Available at
www.ComputerScienceWeb.com
POWERED BY SCIENCE @ DIRECT•

ELSEVIER

Signal Processing 83 (2003) 2539–2557

SIGNAL PROCESSING

www.elsevier.com/locate/sigpro

Biometric identification systems

Rodrigo de Luis-García[a] , Carlos Alberola-López[a,*], Otman Aghzout[b], Juan Ruiz-Alzola[b,c]

[a] *ETSI Telecomunicación, University of Valladolid, Valladolid, Spain*
[b] *Dep. Señales y Comunicaciones, University of Las Palmas GC, Spain*
[c] *Dep. Radiology – SPL, Harvard Medical School, Boston, USA*

Received 16 June 2003; received in revised form 4 July 2003

Abstract

In this paper, we provide an overview of the fundamentals of biometric identification, together with a description of the main biometric technologies currently in use, all of them within a common reference framework. A comparison on different qualitative parameters of these technologies is also given, so that the reader may have a clear perspective of advantages and disadvantages of each. A section on multibiometrics describes the state of the art in making these systems work coordinately. Fusion at different conceptual levels is described. Finally, a section on commercial issues provides the reader a perspective of the main companies currently involved in this field.

Keywords: Biometrics; Iris recognition; Fingerprint recognition; Face recognition; Multibiometrics

1. Introduction

Buying with a credit card, accessing restricted areas or resources, traveling abroad... are just some examples where it is necessary to verify whether we really are who we claim. Identifying ourselves is indeed a very common procedure in modern society. Traditionally, identification strategies are based on something we know, e.g., a password or a personal identification number (PIN), or something we own, e.g., a card, a token, or a key [46]. Unfortunately, passwords can be forgotten or guessed by an intruder, cards can be stolen or lost... . In fact, traditional identification systems are inherently insecure, specially in a global economy where the need for reliable shared virtual spaces increases constantly.

Biometrics is the science of identifying people using physiological features [59]. Biometric identification systems (BISs), i.e., identification based on biometric features, are expected to provide in the near future secure access to physical and virtual resources and spaces since, unlike traditional identification, they are based on what we are (our individual traits). Virtually any physiological feature could be used for identification; however, the most generalized biometric techniques include the automated recognition of fingerprints, faces, iris, retina, hand geometry, voice and signature [50,44,27,59,60,32].

The heightened awareness of security issues (specially since the terrorist events of September 2001) has led to a massive rise in the interest for biometric

[*] Corresponding author.
E-mail addresses: rluigar@neptuno.lpi.tel.uva.es (R. de Luis-García), caralb@yllera.tel.uva.es (C. Alberola-López), otman@ctm.ulpgc.es (O. Idrissi), jruiz@dsc.ulpgc.es (J. Ruiz-Alzola).

0165-1684/$ - see front matter © 2003 Elsevier B.V. All rights reserved.
doi:10.1016/j.sigpro.2003.08.001

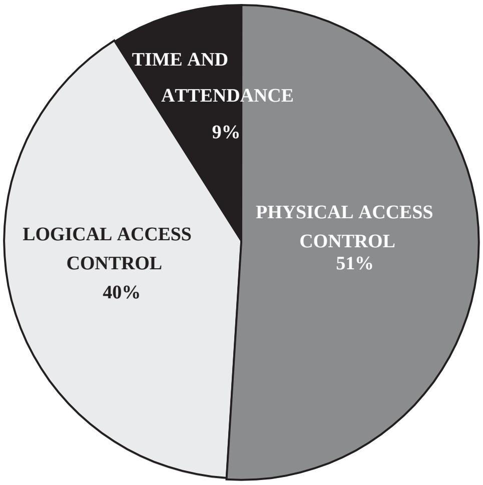

Fig. 1. 2001 biometric market share by category.

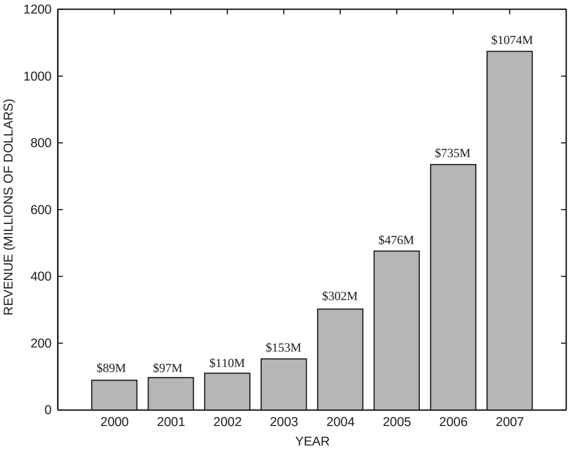

Fig. 2. Total biometrics revenue market: 2000–2007.

technology from a variety of market sectors, including government agencies and corporations pursuing greater accountability of their staff and higher security for their facilities. Fig. 1 shows the distribution of the "Big Three" traditional markets for biometrics—physical access control, logical access control and time and attendance—as it was in 2001 [49]. Industry predictions indicate that the total biometrics market will continue to grow, reaching by 2007 $1074 million revenues [3] (see Fig. 2). With regard to the different biometric technologies in use, fingerprint continues to be

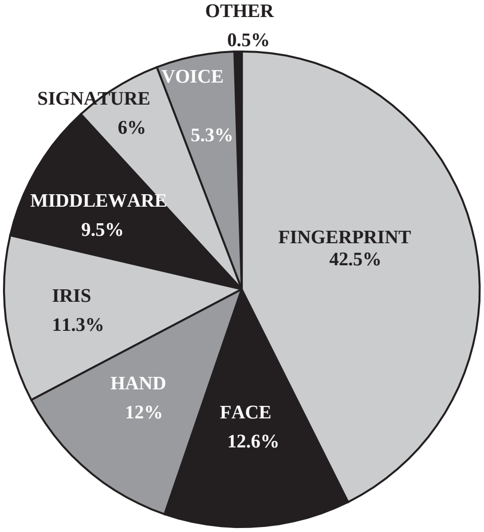

Fig. 3. Biometric market share by technology in 2002.

the leading technology in terms of market share (see Fig. 3 [4]). However, as we will show in the paper, some other biometric techniques have higher discriminative power, so, there might be changes in the early future in this trend.

A BIS can be considered as an automatic pattern recognition system that establishes the authenticity of a specific physiological or behavioral characteristic possessed by an user [50,73]. In a first enrollment stage (system training) the system captures individual physiognomies, which are digitally represented by means of feature vector templates or prototypes. Most often the enrollment stage spans the whole lifetime of the system, as new users can be expected. Afterwards individual users access the BIS, which captures their biometric characteristic, creates the digital representation and compares it with the templates stored in a database to make a decision on the identity of the user.

BISs can operate in two different ways: verification (or authentication) and identification itself. In verification mode, the user claims to be someone, and the system simply accepts or rejects this claim after comparing the biometric feature to the ones stored in the database. In identification mode, the user just accesses the BIS, which extracts biometric features and compares with the ones in the database to decide who the person is among all the enrolled users. Obviously, identification is much more demanding than

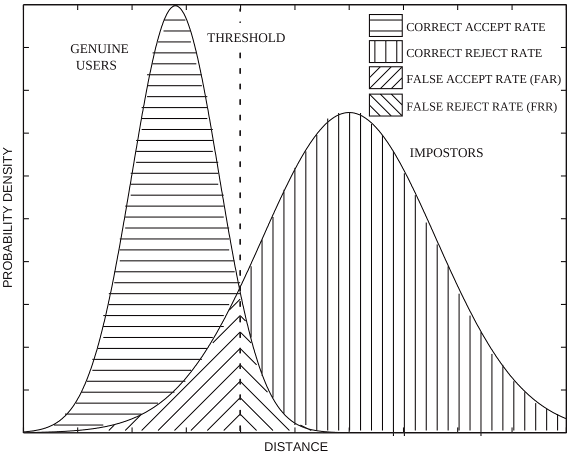

Fig. 4. Decision landscape for biometric systems.

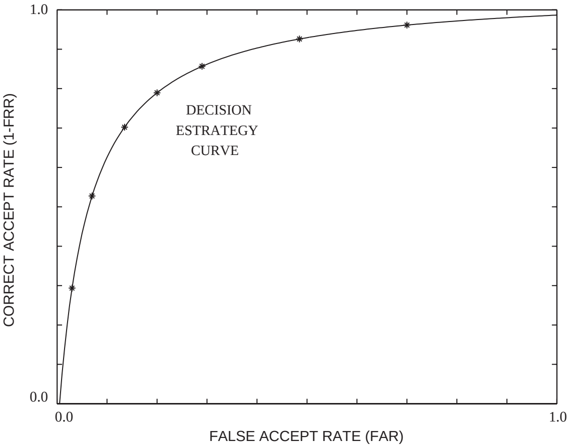

Fig. 5. ROC curve for a biometric system.

verification, firstly because a greater number of comparisons has to be performed and secondly because the overall error probability increases as the number of comparisons grows [18].

