query fingerprint; the matching phase seek for the alignment between the two sets which maximize the number of corresponding minutiae. For the latter method, the ridge features are extracted from the image; those can be extracted more reliably than minutiae, but in general they are of minor discriminatory power. The first two methods (correlation-based and minutiae-based) can be considered as sub cases of the ridges feature-based.

Many different factors may influence the matching process. First of all the position of the finger on the scanner (rotation and translation), may affect the visibility of portions of the fingerprint; also the humidity of the skin can lead to partial images. Nonetheless, the elasticity of the skin combined with the pressure of the finger on the scanner apply non linear transformation to the acquired image. Another source of error is the presence of injuries on the skin surface (voluntary or involuntary) that may lead to temporary or permanent impossibility of correctly acquiring the fingerprint. Moreover, statistics show that for certain population categories (e.g. elderly people) the identification through fingerprint might be inappropriate, and that for 4% of the population, the quality of fingerprint would not suffice for the process [32].

1.3 Biometrics new trends and application

Biometrics has been increasingly adopted in security applications, both in governmental and in the private industry sector. State-of-the-art security systems include at least one biometric trait and this tendency is rising. More and more industries, including e-commerce, cars and cell phones, are embracing the related benefits. The widespread usage of biometric technology advances associated research, increasing the related performances and innovations.

1.3.1 Soft biometrics

The latest addition of soft biometrics (also called *semantic* [33]) can increase the reliability of a biometric system and can provide substantial advantages: soft biometric features reveal biometric information, they can be partly derived from hard biometrics, they do not require enrollment and can be acquired non intrusively without the consent and cooperation of an individual.

Soft biometrics are physical, behavioral or adhered human characteristics classifiable in predefined human compliant categories. These categories are, unlike in the classical biometric case, established and time-proven by humans with the aim of differentiating individuals. In other words the soft biometric trait instances are created in a natural way, used by humans to distinguish their peers.

Traits accepting this definition include but are not limited to: age, gender, weight, height, hair, skin and eye color, ethnicity, facial measurements and shapes, the presence of beard, mustache and glasses, color of clothes, etc. An increase in resources (such as an improved resolution of the sensors, or an increased computational capability) can lead to expanding of the traits amount and furthermore of the trait instances. We refer to trait instances as the sub categories soft biometric traits can be classified into. Example for trait instances of the trait hair color could be: blond, red and black. The nature of soft biometrics features can be binary (for example presence of glasses), continuous (height) or discrete (ethnicity) [34].

Characteristics can be differentiated according to their distinctiveness and permanence, whereby distinctiveness corresponds to the power of a trait to distinguish subjects within a group and permanence relates to the time invariability of a trait. Both of those characteristic are mostly in a lower range for soft biometrics than they are for classical biometrics (c.f. hair color, presence of beard, presence of glasses, etc.). Furthermore it is of interest with which estimation reliability a trait can be extracted from an image or a video. With respect to these three qualities, namely distinctiveness, permanence and estimation reliability, the importance of a soft biometric trait can be determined. We note that the classification of soft biometric traits can be expanded and aspects like accuracy and importance can be evaluated or deduced respectively, depending on the cause for application.

Recently, soft biometric traits have been employed to preliminary narrow down the search in a database, in order to decrease the computational time for the classical biometric trait. A further application approach is the fusion of soft biometric and classical biometric traits to increase the system performance and reliability. Recently soft biometric systems have been employed also for person recognition and continuous user authentication [35].

Jain et al. first introduced the term *soft biometrics* and performed related studies on using soft biometrics [36, 37] for pre-filtering and fusion in combination with classical biometric traits. Recent works perform person recognition [34, 38] and continuous user authentication [35] using soft biometric traits. Further studies evolve traits extraction algorithms concerning eye color [39], weight [40], clothes color [41] or predictability of human metrology [42].

1.3.2 Applications

Applications that make use of biometrics can generally be divided into three main categories: forensic, government, and commercial. They mainly differ for performance requirements. Here we seek to provide some examples that may clarify some of practical uses of biometrics.

1.3.2.1 Forensic applications

The first category is in general devoted to security or control and prevention. This is mainly due to the intrinsic nature of biometric traits that ease the automatic identification task.

Historically the first application of biometrics was theorized and put into practice by Alphonse Bertillon which invented the “Bertillonage”, a system that categorizes and recognizes people according to a biometric signature composed by anthropometric measures. This system was replaced by the more reliable fingerprint recognition system introduced by Francis Galton. The FBI followed assuming responsibility for managing the US national fingerprint collection in 1924 [43], fingerprint matching was performed by human experts. Nowadays the National Crime Information Center (NCIC) contains up to 39 million criminal records, which are stored electronically and can be accessed by 80000 law enforcement agencies for data on wanted persons, missing persons, gang members, as well as other information related to other crimes.

