# Automated biometrics

Nalini K. Ratha, Andrew Senior and Ruud M. Bolle
IBM Thomas J. Watson Research Center
P. O. Box 218
Yorktown Heights, NY 10598
{ratha, aws, bolle}@us.ibm.com

**Abstract**

*Identity verification becomes a challenging task when it has to be automated with high accuracy and non-repudiability. The existing methods such as passwords and photo identity cards are inadequate to meet such heavy demands. Automated biometrics-based authentication methods can meet all the demands. An overview of the fast developing and exciting area of automated biometrics is provided in this paper. Several popular biometrics including fingerprint, face, iris are briefly described and an introduction to evaluation methods is presented.*

## 1 Introduction

In the modern networked society, there is an ever growing need to determine or verify the identity of a person. Where authorization is necessary for any action, be it collecting a child from child-care facilities or boarding an aircraft, authorization is almost always vested in a single individual or a class of individuals. There are a number of existing methods, summarized in table 1 used by society or automated systems to verify identity. Traditional existing methods can be grouped into three classes [24]: (i) possessions; (ii) knowledge and (iii) biometrics. Biometrics is the science of identifying or verifying the identity of a person based on physiological or behavioral characteristics. Physiological characteristics include fingerprints and facial image. The behavioral characteristics are actions carried out by a person in a characteristic way and include signature and voice, though these are naturally dependent on physical characteristics. Very often the three identification methods are used in combination. A key is a physical conveyor of authorization; password plus user ID is a purely knowledge-based method of identification; an ATM card is a possession that requires knowledge to carry out a transaction; a passport is a possession that requires biometric verification.

Early automated authorization relied on possessions and knowledge, but there are several well-known problems associated with these methods, which restrict their use and the trust that can be placed in them. These methods verify attributes which are usually assumed to imply the presence of a given person. The most important drawbacks of these methods are (i) possessions can be lost, forged or easily duplicated; (ii) knowledge can be forgotten; (iii) both knowledge and possessions can be shared or stolen. Consequently (iv) repudiation is easy (it is easy to deny that a given person carried out an action, because only the possessions or knowledge are checked, and these are only loosely coupled to the person's identity). Such drawbacks are not tolerable in applications such as high security physical access control, bank account access and credit card authentication. The science of biometrics provides an elegant solution to these problems by truly verifying the identity of the individual. For contemporary applications biometrics are being automated to eliminate the need for human verification, and a number of new biometrics have been developed, taking advantage of improved understanding of the human body and advanced sensing techniques. Newer physiological biometrics that have been developed

| Method | Examples | Comments |
|---|---|---|
| What you know | userid, password, PIN | Forgotten<br>Shared<br>Many passwords are easy to guess |
| What you have | Cards, badges, keys | Lost or stolen<br>Shared<br>Can be duplicated |
| What you are | Fingerprint, face..... | Non-repudiable authentication |

Table 1: Identification technologies.

include iris patterns, retinal images and hand geometry; newer behavioral biometrics, still in the research are gait and odor.

Measurements of the behavioral characteristics must be insensitive to variations in the biometrics due to the state of health or mood of the user. The physiological characteristics remain fairly constant over time. A biometrics system works on an enrolled data set which is the first step. After enrolling, the user can be a verified many times.

### 1.1 Identification vs. Authentication

Basically, there are two types of application scenarios: (i) identification; and (ii) authentication. In identification, also known as 1:N matching, the system uses the biometric to determine the corresponding person from a database containing many people, or decides that the person is not enrolled in the database. In authentication, also known as 1:1 matching or identity verification, the system matches the input biometric against a single biometric record. The latter could be stored on a card presented at the transaction time, or looked up in a database with the help of a key such as an account number or employee ID. The output of the match is either "Yes" if the two biometrics match or "No" otherwise. Often during the enrollment process, we need to employ an identification system to make sure the person is not already enrolled and the subsequent usages are authentication instances using the unique number assigned to the user during the enroll.