Conventional techniques from pattern classification can be adopted for BISs. Consider P' to be the template corresponding to an enrolled user and P the feature vector extracted from an user accessing the system. A simple hypothesis test let analyze the two possible situations [7]:

$H_0 : P = P'$, the user is genuine,

$H_1 : P \neq P'$, the user is an impostor.

The false accept rate (FAR) is the probability of accepting the null hypothesis when an impostor is on the system. The false reject rate (FRR) is the probability of accepting the alternate hypothesis when a genuine user is on the system. Its complementary to one is the correct accept rate (CAR), i.e., accepting the null hypothesis when a genuine user is on the system. Fig. 4 shows that both parameters are closely related, as it is well known from conventional detection theory. For a particular BIS, the receiver operating characteristic curve (ROC) describes the tradeoffs that can be achieved between CAR and FAR (an example of an ROC curve is shown in Fig. 5).

In this paper, we provide the reader with a sightseeing tour of BISs and their potential applications. We will follow a top–bottom approach, starting with a study of the requirements that BIS are expected to meet in order to be used in real applications. We will then review the main biometric technologies as of today, as well as their combined use (multi-biometrics). We also provide links to manufacturers and interest groups as well as an extensive list of references.

2. BISs requirements

The acceptance of a BIS depends on one hand on its operational, technical, and manufacturing characteristics and, on the other, on the final application and its financial possibilities. In this section, we provide a set of criteria that allow to characterize different BISs and how they fit a specific application domain:

- Reliability—Presenting a correct password in a password-based authentication system always results in the acceptance of the correct one and in the rejection of any other. Nevertheless correct authentication cannot be guaranteed by a BIS. This could be because of sensor noise, limitations of the processing methods, and, more importantly, the variability in both the biometric feature as well as its presentation. Furthermore, the accuracy of a given biometric implementation is sensitive to the target population. To apply a biometric technology to a personal identification application successfully, it is important to understand and evaluate the technology in the context of the target application and the target population [72]. Reliability issues are specially critical for large-scale biometric systems, where an otherwise excellent accuracy may become clearly insufficient.

- Ease of use—There is a practical tradeoff between the complexity of use and the security level to be assured. In order for a BIS system to become practical the difficulty of using and learning how to use (training) the system must explicitly be addressed in the context of the target application and potential users (see user acceptance below). Note that even in the unlikely case that users are willing to accept a difficult system it might not be acceptable for the particular application.
- User acceptance—This will be mainly determined by the BIS obtrusiveness and intrusiveness, which are subjective to the user. Most usually users will not accept cumbersome systems, and they will consider as such any one that is difficult to be used. However, for high security applications, a BIS being complicated to use (and even cumbersome) may not be an obstacle, and even might be welcome as it provides a feeling of higher security. The former is closely connected to the *ease of use* characteristic of the system since any system that is cumbersome to be used will be avoided by most users. Intrusiveness is related to privacy concerns. Despite its obvious strengths, there are a few negative preconceptions about biometrics [66] that often result in the following question: Will biometrics data be used to track people, secretly violating their right to privacy? Biometric technology can prevent this from happening, at least as much as any other identification technique. Most biometric technologies work as a one-direction road as can be seen in the following example: Let us suppose the case of iris identification. When an iris image is captured, features are extracted from it to create a feature vector, which is compared with the corresponding feature vector stored in the database. It is possible to obtain that feature vector from the raw image, but it is *impossible* (but for random coincidences) to recreate an iris image from the feature vector. Thus, it is not the iris' image what is used for identification purposes, but a numerical code extracted from it. Besides, encryption techniques may (and indeed must) be used for the transmission of biometric data, so that it is not possible to capture the "biometric code". Such a privacy protection is by far much more advanced and restrictive than what traditional identification techniques (cards, token, passwords, etc.) can offer.
- Ease of implementation—To foster improvements and encourage widespread deployment, biometric technology needs to be made easily accessible for system integration and implementation. Harnessing and integrating biometric technology is not easy in its present form; one of the reasons is the lack of industry-wide standards [71]. As the pressure to deliver inexpensive authentication services mounts, and as geographically mobile individuals increasingly need to establish their identity as strangers in remote communities, the problem of reliable personal identification becomes more and more difficult. To catapult biometric technology into the mainstream identification market, it is important to encourage its evaluation in realistic contexts, to facilitate its integration into end-to-end solutions, and to encourage innovation and development of inexpensive and user-friendly implementations.
- Cost—Eventhough BISs have developed into very cost effective business solutions, there are a number of issues to consider when estimating the total cost to deploy such a system. These issues might involve equipment, installation and training costs. Software and system maintenance and operation costs should also be added to the tab. Given the increasing availability of inexpensive processing power and mass-scale production of inexpensive sensors, it will become possible to make biometrics accessible to new personal identification application in the near future.

In Table 1, we show the more common biometric technologies and their performance in terms of these practical issues, classified in broad terms.

3. A general BIS model

A general description of a BIS is necessary for better understanding biometric identification technologies, and for comparing apparently disparate systems. Although many generalized models can be proposed [32,60,50,31], a truly general model is desirable, rather than making taxonomies or dividing systems into different stages. Such a model has been proposed by

Table 1
Characteristics of the most important biometric technologies

Biometric type	Accuracy	Ease of use	User acceptance	Ease of implementation	Cost
Fingerprint	High	Medium	Low	High	Medium
Hand geometry	Medium	High	Medium	Medium	High
Voice	Medium	High	High	High	Low
Retina	High	Low	Low	Low	Medium
Iris	Medium	Medium	Medium	Medium	High
Signature	Medium	Medium	High	Low	Medium
Face	Low	High	High	Medium	Low

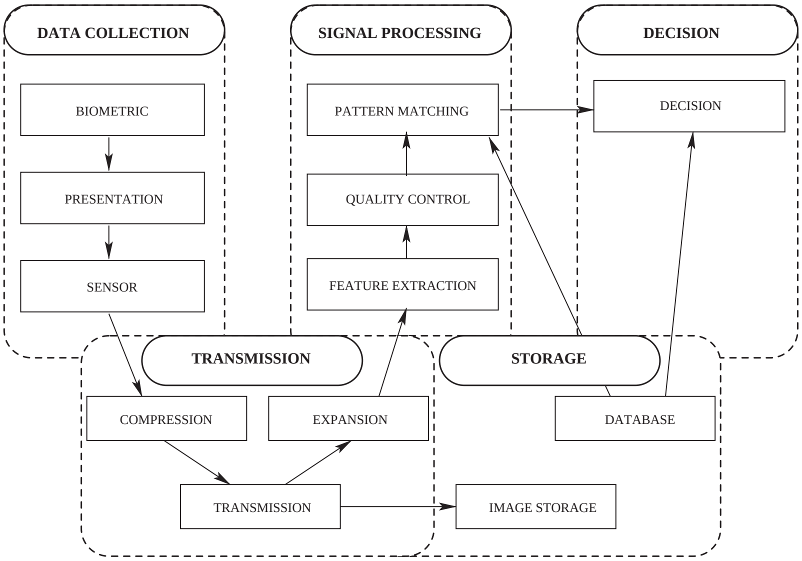

Fig. 6. Generalized model for a biometric system.

James L. Wayman, showing a system diagram with five different subsystems which can be considered independent at first sight [70] (see Fig. 6). A detailed explanation of each subsystem follows:

- The data collection subsystem. This subsystem is responsible for capturing the biometric feature to be analyzed. The biometric characteristic must be discriminant and stable over time. For data collection, the biometric feature is presented to the sensor. Most often, a predetermined presentation is expected (for example, placing the fingertip over the sensor with moderate pressure). The degree of cooperation required from the user, and the environment at which data collection will take place, must be taken into account when designing a BIS in order to introduce as least variation as possible in the data collection step [74].
- The transmission subsystem. In many cases, biometric data collection and processing are held at different locations. Therefore, some kind of transmission is required. Furthermore, data compression may be required to minimize transmission bandwidth. We can think of several different scenarios concerning data transmission:
    - ○ Data are collected at a certain location, and transmitted to another where processing will be held (feature extraction, storage, decision, etc.). Compression standards exist for fingerprints, facial imaging, speech, etc. [70].

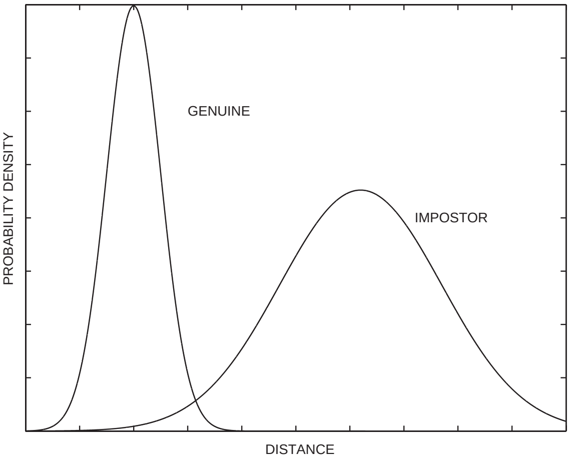

Fig. 7. Genuine and impostor distance distribution.

