Handbook of Biometrics

Handbook of Biometrics

edited by

Anil K. Jain
Michigan State University, USA

Patrick Flynn
University of Notre Dame, USA

Arun A. Ross
West Virginia University, USA

Springer

Anil K. Jain
Michigan State University
Dept. of Computer Science &
Engineering
3115 Engineering Building
East Lansing MI 48824 USA
jain@cse.msu.edu

Patrick Flynn
University of Notre Dame
Dept. of Computer Science &
Engineering
384 Fitzpatrick Hall
Notre Dame IN 46556-5637 USA
flynn@nd.edu

Arun A. Ross
West Virginia University
Dept. of Computer Science &
Electrical Engineering
Morgantown WV 26506-6109 USA
arun.ross@mail.wvu.edu

ISBN-13: 978-0-387-71040-2 e-ISBN-13: 978-0-387-71041-9

Library of Congress Control Number: 2007934776

Printed on acid-free paper.

9 8 7 6 5 4 3 2 1

springer.com

Foreword

Nearly 40 years ago, IBM suggested that a computer user could be recognized at a computer terminal "By something he knows or memorizes.... By something he carries... By a personal physical characteristic". This analysis was done in the context of computer data security - remotely recognizing those authorized to access stored data - and specifically referenced voice recognition as a "personal physical characteristic" useful for human recognition, although automated handwriting, fingerprint, face, and hand geometry systems were, by 1970, also under development. Since that time, automatically recognizing persons by physical and behavioral characteristics has come to be known as "biometric authentication" and applications have broadened far beyond the remote recognition of computer terminal users. Today, biometric technologies are being used in all types of applications not foreseen by the early pioneers and not realizable with "something known" or "something carried", such as in visa and passport issuance, social service administration, and entertainment ticket management systems. There are new technologies available for these tasks: automated iris, hand vein, ear, gait, palm crease and 3-dimensional face recognition systems

This book, edited by Anil K. Jain of Michigan State University and two of his former students, Patrick J. Flynn and Arun Ross - now on the faculties of Notre Dame and West Virginia Universities, respectively- gives us a broad, yet detailed overview of the technologies, applications and implementation challenges of biometric authentication at its current state of development. Chapter authors are some of the best known, and in some cases, the earliest researchers in their fields. With this book, the story is not finished. Rather, it is only beginning. New technologies remain to be discovered. Challenges of incorporating new and existing technologies seamlessly into person-centric systems remain to be resolved. Understanding of the full impact of automated human recognition on both natural rights and social contracts remains to be acquired. In short, this book tells us the very first part of the story of biometric authentication. Future generations will tell us the rest. I fully expect this book to inspire current and future researchers and innovators to think in new ways about the technologies, applications and implications of automated human recognition.

James L. Wayman
San Jose State University

Preface

Biometrics is the science of recognizing the identity of a person based on the physical or behavioral attributes of the individual such as face, fingerprints, voice and iris. With the pronounced need for robust human recognition techniques in critical applications such as secure access control, international border crossing and law enforcement, biometrics has positioned itself as a viable technology that can be integrated into large-scale identity management systems. Biometric systems operate under the premise that many of the physical or behavioral characteristics of humans are distinctive to an individual, and that they can be reliably acquired via appropriately designed sensors and represented in a numerical format that lends itself to automatic decision-making in the context of identity management. Thus, these systems may be viewed as pattern recognition engines that can be incorporated in diverse markets.

While biometric *traits* such as fingerprints have had a long and successful history in forensics, the use of these traits in automated personal recognition systems is a fairly recent accomplishment. But now biometric *technology* is a rapidly evolving field with applications ranging from accessing one's computer to obtaining visa for international travel. The deployment of large-scale biometric systems in both commercial (e.g., grocery stores, Disney World, airports) and government (e.g., US-VISIT) applications has served to increase the public's awareness of this technology. This rapid growth in biometric system deployment has clearly highlighted the challenges associated in designing and integrating these systems. Indeed, the problem of biometric recognition is a "Grand Challenge" in its own right. The past five years has seen a significant growth in biometric research resulting in the development of innovative sensors, novel feature extraction and matching algorithms, enhanced test methodologies and cutting-edge applications. However, there is no single book that succinctly captures the advancements made in biometrics in recent years while presenting the reader with a fundamental understanding of basic concepts in biometrics. The purpose of this book is to address this void by inviting some of the most prominent researchers in biometrics to author individual chapters describing the fundamentals as well as the latest advances

in their respective areas of expertise. The result is an edited volume that embodies most of the salient topics in biometric technology thereby giving its readers an understanding of the spectrum of work constituting the field of biometrics.

This book is divided into three logical sections. The first section discusses individual biometric modalities including fingerprints, face, iris, hand geometry, gait, ear, voice, palmprint, signature, teeth and hand vein. The chapters in this section describe some of the proven feature extraction and matching algorithms that have been designed for processing individual biometric modalities. The chapters in the second section discuss the concept of multibiometrics where two or more sources of biometric information are fused in order to enhance the recognition accuracy of these systems. The third section discusses the impact of deploying biometric systems in both civilian and government applications. Topics related to legal and privacy issues as well as forensic science are presented in this section. Finally, there is a discussion on biometric standards and the use of public domain datasets available for performance evaluation and comparison. Each chapter has an elaborate bibliography associated with it, thereby directing the reader to other pertinent literature on specific topics.

This book would not have been possible but for the cooperation and hardwork of the chapter authors. We would like to thank each one of them for their contribution to this project. Several authors also participated in the review process and their extensive comments were useful in refining individual chapters. Thanks are also due to Mohamed Abdel-Mottaleb (University of Miami), Nicolae Duta (Nuance), Max Houck (West Virginia University) and Steve Krawczyk (Michigan State University) for their valuable input during the review process. Special thanks to Julian Fierrez for providing detailed comments on a preliminary draft of the manuscript. Karthik Nandakumar, Abhishek Nagar and Keron Greene (Michigan State University) spent a considerable amount of time editing and typesetting the final manuscript. Their assistance is gratefully acknowledged.

This book has been designed for professionals composed of students, practitioners and researchers in biometrics, pattern recognition and computer security. It can be used as a primary textbook for an undergraduate biometrics class or as a secondary textbook for advanced-level students in computer science and electrical engineering. We hope that the concepts and ideas presented in this book will stimulate further research in this field even as biometric technology becomes an integral part of society in the 21st century.

Anil K. Jain, East Lansing, MI
Patrick J. Flynn, Notre Dame, IN
Arun Ross, Morgantown, WV
July 2007

Contents

1

Introduction to Biometrics

Anil K. Jain[1] and Arun Ross[2]

[1] Department of Computer Science and Engineering, Michigan State University, East Lansing, MI 48824 USA
jain@cse.msu.edu

[2] Lane Department of Computer Science and Electrical Engineering, West Virginia University, Morgantown, WV 26506 USA
arun.ross@mail.wvu.edu

1.1 Introduction

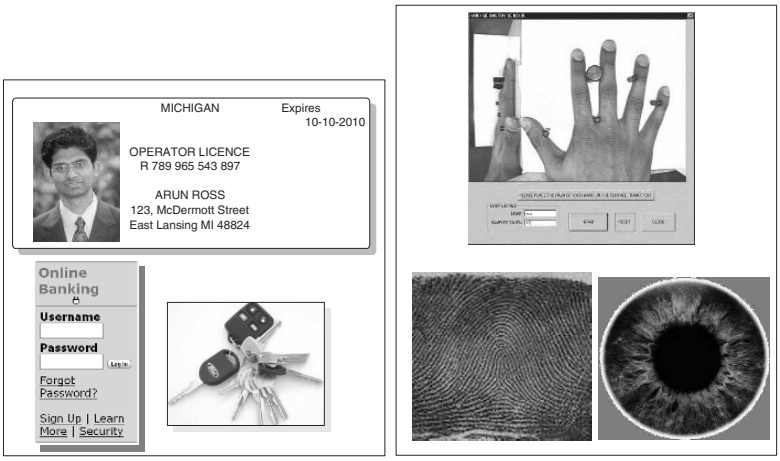
Biometrics is the science of establishing the identity of an individual based on the physical, chemical or behavioral attributes of the person. The relevance of biometrics in modern society has been reinforced by the need for large-scale identity management systems whose functionality relies on the accurate determination of an individual's identity in the context of several different applications. Examples of these applications include sharing networked computer resources, granting access to nuclear facilities, performing remote financial transactions or boarding a commercial flight. The proliferation of web-based services (e.g., online banking) and the deployment of decentralized customer service centers (e.g., credit cards) have further underscored the need for reliable identity management systems that can accommodate a large number of individuals.