### 1.2 Application characteristics

Several applications require biometrics. In general, wherever there is a password or PIN, we can think of replacing them with biometrics. However, each application has a different set of requirements. For example, an ATM requires unattended type of biometrics where as a welfare disbursement center has a supervisor available. An application can be characterized by the following characteristics: (i) attended vs. unattended; (ii) overt vs. covert; (iii) cooperative vs. non-cooperative; (iv) scalable vs. non-scalable and (v) acceptable vs. non-acceptable. By scalable, we mean that the database being scalable with no appreciable performance degradation.

## 2 Pattern recognition-based biometrics systems

Biometric systems can be cast as a generic pattern recognition system as shown in Figure 1. The input subsystem consists of the special sensors needed to acquire the biometric signal. Reliable acquisition of the input signal is a challenge for the sensor designers, in the face of interpersonal and intrapersonal variations and varying

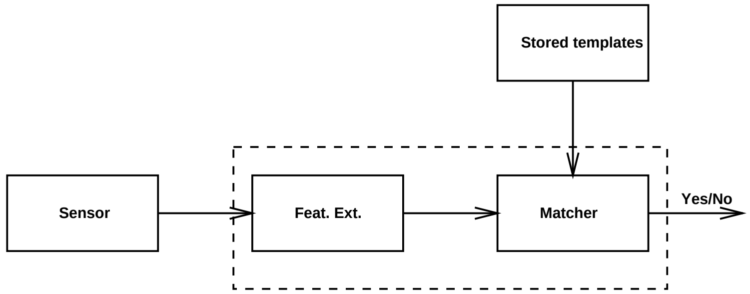


Figure 1: A generic biometrics system.

environmental situations. The signal in its raw form contains the required identifying information hidden among a mass of irrelevant information. Invariant features are extracted from the signal for representation purposes in the feature extraction subsystem. During the enrollment process, representation (feature) templates are stored in the system. The matching subsystem accepts a query and reference templates and returns the degree of match or mismatch as a score. A final decision step compares the score to a decision threshold to deem the comparison a match or non-match. The overall performance of the system depends on the performance of all the subsystems. In addition, the system designer has to focus on efficient storage and retrieval, error free transmission and possible encryption and decryption of the result as well as intermediate signals.

## 2.1 Classification errors and performance evaluation

To assess the performance of a biometric system, we analyze it in a hypothesis testing framework. Let the stored biometric sample or template be pattern $P' = S(B')$ and the acquired one be pattern $P = S(B)$. Then, in terms of hypothesis testing, we have null and alternative hypotheses:

$$\begin{aligned} H_0 :& \quad B = B', \quad \text{the claimed identity is correct} \\ H_1 :& \quad B \neq B', \quad \text{the claimed identity is } \textit{not} \text{ correct.} \end{aligned} \tag{1}$$

Often some similarity measure $s = Sim\,(P, P')$ is defined and $H_0$ is decided if $s \geq T_d$ and $H_1$ is decided if $s < T_d$, with $T_d$ a decision threshold. (Some systems use a distance or dissimilarity measure. Without loss of generality we assume a similarity measure throughout.)

## 2.2 Measures of performance

The measure $s$ is also referred to as the *match score*. When $B = B'$, $s$ is referred to as a *matching score* and $B$ and $B'$ are called a *mated pair* or *matched pair*. When $P \neq P'$, $s$ is referred to as a *nonmatched score* and $B$ and $B'$ are called a *non-mated pair*.

For expression 1, deciding $H_0$ when $H_1$ is true gives a false acceptance; deciding $H_1$ when $H_0$ is true results in a false rejection. The False Accept Rate (FAR) (proportion of non-mated pairs resulting in False acceptance) and False Reject Rate (FRR) (proportion of mated pairs resulting in false rejection) together characterize the accuracy of a recognition system for a given decision threshold. Varying the threshold trades FAR off against FRR. In Figure 2, the FAR is the area under the $H_1$ density function to the right of the threshold and the FRR is the area under the $H_0$ density function to the left of the threshold. In a more general framework, we can express the two errors as False Match Rate (FMR) and False Non-Match Rate (FNMR) [40].