- ○ Data collection and feature extraction are performed at a certain location, and storage and decision are carried out at another. In this case, data compression is unlike to be needed.
- The signal processing subsystem. This subsystem converts the original data (or maybe the degraded data after compression and expansion) into a feature vector, trying to preserve all the discriminant information which could be used to distinguish two different individuals, and removing all redundant information. The objective of feature extraction is to create a compact representation of the biometric information suitable for the pattern matching module, which compares the extracted feature vector to some number of stored feature vectors, one by one, resulting in a numerical measure that quantifies the degree of similarity between the compared patterns. As we can see in Fig. 7, distance distributions of genuine and impostor users are analyzed yielding a decision criterion.

  Feature extraction and pattern matching is the core of all biometric technologies, and these processes are designed to achieve as much separability as possible between genuine and impostor distance distributions, thus allowing lower error rates.
- The storage subsystem, containing the templates corresponding to every user enrolled in the system. This database may be centralized or somehow distributed.
- The decision subsystem. The numerical values obtained from the comparison of the feature vector with stored templates are the inputs to this subsystem, which must apply some strategy to decide whether the user is enrolled in the database. The decision process can be as simple as comparing the distance with a threshold (the value of which is calculated to satisfy some sort of objective criterion). Actions derived from a match or nonmatch will depend on the purpose of the identification system, and may vary from granting access to restricted areas or resources in the case of a match, to repeating the whole process in the case of a nonmatch.

An important element for the adoption of biometric technologies is to establish the performance of individual biometric modalities and overall systems in a credible, objective and standard way [54,63,34]. In particular, the following issues should be considered:

- What should the evaluation and testing methodology be? It is necessary, for performance assessments to be reliable, that a testing protocol is carefully planned and conducted. It is essential that BISs are tested on biometric signatures not previously seen by the system (otherwise the system would only prove its ability to tune to a particular data set).

  In general, for an evaluation to be accepted by the biometric community, the details of the evaluation procedure must be known, as well as the evaluation protocol, performance results, and representative examples of the data set [54]. This way, information about testing should allow anyone to repeat the evaluation. It is also important that the evaluation itself is not too easy or too hard, so that the results are useful for comparison and evaluation of a system abilities or weaknesses.

  For most important biometric technologies, there are public open competitions which are probably the best biometric technology evaluations. In these competitions, several biometric identification systems are tested and compared using a common data set and a well-defined testing procedure. A good example of these competitions is the face recognition technology (FERET) evaluation. These tests, which first took place in August 1994, make use of the FERET database (whose collection began in

1993 and has been growing ever since) a fixed testing procedure, and have become a de facto standard for comparison between different technologies for face recognition from still images [52]. Other relevant competitions include the National Institute of Standards and Technology (NIST) speaker recognition evaluations, or the fingerprint verification competition (FVC) [45].

- What is the influence of the data set used for testing the system? Open competitions use a common database, as it is the case of the FERET evaluation which makes use of the FERET database. This way, comparison between different systems is straightforward, as their abilities are measured identically. However, one cannot dictate researchers and vendors to use a single database, and different data sets will lead to different results. So, how can we compare different systems if they have been tested on different data sets? Measures to characterize a testing data set may help [7], in order to give a measure of its *difficulty*.
- For large-scale systems, how can the accuracy be predicted? Let us suppose a BIS whose accuracy requirements are really high, for example, a FAR rate lower than 10^{-9}. Let us suppose also that we design and implement a system and want to test it to find out if it is accurate enough. Then, for the results to be statistically consistent, let us say that the system must be tested until at least 100 errors occur. In this case, we need 10^{11} comparisons between the biometric representations of different people. It is obviously very difficult to collect sufficient data for that huge number of comparisons. Then, if we cannot use experimentation for assessing the accuracy of the system, prediction has to be applied. Taken a sufficient number of comparisons, the impostors and genuine users distributions can be estimated, and then error rates can be predicted for a given threshold. This method is used for predicting the accuracy of an iris recognition system, as can be seen in [17].

4. Biometric technologies

4.1. Iris identification

Human iris is an extremely valuable source of biometric information, as it is a very complex structure unique to an individual [1]. The visual appearance of the iris is a result of its layered structure [75], being the general structure genetically determined. However, the particular details are critically dependent on circumstances as the initial conditions in the embryonic precursor to the iris. Thus, two different iris are extremely unlike to be equal, even in the case of genetically identical twins, or clones [20]. Several iris recognition systems have been developed, which exploit the complexity and stability over time of iris patterns and claim to be highly accurate [17,75,48].

Data collection is critical an iris recognition system, since it is not easy to obtain a valid image of such a small region with limited user cooperation. If the user will only be asked to stand in front of the system, artificial vision techniques such as the use of stereo cameras may be used to first locate the position of the eye and then capture an image of the region of interest by means of a CCD camera [48]. The complexity of the acquisition can be reduced if the user is asked to place his eye in front of the camera. In this case, some feedback will be needed to help the user to position appropriately [75,17].

Preprocessing follows data collection in order to locate the region of the image corresponding to the iris. In the image, the iris forms a ring, outside the pupil and inside the sclera. In some cases, the iris might be partially occluded by the eyelids and eyelashes. Thus, determining the iris contours is not a trivial task, and several approaches have been applied. The most robust ones consist of operators acting as edge detectors applied along predetermined paths (i.e., circles for the inner and outer boundaries and arcs for the eyelids) based on contour integrals [19] or Hough transforms [75]. Fig. 8 shows an image of the region of interest with the located iris.

The preprocessing also includes a registration step in order to translate the portion of the image corresponding to the iris into a normalized form.

Once preprocessing has been carried out feature extraction can be performed, aiming to represent all the valuable and discriminant information present in the image in a compact form suitable for further comparison using a similarity metric. The uniqueness of each iris is based on details present at different scales. Thus, it is desirable to perform an analysis capable of including information at different levels of detail.

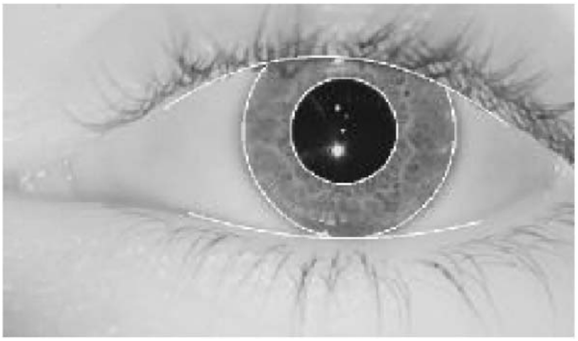

Fig. 8. Human iris located from the region of interest image.

The system proposed by J. Daugman [17] has gained a certain commercial relevance and, due to its technical interest, will be described here so as to provide a comparison reference with other systems. Preprocessing consists of the application of pseudo-polar coordinates (taking into account that the inner and outer circular boundaries may not be completely concentric) and standardizing the radial size of the iris (so that possible dilation of the pupil does not affect the system) [19]. As for feature extraction, 2D Gabor wavelets [26] are used to perform a multiscale analysis of the iris [17,16,15]. A set of quadrature pair frequency-selective filters are used to analyze regions of the image at different scales. These filters obtain information about local phase, which is coded with two bits attending to the sign of the real and imaginary parts:

$$h_{\{\mathrm{Re},\mathrm{Im}\}} = \mathrm{sgn}_{\{\mathrm{Re},\mathrm{Im}\}} \int_\rho \int_\phi I(\rho,\phi) \times \varphi(\rho,\phi,\rho_0,\theta_0,\omega,\alpha,\beta)\,\mathrm{d}\rho\,\mathrm{d}\phi, \tag{1}$$

where $h_{\{\mathrm{Re},\mathrm{Im}\}}$ is the pair of bits whose value depend on the 2D integral; $I(\rho,\phi)$ is the iris image in the pseudo-polar coordinate system (which is size- and translation-invariant); φ is the Gabor wavelet; α and β are the multiscale 2D wavelet parameters; ω is wavelet frequency; and (ρ_0,θ_0) represent the polar coordinates for which the phasor signs $h_{\{\mathrm{Re},\mathrm{Im}\}}$ are computed. In this way, 2048 phase bits are obtained to form a 256-byte code, which represents each iris and is called IrisCode. The similarity metric is based on a test of statistical independence, which is implemented by applying an XOR (exclusive OR) operator between the 256-byte code obtained and the stored template. The norm ($\|\ \|$) of the resultant bit vector is then normalized in order to compute a hamming distance (HD) where 0 would represent a perfect match. The bit vectors are masked to avoid artifacts at some regions of the iris from affecting the iris comparisons. The proposed HD turns out to be

$$\mathrm{HD} = \frac{\|(\mathrm{code}\,A \otimes \mathrm{code}\,B) \cap \mathrm{mask}\,A \cap \mathrm{mask}\,B\|}{\|\mathrm{mask}\,A \cap \mathrm{mask}\,B\|}. \tag{2}$$

Using this similarity metric a low HD value is expected when two images of the same iris are compared. When two different irises are compared, the similarity will be approximately HD=0.5, because any given bit in the IrisCode is equally likely to be 1 or 0, and different irises will be uncorrelated. This comparison method also presents the advantage of being extremely fast to compute, which is an important feature when many comparisons need to be performed. The threshold is set so as to obtain FAR = FRR. Genuine users' and imposters' distributions are approximated experimentally by binomial distributions [17,18]. The achieved FAR = FRR turns out to be 1 out 1.2 million.

