Biometrics: Promising frontiers for emerging identification market

Anil Jain
Michigan State University
East Lansing, MI

Lin Hong
Visionics Corp.
Jersey City, NJ

Sharath Pankanti
IBM Research
Hawthorne, NY

An accurate automatic personal identification is critical to a wide range of application domains such as access control, electronic commerce, and welfare benefits disbursement. Traditional personal identification methods (e.g., passwords, PIN) suffer from a number of drawbacks and are unable to satisfy the security requirement of our highly inter-connected information society. Biometrics refers to automatic identification of an individual based on her physiological or behavioral traits. While biometrics is not an identification panacea, it is beginning to provide very powerful tools for the problems requiring positive identification.

INTRODUCTION

Personal identification is to associate a particular individual with an identity. Identification could be (i) verification: authenticating a claimed identity (Am I who I claim am I?) or (ii) recognition (also sometimes called as "identification"): determining the identity of a given person from a database of persons known to the system (Who am I?). Questions related to the identity of individuals such as *"Is this the person who he or she claims to be?", "Has this applicant been here before?", "Should this individual be given access to our system?"*, *etc.* are asked millions of times every day by hundreds of thousands of organizations in financial services, health care, electronic commerce, telecommunication, government, *etc.* The combined annual estimate of the identity fraud in welfare disbursements ($1 billion) credit card transactions ($1 billion), cellular phone ($1 billion), and ATM withdrawals ($3 billion) totals over $6 billion. Automated identity authentication will provide increased levels of customer satisfaction and higher levels of efficiency in diverse businesses (e.g., security, e-commerce, hospitality, health care, government, and telecommunications), save critical resources, and may serve as key differentiators in the business solutions (see Figure 1). With the rapid evolution of information technology, people are becoming even more and more electronically connected. As a result, the ability to achieve a highly accurate *automatic* personal identification is becoming more critical [5].

Traditionally, two major types of automatic personal identification approaches have been widely used: (*i*) *knowledge-based* and (*ii*) *token-based* [9]. Token-based approaches use "something that you have" to make a personal identification, such as passport, driver's license, ID card, credit card, and keys. Knowledge-based approaches use "something that you know" to make a personal identification, such as *password* and *personal identification number* (PIN). Since these traditional approaches are not based on any inherent attributes of an individual to make a personal identification, they suffer from a number of disadvantages: tokens may be lost, stolen, forgotten, or misplaced; PIN may be forgotten or guessed by the impostors. Surprisingly, 25% of people appear to write their PIN on their ATM card, thus defeating the protection offered PIN when ATM cards are stolen [5]. All of these approaches are also unable to differentiate between an *authorized person* and an *impostor* who fraudulently acquires the "token" or "knowledge" of the authorized person [9]. Therefore, knowledge-based and token-based approaches are *unable* to satisfy the security requirements of our electronically inter-connected information society.

BIOMETRICS

Biometrics, which refers to identifying an individual based on her physiological or behavioral characteristics (biometric identifiers) [5], relies on "who you are or what you do" to make a *positive* personal identification. It is inherently more reliable and more capable than knowledge-based and token-based techniques in differentiating between an authorized person and a fraudulent impostor, because many of the physiological or behavioral characteristics are distinctive to each person.

Biometric System

A *biometric system* is essentially a pattern recognition system which makes a personal identification by establishing the authenticity of a specific physiological or behavioral characteristic possessed by the user. The block diagram of a generic biometric system is depicted in Figure 2. Logically, it can be divided into two modules: (*i*) *enrollment module* and (*ii*) *identification module.* The enrollment module is responsible for enrolling individuals into the biometric system. During the enrollment phase, the biometric characteristic of an individual is first scanned by a biometric sensor to acquire a digital representation of the characteristic. In order to facilitate matching and to reduce the storage requirements, the digital representation is further processed by a feature extractor to generate a compact but expressive representation, called a *template.* Depending on the application, the template may be stored in the central database of the biometric system or be recorded on a *magnetic card* or *smart card* issued to the individual. The identification module is responsible for identifying individuals at the point-of-access. During the operation phase, the biometric reader captures the characteristic of the individual to be identified and converts it to a digital format, which is further processed by the feature extractor to produce the same representation as the template. The resulting representation is fed to the feature matcher which compares it against the template(s) to establish the identity of the individual.