1.3.2.2 Government applications

Many governments started exploring the possibility of using biometrics for identification. Lately the NEXUS program started as joint collaboration of Canada and United States. It is designed to facilitate approved, low-risk travelers to cross the USA-Canada border as fast as possible. The clients of the system (only citizens or permanent residents) can use self check-in gates to speed up the paperwork for crossing the border. The applicant's fingerprints, photographs, and irides are scanned and stored in order to verify his/her identity as needed [44]. A similar project exists between USA and Mexico under the name of Secure Electronic Network for Travelers Rapid Inspection (SENTRI).

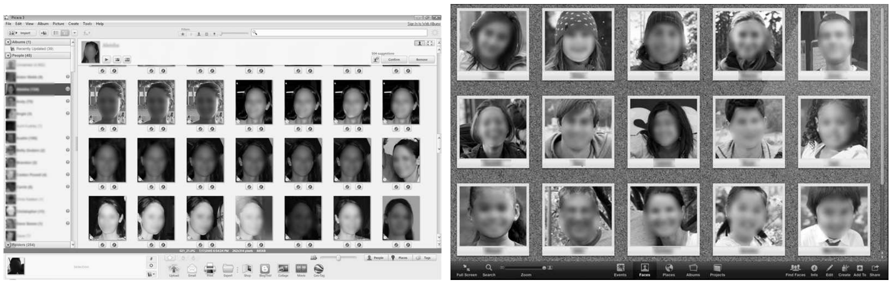
Another promising, though challenging, project is the Multipurpose National Identity Card project, a national Indian project that contemplates the collection of multiple biometric modalities (face appearance, fingerprints, and iris) of a large percentage of the Indian population. According to the specifications of the project [45], the biometric identification profile will be voluntary and for every resident (not only Indians), it will be composed of a random 12 digit number and it will just provide yes/no reply to each authentication query to avoid privacy issues. Many challenges have to be faced, from the acquisition of multiple modalities, to the matching techniques which will involve very large number of queries performed in parallel. In order to promote each citizen to have a biometric profile, the Indian authorities will include the possibility of availing services provided by the government and private sector (e.g. banks, insurances, and benefits).

An additional use of biometrics to guarantee the identification task is the use of biometric traits inside official documents. For example the Biometric Passport (or ePassport) contains a microchip which can store fingerprints scans as well as face appearance, and iris images. Those traits can be read from automatic gates at airports, train stations, or state borders. Nowadays more than 70 countries already adhered to this new identification tool which try to standardize biometric identification across nations.

1.3.2.3 Commercial applications

One of the first commercial systems used for general purposes was the speaker recognition module created for MacOS 9 from Apple [46] which allowed to login and protect files of a user recognized by his/her voice. Lately embedded fingerprint systems have seen an increase in popularity and are present in most laptop and computers, they allow to override the password-typing method for both operating system's login and websites password management. Fingerprint was as well introduced in some portable storing device to be used as keys to decrypt data hidden in the device's memory. VeriSign technology for face recognition was lately added to Lenovo computers which allow now a full face recognition system to login into the operating system.

Additionally to access control, biometric for commercial application has seen important uses in daily applications like the one for photos management. Examples in this sector are iPhoto from Apple and Picasa from Google. Both the systems implement two different (and proprietary) versions of a face recognition module both allowing face tagging over the entire set of pictures so that the virtual albums can be easily indexed by person. Enabling this function the user is able to divide its multimedia collection by persons easing the usability of such systems. A similar technology was lately announced by Facebook to ease the task of tagging friends's pictures. Some airports already exploit biometric technology for identifying passengers. The Stansted Airport of London, in collaboration with Accenture [47], deployed an automatic border control system which makes use of a face recognition module to speed up the security control of passengers. Paris Roissy-Charles de Gaulle Aiport as well provides security and fast lane access through the use of a fingerprint recognition system. Both the systems exploit biometric passport mechanism previously presented, in order to match the live data with the templates stored either in a database or in the microchip that the passports carries.



(a) (b)

FIGURE 1.8
The two interfaces of Google Picasa (a) and Apple iPhoto (b). Both the systems summarize all the persons present in the photo collection. The two programs give the opportunity to look for a particular face among all the others.

1.4 Conclusions

There is no doubt that the exploration of the biometrics domain has reached the top and its commercial exploitation just started blooming. Standards are set and regularly improved so that more commercial applications are created by a number of company which operate in this domain (e.g. L1, Safran-Morpho, Thales, and so on). Commercial applications makes this technology available to a number of people always bigger, insomuch as one of the modern biometric challenges is represented by large-scale systems. UIDAI Indian project is one of these, it targets 1.2 billion users, the entire Indian population [45]. Such tremendous increase of system's users yield numerous challenges. As the scale of such systems grows, problems in both speed and accuracy of employed algorithms have to be carefully addressed.