The other iris identification systems found in the literature are based on similar strategies. We will discuss them briefly:

- Wildes proposed a system which is also based on a multiscale analysis [75]. After locating the iris using a procedure somehow more elaborated and robust than Daugman's, feature extraction is based on an isotropic bandpass decomposition derived from the application of Laplacian of Gaussian filters to the image data. Matching the obtained and the stored iris representations is based on normalized correlation (NC) between both representations. Let $p_1[i,j]$ and $p_2[i,j]$ be the two image arrays of size $n \times m$, and let μ_1, μ_2 and σ_1, σ_2 be their means and standard deviations, respectively. Then, the normalized correlation between p_1 and p_2 can be defined as

$$\mathrm{NC} = \frac{\sum_{i=1}^{n} \sum_{j=1}^{m} (p_1[i,j]-\mu_1)(p_2[i,j]-\mu_2)}{nm\sigma_1\sigma_2}. \tag{3}$$

The Laplacian pyramid representations instantiate four spatial frequency bands, so four scores are obtained, each accounting for the goodness of match at each frequency band. Finally, it is necessary to combine these four opinions into a single final decision. In an opinion fusion scenario, Wildes chooses to use a Fisher's linear discriminant, applying a threshold afterwards [75]. Note that combining the four scores is a problem closely related to those discussed in Section 4.5.

- The system proposed by Boles and Boashash [6] employs a different approach. To represent the discriminant information present in the iris, concentric circles are drawn (after normalization of the iris diameter) and one-dimensional signals are obtained from the corresponding section. These circular sections are then analyzed using a dyadic wavelet transform from which a zero-crossing representation is generated next. Finally, the matching algorithm is based on two different similarity functions that compare the zero-crossing representations.
- In their system, Lim et al. locate the iris region and map it into a rectangular image of fixed size [43]. Feature extraction is performed using Haar wavelets, which are applied four times in order to obtain several sub-images. The feature vector is composed of 84 features from the sub-image of the high-pass filter of the fourth transform and each average value from the three remaining high-pass filter sub-images. In this way, the dimension of the resulting vector is 87, each value is quantized into a binary value so that the iris image is finally represented by 87 bits. Matching and decision stages are performed using a LVQ neural network which, after a training phase, compares two representations and decides whether they correspond to the same or different irises.
- Other methods proposed for iris identification include the analysis of iris patterns and colors [23] or the use of other types of 2D wavelet transforms [77] after a normalization step very similar to that reported in [43].

As we have shown above, a number of algorithms have been developed for iris identification. Because of the multiscale nature of the relevant information present in an iris image, all of them apply multiscale feature extraction methods. Approaches for matching and decision making are heterogeneous but all of them deliver excellent results. However, the major drawback concerning iris recognition is the difficulty of acquiring an acceptable iris image with no need of a cumbersome user cooperation. This problem prevents iris recognition from gaining much more relevance in widespread commercial applications, despite its high accuracy.

4.2. *Fingerprint identification*

Fingerprint identification is probably the best-known biometric technique, because of its widespread application in forensic sciences and law enforcement scenarios. It was in 1893 when the Home Ministry Office, UK, first accepted that no two individuals have the same fingerprints [35]. Since then, the suitability of fingerprints as a biometric source capable for identifying people has been thoroughly studied and proved [51] even in the case of genetically identical twins [38].

Fingerprints have a pattern composed of ridges and valleys that is unique to each individual (even more, it is unique to each finger), and keeps stable along the entire life. For fingerprint identification, data acquisition is carried out by placing the finger over a scanning device. The most popular technology to obtain a live-scan fingerprint (the fingerprint image could also be captured from the impression of an inked finger on a paper, but it is not feasible in the context of an automatic identity authentication system) is based on optical frustrated total internal reflection (FTIR) concept [30]. Other live-scan imaging methods are based on ultrasound total internal reflection, sensing of differential capacitance, noncontact 3D scanning, etc. A scanned fingerprint image can be seen in Fig. 9.

The signal processing block of a fingerprint identification system aims, as in the general model for a BIS stated in Section 3, to convert the acquired biometric information into a compact representation that highlights the uniqueness of each pattern, being at the same time invariant to other changes that are not of interest. So the question is: Which representation can capture the invariant and discriminatory information on a fingerprint image? Most fingerprint identification systems rely on the hypothesis that the uniqueness of

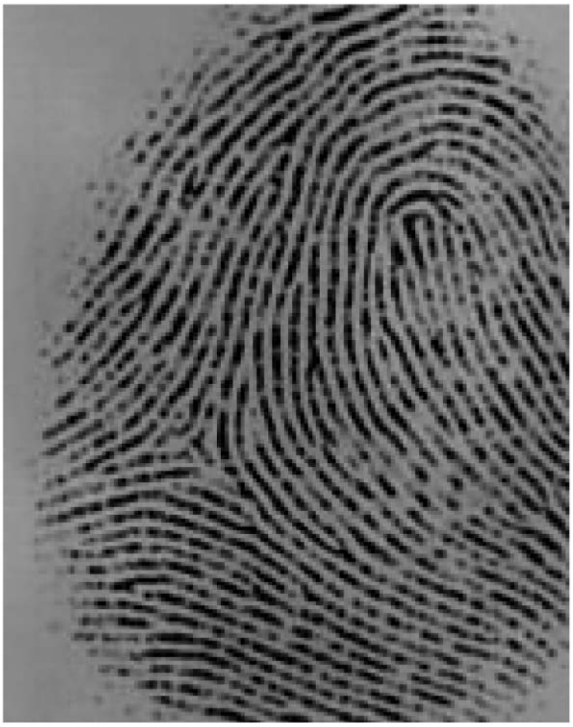

Fig. 9. A typical fingerprint image used for identification.

fingerprints is captured by the local ridge structures and their spatial distributions. Although about one hundred and fifty different types of local ridge structures have been identified [42], typically the two most prominent structures are used: ridge endings and ridge bifurcations. These two structures are background–foreground duals of each other and pressure variations could convert one type of structure into the other, so most schemes do not distinguish between them, calling them collectively minutiae [33]. Fig. 10 shows examples of ridge endings and ridge bifurcations.

Because, as stated before, most fingerprint identification systems represent the uniqueness of a fingerprint by means of its minutiae pattern, we will now describe the system proposed by Jain [33], because it is a complete and well documented system which is very suitable for explanation and further comparison with other systems proposed in the literature. Starting from the fingerprint image this system first determines the positions of the minutiae, which is not a trivial task at all. A method was developed consisting of several steps that we will now describe briefly:

(1) First, an orientation field is estimated. This field represents the orientation of the ridges and valleys at each region of the image, and it is estimated taking into account the vertical and horizontal gradients along all pixels in the image (which has been previously divided into blocks, so that the consistency of the orientation field in the local neighborhood can be computed).

(2) Then, and after the region of interest has been delimited, the ridges are extracted and thinned.

(3) At this point, minutiae points can be easily found. For each minutiae point, its position is stored, as well as the orientation field in this point and a segment of the associated ridge.

Once the minutiae points have been found, a matching strategy has to be developed. As the minutiae representation scheme does not take into account the possible variability between several fingerprint images from the same finger, [1] this problem has to be dealt with in matching stage. Factors that may cause two representations to be different, even though they come from the same individual, include possible rotations, nonlinear deformations caused by the pressure of the finger upon the sensor and the inherent imprecise nature of the extraction minutiae procedure. Therefore, the matching procedure must be based on a somehow "elastic" comparison between both point (minutiae) patterns. Jain's system uses a matching strategy that is divided into two stages:

(1) As the alignment of point patterns is generally a hard task, specially in the presence of noise and deformations, the ridges associated to each minutiae point are used, so that using these corresponding curve segments makes the problem easier and the results more robust.

(2) In a perfect alignment, each pair of the corresponding points would be coincident. However, this does not happen in practice (it must also be taken into account that the alignment algorithm

[1] On the contrary, feature extraction schemes employed for iris identification (see Section 4.1) were invariant to possible changes in size and position of the iris, and tried to minimize the effects of other possible sources of variability, such as reflections or illumination variations.

