1 INTRODUCTION TO BIOMETRICS

Anil Jain
Michigan State University
East Lansing, MI
jain@cse.msu.edu

Ruud Bolle and Sharath Pankanti
IBM T. J. Watson Research Center
Yorktown Heights, NY
{bolle,sharat}@us.ibm.com

Abstract *Biometrics deals with identification of individuals based on their biological or behavioral characteristics. Biometrics has lately been receiving attention in popular media. it is widely believed that biometrics will become a significant component of the identification technology as (i) the prices of biometrics sensors continue to fall, (ii) the underlying technology becomes more mature, and (iii) the public becomes aware of the strengths and limitations of biometrics. This chapter provides an overview of the biometrics technology and its applications and introduces the research issues underlying the biometrics.*

Keywords: *Biometrics, identification, verification, access control, authentication, security, research issues, evaluation, privacy.*

1. Introduction

Associating an identity with an individual is called personal identification. The problem of resolving the identity of a person can be categorized into two fundamentally distinct types of problems with different inherent complexities: (i) verification and (ii) recognition (more popularly known as identification[1]).

[1] The term identification is used in this book either to refer to the general problem of identifying individuals (identification and authentication) or to refer to the specific problem of identifying an individual from a database which involves one to many search. We rely on the context to disambiguate the reference.

Verification (authentication) refers to the problem of confirming or denying a person's claimed identity (Am I who I claim I am?). Identification (Who am I?) refers to the problem of establishing a subject's identity - either from a set of already known identities (closed identification problem) or otherwise (open identification problem). The term *positive personal identification* typically refers (in both verification as well as identification context) to identification of a person with high certainty.

Human race has come a long way since its inception in small tribal primitive societies where every person in the community knew every other person. In today's complex, geographically mobile, increasingly electronically inter-connected information society, accurate identification is becoming very important and the problem of identifying a person is becoming ever increasingly difficult. A number of situations require an identification of a person in our society: have I seen this applicant before? Is this person an employee of this company? Is this individual a citizen of this country? Many situations will even warrant identification of a person at the far end of a communication channel.

2. Opportunities

Accurate identification of a person could deter crime and fraud, streamline business processes, and save critical resources. Here are a few mind boggling numbers: about $1 billion dollars in welfare benefits in the United States are annually claimed by "double dipping" welfare recipients with fraudulent multiple identities [10]. MasterCard estimates the credit card fraud at $450 million per annum which includes charges made on lost and stolen credit cards: unobtrusive positive personal identification of the legitimate ownership of a credit card at the point of sale would greatly reduce the credit card fraud; about 1 billion dollars worth of cellular telephone calls are made by the cellular bandwidth thieves - many of which are made from stolen pins and/or cellular telephones. Again, an identification of the legitimate ownership of the cellular telephones would prevent cellular telephone thieves from stealing the bandwidth. A reliable method of authenticating legitimate owner of an ATM card would greatly reduce ATM related fraud worth approximately $3 billion annually [11]. A positive method of identifying the rightful check payee would also reduce billions of dollars misappropriated through fraudulent encashment of checks each year. A method of positive authentication of each system login would eliminate illegal break-ins into traditionally secure (even federal government) computers. The United States Immigration and Naturalization service stipulates that it could each day detect/deter about 3,000 illegal immigrants crossing the Mexican border without delaying the legitimate people entering the United States if it had a quick way of establishing positive personal identification.

3. Identification Methods

The problem of authentication and identification is very challenging. In a broad sense, establishing an identity (either in a verification context or an identification context) is a very difficult problem; Gertrude Stein's [12] quote "*rose is a rose is a rose is a rose*" summarizes the essence of the difficulty of a positive identification problem: an identity of a person is so much woven into the fabric of everything that a person represents and believes that the answers to the identity of a person transcend the scope of an engineering system and the solutions could (perhaps) only be sought in a philosophical realm. For example, can a brain-dead person be identified as her fully sane counterpart for authenticating an electronic fund transfer? Engineering approach to the (abstract) problem of authentication of a person's identity is to reduce it to the problem of authentication of a concrete entity related to the person (Figure 1.1). Typically, these entities include (i) a person's possession ("*something that you possess*"), e.g., permit physical access to a building to all persons whose identity could be authenticated by possession of a key; (ii) person's knowledge of a piece of information ("*something that you know*"), e.g., permit login access to a system to a person who knows the user-id and a password associated with it. Some systems, e.g., ATMs, use a combination of "something that you have" (ATM card) and "something that you know" (PIN) to establish an identity. The problem with the traditional approaches of identification using possession as a means of identity is that the possessions could be lost, stolen, forgotten, or misplaced. Further, once in control of the identifying possession, by definition, any other "unauthorized" person could abuse the privileges of the authorized user. The problem with using knowledge as an identity authentication mechanism is that it is difficult to remember the passwords/PINs; easily recallable passwords/PINs (e.g., pet's name, spouse's birthday)

Figure 1.1 Prevalent methods of identification based on possession and knowledge: Keys, employee badge, driver license, ATM card, and credit card.

could be easily guessed by the adversaries. It has been estimated that about 25% of the people using ATM cards write their ATM PINs on the ATM card [13], thereby defeating possession/knowledge combination as a means of identification. As a result, these techniques cannot distinguish between an authorized person and an impostor who acquires the knowledge/possession, enabling the access privileges of the authorized person.

Yet another approach to positive identification has been to reduce the problem of identification to the problem of identifying physical characteristics of the person. The characteristics could be either a person's physiological traits, e.g., fingerprints, hand geometry, etc. or her behavioral characteristics, e.g., voice and signature. This method of identification of a person based on his/her physiological/behavioral characteristics is called biometrics[2]. The primary advantage of such an identification method over the methods of identification utilizing "something that you possess" or "something that you know" approach is that a biometrics cannot be misplaced or forgotten; it represents a tangible component of "something that you are". While biometric techniques are not an identification panacea, they, especially, when combined with the other methods of identification, are beginning to provide very powerful tools for problems requiring positive identification.

4. Biometrics

What biological measurements qualify to be a biometric? Any human physiological or behavioral characteristic could be a biometrics provided it has the following desirable properties [15]: (*i*) *universality*, which means that every person should have the characteristic, (*ii*) *uniqueness*, which indicates that no two persons should be the same in terms of the characteristic, (*iii*) *permanence*, which means that the characteristic should be invariant with time, and (*iv*) *collectability*, which indicates that the characteristic can be measured quantitatively. In practice, there are some other important requirements [15,16]: (*i*) *performance*, which refers to the achievable identification accuracy, the resource requirements to achieve an acceptable identification accuracy, and the working or environmental factors that affect the identification accuracy, (*ii*) *acceptability*, which indicates to what extent people are willing to accept the biometric system, and (*iii*) *circumvention*, which refers to how easy it is to fool the system by fraudulent techniques.

5. Biometrics Technology: Overview

No single biometrics is expected to effectively satisfy the needs of all identification (authentication) applications. A number of biometrics have been proposed, researched, and evaluated for identification (authentication) applications. Each biometrics has its strengths and limitations; and accordingly, each biometric appeals

[2] Note the distinction between the terms biometrics and biometry: biometry encompasses a much broader field involving application of statistics to biology and medicine [14].

to a particular identification (authentication) application. A summary of the existing and burgeoning biometric technologies is described in this section.

- Voice
  Voice is a characteristic of an individual [17]. However, it is not expected to be sufficiently unique to permit identification of an individual from a large database of identities (Figure 1.2). Moreover, a voice signal available for authentication is typically degraded in quality by the microphone, communication channel, and digitizer characteristics. Before extracting features, the amplitude of the input signal may be normalized and decomposed into several band-pass frequency channels. The features extracted from each band may be either time-domain or frequency domain features. One of the most commonly used features is cepstral feature - which is a logarithm of the Fourier Transform of the voice signal in each band. The matching strategy may typically employ approaches based on hidden Markov model, vector quantization, or dynamic time warping [17]. Text-dependent speaker verification authenticates the identity of a subject based on a fixed predetermined phrase. Text-independent speaker verification is more difficult and verifies a speaker identity independent of the phrase. Language-independent speaker verification verifies a speaker identity irrespective of the language of the uttered phrase and is even more challenging.

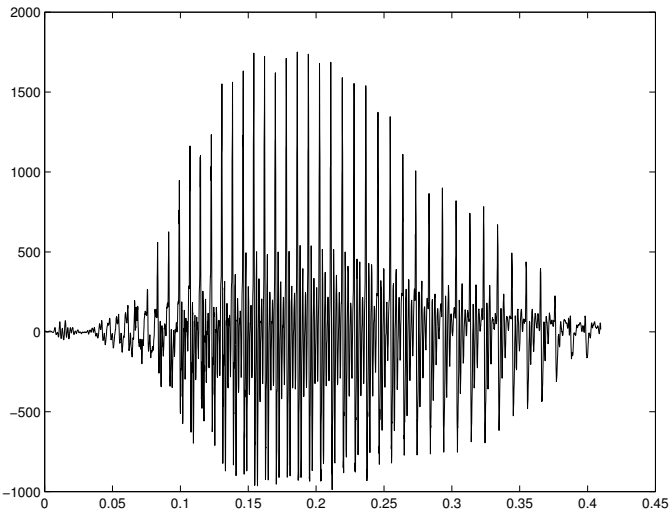


Figure 1.2 Voice signal representing an utterance of the word “seven”. X and Y axes represent time and signal amplitude, respectively.

Voice capture is unobtrusive and voice print is an acceptable biometric in almost all societies. Some applications entail authentication of identity over telephone. In such situations, voice may be the only feasible biometric. Voice is a behavioral biometrics and is affected by a person's health (e.g., cold), stress,

emotions, etc. To extract features which remain invariant in such cases is very difficult. Besides, some people seem to be extraordinarily skilled in mimicking others. A reproduction of an earlier recorded voice can be used to circumvent a voice authentication system in the remote unattended applications. One of the methods of combating this problem is to prompt the subject (whose identity is to be authenticated) to utter a different phrase each time.

- Infrared Facial and Hand Vein Thermograms

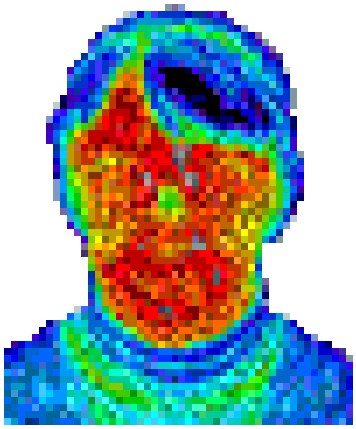


Figure 1.3 Identification based on facial thermograms [1]. The image is obtained by sensing the infrared radiations from the face of a person. The graylevel at each pixel is characteristic of the magnitude of the radiation.

Human body radiates heat and the pattern of heat radiation is a characteristic of each individual body [18]. An infrared sensor could acquire an image indicating the heat emanating from different parts of the body (Figure 1.3). These images are called thermograms. The method of acquisition of the thermal image unobtrusively is akin to the capture of a regular (visible spectrum) photograph of the person. Any part of the body could be used for identification. The absolute values of the heat radiation are dependent upon many extraneous factors and are not completely invariant to the identity of an individual; the raw measurements of heat radiation need to be normalized, e.g., with respect to heat radiating from a landmark feature of the body. The technology could be used for covert identification solutions and could distinguish between identical twins. It is also claimed to provide enabling technology for identifying people under the influence of drugs: the radiation patterns contain signature of each narcotic drug [19]. A thermogram-based system may have to address sensing challenges in uncontrolled environments, where heat emanating surfaces in the vicinity of the body, e.g., room heaters and vehicle exhaust pipes, may drastically affect the image acquisition phase. Infrared facial thermograms seem to be acceptable since their acquisition is a non-contact and non-invasive sensing technique.