The overarching task in an identity management system is the determination (or verification) of an individual's identity (or claimed identity).[3] Such an action may be necessary for a variety of reasons but the primary intention, in most applications, is to prevent impostors from accessing protected resources. Traditional methods of establishing a person's identity include knowledge-based (e.g., passwords) and token-based (e.g., ID cards) mechanisms, but these surrogate representations of identity can easily be lost, shared, manipulated or stolen thereby compromising the intended security. Biometrics[4] offers

[3] The *identity* of an individual may be viewed as the information associated with that person in a particular identity management system [15]. For example, a bank issuing credit cards typically associates a customer with her name, password, social security number, address and date of birth. Thus, the identity of the customer in this application will be defined by these personal attributes (i.e., name, address, etc.).

[4] The term *biometric authentication* is perhaps more appropriate than *biometrics* since the latter has been historically used in the field of statistics to refer to the

a natural and reliable solution to certain aspects of identity management by utilizing fully automated or semi-automated schemes to recognize individuals based on their biological characteristics [13]. By using biometrics it is possible to establish an identity based on *who you are*, rather than by *what you possess*, such as an ID card, or *what you remember*, such as a password (Figure 1.1). In some applications, biometrics may be used to supplement ID cards and passwords thereby imparting an additional level of security. Such an arrangement is often called a dual-factor authentication scheme.



(a) (b)

Fig. 1.1. Authentication schemes. (a) Traditional schemes use ID cards, passwords and keys to validate individuals and ensure that system resources are accessed by a legitimately enrolled individual. (b) With the advent of biometrics, it is now possible to establish an identity based on "who you are" rather than by "what you possess" or "what you remember".

The effectiveness of an authenticator (biometric or non-biometric) is based on its relevance to a particular application as well as its robustness to various types of malicious attacks. O'Gorman [29] lists a number of attacks that can be launched against authentication systems based on passwords and tokens: (a) client attack (e.g., guessing passwords, stealing tokens); (b) host attack (e.g., accessing plain text file containing passwords); (c) eavesdropping (e.g., "shoulder surfing" for passwords); (d) repudiation (e.g., claiming that token was misplaced); (e) trojan horse attack (e.g., installation of bogus log-in screen to steal passwords); and (f) denial of service (e.g., disabling the system by deliberately supplying an incorrect password several times). While some of these

analysis of biological (particularly medical) data [36]. For brevity sake, we adopt the term *biometrics* in this book.

attacks can be deflected by incorporating appropriate defense mechanisms, it is not possible to handle all the problems associated with the use of passwords and tokens.

Biometrics offers certain advantages such as negative recognition and non-repudiation that cannot be provided by tokens and passwords [32]. Negative recognition is the process by which a system determines that a certain individual is indeed enrolled in the system although the individual might deny it. This is especially critical in applications such as welfare disbursement where an impostor may attempt to claim multiple benefits (i.e., double dipping) under different names. Non-repudiation is a way to guarantee that an individual who accesses a certain facility cannot later deny using it (e.g., a person accesses a certain computer resource and later claims that an impostor must have used it under falsified credentials).

Biometric systems use a variety of physical or behavioral characteristics (Figure 1.2), including fingerprint, face, hand/finger geometry, iris, retina, signature, gait, palmprint, voice pattern, ear, hand vein, odor or the DNA information of an individual to establish identity [12, 36]. In the biometric literature, these characteristics are referred to as *traits*, *indicators*, *identifiers* or *modalities*. While biometric systems have their own limitations ([28]) they have an edge over traditional security methods in that they cannot be easily stolen or shared. Besides bolstering security, biometric systems also enhance user convenience by alleviating the need to design and remember passwords.

1.2 Operation of a biometric system

A biometric system is essentially a pattern recognition system that acquires biometric data from an individual, extracts a salient feature set from the data, compares this feature set against the feature set(s) stored in the database, and executes an action based on the result of the comparison. Therefore, a generic biometric system can be viewed as having four main modules: a sensor module; a quality assessment and feature extraction module; a matching module; and a database module. Each of these modules is described below.

1. **Sensor module**: A suitable biometric reader or scanner is required to acquire the raw biometric data of an individual. To obtain fingerprint images, for example, an optical fingerprint sensor may be used to image the friction ridge structure of the fingertip. The sensor module defines the human machine interface and is, therefore, pivotal to the performance of the biometric system. A poorly designed interface can result in a high failure-to-acquire rate (see Section 1.4) and, consequently, low user acceptability. Since most biometric modalities are acquired as images (exceptions include voice which is audio-based and odor which is chemical-based), the quality of the raw data is also impacted by the characteristics of the camera technology that is used.