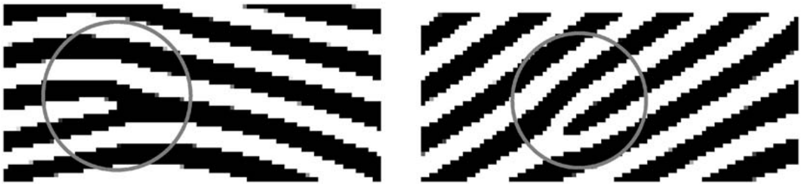

Fig. 10. Ridge ending and ridge bifurcation.

does not model nonlinear deformations, which are an inherent property of fingerprints). Therefore, and elastic algorithm is used which first represents the minutiae patterns as a string and then matches the string using a dynamic programming algorithm to finally obtain a matching score.

A number of similar approaches can be found in the literature [12,64,58] (the system proposed in [64] adds the use of the pores structure present in the fingerprint for the representation scheme). Often a preprocessing step attempts to enhance the fingerprint image to ensure robustness, as the quality of the images may vary significantly.

Even though most of the work found in the literature concerning fingerprint identification is based on minutiae determination and analysis, different approaches have been employed. In fact some authors consider that traditional (minutiae-based) fingerprint identification systems suffer from several major drawbacks. First, it is very difficult to extract complete ridge structures automatically for a considerable fraction of the population, which obviously prevents fingerprint recognition from getting a generalized commercial use. Besides, it is a difficult problem to match two fingerprint representations when they contain a different number of minutiae points [37]. These shortcomings make it a desirable goal to develop new strategies that allow fingerprint recognition gain a much wider use. In his work, Coetzee proposed an approach not making use of any feature, but performing a correlation in the frequency domain of the whole binarized fingerprint image [14]. Somehow in this direction Prabhakar's work is really interesting [57], using a texture-based approach that is radically different to traditional minutiae-based approaches, in order to capture both the local and the global information present in a fingerprint image as a compact representation. To this extent, the method first locates a unique reference point within the image using its orientation field. Next, a bank of Gabor filters is applied using eight different orientations (which are necessary to completely capture the local ridge characteristics in a fingerprint [36]). To make up a feature vector, a circular region of interest is defined around the reference point and divided into 80 sectors (Fig. 11). Each feature value is the average absolute deviation from the mean of each sector S_i of $F_{i\theta}(x, y)$, the image filtered in direction θ:

$$V_{i\theta} = \frac{1}{n_i}\left(\sum_{n_i} |F_{i\theta}(x, y) - P_{i\theta}|\right), \qquad (4)$$

where n_i is the number of pixels in sector S_i and $P_{i\theta}$ is the mean of pixel values of $F_{i\theta}(x, y)$ in that sector. In this way, a feature vector with dimension 640 is obtained, which will be called FingerCode.[2] Matching stage is performed by comparing two FingerCodes using the Euclidean distance. The feature vector is translation invariant (as it is referred to a reference point) but it is not rotation invariant. This problem is solved by cyclically rotating the features in the FingerCode.

This section has presented the fundamentals of fingerprint identification technologies. Minutiae-based approaches, which have been analyzed at a certain level of detail, have reached a high level of refinement but suffer from their serious inherent problems. This is why texture-based approaches have lately gained more interest, and may thus become a promising area of research capable of surpassing today's technology limitations.

[2] Note that this nomenclature is directly inspired by Daugman's IrisCode (see Section 4.1), as this system can be considered as the application of that strategy for fingerprints.

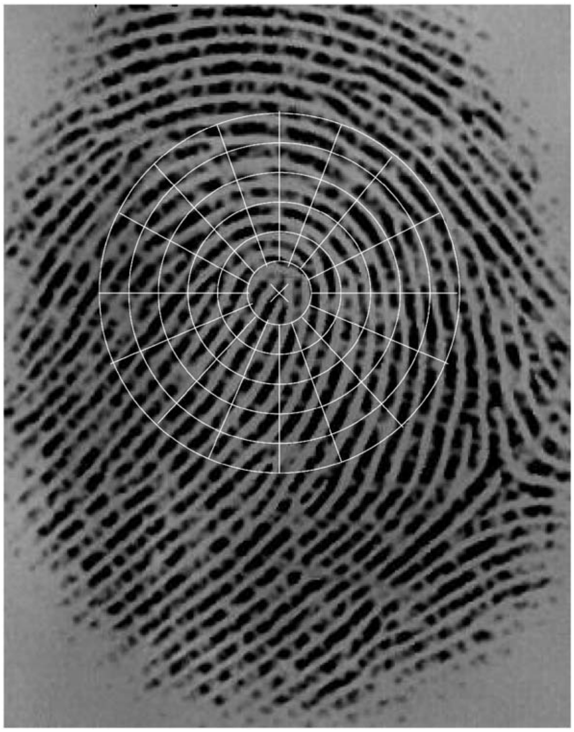

Fig. 11. Fingerprint region of interest divided in sectors for further analysis.

4.3. Face recognition

We humans have an inherent ability to recognize human faces. So, it would seem natural for us that computers recognized our faces as well. This is the main advantage of automatic face recognition: it is a user-friendly method for automatic recognition because it seems natural to us. The use of face recognition includes many applications such as access to secure areas, video surveillance, law enforcement applications, etc. So, as the applications are very heterogeneous, the technical requirements are very diverse too, and a number of different techniques for face recognition have been developed. Besides, the way humans recognize each other has been studied thoroughly, yielding conclusions which might be useful for the design of automatic face recognizing systems [13]. Face recognition can be made from still images, video sequences, stereo, range images, etc. We will focus in this paper on recognizing people from 2D images, for this is probably the most important field in scientific research as well as for commercial applications. We will now explain the foundations of the most popular methods used to recognize faces.

One of the earliest works in computer recognition of faces was reported by Bledsoe [8]. In this work, a number of points were located on the face. Then, given a set of feature point distances of an unknown person, nearest neighbor or other classification methods were employed for identifying the person. Similar approaches were applied in a number of studies afterwards, using different methods to characterize the face in terms of distances and angles between points such as eye corners, mouth extremities, etc.

Much more recent is the use of statistical approaches for face recognition. Turk and Pentland [68] used the Karhunen–Loeve (KL) expansion to obtain a set of eigenvectors known as eigenfaces. Then, any image can be represented using a weighted combination of eigenfaces. The weights are obtained by projecting the image into eigenface components using an inner product operation. The identification of the image is done by locating the image in the database whose weights are the closest (in Euclidean distance) to the weights of the test image.[3] It is important to remark that variations in the type of distance used can affect greatly the system's performance [55]. Registration of the position and size of the face is needed to achieve robustness with respect to image acquisition, as carried out for example in [2]. This system applies the Fourier transform to the standardized image and uses the resulting Fourier spectrum instead of the spatial data for the KL expansion.

Support vector machines are used in [53]. As face recognition is a K class problem, where K is the number of known individuals, and SVMs are a binary classification method, the face recognition problem is reformulated as a two class problem, the classes being dissimilarities between faces of the same person, and dissimilarities between faces of different people. The facial image can be represented as a vector of

[3] For verification, a threshold can be applied given the Euclidean distance between the test and reference eigenface-based representation, deciding the face belongs to a genuine user if the distance is below it. However, most of the effort done in face recognition has focused on identification rather than verification. This is why the different techniques are explained in an identification context.

dimension N, as the original pixel vectorized, metric features or the face expressed as a combination of eigenfaces.

The use of neural networks for face recognition deserves indeed plenty of attention. A number of systems use neural networks not only for face recognition, but also for gender classification and classification of facial expressions. A good review on such systems can be found in [13]. The use of neural networks is an alternative to the use of other classifiers once a feature vector has been obtained. Other neural architectures have also been used for face recognition, as HyperBF networks [10].

Many other feature extraction and matching techniques have been used for face recognition, from Gabor filtering to genetic algorithms. An excellent survey can be found in [13].

We have seen in this section than face recognition is probably the most user friendly biometric technology, because humans are used to recognizing faces. However, computers do not perform as well as humans (research has been made about human recognition of faces, and some systems have been developed based on these results). Although great progress has been made and continues to, the time has not come when computers easily recognize us from our faces.