As for many new technologies an ensemble of concerns about privacy and security is arising also for biometrics. In this direction, several aspects we briefly presented in this chapter are currently discussed. One of the aims is establishing quantitative measures of systems security, as well as increasing robustness against spoofing attacks, and guaranteeing privacy for the users of the biometric system.

Security is the main domain of application for biometry but many other applications are finding the discriminative power of the biometric traits useful. Instant login systems exist for personal computers and banking systems which utilize face or fingerprint recognition. The multimedia explosion driven by social-networks like Facebook or Flickr is empowered by automatic indexing of pictures by automatic face recognition systems.

Furthermore, research boundaries are expanding: shape of ears, stride and gait analysis, soft biometrics, and even *physiological* biometrics (e.g. brain and heart activities) are new experimented traits. This new variety of biometrics creates the ground for new algorithms, theories, and applications. Research still continues and many unsolved challenges exist in this domain. Addressing all these questions will definitely establish biometrics as leading technology for human identification in the next years.

Bibliography

[1] C. A. Nelson. The development and neural bases of face recognition. *Infant and Child Development*, 10(1–2):3–18, 2001.

[2] A. J. O'Toole, D. A. Roark, and H. Abdi. Recognizing moving faces: A psychological and neural synthesis. *Trends in Cognitive Sciences*, 6(6):261–266, 2002.

[3] US NSTC . National Science and Technology Council. Biometrics in government post 9/11. 2008.

[4] Timo Ahonen, Abdenour Hadid, and Matti Pietikäinen. Face recognition with local binary patterns. In Tomás Pajdla and Jirí Matas, editors, *Computer Vision - ECCV 2004*, pages 469–481. Springer Berlin / Heidelberg, 2004.

[5] M. Bicego, A. Lagorio, E. Grosso, and M. Tistarelli. On the use of sift features for face authentication. In *Computer Vision and Pattern Recognition Workshop, 2006. CVPRW '06. Conference on*, 2006.

[6] Di Liu, Dong mei Sun, and Zheng ding Qiu. Bag-of-words vector quantization based face identification. In *Electronic Commerce and Security, 2009. ISECS '09. Second International Symposium on*, volume 2, pages 29–33, May 2009.

[7] R. Cappelli, D. Maio, D. Maltoni, and A. Erol. Synthetic fingerprint-image generation. In *icpr*. Published by the IEEE Computer Society, 2000.

[8] Patrick Grother, Ross Micheals, and P. Phillips. Face recognition vendor test 2002 performance metrics. In Josef Kittler and Mark Nixon, editors, *Audio- and Video-Based Biometric Person Authentication*, volume 2688, chapter Lecture Notes in Computer Science, pages 1057–1057. Springer Berlin / Heidelberg, 2003.

[9] M. Pagani. *Encyclopedia of multimedia technology and networking*. Cybertech Publishing, 2005.

[10] T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino. Impact of artificial gummy fingers on fingerprint systems. In *Proceedings of SPIE*, volume 4677, pages 275–289. Citeseer, 2002.

[11] T. Matsumoto. Artificial Fingers and Irises: importance of Vulnerability Analysis. In *7th International Biometrics 2004 Conference and Exhibition, London, UK*, 2004.

[12] B. Toth. Biometric liveness detection. *Information Security Bulletin*, 10(8), 2005.

[13] Tabularasa EU project. http://http://www.tabularasa-euproject.org/.

[14] Florent Perronnin. *A probabilistic model of face mapping applied to person recognition*. PhD thesis, Thesis, 11 2004.

[15] W. Zhao, R. Chellappa, P. J. Phillips, and A. Rosenfeld. Face recognition: A literature survey. *ACM Comput. Surv.*, 35(4):399–458, December 2003.

[16] M. Kirby and L. Sirovich. Application of the karhunen-loeve procedure for the characterization of human faces. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 12(1):103–108, Jan 1990.

[17] M. A. Turk and A. P. Pentland. Face recognition using eigenfaces. In *Computer Vision and Pattern Recognition, 1991. Proceedings CVPR '91., IEEE Computer Society Conference on*, pages 586–591, jun 1991.

[18] J. R. Beveridge, K. She, B. A. Draper, and G. H. Givens. A nonparametric statistical comparison of principal component and linear discriminant subspaces for face recognition. In *Computer Vision and Pattern Recognition, 2001. CVPR 2001. Proceedings of the 2001 IEEE Computer Society Conference on*, volume 1, 2001.

[19] Timo Ojala, Matti Pietikäinen, and David Harwood. A comparative study of texture measures with classification based on featured distributions. *Pattern Recognition*, 29(1):51–59, 1996.