Biometric Identifiers

An ideal biometric should meet the following requirements [5]: (*i*) *universality*: each person should have the characteristic, (*ii*) *uniqueness*: no two persons should be the same in terms

SEGURIDAD SOCIAL
Tesorería General de la Seguridad Social
DOCUMENTO DE AFILIACION A LA SEGURIDAD SOCIAL
12 3456789012
JUAN
MUESTRA
12345678-K
ESPAÑOL ESPAÑOL
MINISTERIO DE TRABAJO Y SEGURIDAD SOCIAL
Secretaria General para la Seguridad Social
FIRST UNION
100
VISA
VISA Cash

(a) National ID card

(b) Smartcard

(c) ATM

(d) Logon

Figure 1: Applications of biometrics.

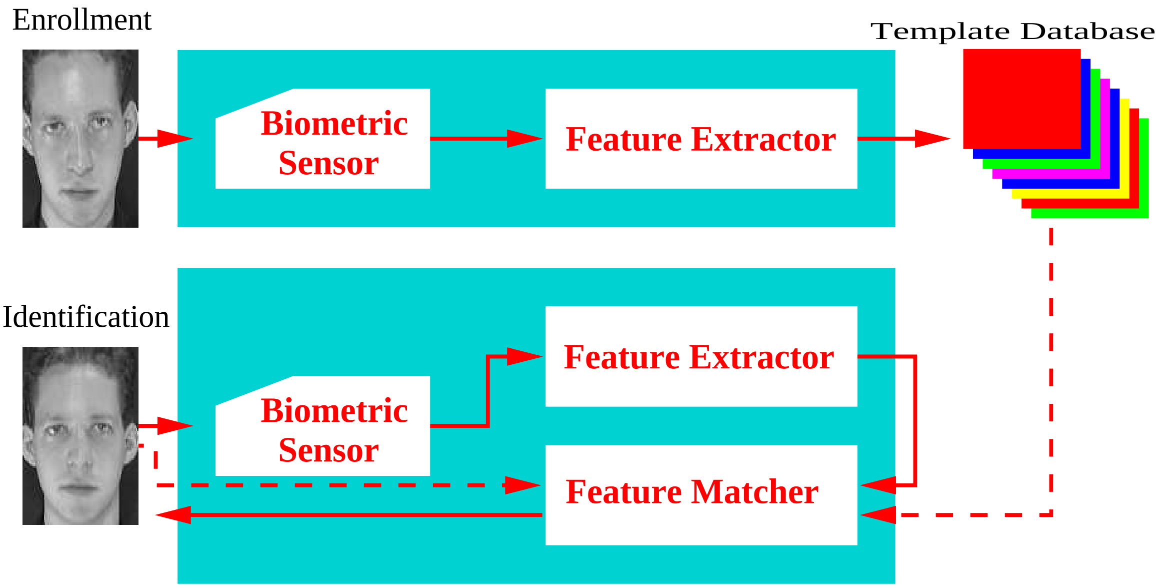


Figure 2: A generic biometric system.

of the characteristic, (*iii*) *permanence*: the characteristic should neither change not could be altered, and (*iv*) *collectability*: the characteristic can be measured quantitatively. However, in practice, a biometric characteristic that satisfies all the above requirements may not always be feasible for a practical biometric system. In a practical biometric system, there are a number of other issues which should be considered, including (*i*) *performance*, which refers to the achievable identification accuracy, speed, robustness, the resource requirements to achieve the desired identification accuracy and speed, as well as operational or environmental factors that affect the identification accuracy and speed, (*ii*) *acceptability*, which indicates the extent to which people are willing to accept a particular biometric identifier in their daily lives, and (*iii*) *circumvention*, which reflects how easy it is to fool the system by fraudulent methods.

Operational Mode

An important issue in designing a practical biometric system is to determine how an individual should be identified. Depending on the application context, a biometric system may be either a *verification (authentication)* system or an *identification* system [5]. A verification system authenticates a person's identity by comparing the captured biometric characteristic with her own biometric template(s) pre-stored in the system. In a verification (authentication) system, an individual desired to be identified submits a claim to an identity to the system usually via a magnetic stripe card, login name, smart card, *etc.*, and the system either rejects or accepts the submitted claim of identity. An identification system recognizes an individual by searching the entire template database for a match. In an identification system, the system establishes a subject's identity (or fails if the subject is not enrolled in the system database) without the subject having to claim an identity.