The Equal Error Rate (EER) is the point at some threshold ($T_{EER}$) where FRR = FAR, *i.e.* where the areas marked under the two curves in Fig. 2 are equal.

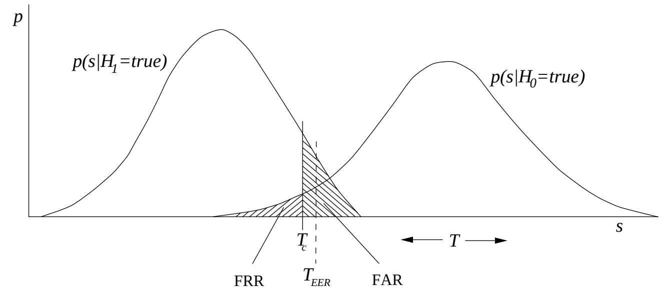


Figure 2: Impostor and genuine distributions with classification error definitions.

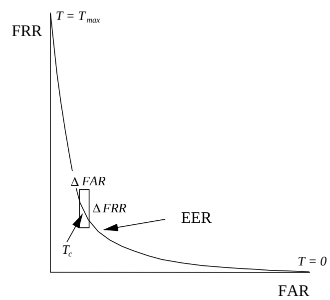


Figure 3: Receiver Operating Curve (ROC).

Rather than showing the error rates in terms of probability densities as in Figure 2, it is desirable to report system accuracy using a Receiver Operating Curve (ROC) [13, 26]. An ROC is a mapping $T_d \rightarrow (\mathrm{FAR}, \mathrm{FRR})$,

$$\mathrm{ROC}(T_d) = (\mathrm{FAR}(T_d), \mathrm{FRR}(T_d)),$$

as shown in Fig. 3.

Note that in a typical recognition system, all the information contained in the PDFs is also contained in the ROC. The ROC can be directly constructed from the probability density functions as

$$\begin{aligned} \mathrm{FAR}(T_d) = \quad & Prob(s \geq T_d | H_1 = true) = \quad [1 - \int_0^{T_d} p(s|H_1 = true)\ \mathrm{d}s] \\ \mathrm{FRR}(T_d) = \quad & Prob(s < T_d | H_0 = true) = \quad \int_0^{T_d} p(s|H_0 = true)\ \mathrm{d}s. \end{aligned}$$

If we let $T_d$ go to zero, the FAR goes to one and the FRR goes to zero; if we let $T$ go to $T_{max}$, the FAR goes to zero and the FRR goes to one.

Quite often a measure of “goodness” $d'$ (d-prime) of a matcher is defined as [9]:

$$d' = \frac{\mu_1 - \mu_2}{\sqrt{(\sigma_1^2 + \sigma_2^2)}}. \tag{2}$$

This measure was originally developed to measure the separability of two equivalent normal distributions.

## 3 Six most commonly used biometrics

The most commonly used automated biometrics are: (i) fingerprint; (ii) face; (iii) voice; (iv) iris; (v) signature and (vi) hand geometry. We will provide a brief description of each of these biometrics.

### 3.1 Fingerprint

Fingerprint is the mother biometric and the most widely used biometric. The advent of several inkless fingerprint scanning technologies coupled with the exponential increase in processor performance has taken fingerprint recognition out of the criminal identification applications to several civilian applications such as access control; time and attendance; and computer user login. Over the last decade, many novel techniques have been developed to acquire fingerprints without the use of ink. These scanners are known as the "livescan" fingerprint scanners. The basic principle in these inkless methods is to sense the ridges and valleys on a finger when the finger is in contact with the surface of the scanner. The livescan image acquisition systems are based on four types of technology:

- Frustrated total internal reflection (FTIR) and other optical methods [14, 31]: This technology is by far the oldest livescan method. A camera looks at the reflected signal from the prism as the subject touches a side of the prism. The typical image size of 1" $\times$ 1" is converted to 500 dpi images using a CCD or CMOS camera. Many variations of this principle, such as use of tactile sensors in place of a prism and the use of a holographic element [23], are also available. The main issue with these scanners is that the reflected light is a function of skin characteristics. If the skin is wet or dry the resulting image is significantly hard to process.