[20] Xiaoyu Wang, Tony X. Han, and Shuicheng Yan. An hog-lbp human detector with partial occlusion handling. In *Computer Vision, 2009 IEEE 12th International Conference on*, pages 32–39, 292009-oct.2 2009.

[21] T. Ojala, M. Pietikainen, and T. Maenpaa. Multiresolution gray-scale and rotation invariant texture classification with local binary patterns. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 24(7):971–987, jul 2002.

[22] P. Jonathon Phillips, Patrick Grother, Ross J. Micheals, Duane M. Blackburn, Elham Tabassi, Mike Bone, North Fairfax Dr, and United Kingdom. Facial recognition vendor test 2002: evaluation report, 2003.

[23] J. Wright, A. Y. Yang, A. Ganesh, S. S. Sastry, and Yi Ma. Robust face recognition via sparse representation. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 31(2):210–227, feb. 2009.

[24] F. Matta and J. Dugelay. A behavioural approach to person recognition. In *2006 IEEE International Conference on Multimedia and Expo*, pages 1461–1464. IEEE, 2006.

[25] Marco Paleari, Carmelo Velardo, Benoit Huet, and Jean-Luc Dugelay. Face dynamics for biometric people recognition. In *MMSP'09, IEEE International Workshop on Multimedia Signal Processing, October 5–7, 2009*, 10 2009.

[26] Andrea F. Abate, Michele Nappi, Daniel Riccio, and Gabriele Sabatino. 2d and 3d face recognition: A survey. *Pattern Recogn. Lett.*, 28(14):1885–1906, October 2007.

[27] J. G. Daugman. High confidence visual recognition of persons by a test of statistical independence. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 15(11):1148–1161, 2002.

[28] A. L. Yuille, P. W. Hallinan, and D. S. Cohen. Feature extraction from faces using deformable templates. *International journal of computer vision*, 8(2):99–111, 1992.

[29] J. Daugman. New methods in iris recognition. *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, 37(5):1167–1175, 2007.

[30] Z. Wei, T. Tan, and Z. Sun. Nonlinear iris deformation correction based on gaussian model. *Advances in Biometrics*, pages 780–789, 2007.

[31] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar. *Handbook of fingerprint recognition.* Springer-Verlag New York Inc, 2009.

[32] A. K. Jain, S. Prabhakar, and S. Pankanti. A filterbank-based representation for classification and matching of fingerprints. In *Neural Networks, 1999. IJCNN '99. International Joint Conference on*, volume 5, pages 3284–3285, 1999.

[33] S. Samangooei, M. Nixon, and B. Guo. The use of semantic human description as a soft biometric. In *Proceedings of BTAS*, 2008.

[34] A. Dantcheva, C. Velardo, A. D'angelo, and J. L. Dugelay. Bag of soft biometrics for person identification: new trends and challenges. *Multimedia Tools and Applications*, 2, 2011.

[35] K. Niinuma, U. Park, and A. K. Jain. Soft biometric traits for continuous user authentication. *Transactions on information forensics and security*, 5(4), December 2010.

[36] A. K. Jain, S. C. Dass, and K. Nandakumar. Soft biometric traits for personal recognition systems. In *Proceedings of ICBA*, pages 1–40. Springer, 2004.

[37] A. K. Jain, S. C. Dass, and K. Nandakumar. Can soft biometric traits assist user recognition? In *Proceedings of SPIE*, volume 5404, pages 561–572, 2004.

[38] A. Dantcheva, J. L. Dugelay, and P. Elia. Person recognition using a bag of facial soft biometrics (bofsb). In *Proceedings of MMSP*, 2010.

[39] C. Boyce, A. Ross, M. Monaco, L. Hornak, and X. Li. Multispectral iris analysis: a preliminary study. In *Proceedings of CVPRW*, 2006.

[40] C. Velardo and J. L. Dugelay. Weight estimation from visual body appearance. In *Proceedings of BTAS*, 2010.

[41] A. D'Angelo and J. L. Dugelay. People re-identification in camera networks based on probabilistic color histrograms. In *Proceedings of Electronic Imaging*, 2011.

[42] D. Adjeroh, D. Cao, M. Piccirilli, and A. Ross. Predictability and correlation in human metrology. In *Proceedings of WIFS*, 2010.

[43] Federal Bureau of Investigation. `http://www.fbi.gov/about-us/cjis/fingerprints_biometrics`.

[44] NEXUS. `http://www.cbp.gov/xp/cgov/travel/trusted_traveler/nexus_prog/nexus.xml`.

[45] UIDAI. `http://uidai.gov.in/`.

[46] D. Pogue. *Mac OS X: the missing manual.* O'Reilly & Associates, Inc. Sebastopol, CA, USA, 2002.

[47] Accenture. http://www.accenture.com/us-en/pages/success-london-stansted-automated-border-clearance-trial-summary.aspx.