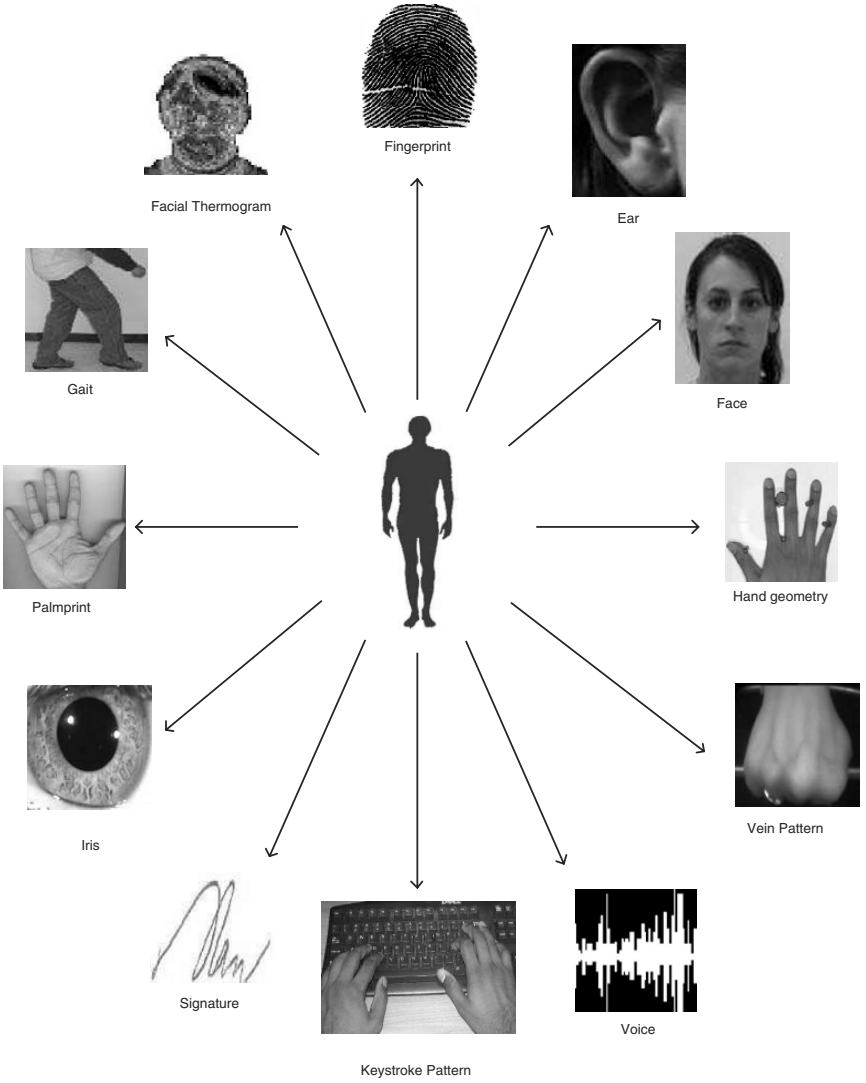


Fig. 1.2. Examples of biometric traits that can be used for authenticating an individual. Physical traits include fingerprint, iris, face and hand geometry while behavioral traits include signature, keystroke dynamics and gait.

2. **Quality assessment and feature extraction module**: The quality of the biometric data acquired by the sensor is first assessed in order to determine its suitability for further processing. Typically, the acquired data is subjected to a signal enhancement algorithm in order to improve its quality. However, in some cases, the quality of the data may be so poor that the user is asked to present the biometric data again. The biometric data is then processed and a set of salient discriminatory features extracted to represent the underlying trait. For example, the position and orientation of minutia points (local ridge and valley anomalies) in a fingerprint image are extracted by the feature extraction module in a fingerprint-based biometric system. During enrollment, this feature set is stored in the database and is commonly referred to as a *template*.
3. **Matching and decision-making module**: The extracted features are compared against the stored templates to generate match scores. In a fingerprint-based biometric system, the number of matching minutiae between the input and the template feature sets is determined and a match score reported. The match score may be moderated by the quality of the presented biometric data. The matcher module also encapsulates a decision making module, in which the match scores are used to either validate a claimed identity or provide a ranking of the enrolled identities in order to identify an individual.
4. **System database module**: The database acts as the repository of biometric information. During the enrollment process, the feature set extracted from the raw biometric sample (i.e., the template) is stored in the database (possibly) along with some biographic information (such as name, Personal Identification Number (PIN), address, etc.) characterizing the user. The data capture during the enrollment process may or may not be supervised by a human depending on the application. For example, a user attempting to create a new computer account in her biometric-enabled workstation may proceed to enroll her biometrics without any supervision; a person desiring to use a biometric-enabled ATM, on the other hand, will have to enroll her biometrics in the presence of a bank officer after presenting her non-biometric credentials.

The template of a user can be extracted from a single biometric sample, or generated by processing multiple samples. Thus, the minutiae template of a finger may be extracted after mosaicing multiple samples of the same finger. Some systems store multiple templates in order to account for the intra-class variations associated with a user. Face recognition systems, for instance, may store multiple templates of an individual, with each template corresponding to a different facial pose with respect to the camera. Depending on the application, the template can be stored in the central database of the biometric system or be recorded on a token (e.g., smart card) issued to the individual.

In the face recognition literature, the raw biometric images stored in the database are often referred to as *gallery images* while those acquired during authentication are known as *probe images*. These are synonymous with the terms *stored images* and *query* or *input images*, respectively.

1.3 Verification versus identification

Depending on the application context, a biometric system may operate either in the verification or identification mode (see Figure 1.3). In the verification mode, the system validates a person's identity by comparing the captured biometric data with her own biometric template(s) stored in the system database. In such a system, an individual who desires to be recognized claims an identity, usually via a PIN, a user name or a smart card, and the system conducts a one-to-one comparison to determine whether the claim is true or not (e.g., "Does this biometric data belong to Bob?"). Verification is typically used for positive recognition, where the aim is to prevent multiple people from using the same identity.

In the identification mode, the system recognizes an individual by searching the templates of all the users in the database for a match. Therefore, the system conducts a one-to-many comparison to establish an individual's identity (or fails if the subject is not enrolled in the system database) without the subject having to claim an identity (e.g., "Whose biometric data is this?"). Identification is a critical component in negative recognition applications where the system establishes whether the person is who she (implicitly or explicitly) denies to be. The purpose of negative recognition is to prevent a single person from using multiple identities. Identification may also be used in positive recognition for convenience (the user is not required to claim an identity). While traditional methods of personal recognition such as passwords, PINs, keys, and tokens may work for positive recognition, negative recognition can only be established through biometrics.

1.4 Performance of a biometric system

Unlike password-based systems, where a *perfect* match between two alphanumeric strings is necessary in order to validate a user's identity, a biometric system seldom encounters two samples of a user's biometric trait that result in exactly the same feature set. This is due to imperfect sensing conditions (e.g., noisy fingerprint due to sensor malfunction), alterations in the user's biometric characteristic (e.g., respiratory ailments impacting speaker recognition), changes in ambient conditions (e.g., inconsistent illumination levels in face recognition) and variations in the user's interaction with the sensor (e.g., occluded iris or partial fingerprints). Thus, seldom do two feature sets originating from the same biometric trait of a user look exactly the same. In

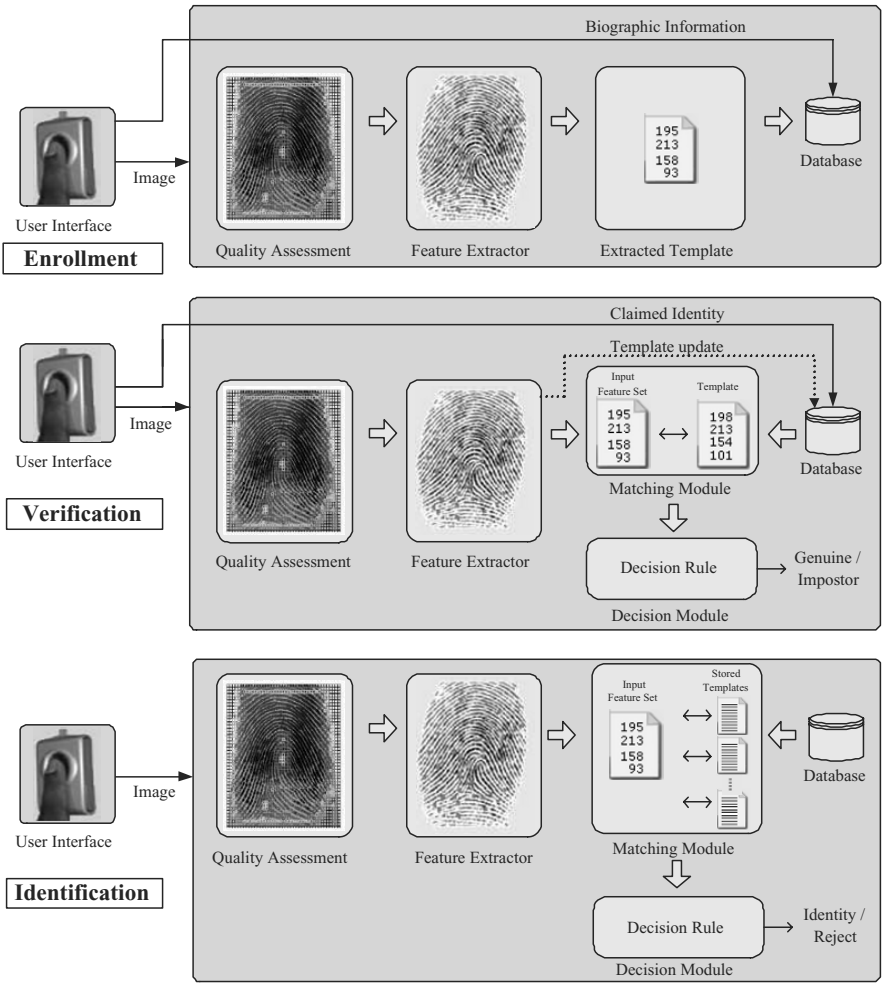


Fig. 1.3. Enrollment and recognition (verification and identification) stages of a biometric system. The quality assessment module determines if the sensed data can be effectively used by the feature extractor. Note that the process of quality assessment in itself may entail the extraction of some features from the sensed data.