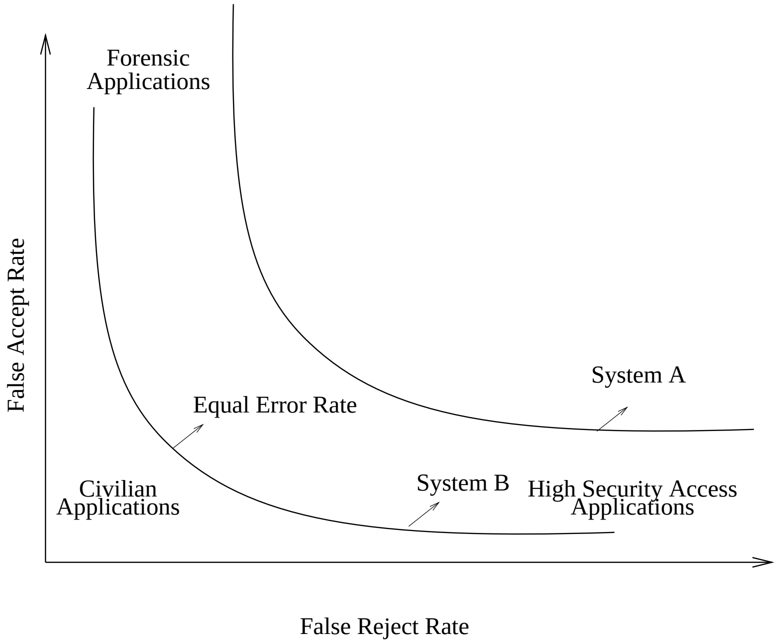


Figure 3: Receiver operating characteristics (ROC) of a system illustrates false reject rate (FRR) and false acceptance rate (FAR) of a matcher at all operating points. Each point on an ROC defines FRR and FAR for a given matcher operating at a particular matching score threshold. Note that System A is consistently inferior to System B in accuracy performance.

Performance

The overall performance of a biometric system is assessed in terms of its (i) accuracy, (ii) speed, and (iii) storage. Several other factors like cost and ease-of-use also affect the efficacy of biometric-identification system. Biometric identification systems are (will be) typically not perfect and make errors in correctly recognizing genuine identities and in correctly rejecting impostors. The error of the first type is called a “false negative” and the second type of error is called a “false positive”. The probability of committing these two types of errors are termed as, *false reject rate* (FRR) and *false acceptance rate* (FAR), respectively; the magnitudes of these errors depend upon how liberally/conservatively a biometric system determines whether two measurements originate from the same individual. A smaller FRR (i.e., a more tolerant system) usually leads to a larger FAR while a smaller FAR (i.e., a less tolerant system) usually implies a larger FRR. The graph showing trade-off between a system’s FAR and FRR at different operating points is called the Receiver Operating Characteristics (ROC) and is a comprehensive measure of the system accuracy (see Figure 3). 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. The error rate of the system at an operating point where FAR equals FRR is called equal error rate (EER) which is often used as a terse description of system accuracy.

The size of a template the number of templates stored per individual, and availability of compression mechanisms determine the storage required per user. When template sizes are large and the templates are stored in a central database, network bandwidth may become a system bottleneck for identification. A typical smartcard may only hold few kilobytes (e.g., 8K) and in systems using smartcards to distribute template storage, template sizes become critical design issue.