Identification systems using facial thermograms are commercially available [1]. A related technology using near infrared imaging [2] is used to scan the back of a clenched fist to determine hand vein structure (Figure 1.4). Infrared sensors are prohibitively expensive which is a factor inhibiting wide spread use of thermograms.

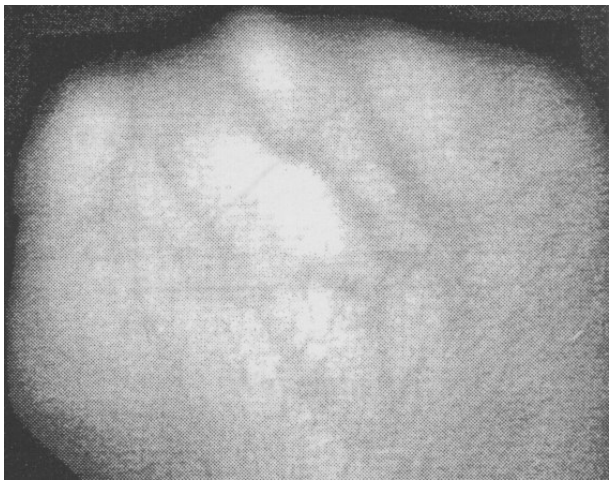


Figure 1.4 Identification based on hand veins [2]. An infrared image of the back of a clenched human fist. The structure of the vasculature could be used for identification.

- Fingerprints

  Fingerprints are graphical flow-like ridges present on human fingers. Their formations depend on the initial conditions of the embryonic development and they are believed to be unique to each person (and each finger). Fingerprints are one of the most mature biometric technologies used in forensic divisions worldwide for criminal investigations and therefore, have a stigma of criminality associated with them. Typically, a fingerprint image is captured in one of two ways: (i) scanning an inked impression of a finger or (ii) using a live-scan fingerprint scanner (Figure 1.5).

  Major representations of the finger are based on the entire image, finger ridges, or salient features derived from the ridges (minutiae). Four basic approaches to identification based on fingerprint are prevalent: (i) the invariant properties of the gray scale profiles of the fingerprint image or a part thereof; (ii) global ridge patterns, also known as fingerprint classes; (iii) the ridge patterns of the fingerprints; (iv) fingerprint minutiae – the features resulting mainly from ridge endings and bifurcations.

(a) (b)

Figure 1.5 A fingerprint image could be captured from the inked impression of a finger or directly imaging a finger using frustrated total internal reflection technology. The former is called an inked fingerprint (a) and the latter is called a live-scan fingerprint (b).

- Face

Face is one of the most acceptable biometrics because it is one of the most common method of identification which humans use in their visual interactions (Figure 1.6). In addition, the method of acquiring face images is non-intrusive. Two primary approaches to the identification based on face recognition are the following: (i) Transform approach [20, 21]: the universe of face image domain is represented using a set of orthonormal basis vectors. Currently, the most popular basis vectors are eigenfaces: each eigenface is derived from the covariance analysis of the face image population; two faces are considered to be identical if they are sufficiently "close" in the eigenface feature space. A number of variants of such an approach exist. (ii) Attribute-based approach [22]: facial attributes like nose, eyes, etc. are extracted from the face image and the invariance of geometric properties among the face landmark features is used for recognizing features.

Facial disguise is of concern in unattended authentication applications. It is very challenging to develop face recognition techniques which can tolerate the effects of aging, facial expressions, slight variations in the imaging environment and variations in the pose of face with respect to camera (2D and 3D rotations) [23].

- Iris

Visual texture of the human iris is determined by the chaotic morphogenetic processes during embryonic development and is posited to be unique for each person and each eye [24]. An iris image is typically captured using a non-contact imaging process (Figure 1.7). The image is obtained using an ordinary CCD

camera with a resolution of 512 dpi. Capturing an iris image involves cooperation from the user, both to register the image of iris in the central imaging area and to ensure that the iris is at a predetermined distance from the focal plane of the camera. A position-invariant constant length byte vector feature is derived from an annular part of the iris image based on its texture. The identification error rate using iris technology is believed to be extremely small and the constant length position invariant code permits an extremely fast method of iris recognition.

Figure 1.6 Identification based on face is one of the most acceptable methods of biometric-based identification.

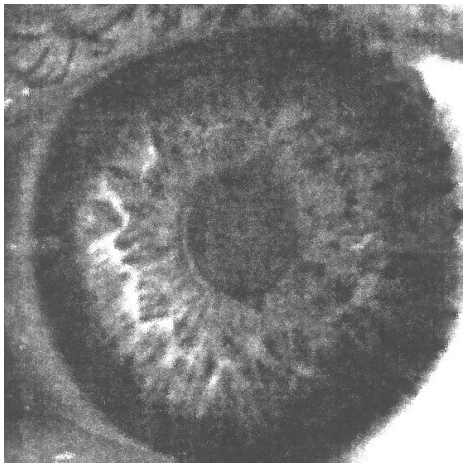


Figure 1.7 Identification Based on Iris. The visual texture of iris could be used for positive person identification.

- Ear

  It is known that the shape of the ear and the structure of the cartilegenous tissue of the pinna are distinctive[3]. The features of an ear are not expected to be unique to each individual. The ear recognition approaches are based on matching vectors of distances of salient points on the pinna from a landmark location (Figure 1.8) on the ear [3]. No commercial systems are available yet and authentication of individual identity based on ear recognition is still a research topic.

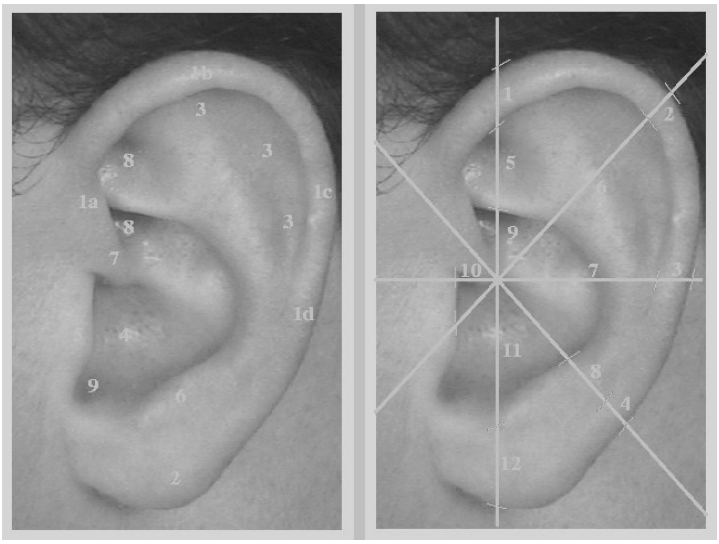


Figure 1.8 An image of an ear and the features used for ear-based identification [3]. Feature vector consists of the distances of various salient locations on the pinna from a landmark location.

- Gait

  Gait is the peculiar way one walks and is a complex spatio-temporal behavioral biometrics. Gait is not supposed to be unique to each individual, but is sufficiently characteristic to allow identity authentication. Gait is a behavioral biometric and may not stay invariant especially over a large period of time, due to large fluctuations of body weight, major shift in the body weight (e.g., waddling gait during pregnancy [25], major injuries involving joints or brain (e.g., cerebellar lesions in Parkinson disease [25]), or due to inebriety (e.g., drunken gait [25]).

  Humans are quite adept at recognizing a person at a distance from his gait. Although, the characteristic gait of a human walk has been well researched in

[3] Department of Immigration and Naturalization in the United States specifically requests photographs of individuals with clearly visible right ear.

biomechanics community to detect abnormalities in lower extremity joints, the use of gait for identification purposes is very recent. Typically, gait features are derived from an analysis of a video-sequence footage (Figure 1.9) of a walking person [26] and consist of characterization of several different movements of each articulate joint. Currently, there do not exist any commercial systems for performing gait-based authentication. The method of input acquisition for gait is not different from that of acquiring facial pictures, and hence gait may be an acceptable biometric. Since gait determination involves processing of video, it is compute and input intensive.

Figure 1.9 Authentication based on gait typically uses a sequence of images of a walking person. One of the frames in the image sequence is illustrated here.

- Keystroke Dynamics
  It is hypothesized that each person types on a keyboard in a characteristic way. This behavioral biometrics is not expected to be unique to each individual but it offers sufficient discriminatory information to permit identity authentication [27]. Keystroke dynamics is a behavioral biometric; for some individuals, one may expect to observe a large variations from typical typing patterns. The keystrokes of a person using a system could be monitored unobtrusively as that person is keying in other information. Keystroke dynamic features are based on time durations between the keystrokes. Some variants of identity authentication use features based on inter-key delays as well as dwell times - how long a person holds down a key. Typical matching approaches use a neural network architecture to associate identity with the keystroke dynamics features. Some commercial systems are already appearing in the market.
- DNA
  DNA (DeoxyriboNucleic Acid) is the one-dimensional ultimate unique code for one's individuality - except for the fact that identical twins have the identical DNA pattern. It is, however, currently used mostly in the context of forensic

applications for identification [4]. Three issues limit the utility of this biometrics for other applications: (i) contamination and sensitivity: it is easy to steal a piece of DNA from an unsuspecting subject to be subsequently abused for an ulterior purpose; (ii) automatic real-time identification issues: the present technology for genetic matching is not geared for online unobtrusive identifications. Most of the human DNA is identical for the entire human species and only some relatively small number of specific locations (polymorphic loci) on DNA exhibit individual variation. These variations are manifested either in the number of repetitions of a block of base sequence (length polymorphism) or in the minor non-functional perturbations of the base sequence (sequence polymorphism) [70]. The processes involved in DNA based personal identification determine whether two DNA samples originate from the same/different individual(s) based on the distinctive signature at one or more polymorphic loci. A major component of these processes now exist in the form of cumbersome chemical methods (wet processes) requiring an expert's skills. There does not seem to be any effort directed at a complete automation of all the processes.(iii) privacy issues: information about susceptibilities of a person to certain diseases could be gained from the DNA pattern and there is a concern that the unintended abuse of genetic code information may result in discrimination in e.g., hiring practices.

Figure 1.10 DNA is double helix structure made of four bases: Adenine (A), Thymine (T), Cytosine (C), and Guanine (G) [4]. The sequence of bases is unique to each individual (with the exception of identical twins) and could be used for positive person identification.

- Signature and Acoustic Emissions

  The way a person signs her name is known to be a characteristic of that individual (Figure 1.11). Although signatures require contact and effort with the writing instrument, they seem to be acceptable in many government, legal, and

commercial transactions[4] as a method of personal authentication. Signatures are a behavioral biometric, evolve over a period of time and are influenced by physical and emotional conditions of the signatories. Signatures of some people vary a lot: even the successive impressions of their signature are significantly different. Further, the professional forgers can reproduce signatures to fool the unskilled eye. Although, the human experts can discriminate genuine signatures from the forged ones, modeling the invariance in the signatures and automating signature recognition process are challenging. There are two approaches to signature verification: static and dynamic. In static signature verification, only geometric (shape) features of the signature are used for authenticating an identity [28]. Typically, the signature impressions are normalized to a known size and decomposed into simple components (strokes). The shapes and relationships of strokes are used as features. In dynamic signature verification, not only the shape features are used for authenticating the signature but the dynamic features like acceleration, velocity, and trajectory profiles of the signature are also employed. The signature impressions are processed as in a static signature verification system. Invariants of the dynamic features augment the static features, making forgery difficult since the forger has to not only know the impression of the signature but also the way the impression was made.