fact, a perfect match between two feature sets might indicate the possibility that a replay attack is being launched against the system. The variability observed in the biometric feature set of an individual is referred to as *intra*-class variation, and the variability between feature sets originating from two different individuals is known as *inter*-class variation. A useful feature set exhibits small intra-class variation and large inter-class variation.

The degree of similarity between two biometric feature sets is indicated by a similarity score. A similarity match score is known as a *genuine* or *authentic* score if it is a result of matching two samples of the same biometric trait of a user. It is known as an *impostor* score if it involves comparing two biometric samples originating from different users. An impostor score that exceeds the threshold η results in a false accept (or, a false match), while a genuine score that falls below the threshold η results in a false reject (or, a false non-match). The *False Accept Rate (FAR)* (or, the False Match Rate (FMR)) of a biometric system can therefore be defined as the fraction of impostor scores exceeding the threshold η. Similarly, the *False Reject Rate (FRR)* (or, the False Non-match Rate (FNMR))[5] of a system may be defined as the fraction of genuine scores falling below the threshold η. The *Genuine Accept Rate (GAR)* is the fraction of genuine scores exceeding the threshold η. Therefore,

$$GAR = 1 - FRR. \tag{1.1}$$

Regulating the value of η changes the FRR and the FAR values, but for a given biometric system, it is not possible to decrease both these errors simultaneously.

The FAR and FRR at various values of η can be summarized using a Detection Error Tradeoff (DET) curve [21] that plots the FRR against the FAR at various thresholds on a *normal deviate* scale and interpolates between these points (Figure 1.4(a)). When a linear, logarithmic or semi-logarithmic scale is used to plot these error rates, then the resulting graph is known as a Receiver Operating Characteristic (ROC) curve [7]. In many instances, the ROC curve plots the GAR (rather than the FRR) against the FAR (see Figure 1.4(b) and (c)). The primary difference between the DET and ROC curves is the use of the normal deviate scale in the former.

It is important to note that the occurrence of false accepts and false rejects is not evenly distributed across the users of a biometric system. There are inherent differences in the "recognizability" of different users. Doddington et al. [6] identify four categories of biometric users based on these inherent differences. Although this categorization (more popularly known as "Doddington's zoo") was originally made in the context of speaker recognition, it is applicable to other biometric modalities as well.

1. Sheep represent users whose biometric feature sets are very distinctive and exhibit low intra-class variations. Therefore, these users are expected to have low false accept and false reject errors.
2. Goats refer to users who are prone to false rejects. The biometric feature sets of such users typically exhibit large intra-class variations.

[5] It behooves us to point out that, strictly speaking, FMR and FNMR are not always synonymous with FAR and FRR, respectively (see [20] and [19]). However, in this book we treat them as being equivalent.

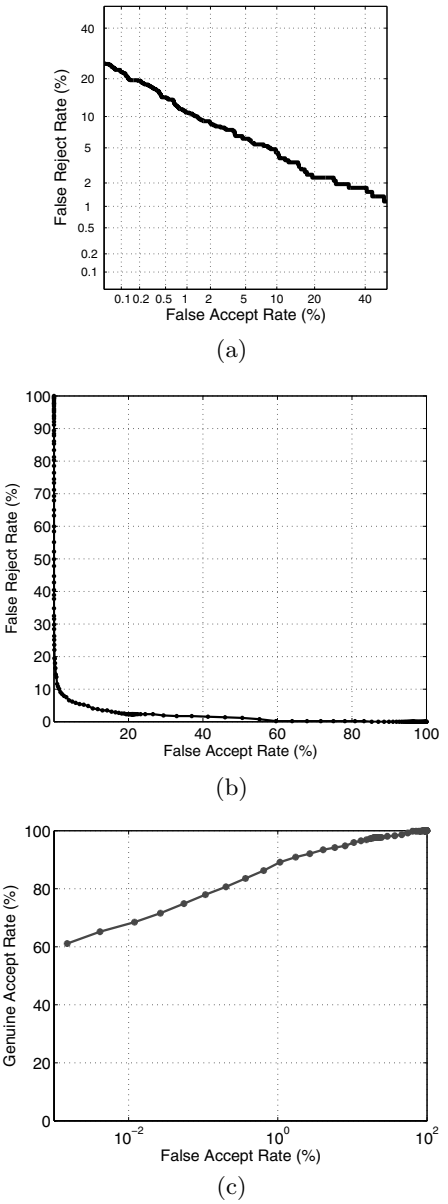


Fig. 1.4. The performance of a biometric system can be summarized using DET and ROC curves. In this example, the performance curves are computed using the match scores of the `Face-G` matcher from the NIST BSSR1 database [25]. The graph in (a) shows a DET curve that plots FRR against FAR in the normal deviate scale. In (b) a ROC curve plots FRR against FAR in the linear scale, while in (c) a ROC curve plots GAR against FAR in a semi-logarithmic scale.

3. Lambs are users whose biometric feature set overlaps extensively with those of other individuals. The biometric feature sets of these users have low inter-class variations. Thus, a randomly chosen user (from the target population) has a high probability of being accepted as a lamb than as a sheep. The false accept rate associated with these users is typically high.
4. Wolves indicate individuals who are successful in manipulating their biometric trait (especially behavioral traits) in order to impersonate legitimately enrolled users of a system. Therefore, these users can increase the false accept rate of the system.

Doddington et al. [6] discuss the use of statistical testing procedures to detect the presence of goats, lambs and wolves in a voice biometric system. A combination of the F-test, Kruskal Wallis test and Durbin test is used to establish the occurrence of these categories of users in the 1998 NIST database of speech segments that was used in the evaluation of speaker recognition algorithms (`http://www.nist.gov/speech/tests/spk/1998/current_plan.htm`).

Besides the two types of errors (viz., false accept and false reject) indicated above, a biometric system can encounter other types of failures as well. The *Failure to Acquire (FTA)* (also known as Failure to Capture (FTC)) rate denotes the proportion of times the biometric device fails to capture a sample when the biometric characteristic is presented to it. This type of error typically occurs when the device is not able to locate a biometric signal of sufficiently good quality (e.g., an extremely faint fingerprint or an occluded face image). The FTA rate is also impacted by sensor wear and tear. Thus, periodic sensor maintenance is instrumental for the efficient functioning of a biometric system. The *Failure to Enroll (FTE)* rate denotes the proportion of users that cannot be successfully enrolled in a biometric system. User training may be necessary to ensure that an individual interacts with a biometric system appropriately in order to facilitate the acquisition of good quality biometric data. This necessitates the design of robust and efficient user interfaces that can assist an individual both during enrollment and recognition.