- CMOS capacitance [17]: The ridges and valleys of a finger create different charge accumulations when the finger touches a CMOS chip grid. With suitable electronics, the charge is converted to a pixel value. Normally at 500 dpi these scanners provide about 0.5" $\times$ 0.5" of scan area. This can be a problem as the two images acquired at two different times may have very little overlap. They also tend to be affected by the skin dryness and wetness. In addition, these devices are sensitive to electrostatic discharge.

- Thermal [21]: The pyro-electric material in the sensor measures temperature changes as the finger is swiped over the scanner and produces an image. This technology is claimed to overcome the dry and wet skin issues in the optical scanners and can sustain higher static discharge. However, the images are not rich in gray values.

- Ultrasound [5]: An ultrasonic beam is scanned across the fingerprint surface to measure the ridge depth from the reflected signal. Skin conditions such as dry, wet and oil on the skin do not affect the imaging and the images better reflect the actual ridge topography. However, these units tend to very bulky and require larger scanning time than the optical scanners.

Recently non-contact [2] fingerprint scanners have been announced to avoid problems related touching a surface for scanning the fingerprint.

The most commonly used features are ridge bifurcation and ridge endings collectively known as *minutia* are extracted from the acquired image. The feature extraction process starts by examining the quality of the input gray-level image. Virtually every published method of feature extraction [28, 22] computes the orientation field of the fingerprint image which reflects the local ridge direction at every pixel. The local ridge orientation has been used to tune filter parameters for enhancement and ridge segmentation. From the segmented ridges, a thinned image is computed to locate the minutiae features. Usually, one has to go through a minutiae post-processing stage to clean up several spurious minutiae resulting from either enhancement, ridge segmentation or thinning artifacts. The main goal of the fingerprint authentication module is to report some sort of distance between two fingerprint feature sets accurately and reliably. The authenticate function has to compensate for (i) translation, (ii) rotation, (iii) missing features, (iii) additional features, (iv) spurious features and, more importantly, (v) elastic distortion between a pair of feature sets. Often storage and transmission of fingerprint images involves compression and decompression of the image. Standard compression techniques often remove the high frequency areas around the minutia features. Hence a novel fingerprint compression scheme called as Wavelet Scalar Quantization (WSQ) is recommended by FBI. One of the main advantages of the fingerprint biometrics is the high accuracy and low cost of the system.

## 3.2 Iris

Even though iris [41] is a relatively young biometric, it has been shown to be very accurate and stable. The colored part of the eye bounded by the pupil and sclera is the iris which is extremely rich in texture. Like fingerprints, this biometric results from the developmental process and is not dictated by genetics. So far in the literature, there has been only a couple of iris recognition systems described. The primary reason being the difficulties in designing a reliable image acquisition stage. Often iris recognition is confused with the retinal recognition system which has a much harder-to-use input acquisition subsystem. In the Daugman system [8] for iris recognition, the texture of the iris is represented using Gabor wavelet responses and the matcher is an extremely simple and fast Hamming distance measure.

## 3.3 Hand geometry

Hand geometry based authentication is a limited scalable but extremely user-friendly biometric. The lengths of the fingers and other hand shape attributes are extracted from images of a hand and used in the representation. To derive such gross characteristics, a relatively inexpensive camera can be employed resulting in a overall low cost of the system. As the computation is also fairly light weight, a standalone system is easy to build. As this biometrics is not seen to compromise user privacy, it is quite widely accepted. However, hand geometry based authentication systems are less accurate than fingerprint-based authentication techniques. It has high FAR and FRR as well.