4.4. Other BISs

Fingerprint recognition is probably the best-known biometric technology, and it is currently employed in a number of real-world applications. Face recognition is also a very popular biometric technique, as it seems to be the most user-friendly, although it does not reach, at the moment, a high degree of accuracy. Iris recognition, although not being quite popular, is probably the most accurate biometric technology developed so far. However, biometric recognition does not stop here. There are many more biometric technologies in use today which deserve attention. We shall now introduce some of them:

- Voice recognition—Working alone or together with face recognition, voice recognition is a quite common biometric technology. A good introduction to the field of speaker verification can be found in [25]. Speaker verification technologies can be divided into two major categories [5]:
  (1) Text-dependent applications, where the system associates a sentence, possibly different, to each client. One particular case of text-dependent speaker verification is known as *text prompted*, where the systems *prompts* the potential client with a sentence, which could be different for each access. The main methods used for text-dependent speaker verification are dynamic time warping, which consists on representing the speech utterance by a sequence of acoustic vectors and then compute the distance between the access utterance and the client utterance, using a dynamic programming method to compare sequences of different sizes, and the use of hidden markov models (HMMs).
  (2) Text-independent applications, where the client is not requested to say the same sentence during each access. Thus, the only information used by the system are the acoustic characteristics of the client. The most common methods for text-independent speaker verification are vector quantization, sphericity distance, and Gaussian mixture models [5].
- Hand geometry—This biometric technique is based on the fact that virtually every person's hand is uniquely shaped, and this shape does not significantly change after a certain age. Hand geometry biometric techniques usually represent the hand geometry in terms of features comprising the lengths of the fingers, their widths and widths of the palm at various locations [39].
- Retina recognition—A retina-based BIS analyzes the layer of blood vessels situated at the back of the eye. Although it is considered as a highly accurate technology, its being intrusive is a major drawback for this kind of biometric technique. For capturing the retina patterns, an infrared light source is used, and then the pattern is analyzed for characteristic points which form the discriminant information.
- Signature verification—This biometric has a long history, and has a wide current usage in document authentication and transaction authorization [59]. There is a natural division between on-line and off-line recognition. Off-line recognition requires that signatures are scanned from paper documents and then analyzed, whereas on-line recognition uses devices that capture the dynamic

information as the signature is being written (pen tip location through time, and even pen angle and contact pressure) [47,21]. Because of the special hardware for an on-line signature recognition, it seems unlikely that it will spread beyond the domains where it is already used.
- Other biometric identification technologies include keystroke recognition, palm-print features [29] or ear recognition [11].

4.5. Multimodal BISs

As no single biometric feature seems to be able to provide as much accuracy and reliability as needed in some contexts, multimodal biometric systems (also referred to as multibiometrics systems) are emerging as a possible alternative strategy. We can define a multimodal biometric system as one using more than one different biometric characteristics to identify a person. For example, voice and face recognition can be combined to form a multimodal biometric system [24]. It is probably necessary to extend this definition by including also those biometric systems that use several methods based upon the same biometric source.

The term multibiometrics is closely related to the field of information fusion, which has been thoroughly studied specially in decision theory. There are many and very heterogeneous ways to combine information in multibiometrics, and several taxonomies have been proposed [61,62]. The latter is very suitable to provide an overview on multibiometric systems, and states four different ways for combining information:

- Sensor data level fusion. In this case, the raw data from sensors are combined [28]. It is necessary that the data be commensurate, that is, having a common measure. There are two main methods used for sensor data fusion: weighted summation (for example, combining data from various microphones to reduce the effects of noise) and mosaic construction (for example, to create one image out of images from several cameras, each camera observing a different part of the same object).
- Feature level fusion. This means that the representations obtained from data from different sensors (or from the same sensor but using different feature extraction techniques) are combined. Again, the combination can be carried out by weighted summation (if the features are commensurate) or by means of a simple vector concatenation if the features are not commensurate.
- Decision level fusion. In this case, we can consider different biometric systems as independent units, each one making a decision about the authenticity of the user. Then, a *supervisor* will combine the decisions to yield a final decision. Typical ways for combining decisions are majority voting, combination of ranked lists or the use of the AND & OR operators. More sophisticated methods taken from decision theory and based on Bayes or Neyman–Pearson theory, even with quality information about the decisions [67] could also be applied; they are designed to get the maximum performance with a minimum information exchange needed between the sensors and the controller, provided they are located physically distant.
- Opinion fusion. If information exchange is not an issue, the different (experts) systems used for decision fusion may not provide a *hard* decision, but rather an opinion, either in numerical or linguistic format; then the controller should combine these opinions. In this case, since the amount of information gathered is higher, performance is expected to be higher too. The opinions can be the similarity or dissimilarity scores usually obtained in most biometric systems, and can be forced to be commensurated by mapping them to the $[0,1]$ interval. Typical methods for combining opinions are weighted summation or product, or the use of a postclassifier.

A good review on the *art* of combining classifiers can be found in [40]. For biometric identification purposes, Daugman, in [18], illustrates the limitations of a simple approach to decision level fusion in multibiometrics systems, based on the use of the AND & OR operators. In terms of FAR and FRR, this scheme is only able to enhance one of the parameters while worsening the other. Therefore, more complex schemes have been proposed for multimodal biometric systems. Most of them are based on the idea of opinion fusion.

The combination of three biometric modalities (face, fingerprint and hand geometry) studied by Ross et al. [61] illustrates an opinion fusion approach to the problem of information fusion in biometrics. Given three matching scores obtained from the three different biometric systems mentioned above, the problem is to develop a fusion scheme to reach an overall decision. As the three biometric systems are complete and independent on their own, it is quite clear that only opinion fusion or decision fusion can be applied in this case. Opinion fusion is expected to yield better results as it uses a greater amount of information. Ross et al. propose and experiment with three different fusion schemes: the use of weighted summation (applying equal weights to all the opinions, so that the rule is equivalent to an arithmetic mean), decision trees and a linear discriminant. In their experiments, the three schemes show better results than using a single biometric modality, and weighted summation performs the best. However, it is not clear that this fusion strategy can be successfully applied to other multibiometric systems.

Opinion fusion schemes can be much more complicated. Brunelli and Falavigna [9] propose two different methods for combining five opinions. Since the source of the opinions (scores, in the author's terminology) are fairly different (two speech features and three image features) a common reference framework is needed prior to fusion. This framework basically changes scales and eliminates biases in the opinion quantities. Then a nonlinear function maps the opinions within the segment $[0, 1]$. As for the opinion fusion schemes, the first one calculates an weighted geometric average of the scores, the weights of which are defined in terms of the dispersion of the opinions; then the acceptance/rejection decision is carried out by means of a linear classifier as before. The second procedure is claimed to integrate the classifiers in two levels of abstraction (both scores and ranks of the scores); the fusion is posed as a learning problem which is solved by means of a HyperBF network [56]. In both cases, results are comparable, and clearly superior than using any of the classifiers alone. However, no comparative results with other methods are described.

Another approach is the work of Bigun et al. [22]; here the fusion scheme (the controller as the authors say) is designed within a Bayesian probabilistic framework; as before opinions from each classifier (i.e., from each expert) are nonlinearly normalized; then an overall decision is reached by thresholding the posterior probability of a correct choice. Results are compared with a thresholded arithmetic mean of the opinions of each expert. Results clearly favor the Bayesian scheme with respect to the mean scheme; however, no other comparisons are carried out with, for instance, the previous approach. Other examples of opinion fusion strategies and complex multibiometric schemes can be seen in [76,65,41,69].

As we have shown above, many opinion fusion strategies have been proposed for multibiometric systems. Although they have clearly demonstrated that the use of multiple biometrics yields better results than using a unique biometric modality, one question still remains unanswered: Which is the best method for combining the different experts' opinions? The search for this answer has led to very heterogeneous and complex multimodal biometric schemes, where information fusion theory has provided an starting point from which virtually innumerable possibilities arise.

5. A glimpse on the market

Nowadays, the prices of biometric products and systems are dropping as demand for the technology grows and a wide variety of vendors enter the market [78,79,97–100]. In fact the biometrics industry has combined forces and agreed on a common platform, such as The BioAPI Consortium, an industry initiative formed by Compaq Computer Corp., IBM Corp., Identicator Technology, Microsoft Corp., Miros Inc., and Novell Inc., with the goal of developing an industry standard Biometric API specification [79], which will allow different manufacturers of biometric software to interact. A biometric API standard defines an open system API that allows software applications to communicate with a broad range of biometric technologies in a common way. Additional information on the Biometric Consortium, the hosting organization and an important list of Biometric Vendors and manufacturers can be found in [101,88,78,84]. In addition, information on some leading Biometric Companies and products can be found in [85–87,89].

Currently most of these companies are providing different recognition solutions for face, fingerprint, iris, signature, voice, and lip movement. For example, the Dialog Communication Systems (DCS AG) developed by BioID [80] is a multimodal identification system that uses three different features—face, voice and lip movement—to identify people. The mentioned technologies have also been addressed by several companies such as Authentec [81], Veridicom [82] and Infineon [83]. Similarly AcSys Biometrics Corp [90] leads the biometrics market with its Face Recognition models [91]. AcSys' list of partners continues to grow and includes companies and organizations such as CHUBB PLC, Litton Industries' PRC Inc., and the US State Department, Consular Services Branch. We can refer also to other competitive companies like Nexus and Group International Inc. [93], Graphco Technologies, Inc. G-TEC^{TM} [94], TouchChiP^{TM} develops Biometrics Fingerprint, etc. [95]. IBG is a biometric industry's leading consulting and technology services firm [92]; IBG also provides technology-neutral and vendor-independent biometric services and solutions to financial institutions, government agencies, systems integrators, and high-tech firms since 1996. IBG leverages real world, hands-on experience with all biometrics including fingerprint, face, and iris systems to successfully evaluate, design, and deploy access control, IT security, transportation, smart card, and identification systems solutions.