There is a tradeoff between the FTE rate and the perceived system accuracy as measured by FAR/FRR. FTE errors typically occur when the system rejects poor quality inputs during enrollment; consequently, if the threshold on quality is high, the system database contains only good quality templates and the perceived system accuracy improves. Because of the interdependence among the failure rates and error rates, all these rates (i.e., FTE, FTC, FAR, FRR) constitute important performance specifications of a biometric system, and should be reported during system evaluation along with the target population using the system.

The performance of a biometric system may also be summarized using other single-valued measures such as the Equal Error Rate (EER) and the d-prime value. The EER refers to that point in a DET curve where the FAR equals the FRR; a lower EER value, therefore, indicates better performance.

The d-prime value (d') measures the separation between the means of the genuine and impostor probability distributions in standard deviation units and is defined as,

$$d' = \frac{\sqrt{2} \mid \mu_{genuine} - \mu_{impostor} \mid}{\sqrt{\sigma^2_{genuine} + \sigma^2_{impostor}}},$$

where the μ's and σ's are the means and standard deviations, respectively, of the genuine and impostor distributions. A higher d-prime value indicates better performance. If the genuine and impostor distributions indeed follow a normal (Gaussian) distribution with equal variance (a very unlikely situation in the practical biometric domain), then d' reduces to the normal deviate value [35]. Poh and Bengio [31] introduce another single-valued measure known as F-Ratio which is defined as,

$$\text{F-ratio} = \frac{\mu_{genuine} - \mu_{impostor}}{\sigma_{genuine} + \sigma_{impostor}}.$$

If the genuine and impostor distributions are Gaussian, then the EER and F-ratio are related according to the following expression:

$$\text{EER} = \frac{1}{2} - \frac{1}{2}\text{erf}\left(\frac{\text{F-ratio}}{\sqrt{2}}\right),$$

where

$$\text{erf}(x) = \frac{2}{\sqrt{\pi}} \int_0^x e^{-t^2} dt.$$

In the case of identification, the input feature set is compared against all templates residing in the database in order to determine the top match (i.e, the best match). The top match can be determined by examining the match scores pertaining to all the comparisons and reporting the identity of the template corresponding to the largest similarity score. The *identification rate* indicates the proportion of times a previously enrolled individual is successfully mapped to the correct identity in the system. Here, we assume that the question being asked is, "Does the top match correspond to the correct identity?" An alternate question could be, "Does any one of the top k matches correspond to the correct identity?" (see [23]). The rank-k identification rate, R_k, indicates the proportion of times the correct identity occurs in the top k matches as determined by the match score. Rank-k performance can be summarized using the Cumulative Match Characteristic (CMC) curve ([23]) that plots R_k against k, for $k = 1, 2, \ldots M$ with M being the number of enrolled users. The relationship between CMC and DET/ROC curves has been discussed by Grother and Phillips [9], and Bolle at al. [1].

The biometric of choice for a particular application is primarily dictated by the error rates and failure rates discussed above. Other factors such as the

cost of the system, throughput rate, user acceptance, ease of use, robustness of the sensor, etc. also determine the suitability of a biometric system for an application.

1.5 Applications of biometrics

Establishing the identity of a person with high confidence is becoming critical in a number of applications in our vastly interconnected society. Questions like "Is she really who she claims to be?", "Is this person authorized to use this facility?" or "Is he in the watchlist posted by the government?" are routinely being posed in a variety of scenarios ranging from issuing a driver's licence to gaining entry into a country. The need for reliable user authentication techniques has increased in the wake of heightened concerns about security, and rapid advancements in networking, communication and mobility. Thus, biometrics is being increasingly incorporated in several different applications. These applications can be categorized into three main groups (see Table 1.1):

1. Commercial applications such as computer network login, electronic data security, e-commerce, Internet access, ATM or credit card use, physical access control, mobile phone, PDA, medical records management, distance learning, etc.
2. Government applications such as national ID card, managing inmates in a correctional facility, driver's license, social security, welfare-disbursement, border control, passport control, etc.
3. Forensic applications such as corpse identification, criminal investigation, parenthood determination, etc.

Table 1.1. Authentication solutions employing biometrics can be used in a variety of applications which depend on reliable user authentication mechanisms.

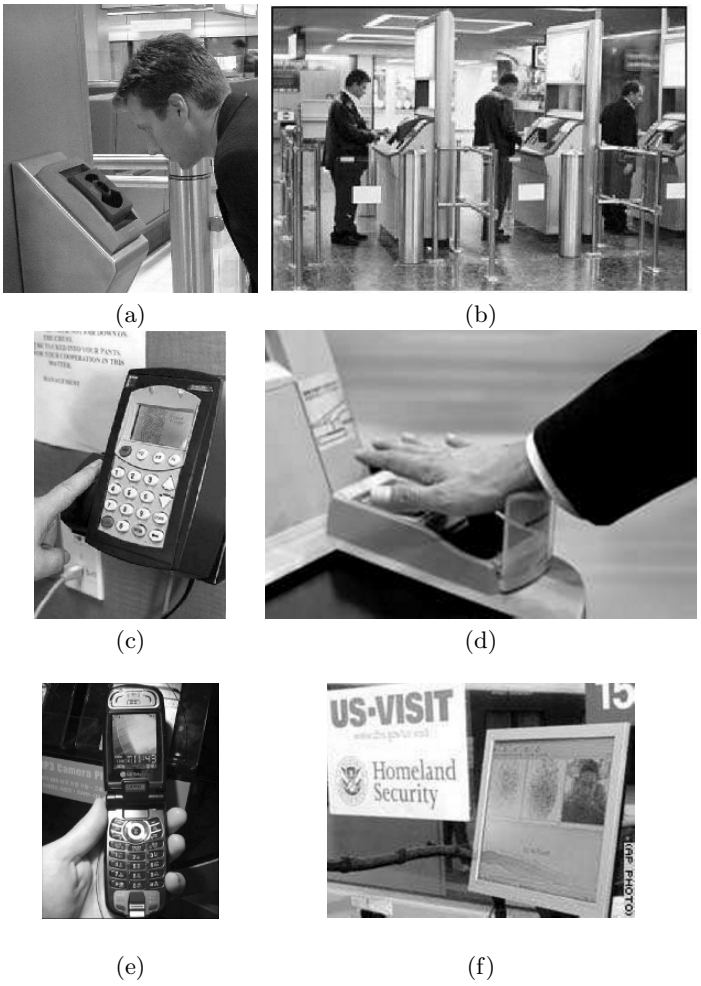
FORENSICS	**GOVERNMENT**	**COMMERCIAL**
Corpse identification	National ID card	ATM
Criminal investigation	Drivers license; voter registration	Access control; computer login
Parenthood determination	Welfare disbursement	Mobile phone
Missing children	Border crossing	E-commerce; Internet; banking; smart card

Examples of a few applications where biometrics is being used for authenticating individuals are presented below (also see Figure 1.5).

1. The *Schiphol Privium* scheme at Amsterdam's Schipol airport employs iris-scan smart cards to speed up the immigration procedure. Passengers

who are voluntarily enrolled in this scheme insert their smart card at the gate and peek into a camera; the camera acquires the eye image of the traveler and processes it to locate the iris, and computes the Iriscode [3]; the computed Iriscode is compared with the data residing in the smart card to complete user verification. A similar scheme is also being used to verify the identity of Schiphol airport employees working in high-security areas. This is a good example of a biometric system that is being used to enhance user convenience while improving security.