A related technology is authentication of an identity based on the characteristics of the acoustic emissions emitted during a signature scribble. These acoustic emissions are claimed to be a characteristic of each individual [29].

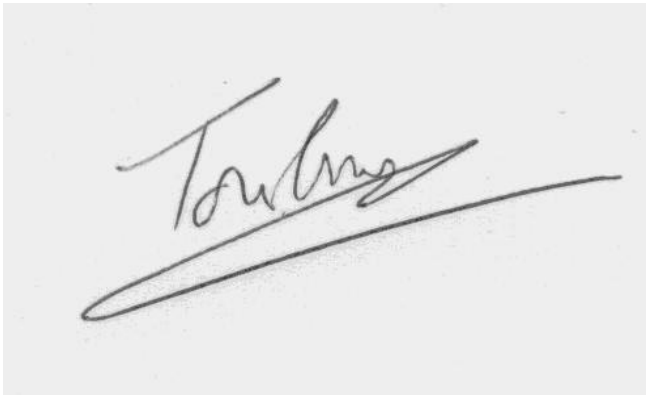


Figure 1.11 Identification based on signature. Signatures have long been accepted as a legitimate means of identification.

- Odor

  It is known that each object exudes an odor that is characteristic of its chemical composition and could be used for distinguishing various objects. Among other things, the automatic odor detection technology [30] is presently being

[4] In some developing countries with low literacy rates, "thumbprint" is accepted as a legal signature.

investigated for detecting land mines [31]. A whiff of air surrounding an object is blown over an array of chemical sensors, each sensitive to a certain group of (aromatic) compounds. The feature vector consists of the signature comprising of the normalized measurements from each sensor. After each act of sensing, the sensors need to be initialized by a flux of clean air.

Body odor serves several functions including communication, attracting mates, assertion of territorial rights, and protection from a predator. A component of the odor emitted by a human (or any animal) body is distinctive to a particular individual. It is not clear if the invariance in a body odor could be detected despite deodorant smells, and varying chemical composition of the surrounding environment. Currently, no commercial odor-based identity authentication systems exist.

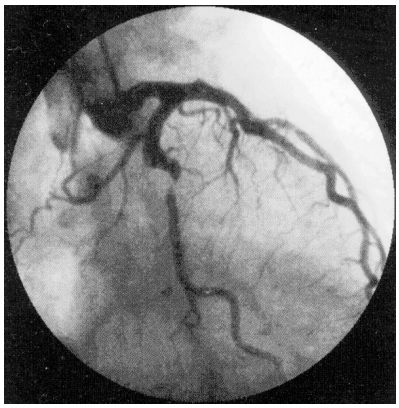


Figure 1.12 Identification based on retinal scan is perceived to be the most secure method of authenticating an identity.

- Retinal Scan
  The retinal vasculature is rich in structure and is supposed to be a characteristic of each individual and each eye (Figure 1.12). It is claimed to be the most secure biometrics since it is not easy to change or replicate the retinal vasculature. Retinal scans, glamorized in movies and military installations, are mostly responsible for the "high-tech-expensive" impression of the biometric technology[5]. The image capture requires a person to peep into an eye-piece and focus on a specific spot in the visual field so that a predetermined part of the retinal vasculature could be imaged. The image acquisition involves cooperation of the subject, entails contact with the eyepiece, and requires a conscious effort on the part of the user. All these factors adversely affect the public acceptability of retinal biometric. A number of retinal scan-based identity authentication installations are in operation which boast *zero* false positives in all the installations to-date[6]. Retinal vasculature can reveal some medical conditions,

[5] Although, iris scanning appears to be more expensive than retinal scanning.
[6] These systems were operating at an unknown high false negative rates [32].

e.g., hypertension, which is another factor standing in the way of public acceptance of retinal scan based-biometrics.

Figure 1.13 Authentication based on hand geometry. Although two-dimensional profile of a hand is illustrated here, in commercial hand geometry-based authentication systems, three-dimensional profile of the hand is sensed.

- Hand and Finger Geometry
  In recent years, hand geometry (Figure 1.13) has become a very popular access control biometrics which has captured almost half of the physical access control market [33]. Some features related to a human hand, e.g., length of fingers, are relatively invariant and peculiar (although, not unique) to each individual. The image acquisition system requires cooperation of the subject and captures frontal and side view images of the palm flatly placed on a panel with outstretched fingers. The registration of the palm is accomplished by requiring the subject's fingers to be aligned with a system of pegs on the panel which is not convenient for subjects with limited flexibility of palm, e.g., those suffering from arthritis. The representational requirements of the hand are very small (9 bytes) which is an attractive feature for bandwidth and memory limited systems. The hand geometry is not unique and cannot be scaled up for systems requiring identification of an individual from a large population of identities. In spite of this, hand geometry has gained acceptability in a number of the installations in last few years for identity authentication applications.

  Finger geometry [34] is a variant of hand geometry and is a relatively new technology which relies only on geometrical invariants of fingers (index and middle). A finger geometry acquisition device closely resembles that for hand geometry but is more compact. It is claimed to be more accurate than hand geometry. However, the technology for finger geometry based authentication is not as mature as that for hand geometry.

Biometrics	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	High	Low	Medium	High	Low	High	Low
Fingerprint	Medium	High	High	Medium	High	Medium	High
Hand Geometry	Medium	Medium	Medium	High	Medium	Medium	Medium
Keystrokes	Low	Low	Low	Medium	Low	Medium	Medium
Hand Vein	Medium	Medium	Medium	Medium	Medium	Medium	High
Iris	High	High	High	Medium	High	Low	High
Retinal Scan	High	High	Medium	Low	High	Low	High
Signature	Low	Low	Low	High	Low	High	Low
Voice Print	Medium	Low	Low	Medium	Low	High	Low
F. Thermograms	High	High	Low	High	Medium	high	High
Odor	High	High	High	Low	Low	Medium	Low
DNA	High	High	High	Low	High	Low	Low
Gait	Medium	Low	Low	High	Low	High	Medium
Ear	Medium	medium	High	medium	Medium	High	Medium

Table 1.1 Comparison of biometrics technologies. The data are based on perception of three biometrics experts.

6. Biometrics Technologies: A Comparison

Each biometric technology has its strengths and limitations. No single biometrics is expected to effectively meet the needs of all the applications. A brief comparison of 14 different biometric techniques that are either widely used or under investigation, including face, fingerprint, hand geometry, keystroke dynamics, hand vein, iris, retinal pattern, signature, voice-print, facial thermograms, odor, DNA, gait, and ear [15, 35, 24, 16, 36, 1, 2, 27, 31, 4, 3] is provided in Table 1.1. Although each of these biometric techniques, to a certain extent, possesses the above mentioned desirable properties and has been used in practical systems [15, 35, 24, 16] or has the potential to become a valid biometric technique [16], not many of them are acceptable (in court of law) as indisputable evidence of identity.

Which biometrics should be used for a given application? The match between a biometrics and an application is determined depending upon the requirements of the given application, the characteristics of the application, and properties of the biometrics. In the context of biometrics-based identification (authentication) systems, an application is characterized by the following properties: (i) does the application need identification or authentication? The applications requiring an identification of a subject from a large database of identities need scalable and relatively more unique biometrics. (ii) Is it attended (semi-automatic) or unattended (completely automatic)? An application may or may not afford a human operator at or near the biometric acquisition stage. In the applications deployed at remote locations with unfriendly or unsafe climate, for instance, the use of biometrics requiring an operator assistance for the capture of physiological or behavioral measurement may not be feasible. (iii) Are the users habituated (or willing to be habituated) to the given biometrics? Performance of a biometrics-based system improves steadily as the subjects instinctively learn to give "good" biometric measurements. This is more true for some biometrics than others; e.g., it is more difficult to give bad retinal image than a fingerprint image. Some applications may tolerate the less effective learning phase of the application deployment for a longer time than others. (iv) Is the application covert or overt? Not all biometrics can be captured without the knowledge of the subject to be identified. Even the biometrics which could be captured without the knowledge of a subject may not be used in some countries due to privacy legislations. (v) Are the subjects cooperative or non-cooperative? Typically, applications involving non-cooperative subjects warrant the use of physiological biometrics which cannot be easily changed. For instance, it is easy to change one's voice compared to changing one's retinal vasculature. (vi) What are the storage requirement constraints? Different applications impose varying limits on the size of the internal representation for the chosen biometrics. (vii) How stringent are the performance requirement constraints? For example, applications demanding higher accuracies need more unique biometrics. (viii) What types of biometrics are acceptable to the users? Different biometrics are acceptable in applications deployed in different demographics depending on the cultural, ethical, social, religious, and hygienic standards of that society. The

acceptability of a biometrics in an application is often a compromise between the sensitivity of a community to various perceptions/taboos and the value/convenience offered by a biometrics-based identification.

7. Automatic Identification

The concept of individuality of personal traits has a long history, and identification of a person based on his physical characteristics is not new. Humans (and other animals) recognize each other based on their physical characteristics. As we pick up the telephone, we expect our friends to recognize us based on our voice. We know from a number of archeological artifacts (Figure 1.14) that our ancestors recognized the individuality of fingerprint impressions [5] on their picture drawings. Prehistoric Chinese have been known to recognize that fingerprints can help establish the identity of an individual uniquely [5]. In 1882 Alphonse Bertillon, chief of criminal identification of Paris police department developed a very detailed method of identification based on a number of bodily measurements, physical description, and photographs [37]. The Bertillon System of Anthropometric Identification system gained wide acceptance before getting superseded by fingerprint based identification systems. Some of the physical characteristics, e.g., DNA, fingerprints, and signatures, have gained a legal status and these characteristics could be used as evidence in the court of law to establish a proof of identity. Having gained the legitimacy, elaborate systems of rules have been developed for (i) matching these biometrics to decide whether a pair of biometric measurements, e.g., two fingerprints, belong to the same person or not; (ii) searching a given biometric measurement in a database consisting of a number of other measurements of the same biometrics. These rules are derived from manual systems of matching and indexing because of historical reasons, and require trained experts for operation of manual/semi-automatic identification systems. For example, the traditional fingerprint identification systems used in the forensic applications require well-trained experts in acquisition of fingerprints, classifying/indexing the fingerprint, and fingerprint matching.

On the other hand, use of biometrics in *fully* automated applications is a relatively new and emerging phenomenon. There is a growing interest in biometrics from a wide cross-section of society: engineers, technologists, scientists, and, government and corporate executives. The excitement of the emergence of biometrics-based technology is evident by publication of dozens of biometrics articles in the popular press [38], organization of exclusive technical conferences devoted to biometrics [39, 40, 41, 42, 43], organization of biometrics related workshops [44, 45], increasing focus on biometrics in security and financial trade-shows [46, 47], institution of biometric consortia [48, 49], special issues of reputed technical journals [50], publication of a few periodicals devoted to biometrics [51, 52], and even establishment of an exclusive biometric shop [38] in the last couple of years.