## 3.4 Face recognition

Face recognition [7, 30] is a particularly compelling biometric because it is one used every day by nearly everyone on earth. Since the advent of photography it has been institutionalized as a guarantor of identity in passports and identity cards. Since faces are easily captured by conventional optical imaging devices, there are vast legacy databases, of police mug-shots or television footage for instance, which face recognition will enable us to search. Because of its naturalness, face recognition is more acceptable than most biometrics, and the fact that cameras can acquire the biometric passively means that it can be very easy to use — indeed surveillance systems rely on capturing the face image without the cooperation of the person being imaged.

Despite these attractions, face recognition is not sufficiently accurate to accomplish the large-population identification tasks tackled with fingerprint or iris. One clear limit is the similarity of appearance of identical twins, but determining the identity of two photographs of the same person is hindered by all of the following problems which we can divide into three classes.

- **Physical changes:** expression change; aging; personal appearance (make-up, glasses, facial hair, hairstyle, disguise).
- **Acquisition geometry changes:** change in scale, location and in-plane rotation of the face (facing the camera) as well as rotation in depth (facing the camera obliquely).
- **Imaging changes:** lighting variation; camera variations; channel characteristics (especially in broadcast, or compressed images).

No current system can claim to handle all of these problems well. Indeed there has been little research on making face recognition robust to aging. In general, constraints on the problem definition and capture situation are used to limit the amount of invariance that needs to be afforded algorithmically.

The main challenges of face recognition today are handling rotation in depth and broad lighting changes, together with personal appearance changes. Even under good conditions, however, accuracy could be improved. There is interest in other acquisition modalities such as 3D shape through stereo or range-finders; near infrared or facial thermograms, all of which have attractions, but lack the compelling reasons for visible-light face recognition outlined above.

In general, face recognition systems proceed by detecting the face in the scene, thus estimating and normalizing for translation, scale and in-plane rotation. Approaches then divide [6] into appearance-based and geometric approaches, analyzing the appearance of the face and the distances between features respectively. In many systems these are combined, and indeed to apply appearance-based methods in the presence of facial expression changes requires generating an expressionless 'shape-free' face by image warping. Appearance based methods can be global [18, 34, 4, 12] where the whole face is considered as a single entity, or local, where many representations of separate areas of the face are created. [33, 42, 32].

Considerable progress has been made in recent years, with much commercialization of face recognition, but a lot remains to be done towards the 'general' face recognition problem.

### 3.5 Speaker identification

Like face, speaker identification [15] has attractions because of its prevalence in human communication. We expect to pick up the phone and be able to recognize someone by their voice after only a few words, although clearly the human brain is very good at exploiting context to narrow down the possibilities. Telephony is the main target of speaker identification, since it is a domain with ubiquitous existing hardware where no other biometric can be used. Increased security for applications such as telephone banking and 'm-commerce' means the potential for deployment is very large. Speaking solely in order to be identified can be somewhat unnatural, but in situations where the user is speaking anyway (e.g. a voice-controlled computer system, or when ordering something by phone) the biometric authentication becomes 'passive'. Physical and computer security by speaker ID have received some attention, but here it is less natural and poorer performing than other biometrics. Speaker ID is necessary for audio and video- indexing. Where a video signal is available lip-motion identification has also been used [19, 11, 20].

Speaker identification suffers considerably from any variations in the microphone [16, 29] and transmission channel, and performance deteriorates badly when enrollment and use conditions are mismatched — as inevitably happens when a central server carries out speaker ID on telephone signals. Background noise can also be a considerable problem in some circumstances, and variations in voice due to illness, emotion or aging are further problems that have received little study.

Speaker verification is particularly vulnerable to replay attacks because of the ubiquity of sound recording and play-back devices. Consequently more thought has been given in this domain to avoiding such attacks. We can categorize speaker ID systems depending on the freedom in what is spoken, this taxonomy based on increasingly complex tasks also corresponds to the sophistication of algorithms used and the progress in the art over time.

- **Fixed text:** The speaker says a predetermined word or phrase which was recorded at enrollment. The word may be secret, so acts as a password, but once recorded a replay attack is easy, and re-enrollment is necessary to change the password.