2. The Ben Gurion International Airport at Tel Aviv employs automated hand geometry-based identification kiosks to enable Israeli citizens and frequent international travelers to rapidly go through the passport inspection process. Currently more than 160,000 Israeli citizens are enrolled in this program. The kiosk-based system uses the credit card of the traveler to begin the verification process. The hand geometry information is then used for validating the traveler's identity and ensuring that the individual is not a security hazard. The automated inspection process takes less than 20 seconds and has considerably reduced the waiting time for passengers.
3. Some financial institutions in Japan have installed palm-vein authentication systems in their ATMs to help validate the identity of a customer intending to conduct a transaction. A contactless sensor is used to image the vein pattern pertaining to the customer's palm using a near infrared lighting source. Thus, a person does not have to directly place the palm on the device.
4. Kroger, a US supermarket chain, has deployed fingerprint scanners in some of its stores in order to help customers cash payroll checks or render payment after a purchase. Interested customers can enroll their index finger along with details of their credit/debit card (or electronic check); the customer's driver's licence is used to validate the identity during the time of enrollment.
5. The United States Visitor and Immigration Status Indicator Technology (US-VISIT) is a border security system that has been deployed at 115 airports, 15 seaports and in the secondary inspection areas of the 50 busiest land ports of entry. Foreign visitors entering the United States have their left and right index fingers scanned by a fingerprint sensor. The biometric data acquired is used to validate an individual's travel documents at the port of entry. A biometric exit procedure has also been adopted in some airports and seaports to facilitate a visitor's future trips to the country. Although two-print information is currently being used, the system might employ all ten fingers of a person in the future; this would ensure that the US-VISIT fingerprint database is compatible with the ten-print database maintained by the FBI in its Integrated Automated Fingerprint Identification System (IAFIS - see `http://www.fbi.gov/hq/cjisd/iafis.htm`).



(a) (b) (c) (d) (e) (f)

Fig. 1.5. Biometric systems are being deployed in various applications. (a) The Schiphol Privium program at the Amsterdam airport uses iris scans to validate the identity of a traveler (`www.cl.cam.ac.uk`). (b) The Ben Gurion airport in Tel Aviv uses Express Card entry kiosks fitted with hand geometry systems for security and immigration (`www.airportnet.org`). (c) A few Kroger stores in Texas use fingerprint verification systems that enable customers to render payment at the check-out counter. (`www.detnews.com`). (d) Contactless palm-vein systems have been installed in some ATMs in Japan (`www.fujitsu.com`). (e) A cell-phone that validates authorized users using fingerprints and allows them access to functionalities such as mobile-banking (`www.mobileburn.com`). (f) The US-VISIT program currently employs two-print information to validate the travel documents of visitors to the United States (`www.dhs.gov`).

1.6 Biometric characteristics

A number of biometric characteristics are being used in various applications. Each biometric has its pros and cons and, therefore, the choice of a biometric trait for a particular application depends on a variety of issues besides its matching performance (Table 1.2). Jain et al. [12] have identified seven factors that determine the suitability of a physical or a behavioral trait to be used in a biometric application.

1. **Universality**: Every individual accessing the application should possess the trait.
2. **Uniqueness**: The given trait should be sufficiently different across individuals comprising the population.
3. **Permanence**: The biometric trait of an individual should be sufficiently invariant over a period of time with respect to the matching algorithm. A trait that changes significantly over time is not a useful biometric.
4. **Measurability**: It should be possible to acquire and digitize the biometric trait using suitable devices that do not cause undue inconvenience to the individual. Furthermore, the acquired raw data should be amenable to processing in order to extract representative feature sets.
5. **Performance**: The recognition accuracy and the resources required to achieve that accuracy should meet the constraints imposed by the application.
6. **Acceptability**: Individuals in the target population that will utilize the application should be willing to present their biometric trait to the system.
7. **Circumvention**: This refers to the ease with which the trait of an individual can be imitated using artifacts (e.g., fake fingers), in the case of physical traits, and mimicry, in the case of behavioral traits.

No single biometric is expected to effectively meet all the requirements (e.g., accuracy, practicality, cost) imposed by all applications (e.g., Digital Rights Management (DRM), access control, welfare distribution). In other words, no biometric is *ideal* but a number of them are *admissible*. The relevance of a specific biometric to an application is established depending upon the nature and requirements of the application, and the properties of the biometric characteristic. A brief introduction to some of the commonly used biometric characteristics is given below:

1. **Face**: Face recognition is a non-intrusive method, and facial attributes are probably the most common biometric features used by humans to recognize one another. The applications of facial recognition range from a static, controlled "mug-shot" authentication to a dynamic, uncontrolled face identification in a cluttered background. The most popular approaches to face recognition [17] are based on either (i) the location and shape of facial attributes, such as the eyes, eyebrows, nose, lips, and chin and their spatial relationships, or (ii) the overall (global) analysis of the face image

that represents a face as a weighted combination of a number of canonical faces. While the authentication performance of the face recognition systems that are commercially available is reasonable [30], they impose a number of restrictions on how the facial images are obtained, often requiring a fixed and simple background with controlled illumination. These systems also have difficulty in matching face images captured from two different views, under different illumination conditions, and at different times. It is questionable whether the face itself, without any contextual information, is a sufficient basis for recognizing a person from a large number of identities with an extremely high level of confidence. In order for a facial recognition system to work well in practice, it should automatically (i) detect whether a face is present in the acquired image; (ii) locate the face if there is one; and (iii) recognize the face from a general viewpoint (i.e., from any pose) under different ambient conditions.

2. **Fingerprint**: Humans have used fingerprints for personal identification for many decades. The matching (i.e., identification) accuracy using fingerprints has been shown to be very high [37]. A fingerprint is the pattern of ridges and valleys on the surface of a fingertip whose formation is determined during the first seven months of fetal development. It has been empirically determined that the fingerprints of identical twins are different and so are the prints on each finger of the same person [19]. Today, most fingerprint scanners cost less than US $50 when ordered in large quantities and the marginal cost of embedding a fingerprint-based biometric in a system (e.g., laptop computer) has become affordable in a large number of applications. The accuracy of the currently available fingerprint recognition systems is adequate for authentication systems in several applications, particularly forensics. Multiple fingerprints of a person (e.g., ten-prints used in IAFIS) provide additional information to allow for large-scale identification involving millions of identities. One problem with large-scale fingerprint recognition systems is that they require a huge amount of computational resources, especially when operating in the identification mode. Finally, fingerprints of a small fraction of the population may be unsuitable for automatic identification because of genetic factors, aging, environmental or occupational reasons (e.g., manual workers may have a large number of cuts and bruises on their fingerprints that keep changing).
3. **Hand geometry**: Hand geometry recognition systems are based on a number of measurements taken from the human hand, including its shape, size of palm, and the lengths and widths of the fingers [39]. Commercial hand geometry-based authentication systems have been installed in hundreds of locations around the world. The technique is very simple, relatively easy to use, and inexpensive. Environmental factors such as dry weather or individual anomalies such as dry skin do not appear to adversely affect the authentication accuracy of hand geometry-based systems. However, the geometry of the hand is not known to be very distinc-

tive and hand geometry-based recognition systems cannot be scaled up for systems requiring identification of an individual from a large population. Furthermore, hand geometry information may not be invariant during the growth period of children. In addition, an individual's jewelry (e.g., rings) or limitations in dexterity (e.g., from arthritis), may pose challenges in extracting the correct hand geometry information. The physical size of a hand geometry-based system is large, and it cannot be embedded in certain devices like laptops. There are authentication systems available that are based on measurements of only a few fingers (typically, index and middle) instead of the entire hand. These devices are smaller than those used for hand geometry, but still much larger than those used for procuring certain other traits (e.g., fingerprint, face, voice).