The perception that biometric technologies are hi-tech, high-cost systems and can only be afforded in forensics and high-security military installations is rapidly changing. Spiraling increase in the availability of inexpensive computing resources, advances in image understanding, better matching strategies provided by progress in

pattern recognition and computer vision field, cheaper sensing technologies, and increasing demand for the identification needs, are forcing biometric technology into new applications/markets requiring positive personal identification.

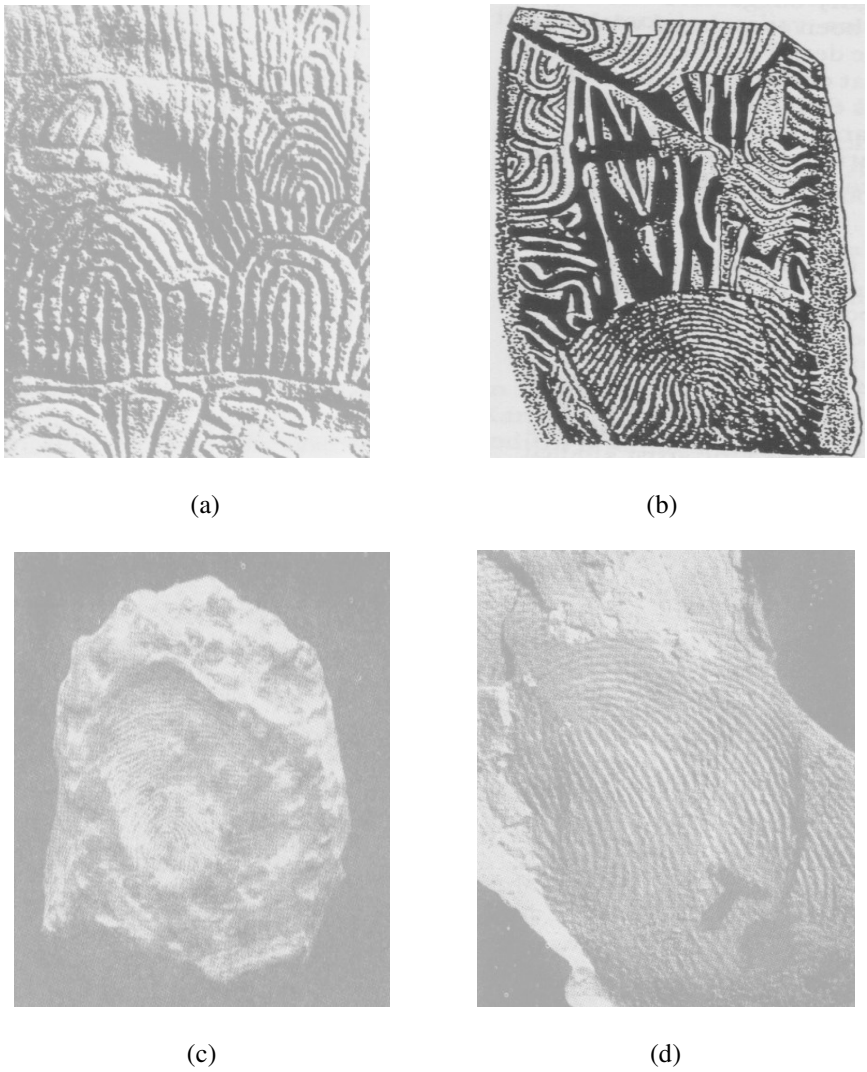


Figure 1.14 Archeological artifacts depicting fingerprint impressions: (a) Neolithic Carvings at Gavrinis Island; (b) Standing Stone at Goat Island (2,000 B.C.); (c) A Chinese clay seal (300 B.C.); and (d) An impression on a Palestinian lamp (400 A. D.) [5]. The Chinese clay seal and Palestinian lamp impressions indicate the identity of their respective owners.

The biometrics-based identification (authentication) technology is being either adopted or contemplated in a very broad range of civilian applications: (*i*) *banking security* such as electronic fund transfers, ATM security, internet commerce, check cashing, and credit card transactions, (*ii*) *physical access control* such as airport access control, (*iii*) *information system security* like access to databases via login privileges, (*iv*) *government benefits distribution* such as welfare disbursement programs [53], (*v*) *customs and immigration* such as *INS* Passenger Accelerated Service System (INSPASS) which permits faster immigration procedures based on hand geometry [54], (*vi*) *national ID systems* which provide a unique ID to the citizens and integrate different government services [55], (*vii*) *voter and driver registration* providing registration facilities for voters and drivers. (*viii) customer loyalty/preference* schemes providing incentives to repeat/preferred customers of a business establishment, and (*ix*) *Telecommunications* such as cellular bandwidth access control.

8. Research Issues

The general problem of personal identification raises a number of important research issues: what identification technologies are the most effective to achieve accurate and reliable identification of individuals? In this section, we summarize the challenges in biometrics research [56]. Some of these problems are well-known open problems in the allied areas (e.g., pattern recognition and computer vision), while the others need a systematic cross-disciplinary effort.

We believe that biometrics technology alone may not be sufficient to resolve these issues effectively; the solutions to the outstanding open problems may lie in innovative engineering designs exploiting constraints otherwise unavailable to the applications and in harnessing the biometric technology in combination with other allied technologies.

Design

It is not clear whether the use of the features and philosophies underlying the identification systems heavily tuned for human use (e.g., faces and fingerprints) is as effective for fully automatic processes (Figure 1.15). Nor do we know whether identification technologies inspired and used by humans are indeed as amenable and effective for completely automatic identification systems. In fact, it is not even clear if the solutions solely relying on biometrics-based identifications are the most desirable engineering solutions in many real-world applications. Both, a different set of functional requirements demanded by the emerging market applications and the retrospective wisdom of futility of myopic dependence on human intuition for engineering designs suggest that full automation of the biometrics-based identification systems warrant a careful examination of all the underlying components of the positive identifications of the emerging applications.

A biometric-based identification (authentication) system operates in two distinct modes (Figure 1.16): enrollment and identification (authentication). During

enrollment, biometric measurements are captured from a given subject, relevant information from the raw measurement is gleaned by the feature extractor, and (feature, person) information is stored in a database. Additionally, some form of ID for the subject may be generated for the subject (along with the visual/machine representation of the biometrics). In identification mode, the system senses the biometric measurements from the subject, extracts features from the raw measurements, and searches the database using the features thus extracted. The system may either be able to determine the identity of the subject or decide the person is not represented in the database. In authentication mode of operation, the subject presents his system assigned ID and the biometric measurements, the system extracts (input) features from the measurements, and attempts to match the input features to the (template) features corresponding to subject's ID in the system database. The system may, then, either determine that the subject is who he claims to be or may reject the claim. In some situations, a single system operates as both an identification and an authentication system with a common database of (identity, feature) associations.

Figure 1.15 Human vision is fooled by many subtle perceptual tricks and it is hoped that machine vision may be better equipped in correctly recognizing the deceit in such situations. Although, a typical human subject may wrongly believe the faces shown in this picture to belong to Al Gore and President Bill Clinton, on closer inspection, one could recognize that both the faces in the picture identically show Bill Clinton's facial features and the crown of hair on one of the faces has been digitally manipulated to appear similar to that of Al Gore [6].

Design of a biometrics-based identification system could essentially be reduced to the design of a pattern recognition system. The conventional pattern recognition system designers have adopted a sequential phase-by-phase modular architecture (Figure 1.17). Although, it is generally known in the research community that more integrated, parallel, active system architectures involving feedback/feed-forward control have a number of advantages, these concepts have not yet been fully exploited in commercial biometrics-based systems.

Given the speed, accuracy, and cost performance specifications of an end-to-end identification system, the following design issues need to addressed: (i) how to acquire the input data/measurements (biometrics)? (ii) what internal representation (features) of the input data is invariant and amenable for an automatic feature extraction process? (iii) given the input data, how to extract the internal representation from it? (iv) given two input samples in the selected internal representation, how to define a matching metric that translates the intuition of ``similarity'' among the patterns? (v) how to implement the matching metric? Additionally, for reasons of efficiency, the designer may also need to address the issues involving (vi) organization of a number of (representations) input samples into a database and (vii) effective methods of searching a given input sample representation in the database.

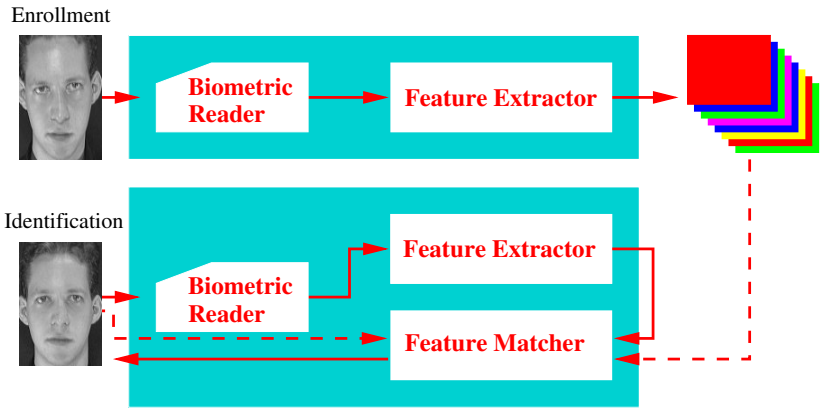


Figure 1.16 Architecture of a typical biometric system.

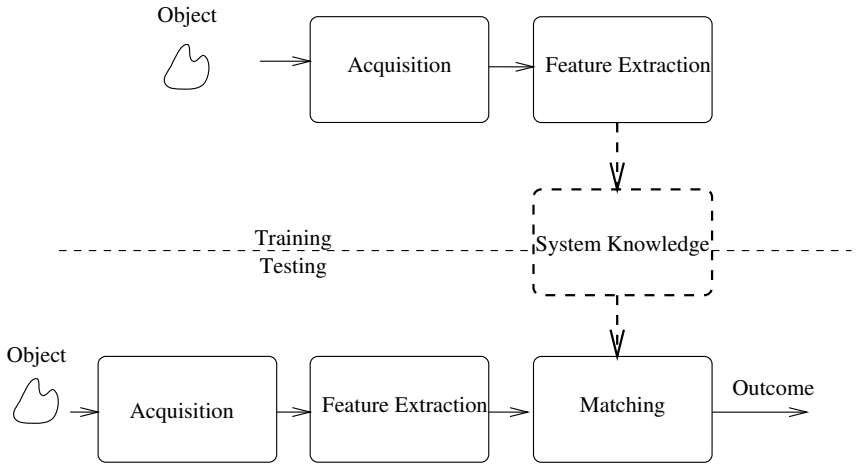


Figure 1.17 Architecture of a typical pattern recognition system.

Researchers in pattern recognition have realized that effectively resolving these issues is very difficult and there is a need to constrain the environment to engineer feasible solutions. We will describe some of the research problems in the design of biometrics-based identification systems.

1. **Acquisition.** Acquiring relevant data for the biometrics is one of the critical processes which has not received adequate attention. The amount of care taken in acquiring the data (often) determines the performance of the entire system. Two of the associated tasks are: (a) quality assessment; automatically assessing the suitability of the input data for automatic processing and (b) segmentation; separation of the input data into foreground (object of interest) and background (irrelevant information).

   A number of opportunities exist for incorporating (i) the context of the data capture which may further help improve the performance of the system and (ii) avoiding undesirable measurements (and subsequent recapture of desirable measurements). With inexpensive desktop computing and large input bandwidth, typically the context of the data capture could be made richer to improve the performance. For instance, a fingerprint is traditionally captured from its 2D projection on a flat surface. Why not capture a 3D image? Why not take a color image? Why not use active sensing? Such enhancements may often improve the performance of the biometric systems.