- **Text dependent:** The speaker is prompted by the system to say a specific thing. The machine aligns the utterance with the known text to determine the user. For this, enrollment is usually longer, but the prompted text can be changed at will. Limited systems (e.g. just using digit strings) are vulnerable to splicing-based replay attacks.

- **Text independent:** The speaker ID system processes any utterance of the speaker. Here the speech can be task-oriented, so it is hard to acquire speech that also accomplishes the impostor's goal. Monitoring can be continuous — the more that is said the greater the system's confidence in the identity of the user. The advent of trainable speech synthesis might enable attacks on this approach. Such systems can even identify a person when they switch language.

While traditionally used for verification, more recent technologies have started to do identification, one particular domain being in audio and video indexing [3].

### 3.6 Signature verification

Signature verification [25] is another biometric that has a long pedigree before the advent of computers, with considerable legal recognition and wide current usage in document authentication and transaction authorization in the form of checks and credit card receipts. Here the natural division is into on-line and off-line, depending on the sensing modality. Off-line or 'static' signatures are scanned from paper documents where they were written in the conventional way [27]. On-line or 'dynamic' signatures are written with an electronically instrumented device and the dynamic information (pen tip location through time) is usually available at high resolution, even when the pen is not in contact with the paper. Some on-line signature capture systems can also measure pen angle and contact pressure [10], providing a much richer signal than is available in the on-line case, and making the identification problem correspondingly easier. These additional data make on-line signatures very robust to forgery. While forgery is a very difficult subject to research thoroughly, it is widely believed that most forgery is very simple and can be prevented with even relatively simple algorithms.

Because of the special hardware needed for the more robust on-line recognition, it seems unlikely that signature verification will spread beyond the domains where it is already used, but the volume of signature authorized transactions today is huge, making automation through signature verification very important.

Naturally, signature verification can be generalized to writer identification with the same categories (text dependent/independent) as speaker verification, but as a working biometric technology, attention has focussed on signature.

## 4 Standards, standard databases and interoperability issues

For wide acceptance of biometrics, standards for interfaces and performance evaluation are necessary. Several standards are in the process of being developed and promoted. NIST has been playing an important role in designing several fingerprint databases [37, 38, 35, 36, 39] and conducting speaker verification tests. The US Dept. of Defense runs the FERET face recognition test. BioAPI [1] is a standard for the application programmer interface allowing the decoupling of biometrics-technologies from the applications that use them. At the hardware level, the devices for biometrics still remain non-interoperable except when sharing a common existing standard such as NTSC video.

### 4.1 Which biometric?

In this section, we will compare the six biometrics presented earlier. The comparison is based on the following factors: (i) cost; (ii) accuracy; (iii) representation size; (iv) scalability; (v) maturity and (vi) obtrusiveness; and is summarized in table 2. Depending on the application in hand, not all biometrics will be suitable for it.

| | Fingerprint | Speech | Face | Iris | Hand | Signature |
|---|---|---|---|---|---|---|
| Maturity | very high | high | medium | high | medium | medium |
| Best FAR | $10^{-8}$ | $10^{-2}$ | $10^{-2}$ | $10^{-10}$ | $10^{-4}$ | $10^{-4}$ |
| Best FRR | $10^{-3}$ | $10^{-3}$ | $10^{-2}$ | $10^{-4}$ | $10^{-4}$ | $10^{-4}$ |
| Scalability | High | Medium | Medium | Very high | low | medium |
| Sensor cost | <$100 | <$5 | <$50 | <$3000 | <$500 | <$300 |
| Sensor type | Contact | Unobtrusive | Unobtrusive | Unobtrusive | contact | contact |
| Sensor size | small | very small | small | medium | large | medium |
| template size | <200 bytes | < 2K bytes | <2k Bytes | 256 bytes | <10 bytes | <200 bytes |

Table 2: Comparison of six popular biometrics.