4. **Palmprint**: The palms of the human hands contain pattern of ridges and valleys much like the fingerprints. The area of the palm is much larger than the area of a finger and, as a result, palmprints are expected to be even more distinctive than the fingerprints [38]. Since palmprint scanners need to capture a large area, they are bulkier and more expensive than the fingerprint sensors. Human palms also contain additional distinctive features such as principal lines and wrinkles that can be captured even with a lower resolution scanner, which would be cheaper. Finally, when using a high-resolution palmprint scanner, all the features of the hand such as geometry, ridge and valley features (e.g., minutiae and singular points such as deltas), principal lines, and wrinkles may be combined to build a highly accurate biometric system.
5. **Iris**: The iris is the annular region of the eye bounded by the pupil and the sclera (white of the eye) on either side. The visual texture of the iris is formed during fetal development and stabilizes during the first two years of life (the pigmentation, however, continues changing over an extended period of time. The complex iris texture carries very distinctive information useful for personal recognition [4]. The accuracy and speed of currently deployed iris-based recognition systems is promising and support the feasibility of large-scale identification systems based on iris information. Each iris is distinctive and even the irises of identical twins are different. It is possible to detect contact lenses printed with a fake iris (see [3]). The hippus movement of the eye may also be used as a measure of liveness for this biometric. Although early iris-based recognition systems required considerable user participation and were expensive, the newer systems have become more user-friendly and cost-effective [26, 8]. While iris systems have a very low False Accept Rate (FAR) compared to other biometric traits, the False Reject Rate (FRR) of these systems can be rather high [11].
6. **Keystroke**: It is hypothesized that each person types on a keyboard in a characteristic way. This biometric is not expected to be unique to each individual but it may be expected to offer sufficient discriminatory information to permit identity verification [22]. Keystroke dynamics is a be-

havioral biometric; one may expect to observe large intra-class variations in a person's typing patterns due to changes in emotional state, position of the user with respect to the keyboard, type of keyboard used, etc. The keystrokes of a person could be monitored unobtrusively as that person is keying in information. This biometric permits "continuous verification" of an individual's identity over a session after the person logs in using a stronger biometric such as fingerprint or iris.

7. **Signature**: The way a person signs her name is known to be a characteristic of that individual [24, 16]. Although signatures require contact with the writing instrument and an effort on the part of the user, they have been accepted in government, legal, and commercial transactions as a method of authentication. With the proliferation of PDAs and Tablet PCs, on-line signature may emerge as the biometric of choice in these devices. Signature is a behavioral biometric that changes over a period of time and is influenced by the physical and emotional conditions of the signatories. Signatures of some people vary substantially: even successive impressions of their signature are significantly different. Further, professional forgers may be able to reproduce signatures that fool the signature verification system [10].
8. **Voice**: Voice is a combination of physical and behavioral biometric characteristics [2]. The physical features of an individual's voice are based on the shape and size of the appendages (e.g., vocal tracts, mouth, nasal cavities, and lips) that are used in the synthesis of the sound. These physical characteristics of human speech are invariant for an individual, but the behavioral aspect of the speech changes over time due to age, medical conditions (such as common cold), emotional state, etc. Voice is also not very distinctive and may not be appropriate for large-scale identification. A text-dependent voice recognition system is based on the utterance of a fixed predetermined phrase. A text-independent voice recognition system recognizes the speaker independent of what she speaks. A text-independent system is more difficult to design than a text-dependent system but offers more protection against fraud. A disadvantage of voice-based recognition is that speech features are sensitive to a number of factors such as background noise. Speaker recognition is most appropriate in telephone-based applications but the voice signal is typically degraded in quality by the communication channel.
9. **Gait**: Gait refers to the manner in which a person walks, and is one of the few biometric traits that can be used to recognize people at a distance. Therefore, this trait is very appropriate in surveillance scenarios where the identity of an individual can be surreptitiously established. Most gait recognition algorithms attempt to extract the human silhouette in order to derive the spatio-temporal attributes of a moving individual. Hence, the selection of a good model to represent the human body is pivotal to the efficient functioning of a gait recognition system. Some algorithms use the optic flow associated with a set of dynamically extracted moving points

on the human body to describe the gait of an individual [27]. Gait-based systems also offer the possibility of tracking an individual over an extended period of time. However, the gait of an individual is affected by several factors including the choice of footwear, nature of clothing, affliction of the legs, walking surface, etc.

Table 1.2. The false accept and false reject error rates (FAR and FRR) associated with the fingerprint, face, voice and iris modalities. The accuracy estimates of biometric systems depend on a number of test conditions including the sensor employed, acquisition protocol used, subject disposition, number of subjects, number of biometric samples per subject, demographic profile of test subjects, subject habituation, time lapse between data acquisition, etc.

Biometric Trait	**Test**	**Test Conditions**	**False Reject Rate**	**False Accept Rate**
Fingerprint	FVC 2004 [18]	Exaggerated skin distortion, rotation	2%	2%
Fingerprint	FpVTE 2003 [37]	US Government operational data	0.1%	1%
Face	FRVT 2002 [30]	Varied lighting, outdoor/indoor, time	10%	1%
Voice	NIST 2004 [33]	Text independent, multi-lingual	5-10%	2-5%
Iris	ITIRT 2005 [11]	Indoor environment, multiple visits	0.99%	0.94%

1.7 Summary

Rapid advancements in the field of communications, computer networking and transportation, coupled with heightened concerns about identity fraud and national security, has resulted in a pronounced need for reliable and efficient identity management schemes in a myriad of applications. The process of identity management in the context of a specific application involves the creation, maintenance and obliteration of identities while ensuring that an impostor does not fraudulently gain privileges associated with a legitimately enrolled individual. Traditional authentication techniques based on passwords and tokens are limited in their ability to address issues such as negative recognition and non-repudiation. The advent of biometrics has served to address some of the shortcomings of traditional authentication methods. Biometric systems use the physical and behavioral characteristics of an individual such as fingerprint, face, hand geometry, iris, gait and voice to establish identity.

A broad spectrum of establishments can engage the services of a biometric system including travel and transportation, financial institutions, health care, law enforcement agencies and various government sectors.

The deployment of biometrics in civilian and government applications has raised questions related to the privacy accorded to an enrolled individual [5]. Specifically, questions such as (i) "Will biometric data be used to track people covertly thereby violating their right to privacy?", (ii) "Can the medical condition of a person be surreptitiously elicited from the raw biometric data?", (iii) "Will the acquired biometric data be used only for the intended purpose, or will it be used for previously unexpressed functions, hence resulting in *functionality creep*?", (iv) "Will various biometric databases be linked in order to deduce an individual's social and financial profile?", and (v) "What are the consequences of compromising a user's biometric data?", have advocated societal concerns about the use of biometric solutions in large-scale applications. The promotion of Privacy-Enhancing Technologies (PETs) can assuage some of the legitimate concerns associated with biometric-enabled technology [34, 14]. For example, the use of personal smart cards to store and process the biometric template of an individual can mitigate public concerns related to placing biometric information in a centralized database. Apart from technological solutions to address privacy concerns, government regulations are also required in order to prevent the inappropriate transmission, exchange and processing of biometric data.