   Although a number of existing identification systems routinely assign a quality index to the input measurement indicating its desirability for matching (Figure 1.18), the approach to such a quality assessment metric is subjective, debatable, and typically inconsistent. A lot of research effort needs to be focussed in this area to systematize both (i) the rigorous and realistic models of the input measurements and (ii) metrics for assessment of quality of a measurement. When the choice of rejecting a poor quality input measurement is not available (e.g., in legacy databases), the system may optionally attempt at gleaning useful signal from the noisy input measurements. Such operation is referred to as signal/image enhancement (Figure 1.19) and is computationally intensive. How to enhance the input measurements without introducing any artifacts is an active research topic.

   Similarly, the conventional foreground/background separation (Figure 1.20) typically relies on an *ad hoc* processing of input measurements and enhancing the information bandwidth of input channel (e.g., using more sensory channels) often provides very effective avenues for segmentation. Further, robust and realistic models of the object of interest often facilitate cleaner and better design of segmentation algorithms.

2. **Representation**

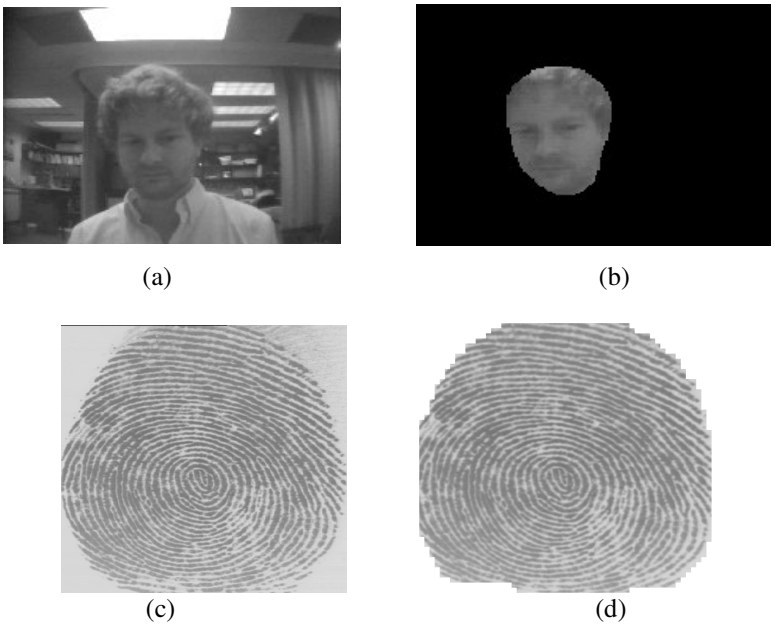
   Which machine-readable representations completely capture the invariant and discriminatory information in the input measurements? This representation issue constitutes the essence of system design and has far reaching implications on the design of the rest of the system. The unprocessed measurement values are typically not invariant over the time of capture and there is a need to determine

salient features of the input measurement which both discriminate between the identities as well as remain invariant for a given individual. Thus, the problem of representation is to determine a measurement (feature) space which is invariant (less variant) for the input signals belonging to the same identity and which differ maximally for those belonging to different identities (high *interclass*) variation and low *intraclass* variation). To systematically determine the discriminatory power of an information source and arrive at an effective feature space is a challenging problem.

Figure 1.18 Fingerprint Quality: Automatically and consistently determining suitability of a given input measurement for automatic identification is a challenging problem. A fingerprint quality assessment algorithm quantifies suitability of fingerprint images for automatic fingerprint identification system by assigning a quality index in the range of [0,1]; numbers closer to zero indicate poor quality images.

(a) (b)

Figure 1.19 Enhancement: Automatically enhancing fingerprint images without introducing artifacts is a challenging problem: (a) a poor quality fingerprint image; (b) result of image enhancement of fingerprint image shown in (a) [8].



(a) (b)

(c) (d)

Figure 1.20 Segmentation: Determining the region containing the object of interest from a given image is a challenging problem. (a) image showing a face; (b) a face detection algorithm identifying the region of interest in (a) for a face recognition system; (c) a fingerprint image; and (d) foreground/background separation of the fingerprint image shown in (c) [7].

A related issue about representation is the *saliency* of a measurement signal and its representation. More distinctive biometric signals offer more reliable identity authentication. Less complex measurement signals inherently offer a less reliable identification. This phenomenon has a direct impact in many biometrics-based identification, e.g., signature, where less distinctive signatures could be easily forged. A systematic method of quantifying distinctiveness of a specific signal associated with an identity and its representation is needed for effective identification systems.

Additionally, in some applications, storage space is at a premium, e.g., in a smart card application, typically, about 2K bytes of storage is available. In such situations, the representation also needs to be parsimonious. The issues of most salient features of an information source also need to be investigated.

Representation issues cannot be completely resolved independent of a specific biometric domain and involve complex trade-offs. Take, for instance, the fingerprint domain. Representations based on the entire gray scale profile of a fingerprint image are prevalent among the verification systems using optical matching [57, 58]. However, the utility of the systems using such representation schemes may be limited due to factors like brightness variations, image quality variations, scars, and large global distortions present in the fingerprint image because these systems are essentially resorting to template matching strategies for verification. Further, in many verification applications terser representations are desirable which preclude representations that involve the entire gray scale profile of fingerprint images. Some system designers attempt to circumvent this problem by restricting that the representation be derived from a *small* (but consistent) part of the finger [57]. However, if this same representation is also being used for identification applications, then the resulting systems might stand at a risk of restricting the number of unique identities that could be handled, simply because of the fact that the number of distinguishable templates is limited. On the other hand, an image-based representation makes fewer assumptions about the application domain (fingerprints) and, therefore, has the potential to be robust to wider varieties of fingerprint images. For instance, it is extremely difficult to extract a landmark-based representation from a (degenerate) finger devoid of any ridge structure.

3. Feature Extraction

Given raw input measurements, automatically extracting the given representation is an extremely difficult problem, especially where input measurements are noisy (see Figure1.21).

A given arbitrarily complex representation scheme should be amenable to automation without any human intervention. For instance, the manual system of fingerprint identification uses as much as a dozen features [59]. However, it is not feasible to incorporate these features into a fully automatic fingerprint system

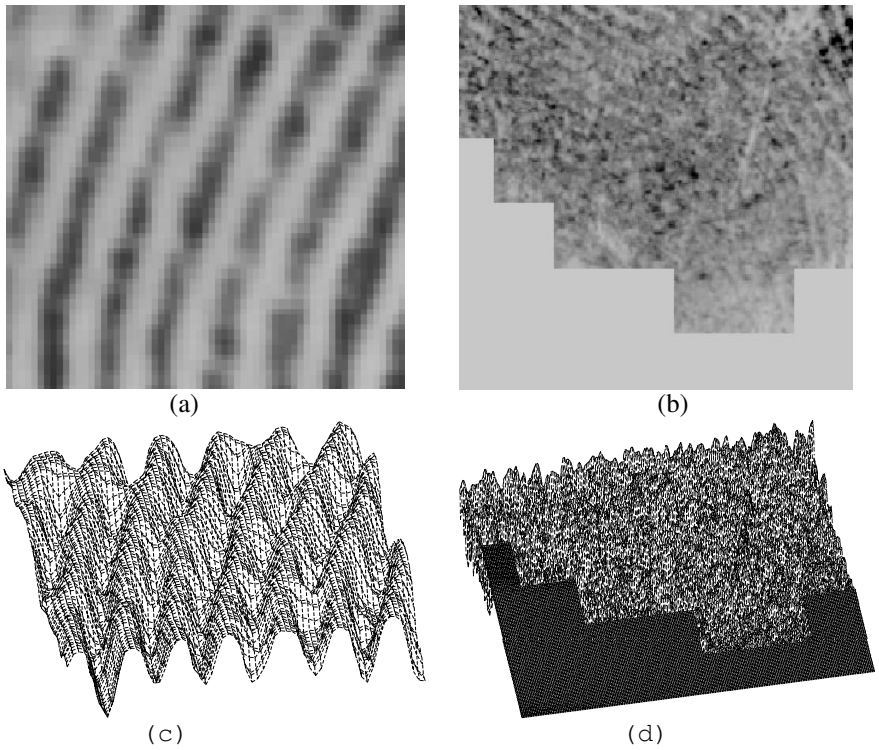


Figure 1.21 Automatically gleaning finger features from the fingerprint images is extremely difficult, especially, when the fingerprint is of poor quality (a) a portion of good quality fingerprint image; (b) a portion of poor quality fingerprint image; (c) 3-dimensional visualization of (a); and (d) 3-dimensional visualization of (b).

because it not easy to reliably detect these features using state-of-the-art image processing techniques. Determining features that are amenable to automation has not received much attention in computer vision and pattern recognition research and is especially important in biometrics which are entrenched in the design philosophies of an associated mature manual system of identification.

Traditionally, the feature extraction system follows a staged sequential architecture which precludes effective integration of extracted information available from the measurements. Increased availability of inexpensive computing and sensing resources makes it possible to use better architectures/methods for information processing to detect the features reliably.

Once the features are determined, it is also a common practice to design feature extraction process in a somewhat ad hoc manner. The efficacy of such methods is limited especially when input measurements are noisy. Rigorous models of feature representations are helpful in a reliable extraction of the

features from the input measurements, especially, in noisy situations. Determining terse and effective models for the features is a challenging research problem.

4. **Matching**

The crux of a matcher is a similarity function which quantifies the intuition of similarity between two representations of the biometric measurements. Determining an appropriate similarity metric is a very difficult problem since it should be able to discriminate between the representations of two different identities despite noise, structural and statistical variations in the input signals, aging, and artifacts of the feature extraction module. In many biometrics, say signature verification, it is difficult to even define the ground truth [28]: do the given two signatures belong to the same person or different persons?

A representation scheme and a similarity metric determine the accuracy performance of the system for a given population of identities; hence the selection of appropriate similarity scheme and representation is critical.

Given a complex operating environment, it is critical to identify a set of valid assumptions upon which the matcher design could be based. Often, there is a choice between whether it is more effective to exert more constraints by incorporating better engineering design or to build a more sophisticated similarity function for the given representation. For instance, in a fingerprint matcher, one could constrain the elastic distortion altogether and design the matcher based on a rigid transformation assumption or allow arbitrary distortions and accommodate the variations in the input signals using a clever matcher. Where to strike the compromise between the complexity of the matcher and controlling the environment is an open problem.

Consider design of a matcher in the domain of fingerprint-based identification systems (see Figure 1.22). Typically, the fingerprint imaging system presents a number of peculiar and challenging situations some of which are unique to fingerprint image capture scenario: (I) Inconsistent contact: the act of sensing distorts the finger. The three-dimensional shape of the finger gets mapped onto the two-dimensional surface of the glass platen. Typically, this (non-homogeneous) mapping function is determined by the pressure and contact of the finger on the glass platen (see Figure 1.23). (ii) Non-uniform contact: the ridge structure of a finger would be completely captured if ridges of the part of the finger being imaged are in complete optical contact with the glass platen. However, the dryness of the skin, skin disease, sweat, dirt, humidity in the air all confound the situation resulting in a non-ideal contact situation: some parts of the ridges may not come in complete contact with the platen and regions representing some valleys may come in contact with the glass platen. This results in “noisy” low contrast images, leading to either spurious minutiae or missing minutiae. (iii) Irreproducible contact: vigorous manual work, accidents etc. inflict injuries to the finger, thereby, changing the ridge structure of the finger either permanently or semi-permanently. This may introduce additional spurious minutiae. (iv) Feature

extraction artifacts: the feature extraction algorithm is imperfect and introduces measurement errors. Various image processing operations might introduce inconsistent biases to perturb the location and orientation estimates of the reported minutiae from their gray scale counterparts. (vi) The act of sensing itself adds noise to the image. For example, residues are leftover on the glass platen from the previous fingerprint capture. A typical imaging system distorts the image of the object being sensed due to imperfect imaging conditions. In the frustrated total internal reflection (FTIR) sensing scheme, for example, there is a geometric distortion because the image plane is not parallel to the glass platen.