## 5 Conclusions

The existing methods of automatic authentication involving knowledge or possessions have a number of limitations, particularly in that they can be transferred from one person to another. Automated biometrics can address that problem while overcoming the other problems such as lost, sharing and forgery of other authentication methods. Automated biometric systems can be modeled as a pattern recognition systems. We have presented six popular biometrics and a comparative evaluation of them.

## References


[1] *BioAPI – http://www.bioapi.org*.

[2] *Non-contact fingerprint scanner: http://www.ddsi-cpc.com/pages/products/cscan300.html*.

[3] H. S. M. Beigi, S. H. Maes, U. V. Chaudhari, and J. S. Sorensen. IBM model-based and frame-by-frame speaker recognition. In *Speaker Recognition and its Commercial and Forensic Appications*, Avignon, April 1998.

[4] P. Belhumeur, J. Hespanha, and D. J. Kriegmand. Eigenfaces vs. Fisherfaces: Recognition using class specific linear projection. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 19(7):711–720, July 1997.

[5] W. Bicz, Z. Gurnienny, and M. Pluta. Ultrsound sensor for fingerprints recognition. In *Proc. of SPIE, Vol. 2634, Optoelectronic and electronic sensors*, pages 104–111, June 1995.

[6] R. Brunelli and T. Poggio. Face recognition: Features versus templates. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 15(10):1042–1052, October 1993.

[7] R. Chellappa, C. L. Wilson, and S. Sirohey. Human and machine recognition of faces: A survey. *Proceedings of the IEEE*, 83(5):705–740, May 1995.

[8] J. G. Daugman. High confidence visual recognition of persons by a test of statistical independence. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 15(11):1148–1161, Nov. 1993.

[9] J. G. Daugman and G. O. Williams. A proposed standard for biometric decidability. In *CardTechSecureTech*, pages 223–234, Atlanta, GA, 1996.

[10] J. G. A. Dolfing, E. H. L. Aarts, and v. J. J. G. M. On-line signature verification with hidden Markov models. In *Proceedings of the International Conference on Pattern Recognition*, pages 1309–12, August 1998.

[11] B. Duc, E. S. Bigün, J. Bigün, G. Maître, and S. Fischer. Fusion of audio and video information for multi modal person authentication. *Pattern Recognition Letters*, 18(9):835–843, 1997.

[12] G. J. Edwards, C. J. Taylor, and T. F. Cootes. Interpreting faces using active appearance models. In *International Conference on Face and Gesture Recognition*, number 3, pages 300–305, April 1998.

[13] B. G. et al. Issues in large scale automatic biometric identification. In *IEEE Workshop on Automatic Identification Advanced Technologies*, pages 43–46, Stony Brook, NY, Nov. 1996.

[14] D. T. Follette, E. B. Hultmark, and J. G. Jordan. *Direct optical input system for fingerprint verification*. IBM Technical Disclosure Bulletin: 04-74p3572, April 1974.

[15] S. Furui. Recent advances in speaker recognition. In B. Bigun, Chollet, editor, *Audio- and Video-based Biometric Person Authentication*, volume 1206 of *Lecture Notes in Computer Science*, pages 237–252. Springer, 1997.

[16] L. P. Heck and M. Weintraub. Handset-dependent background models for robust text-independent speaker recognition. In *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing*, April 1997.

[17] S. Jung, R. Thewes, T. Scheiter, K. F. Gooser, and W. Weber. A low-power and high-performance cmos fingerprint sensing and encoding architecture. *IEEE Journal of Solid-state Cicuits*, 34(7):978–984, July 1999.

[18] M. Kirby and L. Sirovich. Application of the Karhunen-Loève procedure for the characterization of human faces. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 12(1):103–108, 1990.

[19] J. Kittler, Y. Li, J. Matas, and M. Ramos Sánchez. Lip-shape dependent face verification. In J. Bigün, G. Chollet, and G. Borgefors, editors, *Audio- and Video-based Biometric Person Authentication*, volume 1206 of *Lecture Notes in Computer Science*, pages 61–68. Springer, March 1997.