In academia there are some laboratories and research groups that are developing algorithms in order to be used by the companies cited above, such as the Biometrics Program of the University of Southern Carolina (USC) [108], the University of Maryland (UMD) [109] and the Massachusetts Institute of Technology (MIT) Media Laboratory [110]. The MIT and USC algorithms have also become the basis for commercial systems. For example Viisage, a leading face recognition company [111], uses the eigenface-based recognition algorithm developed at the MIT Media Laboratory.

There are some biometric servers that demonstrated the highest level of accuracy with large databases. The most important ones are the BioAccess server, which is an Access Control system that uses Biometrics for authentication [101]; Oss Nakalva provides support for client-server operation, which is characterized by high reliability, security, scalability, and performance [103]. Cyber-SIGN is also a licensed technology that requires integration into a client/server application and is the technology leader for enterprise (TCP/IP client/server) [104].

For more details the following pages contain more information about biometric products, research groups, and other useful links: [96,102,112–119, 105–107].

6. Conclusions

This paper has provided an overview of the current state of the art in BISs. Technical details have been kept moderately low to provide a high-level and comparative description of the main BISs currently in use. Whether or not BISs will be of widespread use in the near of mid-term future is a matter of discussion, since many nontechnical aspects are involved: perceived reliability, willingness to cooperate with the BISs, etc. In any case, since technical parameters measuring reliability give no room for doubt that BISs are to be trusted, it is probably a matter of time to see BISs deployed in more scenarios than today, although not necessarily for the public use. About multibiometrics, current proposals show that fusing BISs provides better results than the stand-alone use of each; however, many questions still remain unanswered about how to choose a particular multibiometric scheme for a specific application.

Acknowledgements

The authors acknowledge the Spanish CICYT for research Grant TIC2001-3808-C02.

References

[1] F.H. Adler, Physiology of the Eye, St. Louis, MO, United States, Mosby, 1965.

[2] S. Akamatsu, T. Sasaki, H. Fukamachi, Y. Suenaga, A robust face identification scheme—kl expansion of an invariant feature space, SPIE Proc.: Intell. Robots Comput. Vision X: Algorithms Techn. 1607 (1991) 71–84.

[3] Biometric Systems: Worldwide Deployments, Market Drivers, and Major Players, Allied Business Intelligence, Oyster Bay, NY, 2002.

[4] 2002 market review, Biometric Technol. Today, 11 (January 2003) 9–11.

[5] S. Bengio, J. Mariethoz, S. Marcel, Evaluation of biometric technology on xm2vts, Technical Report IDIAP-RR 01-21, Dalle Molle Institute for Perceptual Artificial Intelligence, July 2001.

[6] W.W. Boles, B. Boashash, A human identification technique using images of the iris and wavelet transform, IEEE Trans. Signal Process. 46 (4) (1998) 1185–1188.

[7] R.M. Bolle, S. Pankanti, N.K. Ratha, Evaluation techniques for biometrics-based authentication systems (frr), in: Int. Conf. Pattern Recognition (ICPR), Vol. 2, Barcelona, 2000.

[8] W.W. Bledsoe, The model method in facial recognition, Panoramic Research Inc., Palo Alto, CA, Technical Report, Technical Report PRI:15, 1964.

[9] R. Brunelli, D. Falavigna, Person identification using multiple cues, IEEE Trans. Pattern Anal. Mach. Intell. 12 (1995) 955–966.

[10] R. Brunelli, T. Poggio, Face recognition: features versus templates, IEEE Trans. Pattern Anal. Mach. Intell. 15 (1993) 1042–1052.

[11] M. Burge, W. Burger, Ear biometrics, in: A. Jain, R. Bolle, S. Pankanti (Eds.), Biometrics: Personal Identification in Networked Society, Kluwer Academics, Dordrecht, 1998.

[12] G.M. Candea, M.C. Moy, Sureid a fingerprint-based authentication system for insecure networks, Class project paper for 6857: Network and Computer Security, Massachussetts Institute of Technology, April 1997.

[13] R. Chellappa, C.L. Wilson, S. Sirohey, Human and machine recognition of faces: a survey, Proc. IEEE 83 (5) (May 1995) 705–740.

[14] L. Coetzee, Fingerprint recognition, M.S. Dissertation, Faculty of Electronic and Computer Engineering. University of Pretoria, 1992.

[15] J. Daugman, Uncertainty relation for resolution in space, spacial frequency, and orientation optimized by two-dimensional visual cortical filters, J. Opt. Soc. Amer. A 2 (7) (1985) 1160–1169.

[16] J. Daugman, Complete discrete 2d gabor transforms by neural networks for image analysis and compression, Trans. Acoust. Speech and Signal Process. 36 (7) (1988) 1169–1179.

[17] J. Daugman, High confidence recognition of persons by a test of statistical independence, IEEE Trans. Pattern Anal. Mach. Intell. 15 (11) (1993) 1148–1161.

[18] J. Daugman, Biometric decision landscapes, Technical Report TR482, University of Cambridge Computer Laboratory, 1999.

[19] J. Daugman, How iris recognition works, URL:www.cl.cam.ac.uk/users/jgdl000/irisrecog.pdf.

[20] J. Daugman, C. Downing, Epigenetic randomness, complexity, and singularity of human iris patterns, Proc. Roy. Soc. 268 (2001) 1737–1740.

[21] J.G.A. Dolfing, E.H.L. Aarts, On-line signature verification with hidden markov models, in: Proceedings of the International Conference on Pattern Recognition, August 1998, pp. 1309–1312.

[22] B. Duc, E.S. Bigun, J. Bigun, G. Maitre, S. Fischer, Fusion of audio and video information for multimodal person authentication, Pattern Recogn. Lett. 18 (1997) 835–843.

[23] L. Flom, A. Safir, Iris recognition system, 1987, U.S. Patent No. 4,641,349.

[24] R.W. Frischholz, U. Dieckmann, Bioid: a multimodal biometric identification system, Computer 33 (2) (2000) 64–68.

[25] S. Furui, Recent advances in speaker recognition, in: J. Bigün, G. Chollet, G. Borgeford (Eds.), Audio and Video-based Biometric Person Authentication, Springer, Berlin, 1997, pp. 237–252.

[26] D. Gabor, Theory of communication, J. Inst. Electr. Eng. 93 (1946) 429–457.

[27] T. Greene, Biometric security—practical and affordable! Information Security Regarding Room, Sans Institute, January 2001.

[28] D.L. Hall, J.L. Llinas, Multisensor data fusion, in: D.L. Hall, J. Llinas (Eds.), Handbook of Multisensor Data Fusion, CRC Press, USA, 2001, pp. 1–10.

[29] C.-C. Han, H.-L. Cheng, C.-L. Lin, K.-C. Fan, Personal authentication using palm-print features, Pattern Recogn. 36 (2003) 371–381.

[30] M. Hartman, Compact fingerprint scanner techniques, in: Proceedings of the Biometric Consortium Eighth Meeting, San Jose, CA, June 1996.

[31] A. Jain, R.M. Bolle, S. Pankanti, Biometrics: Personal Identification in Networked Society, Kluwer Academic Publishers, Dordrecht, 1999.

[32] A. Jain, L. Hong, S. Pankanti, Biometric identification, Comm. ACM 43 (2) (February 2000) 91–98.

[33] A. Jain, L. Hong, S. Pankanti, R. Bolle, An identity authentication system using fingerprints, Proc. IEEE 85 (9) (1997) 1365–1388.

[34] A. Jain, S. Pankanti, Biometrics systems: anatomy of performance, IEICE Trans. Fund. E84-D (7) (2001) 788–799.

[35] A.K. Jain, S. Pankanti, S. Prabhakar, A. Ross, Recent advances in fingerprint verification, Lecture Notes Comput. Sci. 2091 (2001) 182–190.

[36] A.K. Jain, S. Prabhakar, L. Hong, A multichannel approach to fingerprint classification, IEEE Trans. Pattern Anal. Mach. Intell. 21 (4) (1999) 348–359.

[37] A.K. Jain, S. Prabhakar, L. Hong, S. Pankanti, Filterbank-based fingerprint matching, IEEE Trans. Image Process. 9 (5) (May 2000) 846–859.

[38] A.K. Jain, S. Prabhakar, S. Pankanti, Twin test: on discriminability of fingerprints, Lecture Notes Comput. Sci. 2091 (2001) 211–216.

[39] A.K. Jain, A. Ross, S. Pankanti, A prototype hand geometry-based verification system, Second International Conference on Audio and Video-based Biometric Person Authentication, Washington DC, USA, March 1999.