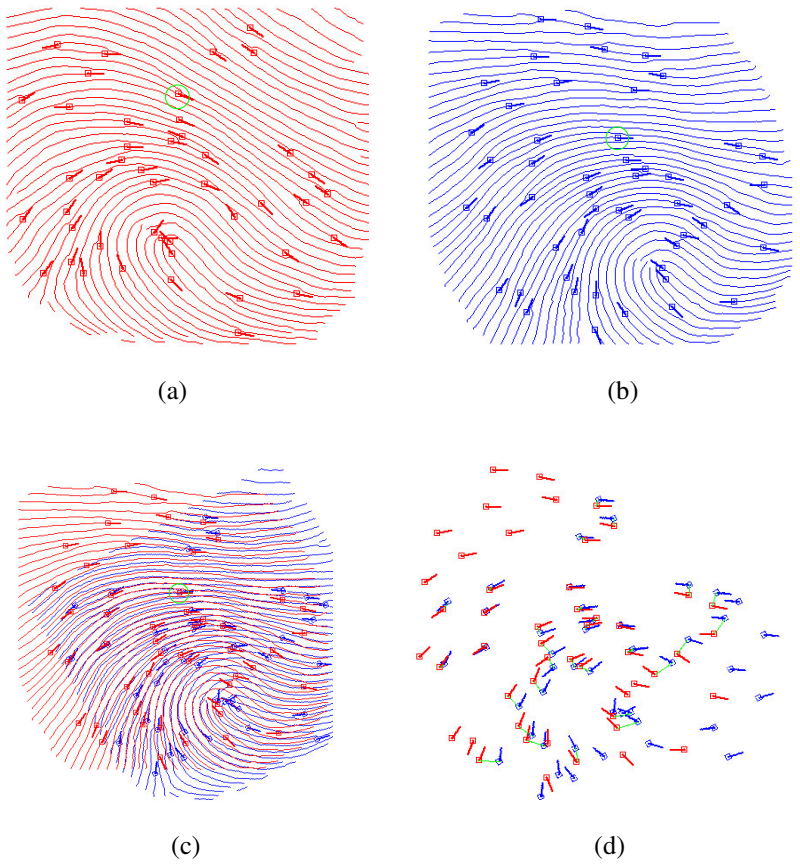


Figure 1.22 Fingerprint Matcher: Results of applying the matching algorithm [7] to an input and a template minutiae set; (a) input minutiae set; (b) template minutiae set; (c) input and template fingerprint are aligned based on the minutiae marked with green circles; and (d) matching result where template minutiae and their correspondences are connected by green lines. The matching score for the fingerprints was 37. The score range was 0--100; scores closer to 100 indicate better match.

Figure 1.23 Impressions of a finger captured by exerting different (magnitude/direction) forces on the finger during fingerprint acquisition results in a significant non-homogenous distortion of the ridge structures; consequently, the fingerprints are difficult to match.

In light of the operational environments mentioned above, the design of the similarity functions and matching algorithms needs to establish and characterize a realistic model of the variations among the representations of mated pairs. Is the distortion, for instance, significant for the given imaging? Is it easier to prevent distortion or is it more effective to take into account all the distortions possible and formulate a clever similarity function?

5. Search, Organization, and Scalability

Systems dealing with a large number of identities should be able to effectively operate as the number of users in the system increases to its operational capacity and should only gracefully degrade as the system accommodates more users than envisaged at the time of its design. As civilian applications (e.g., driver and voter registration, National ID systems and IDs for health, medical, banking, cellular, transportation, and e-commerce applications) enrolling a very large number of identities (e.g., tens of millions) are being designed and integrated, we are increasingly looking toward biometrics to solve authentication and identification problems.

In identity authentication systems, biometrics are cost effective and are easier to maintain because these systems do not have to critically depend on issuing/reissuing other identity (magnetic stripe/smart/2D bar code) cards. Tasks like maintaining the database of identities, selection of a record etc. may require more resources, but the technical complexity of matching a biometric representation offered by the user to that stored in the system does not increase as the number of identities handled by the system increases arbitrarily.

On the other hand, identification of an individual among a large number of identities becomes increasingly complex as the number of identities stored in the

system increases. Many applications like National ID systems, passport and visa issuance further require a constant throughput and a very small turnaround time. A designer of such systems needs to adopt radically different strategies and mode of operation than those adopted by traditional forensic identification systems. This has a profound influence on every aspect of the system, including the choice of biometrics, features, metric of similarity, matching criteria, operating point, etc. None of these design issues have been rigorously studied, neither in biometrics nor even in pattern recognition research.

All these criteria point to using those biometrics which remain invariant over a long period of time. Designing constant length, one-dimensional, indexable features will become increasingly important for identification applications involving a large number of identities.

Evaluation

An end-user is interested in determining the performance of the biometric system for *his specific application*: does the system make an accurate identification? Is the system sufficiently fast? How much would be the cost of the system? Among these issues, characterizing the accuracy performance is the most difficult; we will only address accuracy performance issues here.

No metric is sufficiently adequate to give a reliable and convincing indication of the identification accuracy of a biometric system. A decision made by a biometric system is either a *genuine individual* type of decision or an *impostor* type of decision, which can be represented by two statistical distributions called genuine distribution and impostor distribution, respectively (see Figure 1.24). For each type of decision, there are two possible decision outcomes, true or false. Therefore, there are a total of four possible outcomes: (*i*) a genuine individual is accepted, (*ii*) a genuine individual is rejected, (*iii*) an impostor is rejected, and (*iv*) an impostor is accepted. Outcomes (*i*) and (*iii*) are correct whereas (*ii*) and (*iv*) are incorrect. In principle, we can use the false (impostor) acceptance rate (FAR), the false (genuine individual) reject rate (FRR) and the equal error rate (EER)[7] to indicate the identification accuracy of a biometric system [24, 60]. Unfortunately, the performance of a system in the context of a given population (database) is a random variable and, strictly speaking, it cannot be computed or measured but can only be estimated from empirical data and the estimates of the performance are very data dependent. Therefore, they are meaningful only for a specific database in a specific test environment. For example, the performance of a particular biometric system claimed by its manufacturer had a FRR of 0.3% and a FAR of 0.1%. An independent test by the Sandia National Lab. found that the same system had a FRR of 25% with an unknown FAR [61]! In order to provide a more reliable assessment of a biometric system, some more descriptive performance measures are necessary. Receiver operating curve (ROC) and *d'* are the two other commonly used measures. A receiver operating curve provides an empirical assessment of the system performance at different operating points which is

[7] Equal error rate is defined as the value of FAR/FRR at an operating point on ROC where FAR and FRR are equal.

more informative than FAR and FRR. The statistic *d'* gives an indication of the separation between the genuine distribution and impostor distribution [60]. The existing performance metrics are empirical and provide us means of estimating performance with respect to a specific database. For such empirical performance metric to be able to precisely generalize to the entire population of interest, the test data should (*i*) be large enough to represent the population and (*ii*) contain enough samples from each category of the population [60].

To obtain fair and honest test results, enough samples should be available, the samples should be representative of the population, and adequately represent all the categories (impostors and genuine). In reality, especially for emerging applications, we do not have access to a sufficient number of test samples nor are the samples representative of the actual population of interest. In such situations, there is a need to obtain predictive models of performance in terms of controllable and measurable parameters of the available data. Such predictive models of performance may be useful both for bootstrapping a small number of available samples as well as obtaining realistic estimates of the performance of a given biometric technology to a given application.

Irrespective of the choice of a performance metric, error bounds that indicate the confidence of the estimates are valuable for understanding the significance of the test results. Estimating confidence measures without using unrealistic naive models of the hypothesized population distributions is challenging.

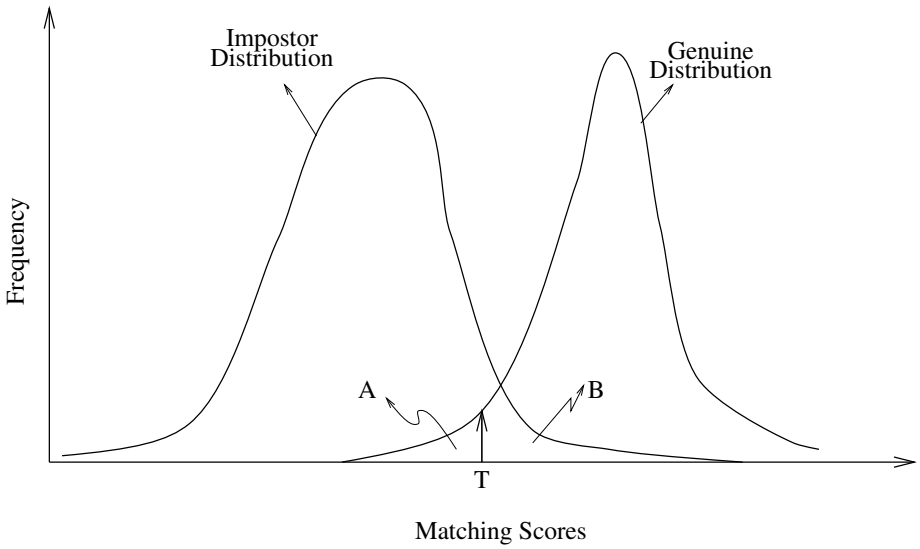


Figure 1.24 The distributions of matching scores obtained by matching input measurements from the same identities (genuine distribution) and those obtained from different identities (impostor distribution). Given a matching score threshold (T), the areas A and B represent false rejection rate (FRR) and false acceptance rate (FAR), respectively.

Integration

The accuracy of an identification system obviously will improve as we effectively utilize and integrate an increasing number of information sources related to an individual to confirm her identity. It also becomes increasingly difficult to abuse the system privileges. However, the challenge of integration is to ascertain that the system performance degrades gracefully as some of the information sources become unavailable or unreliable. As better performance is demanded of identification systems and as a variety of different sensors become affordable, integration of different biometrics will become an important issue [62, 63, 64, 65, 66]. Integration of different technologies is also becoming critical for imparting capabilities to the identification system. For instance, biometric sensor integrated smart cards could provide facilities for identity authentication without divulging any information about biometric measurements.