[20] J. Luettin, N. A. Thacker, and S. W. Beet. Speaker identification by lipreading. In *Proceedings of the 4th International Conference on Spoken Language Processing (ICSLP'96)*, volume 1, pages 62–65, 1996.

[21] J.-F. Mainguet, M. Pegulu, and J. B. Harris. Fingerchip$^{TM}$: thermal imaging and finger sweeping in a silicon fingerprint sensor. In *Proc. of AutoID 99*, pages 91–94, October 99.

[22] D. Maio and D. Maltoni. Direct gray-scale minutiae detection in fingerprints. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 19(1):27–40, January 1997.

[23] M. H. Metz, Z. A. Coleman, N. J. Phillips, and C. Flatow. Holographic optical element for compact fingerprint imaging system. In *Proc. of SPIE, Vol. 2659, Optical security and counterfeit deterrance techniques*, pages 141–151, 1996.

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

[25] V. S. Nalwa. Automatic on-line signature verification. *Proceedings of the IEEE*, 85(2):215–239, February 1997.

[26] W. Peterson, T. Birdsall, and W. Fox. The theory of sigmal detectability. *Transactions of the IRE*, PGIT-4:171–212, April 1954.

[27] R. Plamondon and G. Lorette. Automatic signature verification and writer identification — The state of the art. *Pattern Recognition*, 22(2):107–129, 1989.

[28] N. K. Ratha, S. Chen, and A. K. Jain. Adaptive flow orientation based texture extraction in finger print images. *Pattern Recognition*, 28(11):1657–1672, November 1995.

[29] D. A. Reynolds. The effects of handset variability on speaker recognition performance: Experiments on the Switchboard Corpus. In *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing*, May 1996.

[30] A. Samal and P. Iyengar. Automatic recognition and analysis of human faces and facial expressions: A survey. *Pattern Recognition*, 25(1):65–77, 1992.

[31] S. E. Schuster. *Fingerprinting method.* IBM Technical Disclosure Bulletin: 12-70p1852, Dec. 1970.

[32] A. W. Senior. Recognizing faces in broadcast video. In *IEEE International Workshop on Recognition, Analysis, and Tracking of Faces and Gestures in Real-Time Systems*, pages 105–110, September 1999.

[33] D. L. Swets and J. J. Weng. Using discriminant eigenfeatures for image retrieval. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 18(8):831–836, Aug. 1996.

[34] M. Turk and A. Pentland. Eigenfaces for recognition. *Journal of Cognitive Neuro Science*, 3(1):71–86, 1991.

[35] C. I. Watson. *NIST special database 10: Supplemental Fingerprint Card Data for NIST Special Database 9*. Advanced Systems Division, Image Recognition Group , National Institute for Standards and Technology, February 1993.

[36] C. I. Watson. *NIST special database 14: Fingerprint Card Pairs 2*. Advanced Systems Division, Image Recognition Group , National Institute for Standards and Technology, February 1993.

[37] C. I. Watson. *NIST special database 4: 8-bit Gray scale Images of Fingerprint Image Groups*. Advanced Systems Division, Image Recognition Group , National Institute for Standards and Technology, February 1993.

[38] C. I. Watson. *NIST special database 9: Mated Fingerprint Card Pairs*. Advanced Systems Division, Image Recognition Group , National Institute for Standards and Technology, February 1993.

[39] C. I. Watson. *NIST special database 24: NIST Digital Video of Live-scan Fingerprint Database*. Advanced Systems Division, Image Recognition Group , National Institute for Standards and Technology, February 1998.

[40] J. L. Wayman. Error rate equations for the general biometrics system. *IEEE Automation and Robotics Magazine*, 6(1):35–48, March 1999.

[41] R. P. Wildes. Iris recognition: An emerging biometric technology. *Proc. of IEEE*, 85(9):1348–1363, Sept. 1997.

[42] L. Wiskott and C. von der Malsburg. Recognizing faces by dynamic link matching. In *Proceedings of the International Conference on Artificial Neural Networks*, pages 347–352, 1995.