[40] J. Kittler, M. Hatef, R.P.W. Duin, J. Matas, On combining classifiers, IEEE Trans. Pattern Anal. Mach. Intell. 20 (3) (1998) 226–239.

[41] J. Kittler, J. Matas, K. Jonsson, M.U. Ramos-Sanchez, Combining evidence in personal identity verification systems, Pattern Recogn. Lett. 18 (1997) 845–852.

[42] H.C. Lee, E.R.E. Gaensslen, Advances in Fingerprint Technology, Elsevier, New York, 1991.

[43] S. Lim, K. Lee, O. Byeon, T. Kim, Efficient iris recognition through improvement of feature vector and classifier, ETRI J. 23 (2) (June 2001) 61–70.

[44] S. Liu, M. Silverman, A practical guide to biometric security technology, IT Professional 3 (1) (2001) 27–32.

[45] D. Maio, D. Maltoni, R. Cappelli, J.L. Wayman, A.K. Jain, Fvc2000: fingerprint verification competition, IEEE Trans. Pattern Anal. Mach. Intell. 24 (3) (March 2002) 402–412.

[46] B. Miller, Vital signs of identity, IEEE Spectrum 31 (2) (February 1994) 22–30.

[47] V.S. Nalwa, Automatic on-line signature verification, Proc. IEEE 85 (2) (February 1997) 215–239.

[48] M. Negin, T.A.C. Jr., M. Salganicoff, T.A. Camus, U.M.C. von Seelen, P.L. Venetianer, G.G. Zhang, An iris biometric system for public and personal use, Computer 33 (2) (2000) 70–75.

[49] R. Norton, The evolving biometric marketplace to 2006, Biometric Technol. Today 11 (October 2002) 7–8.

[50] S. Pankanti, R.M. Bolle, A. Jain, Biometrics: the future of identification, Computer 33 (2) (2000) 46–49.

[51] S. Pankanti, S. Prabhakar, A.K. Jain, On the individuality of fingerprints, in: Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR), Hawaii, US, December 2001.

[52] J. Phillips, H. Moon, S.A. Rizvi, P.J. Rauss, The feret evaluation methodology for face-recognition algorithms, IEEE Trans. Pattern Anal. Mach. Intell. 22 (10) (2000) 1090–1104.

[53] P.J. Phillips, Support vector machines applied to face recognition, Technical Report, NISTIR 6241, National Institute of Standards and Technology, 1999.

[54] P.J. Phillips, A. Martin, C.L. Wilson, M. Przybocki, An introduction to evaluating biometric systems, Computer 33 (2) (2000) 56–63.

[55] P.J. Phillips, A.J. O'Toole, Y. Cheng, B. Ross, H.A. Wild, Assessing algorithms as computational models for human face recognition, Technical Report, Technical Report NISTIR 6348, 1999, National Institute of Standards and Technology.

[56] T. Poggio, F. Girosi, Regularization algorithms for learning that are equivalent to multilayer networks, Science 247 (1990) 978–982.

[57] S. Prabhakar, Fingerprint classification and matching using a filterbank, Ph.D. Dissertation, Department of Computer Science and Engineering, Michigan State University, 2001.

[58] N. Ratha, S. Chen, A.K. Jain, Adaptive flow orientation based feature extraction in fingerprint images, Pattern Recogn. 28 (8) (1995) 799–813.

[59] N.K. Ratha, A. Senior, R.M. Bolle, Tutorial on automated biometrics, in: Proceedings of International Conference on Advances in Pattern Recognition, Rio de Janeiro, Brazil, March 2001.

[60] Z. Řiha, V. Matyáš, Biometric authentication systems, Technical Report, FIMU-RS-2000-08, Faculty of Informatics, Masaryk University, 2000.

[61] A. Ross, L. Hong, S. Pankanti, R. Bolle, Information fusion in biometrics, in: Proceedings AVBPA'01, Halmstad, Sweden, June 2001, pp. 354–359.

[62] C. Sanderson, Information fusion and person verification using speech and face information. Technical Report IDIAP-RR 02-33, Dalle Molle Institute for Perceptual Artificial Intelligence. September 2002.

[63] W. Shen, M. Surette, R. Khanna, Evaluation of automated biometrics-based identification and verification systems, Proc. IEEE 85 (September 1997) 1464–1478.

[64] J.D. Stosz, L.A. Alyea, Automated system for fingerprint authentication using pores and ridge structure, Department of Defense, 1993.

[65] N.P.H. Thian, S. Bengio, J. Korczak, A multi-sample multi-source model for biometric authentication, Technical Report IDIAP-RR 02-14, Dalle Molle Institute for Perceptual Artificial Intelligence, April 2002.

[66] G. Tomko, Privacy implications of biometrics—a solution in biometric encryption, in: Proceedings of the English Annual Conference on Computers, Austin, TX, August 1998, pp. 1309–1312.

[67] S.C. Thomopoulos, R. Viswanathan, D.C. Bougoulias, Optimal decision fusion in multiple sensor systems, IEEE Trans. Aerospace Electron. Systems 23 (5) (September 1987) 644–653.

[68] M.A. Turk, A.P. Pentland, Face recognition using eigenfaces, in: Proc. Internat. Conf. Pattern Recognition, Hawaii, 1991, pp. 586–591.

[69] P. Verlinde, P. Druyts, G. Chollet, M. Acheroy, A multi-level data fusion approach for gradually upgrading the performances of identity verification systems, Proc. SPIE 3719 (1999) 14–25.

[70] J.L. Wayman, Generalized biometric identification system model, in: Proceedings of 31st IEEE Asilomar Conference on Signals, Systems and Computing, Pacific Grove, CA, 1997.

[71] J.L. Wayman, Biometric identification standards research, Technical Report, Final Report, San Jose State University, San Jose, CA, 1997.

[72] J.L. Wayman, Technical testing and evaluation of biometric identification devices, in: Biometrics: Personal Identification in a Networked Society, Kluwer Academic Publishers, Dordrecht, 1999.

[73] J.L. Wayman, A definition of biometrics, National Biometric Test Center Collected Works 1997–2000, San Jose State University, 2000, pp. 21–23.

[74] J.L. Wayman, Fundamentals of biometric authentication technologies, National Biometric Test Center Collected Works 1997–2000, San Jose State University, 2000, pp. 1–19.

[75] R.P. Wildes, Iris recognition: an emerging biometric technology, Proc. IEEE 85 (1997) 1348–1363.

[76] S.B. Yacoub, Y. Abdeljaoued, E. Mayoraz, Fusion of face and speech data for person identity verification, IEEE Trans. Neural Networks 10 (5) (1999) 1065–1074.

[77] Y. Zhu, T. Tan, Y. Wang, Biometric personal identification based on iris patterns, National Laboratory of Pattern Recognition (NLPR), Institute of Automation, Chinese Academy of Sciences.

[78] http://www.biodigest.com/

[79] http://www.bioapi.org/

[80] http://www.bioid.com/

[81] http://www.authentec.com

[82] http://www.Veridicom.com

[83] http://www.infineon.com

[84] http://www.findbiometrics.com/

[85] http//www.ibia.org/apibull.htm

[86] http://filebox.vt.edu/users/teastman/pages/otherlinks.htm

[87] http://www.keyware.com/

[88] http://www.biometrics.org

[89] http://euro.ecom.cmu.edu/resources/elibrary/ectlinks.shtml

[90] http://www.acsysbiometricscorp.com

[91] http://www.gslis.utexas.edu/palmquis/courses/project98/comvision/facerec.htm

[92] http://www.biometricgroup.com/index.html

[93] http://www.nxsgrp.com/

[94] http://www.graphcotech.com/

[95] http://www.st.com/stonline/products/support/touchip/index.htm

[96] http://www.biometricsmi.com

[97] http://www.biometrics-today.com/

[98] http://www.purchasingresearchservice.com/

[99] http://www.timberlinetechnologies.com/products/biometric.html

[100] http://www.business.com/directory/computers_and_software/hardware_and_accessories/security_products/authentication/biometrics/

[101] http://www.biometrics.co.za

[102] http://attrasoft.com/

[103] http://www.oss.com/products/biometrics/biosupport.html

[104] http://www.cybersign.com/

[105] http://www.all-internet-security.com/authentication/

[106] http://www.imagistechnologies.com/?source=google_adwords

[107] http://www.cadix.com/

[108] http://www.usc.edu/

[109] http://www.umd.edu/

[110] http://www.media.mit.edu/

[111] http://www.viisage.com/

[112] http://amp.ece.cmu.edu/

[113] http://www.tech.purdue.edu/it/resources/biometrics/

[114] http://biometrics.cse.msu.edu/

[115] http://www.hh.se/ide/islab/isprojekt.htm

[116] http://www.engr.sjsu.edu/biometrics/

[117] http://www-white.media.mit.edu/vismod/

[118] http://mambo.ucsc.edu/psl/fanl.html

[119] http://biometrics.ag.uq.edu.au/