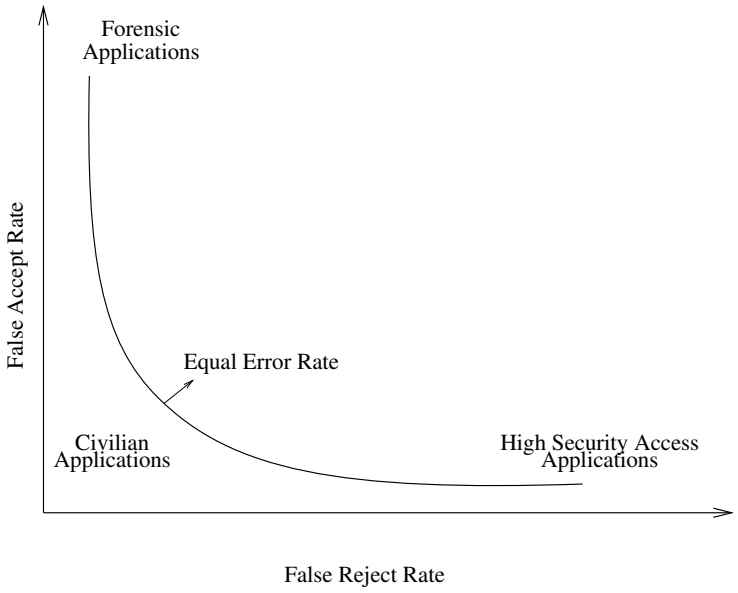


Figure 1.25 Receiver operating characteristics (ROC) of a system illustrates false reject rate (FRR) and false acceptance rate (FAR) of a matcher at all operating points. Each point on an ROC defines FRR and FAR for a given matcher operating at a particular matching score threshold. High security access applications are concerned about break-ins and hence operate the matcher at a point on ROC with small FAR. Forensic applications desire to catch a criminal even at the expense of examining a large number of false accepts and hence operate their matcher at a high FAR. Civilian applications attempt to operate their matchers at the operating points with both, low FRR and low FAR.

Deciding efficient architectures for integration is an open research problem and it is perhaps the single most factor in determining the behavior of an integrated system. Decision level, feature level, and measurement level integration architectures have been studied in the literature [67, 68]. Determination of which integration strategies are appropriate for a given identification application needs more focussed research.

Circumvention

Some problems plague all identification technologies (based on possession, knowledge, or biometrics) alike. Fraud in an identification system is possible in different forms. Some forms of fraud are characterized as loopholes in the system: possibilities of illegitimate access to a system not envisaged by its designers. Other forms involve transcending the means and mechanisms of identification used by the system (super-system) and hence, in principle, cannot be completely eliminated using any strategies embedded inside the system (intra-system). The latter type of fraud could be categorized as follows:

- Collusion: In any application, some operators of the system will have a super-operator status which allows them to bypass the identification component of the processing and to overrule the decision made by the system. This facility is incorporated in the system work-flow to permit handling of exceptional situations, e.g., processing of individuals with no fingers in a fingerprint-based identification system. This could potentially lead to an abuse of the system by way of collusion between the super-operators and the users.
- Coercion: The genuine users could be potentially coerced to identify themselves to the system. The identification means could be forcibly extracted from a genuine user to gain access to the system with concomitant privileges. For instance, an ATM user could be forced to give away her ATM card and PIN at a gun point. It is desirable to reliably detect instances of coercion without endangering the lives of genuine users and take an appropriate action.
- Denial: It is possible that a genuine user may identify himself to the system using the legitimate means of the identification to gain access to the privileges and is subsequently denied such an access.
- Covert Acquisition: It is possible that the means of identification could be compromised without the knowledge of a legitimate user and be subsequently abused. For instance, a significant amount of fraud in telecommunication theft is ascribed to video-snooping: video-recording the scenes of users punching their pins at, say, a public telephone.

As mentioned earlier, many of these problems may not be fully eliminated. Currently, attempts to reduce fraud in an identification system are process-based and ad hoc. There is a need to focus research effort on systematic and technology-intensive approaches to combat fraud in the system. This is especially true in terms of biometrics-based identification systems where the captured biometric measurements and context may have sufficient information to deter and detect some forms of fraud. In particular, multi-biometrics may show promise in approaching solutions to many of the above mentioned problems.

Some other problems related to identification are more specific to biometrics-based systems. For instance, skilled humans have an uncanny ability to disguise their identity and are able to assume (forge/mimic) a different (specific) identity (Figure 1.26). The "chameleon identities" pose an additional problem to the reliability of the identification systems based on some biometrics and warrant more research.

9. Privacy

- Privacy: Any biometrics-based technology is traditionally perceived as dehumanizing and as a threat to an individual's privacy rights (see Figure 1.27). As identification technologies become more and more foolproof, the process of getting identified itself leaves trails of undeniable private information. e.g., where is an individual? What is the individual buying?, etc. In case of biometrics-based identification, this problem is even more serious because the biometric features may additionally inform others about the medical history or susceptibilities of an individual, e.g., retinal vasculature may divulge information about diabetes or hypertension [69]. Consequently, there is a legitimate concern about privacy issues associated with the biometrics-based identification.

Figure 1.26 Multiple Personalities: All the people in this image are the same person (The New York Times Magazine, September 1, 1996/section 6, pages 48-49, reproduced with permission of Robert Trachtenberg).

- Proscription: This issue is somewhat related to the previous issue. When a biometric measurement is offered to a given system, the information contained in it should not be used for any other purpose than its intended use. In any (networked) information processing system, it is difficult to ensure that the biometric measurements captured will only be used for its intended purpose.

Wide-spread use of biometrics-based identification systems should not only address the above mentioned issues from technical standpoint but also from the public perception point of view. This is especially true for assuring the users that their biometric information will remain private and will only be used for the expressed purpose for which it was collected.

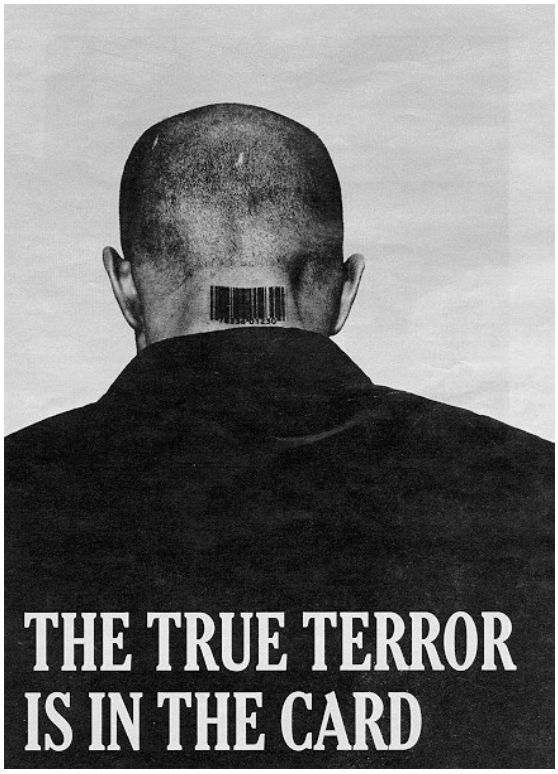


Figure 1.27 "The true terror is in the card", an illustration from Robert E. Smith's article [9] in the New York Times Magazine summarizes the essence of public perception about biometric technology: it is dehumanizing and is a threat to privacy rights of an individual. The original picture by Jana Sterback, "Generic Man", 1989.

10. Novel Applications

As biometric technology matures, there will be an increasing interaction among the (biometric) market, (biometric) technology, and the (identification) applications. The emerging interaction is expected to be influenced by the added value of the technology, the sensitivities of the population, and the credibility of the service

provider. It is too early to predict where, how, and which biometric technology would evolve and be mated with which applications.

Applications like automating identification for more convenient travel, for transactions via e-commerce, etc. seem to be ready for commercialization, but perhaps, biometric technology could open up a whole new genre of futuristic hi-tech applications that were not foreseen before.

Take for instance, the application of content-based search of digital libraries and in particular, video. One of the tasks in content-based search involves ascription of sound bytes to individuals (identities) depicted in the corresponding video segment. The association of the sound to identity is essentially a closed identification problem. What makes this problem interesting is the opportunity to exploit the context and clues offered from the vision-based processing (e.g., number of people in the video and lip movements) of the video. Voice-based clues could generate plausible hypotheses about identities of visual entities. From the visual input, the hypothesis could either be accepted or rejected depending on the coherency of the sound and vision based results.

Or imagine, in a hi-tech mall, the features extracted from DNA of millions of cells shredded by the body of a passing individual (and a potential customer) would be instantly matched to determine the exact identity or a possible category of population. That individual would then be treated exclusively depending upon his spending pattern. Perhaps, there would be data mining based on the biometric characteristics!

Interesting scenarios might materialize as a number of civilian applications of identification are integrated based on a single or multiple biometric technologies. This will certainly have a profound influence on the way we conduct our business.

11. Summary

Biometrics is a science of automatically identifying individuals based on their unique physiological or behavioral characteristics. A number of civilian and commercial applications of biometrics-based identification are emerging. At the same time, a number of legitimate concerns are being raised against the use of biometrics for various applications; three of them appear to be the most significant: cost, privacy, and performance.

As more and more legislations are brought into effect, both, protecting the privacy rights of the individuals as well as endorsing the use of biometrics for legitimate uses and as the prices of the biometric sensors continues to fall, the added value of the biometrics-based systems will continue to attract more applications. It is expected that in the next five years, the rising number of applications may increase the demand for the biometric sensors to drive a volume-based pricing.

For the wide-spread use of the biometrics to materialize, it is necessary to undertake systematic studies of the fundamental research issues underlying the design and evaluation of identification systems. Further, it is critical to engineer the match between the application needs and the available technologies.

Acknowledgments

We would like to thank Biometric Consortium and discussions on its list server for providing a rich and up to date source of information. We are grateful to Tulasi Perali for pointing out specific medical pathologies. Jon Connell provided the face foreground/background separation images shown in Figures 1.20 (a) and (b). Iris (Figure1.7) and retina (Figure 1.12) images were scanned from the product literatures from IriScan and EyeDentify, respectively. We thank Lin Hong for reviewing this chapter and lending a number of images from his PhD thesis.

References

[1] "Technology recognition systems homepage," *http://www.betac.com/~imagemap/subs?-155,150*, 1997.

[2] J. Rice, "Veincheck homepage," *http://innotts.co.uk/~joerice/*, 1997.

[3] M. Burge and W. Burger, "Ear biometrics for machine vision," in *21st Workshop of Austrian Association for Pattern Recognition*, *http://www.cast.uni-linz.ac.at/st/vision/-Papers/oagm-97/*, (Hallstatt), ÖAGM, Verlag R Oldenbourg, May 1997.

[4] Federal Bureau of Investigation Educational Internet Publication, "DNA testing," *http://www.fbi.gov/kids/dna/dna.htm*, 1997.

[5] A. Moenssens, *Fingerprint Techniques*. Chilton Book Company, London, 1971.

[6] P. Sinha and T. Poggio, "I think I know that face...," *Nature*, Vol. 384, No. 6608, p. 406, 1996.

[7] A. Jain, L. Hong, S. Pankanti, and R. Bolle, "On-line identity authentication system using fingerprints," *Proceedings of IEEE (Special Issue on Automated Biometrics)*, Vol. 85, pp. 1365-1388, September 1997.

[8] L. Hong, Y. Wan, and A. Jain, "Fingerprint image enhancement: Algorithm and performance evaluation," *IEEE Trans. Pattern Analysis and Machine Intelligence*, 1998 (To appear).

[9] R. E. Smith, "The true terror is in the card," in *The New York Times Magazine, September 8, 1996*, pp. 58.

[10] J. D. Woodward, "Biometrics: Privacy's foe or privacy's friend?," *Proceedings of the IEEE (Special Issue on Automated Biometrics)*, Vol. 85, pp. 1480-1492, September 1997.