References

1. R. Bolle, J. Connell, S. Pankanti, N. Ratha, and A. Senior. The Relationship Between the ROC Curve and the CMC. In *Proceedings of Fourth IEEE Workshop on Automatic Identification Advanced Technologies (AutoID)*, pages 15–20, Buffalo, USA, October 2005.
2. J. P. Campbell. Speaker Recognition: a Tutorial. *Proceedings of the IEEE*, 85(9):1437–1462, September 1997.
3. J. Daugman. Recognizing Persons by their Iris Patterns. In A. K. Jain, R. Bolle, and S. Pankanti, editors, *Biometrics: Personal Identification in Networked Society*, pages 103–122. Kluwer Academic Publishers, London, UK, 1999.
4. J. Daugman. How Iris Recognition Works? *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1):21–30, 2004.
5. S. Davies. Touching Big Brother: How Biometric Technology Will Fuse Flesh and Machine. *Information Technology and People*, 7(4), 1994.
6. G. Doddington, W. Liggett, A. Martin, M. Przybocki, and D. Reynolds. Sheep, Goats, Lambs and Wolves: A Statistical Analysis of Speaker Performance in the NIST 1998 Speaker Recognition Evaluation. In *CD-ROM Proceedings of the Fifth International Conference on Spoken Language Processing (ICSLP)*, Sydney, Australia, November/December 1998.
7. J. Egan. *Signal Detection Theory and ROC Analysis*. Academic Press, New York, 1975.

8. C. L. Fancourt, L. Bogoni, K. J. Hanna, Y. Guo, R. P. Wildes, N. Takahashi, and U. Jain. Iris Recognition at a Distance. In *Fifth International Conference on Audio- and Video-based Biometric Person Authentication (AVBPA)*, pages 1–13, Rye Brook, USA, July 2005.
9. P. Grother and P. J. Phillips. Models of Large Population Recognition Performance. In *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR)*, volume 2, pages 68–75, Washington D.C., USA, June/July 2004.
10. W. R. Harrison. *Suspect Documents, their Scientific Examination.* Nelson-Hall Publishers, 1981.
11. International Biometric Group. Independent Testing of Iris Recognition Technology: Final Report. Available at `http://www.biometricgroup.com/reports/public/ITIRT.html`, May 2005.
12. A. K. Jain, R. Bolle, and S. Pankanti, editors. *Biometrics: Personal Identification in Networked Society.* Kluwer Academic Publishers, 1999.
13. A. K. Jain, A. Ross, and S. Prabhakar. An Introduction to Biometric Recognition. *IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics*, 14(1):4–20, January 2004.
14. S. Kenny and J. J. Borking. The Value of Privacy Engineering. *The Journal of Information, Law and Technology (JILT)*, 7(1), 2002.
15. S. Kent and L. Millett. *Who Goes There? Authentication Technologies through the Lens of Privacy.* National Academy Press, 2003.
16. L. Lee, T. Berger, and E. Aviczer. Reliable On-Line Human Signature Verification Systems. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 18(6):643–647, June 1996.
17. S. Z. Li and Anil K. Jain, editors. *Handbook of Face Recognition.* Springer-Verlag, 2005.
18. D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain. FVC2004: Third Fingerprint Verification Competition. In *Proceedings of International Conference on Biometric Authentication (ICBA)*, pages 1–7, Hong Kong, China, July 2004.
19. D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar. *Handbook of Fingerprint Recognition.* Springer-Verlag, 2003.
20. A. J. Mansfield and J. L. Wayman. Best Practices in Testing and Reporting Performance of Biometric Devices, Version 2.01. Technical Report NPL Report CMSC 14/02, National Physical Laboratory, August 2002.
21. A. Martin, G. Doddington, T. Kam, M. Ordowski, and M. Przybocki. The DET Curve in Assessment of Detection Task Performance. In *Proceedings of the Fifth European Conference on Speech Communication and Technology*, volume 4, pages 1895–1898, Rhodes, Greece, September 1997.
22. F. Monrose and A. Rubin. Authentication Via Keystroke Dynamics. In *Proceedings of Fourth ACM Conference on Computer and Communications Security*, pages 48–56, Zurich, Switzerland, April 1997.
23. H. Moon and P. J. Phillips. Computational and Performance Aspects of PCA-based Face Recognition Algorithms. *Perception*, 30(5):303–321, 2001.
24. V. S. Nalwa. Automatic On-Line Signature Verification. *Proceedings of the IEEE*, 85(2):215–239, February 1997.
25. National Institute of Standards and Technology. NIST Biometric Scores Set. Available at `http://http://www.itl.nist.gov/iad/894.03/biometricscores`.

26. M. Negin, T. A. Chmielewski, M. Salganicoff, T. A. Camus, U. M. C. von Seelan, P. L. Venetianer, and G. G. Zhang. An Iris Biometric System for Public and Personal Use. *IEEE Computer*, 33(2):70–75, February 2000.
27. M. S. Nixon, J. N. Carter, D. Cunado, P. S. Huang, and S. V. Stevenage. Automatic Gait Recognition. In A. K. Jain, R. Bolle, and S. Pankanti, editors, *Biometrics: Personal Identification in Networked Society*, pages 231–249. Kluwer Academic Publishers, London, UK, 1999.
28. L. O'Gorman. Seven Issues with Human Authentication Technologies. In *Proc. of Workshop on Automatic Identification Advanced Technologies (AutoID)*, pages 185–186, Tarrytown, USA, March 2002.
29. L. O'Gorman. Comparing Passwords, Tokens, and Biometrics for User Authentication. *Proceedings of the IEEE*, 91(12):2019–2040, December 2003.
30. P. J. Phillips, P. Grother, R. J. Micheals, D. M. Blackburn, E. Tabassi, and J. M. Bone. FRVT2002: Overview and Summary. Available at `http://www.frvt.org/FRVT2002`, March 2003.
31. N. Poh and S. Bengio. An Investigation of F-ratio Client-Dependent Normalisation on Biometric Authentication Tasks. In *Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, volume 1, pages 721–724, Philadelphia, USA, March 2005.
32. S. Prabhakar, S. Pankanti, and A. K. Jain. Biometric Recognition: Security and Privacy Concerns. *IEEE Security and Privacy Magazine*, 1(2):33–42, March-April 2003.
33. M. Przybocki and A. Martin. NIST Speaker Recognition Evaluation Chronicles. In *Odyssey: The Speaker and Language Recognition Workshop*, pages 12–22, Toledo, Spain, May 2004.
34. M. Rejman-Greene. Privacy Issues in the Application of Biometrics: A European Perspective. In J. L. Wayman, A. K. Jain, D. Maltoni, and D. Maio, editors, *Biometric Systems: Technology, Design and Performance Evaluation*, pages 335–359. Springer, 2005.
35. J. A. Swets, W. P. Tanner, and T. G. Birdsall. Decision Processes in Perception. *Psychological Review*, 68(5):301–340, 1961.
36. J. L. Wayman, A. K. Jain, D. Maltoni, and D. Maio, editors. *Biometric Systems: Technology, Design and Performance Evaluation*. Springer, 2005.
37. C. Wilson, A. R. Hicklin, M. Bone, H. Korves, P. Grother, B. Ulery, R. Micheals, M. Zoepfl, S. Otto, and C. Watson. Fingerprint Vendor Technology Evaluation 2003: Summary of Results and Analysis Report. NIST Technical Report NISTIR 7123, National Institute of Standards and Technology, June 2004.
38. D. Zhang, A. W.-K. Kong, J. You, and M. Wong. Online Palmprint Identification. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 25(9):1041–1050, 2003.
39. R. Zunkel. Hand Geometry Based Authentication. In A. K. Jain, R. Bolle, and S. Pankanti, editors, *Biometrics: Personal Identification in Networked Society*, pages 87–102. Kluwer Academic Publishers, London, UK, 1999.