[11] L. Lange and G. Leopold, "Digital identification: It's now at our fingertips," *EEtimes at http://techweb.cmp.com/eet/823/, March 24*, Vol. 946, 1997.

[12] G. Stein, "Sacred emily," in *The Oxford Book of American Light Verse* (W. Harmon, ed.), pp. 286-294, Oxford University Press, 1979.

[13] J. R. Parks, "Personal identification - biometrics," *in Information Security* (D. T. Lindsay and W. L. Price, eds.), pp. 181-191, North Holland: Elsevier Science, 1991.

[14] R. G. D. Steel and J. H. Torrie, *Principles and Procedures of Statistics: A Biometrical Approach* (McGraw-Hill Series in Probability and Statistics), New York: McGraw-Hill, third ed., 1996.

[15] R. Clarke, "Human identification in information systems: Management challenges and public policy issues," *Information Technology & People*, Vol. 7, No. 4, pp. 6-37, 1994.

[16] E. Newham, *The Biometric Report*. http://www.sjb.com/: SJB Services, New York, 1995.

[17] S. Furui, "Recent advances in speaker recognition," in *Lecture Notes in Computer Science 1206, Proceedings of Audio- and Video Biometric Person Authentication AVBPA'97, First*

International Conference, Crans-Montana, Switzerland, March 12-14, pp. 237-252, Springer-Verlag, Berlin, 1997.

[18] F. J. Prokoski, R. B. Riedel, and J. S. Coffin, "Identification of individuals by means of facial thermography," in *Proceedings of The IEEE 1992 International Carnahan Conference on Security Technology: Crime Countermeasures, Atlanta, GA, USA 14-16 Oct.*, pp. 120-125, IEEE, 1992.

[19] F. J. Prokoski, "NC-TEST: noncontact thermal emissions screening technique for drug and alcohol detection," in *Proc. SPIE: Human Detection and Positive Identification: Methods and Technologies* (L. A. Alyea and D. E. Hoglund, eds.), Vol. 2932, pp. 136-148.

[20] M. Turk and A. Pentland, "Eigenfaces for recognition", *Journal of Cognitive Neuroscience*, Vol. 3, No. 1, pp. 71-86, 1991.

[21] D. Swets and J. J. Weng, "Using discriminant eigenfeatures for image retrieval," *IEEE Trans. Pattern Analysis and Machine Intelligence*, Vol. 18, pp. 831-836, August 1996.

[22] J. J. Atick, P. A. Griffin, and A. N. Redlich, "Statistical approach to shape from shading: Reconstruction of 3-dimensional face surfaces from single 2-dimensional images," *Neural Computation*, Vol. 8, pp. 1321-1340, August 1996.

[23] P. J. Phillips, P. J. Rauss, and S. Z. Der, "The FERET (Face Recognition Technology) evaluation methodology," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition 97, June 17-19*, (San Juan, Puerto Rico), 1997.

[24] J. G. Daugman, "High confidence visual recognition of persons by a test of statistical independence," *IEEE Trans. Pattern Analysis and Machine Intelligence*, Vol. 15, No. 11, pp. 1148-1161, 1993.

[25] T. Julian, L. A. Vontver, and D. Dumesic, *Review of Obstetrics & Gynecology*. Stanford, CT: Appleton and Lange, 1995.

[26] D. Cunado, M. S. Nixon, and J. N. Carter, "Using gait as a biometric, via phase-weighted magnitude spectra," in *Lecture Notes in Computer Science 1206, Proceedings of Audio- and Video- Biometric Person Authentication AVBPA'97, First International Conference, Crans-Montana, Switzerland, March 12-14* (J. Bigun, G. Chollet, and G. Borgefors, eds.), pp. 95-102, Springer-Verlag, Berlin, 1997.

[27] S. A. Bleha and M. Obaidat, "Computer users verification using the perceptron algorithm," *IEEE Trans. Systems Man Cybernetics*, Vol. 23, pp. 900-902, 1993.

[28] V. Nalwa, "Automatic on-line signature verification," *Proceedings of the IEEE*, Vol. 85, pp. 213-239, February 1997.

[29] British Technology Group, "Automatic signature verification using acoustic emissions," *http://www.btgusa.com/security/prod1.html*, 1997.

[30] T. A. Dickinson, J. White, J. S. Kauer, and D. R. Walt, "A chemical-detecting system based on a cross-reactive optical sensor array," *Nature*, Vol. 382, pp. 697-700, 1996.

[31] M. Howard, "Artificial nose may be able to sniff out land mines," *http://www.tufts.edu/communications/tech.html*, 1997.

[32] RAYCO Security, "Eyedentify retina biometric reader," http://www.raycosecurity.com/-*hirsch/EyeDentify.html*, 1997.

[33] "Biometric Technology Today," *http://www.sjb.co.uk/*, November 1996.

[34] Biomet Partners Inc., "Positive verification of a person's identity: Digi-2 3-dimensional finger geometry," *http://www.webconsult.ch/biomet.htm*, 1997.

[35] S. C. Davies, "Touching big brother: How biometric technology will fuse flesh and machine," *Information Technology & People*, Vol. 7, No. 4, pp. 60-69, 1994.

[36] B. Miller, "Vital signs of identity," *IEEE Spectrum*, Vol. 31, No. 2, pp. 22-30, 1994.

[37] H. T. F. Rhodes, *Alphonse Bertillon: Father of Scientific Detection*. Abelard-Schuman, New York, 1956.

[38] America Online, "Biometrics in news," *http://members.aol.com/biometric/news.html*, 1997.

[39] J. Bigun, C. Chollet, and C. Borgefors, (editors), *Lecture Notes in Computer Science 1206, Proceedings of Audio- and Video- Biometric Person Authentication AVBPA'97, First International Conference, Crans-Montana, Switzerland, March 12-14*. Springer-Verlag, Berlin, 1997.

[40] "Asian Conference on Computer Vision: Special Session on Biometrics, January 8-11, Hong Kong," *http://www.vic.ust.hk/accv98*, 1998.

[41] *Proceedings of Biometric Consortium Eighth Meeting, San Jose, California*. June 1996.

[42] *Proceedings of Biometric Consortium Ninth Meeting, Crystal City, Virginia*. April 1997.

[43] "31st Asilomar Conference on Signals, Systems, and Computers, Pacific Grove, CA, November 2-5," *http://dubhe.cc.nps.navy.mil/asilomar/*, 1997.

[44] "Workshop on Automatic Identification and Technology, November 6-7, Stony Brook, NY," *http://www.cs.sunysb.edu/simtheo/waiat*, 1998.

[45] "Face Recognition: From Theory to Applications, NATO Advanced Study Institute (ASI) Program, June 23 - July 4, Stirling, Scotland, UK," *http://chagall.gmu.edu/faces97-/natoasi/*, 1997.

[46] *CardTech/SecurTech: Technology and Applications*. May 1997.

[47] "Biometricon'97, Arlington, VA, March 13-14," *http://www.ncsa.com/cbdc/cbdc-c.html*, 1997.

[48] "The Biometric Consortium," http://www.biometrics.org/.

[49] "Commercial Biometrics Developer Consortium (CBDC)," *http//www.ncsa.com/cbdc/*, 1997.

[50] *Proceedings of the IEEE (Special Issue on Automated Biometrics)*, Vol. 85, September 1997.

[51] "Biometric Technology Today," http://www.sjb.co.uk/.

[52] "Automatic I. D. News homepage," *http://www.autoidnews.com/*, 1997.

[53] D. Mintie, "Welfare ID at the point of transaction using fingerprint and 2D bar codes," in *Proc. CardTech/SecurTech, Volume II: Applications*, (Atlanta, Georgia), pp. 469-476, May 1996.

[54] "INS Passenger Accelerated Service System (INSPASS)," *http://www.biometrics.org:8080/~BC/REPORTS/INSPASS.html*, 1996.

[55] S. Hunt, "National ID programs around the world," in *Proc. CardTech/SecurTech, Vol. II: Applications*, (Atlanta, Georgia), pp. 509-520, May 1996.

[56] R. Bolle, N. Ratha, and S. Pankanti, "Research issues in biometrics," in *Proceedings of Asian Conference on Computer Vision: Special Session on Biometrics, January, 8-11, Hong Kong*, (http://www.vic.ust.hk/accv98), 1998.

[57] Mytec Technologies, "Access control applications using optical computing," *http//www.mytec.com/*, 1997.

[58] R. Bahuguna, "Fingerprint verification using hologram matched filterings," in *Proceedings Biometric Consortium Eighth Meeting*, (San Jose, California), June 1996.

[59] Federal Bureau of Investigation*, The Science of Fingerprints: Classification and Uses*. Washington, D.C.: U.S. Government Printing Office, 1984.

[60] J. G. Daugman and G. O. Williams, "A proposed standard for biometric decidability," in *Proc. CardTech/SecureTech Conference*, (Atlanta, CA), pp. 223-234, 1996.

[61] J. P. Campbell, L. A. Alyea, and J. S. Dunn, "Biometric security: Government applications and operations," *http://www.biometrics.org/,* 1996.

[62] J. Kittler, Y. P. Li, J. Matas, and M. U. Ramos Sànchez, "Combining evidence in multimodal personal identity recognition systems," in *Lecture Notes in Computer Science 1206, Proceedings of Audio- and Video- Biometric Person Authentication AVBPA'97, First International Conference, Crans-Montana, Switzerland, March 12-14*, pp. 327-334, Springer-Verlag, Berlin, 1997.

[63] R. Brunelli and D. Falavigna, "Person identification using multiple cues," *IEEE Trans. Pattern Analysis and Machine Intell*igence, Vol. 10, pp. 955-966, October 1995.

[64] U. Dieckmann, P. Lankensteiner, R. Schamburger, B. Froba, and S. Meller, "SESAM: A biometric person identification system using sensor fusion," in *Lecture Notes in Computer Science 1206, Proceedings of Audio- and Video- Biometric Person Authentication AVBPA'97, First International Conference, Crans-Montana, Switzerland, March 12-14*, pp. 301-310, Springer-Verlag, Berlin, 1997.

[65] E. S. Bigun, J. Bigun, B. Duc, and S. Fischer, "Expert conciliation for multi modal person authentication system by Bayesian statistics," in *Lecture Notes in Computer Science 1206, Proceedings of Audio- and Video- Biometric Person Authentication AVBPA'97, First International Conference, Crans-Montana, Switzerland, March 12-14*, pp. 291-300, Springer-Verlag, Berlin, 1997.

[66] L. Hong and A. Jain, "Integrating faces and fingerprints for personal identification," in *Proceedings of Asian Conference on Computer Vision: Special Session on Biometrics, January, 8-11, Hong Kong*, (http://www.vic.ust.hk/accv98), 1998.

[67] R. R. Tenney and N. R. Sandell, "Structures for distributed decision making," *IEEE Trans. on Systems, Man, and Cybernetics*, Vol. 11, pp. 517-526, August 1981.

[68] R. R. Tenney and N. R. Sandell, "Strategies for distributed decision making," *IEEE Trans. on Systems, Man, and Cybernetics*, Vol. 11, pp. 527-538, August 1981.

[69] S. J. McPhee, M. A. Papadakis, L. M. Tierney, and R. Gonzales, *Current Medical Diagnosis and Treatment*. Stamford, CT: Appleton and Lange, 1997.

[70] K. Inman, and N. Rudin, *An Introduction to Forensic DNA Analysis*. CRC Press, Boca Raton, Florida, 1997.