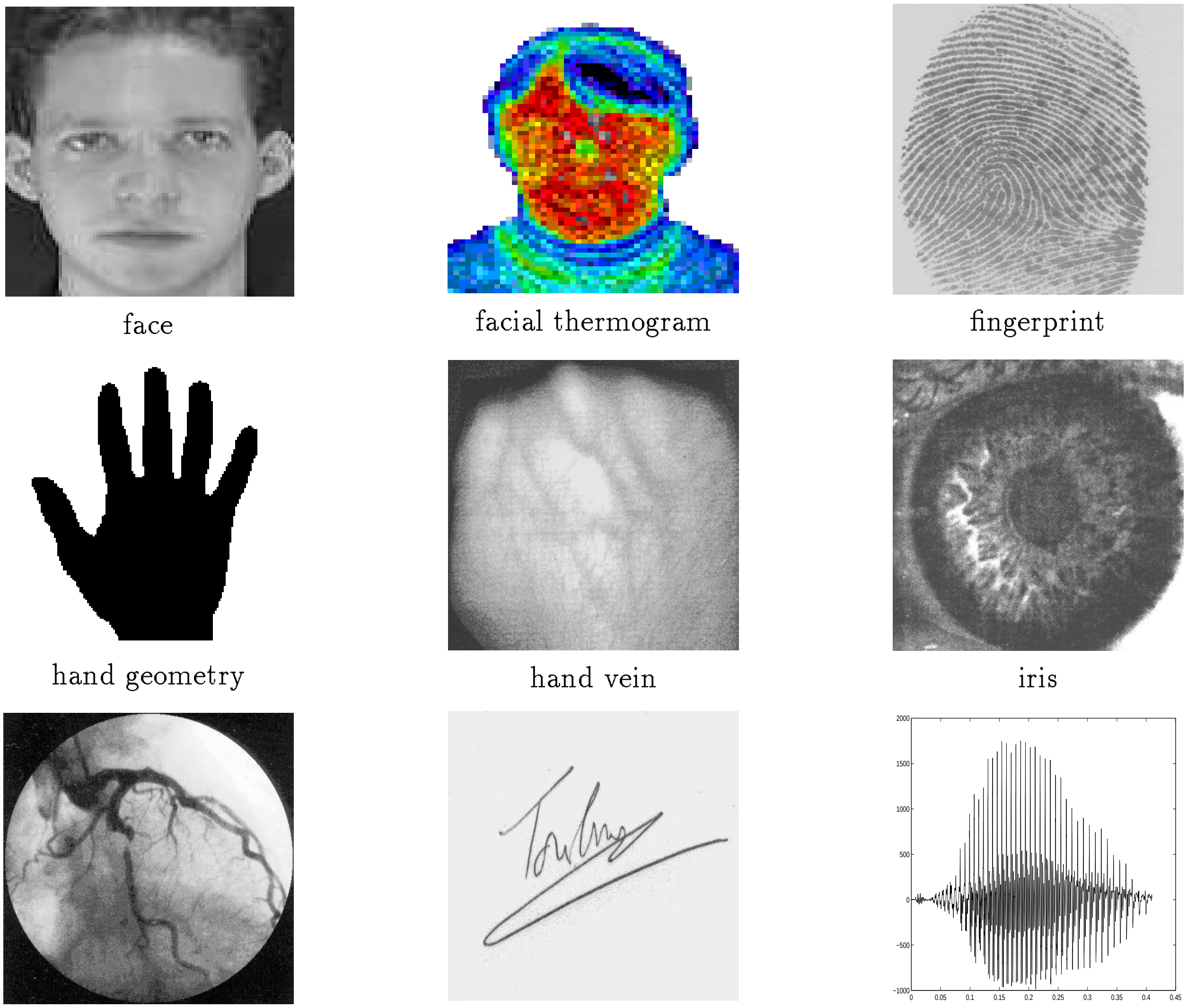
The time required by a biometric system to make an identification decision is critical to many applications. For a typical access control application, the system needs to make an authentication decision in real-time. In an ATM application, for instance, it is desirable to accomplish the authentication within about one second. For forensic applications, however, the time requirements may not be very stringent.

All other factors remaining identical, the widespread use of biometrics will be stimulated by its adoption in the consumer market. The single most important factor affecting this realization is the cost of the biometrics systems; this includes the cost of the sensors and the related infrastructure. Some sensors are already very inexpensive (e.g., microphones). Others types of sensors are already becoming standard peripherals in a personal computing environment (e.g., camera). With the recent availability of solid state technology, fingerprint sensors will become sufficiently inexpensive in the next few years. The storage requirements for representing biometric measurements (templates) and processing requirements for matching are among the two major considerations towards the infrastructure cost.

The human factors issue is also a critical factor to the success of a biometric-based identification. How easy and comfortable to acquire a given biometric? For example, non-contact biometrics like face, voice, iris, may be perceived as more user-friendly. Additionally, biometric technologies requiring very little cooperation/participation from users (e.g., face and thermograms), may be perceived as more convenient to users. A related issue is public acceptance. There may be a generally prevalent perception that biometrics are a threat to the privacy of an individual. The general masses need to be educated that biometrics could be one of the effective (i.e.,profitable in long term) means of protecting individual privacy. Like in any industry, government regulations directives may lead to boost or demise of certain types of biometric technologies. The upcoming legislations (e.g., Health Information Portability Act – HIPA) may have a favorable impact on the biometrics industry. It is quite likely that some of the well-established companies may be trusted for handling a “third-party” biometric-based authentication. Another “less-resistant” avenue for both piloting and gaining gradual acceptance of a biometrics solution could be to introduce it in a captive market, e.g., intra-business solutions like time and attendance monitoring for employees within an organization.

APPLICATIONS

Biometrics is a rapidly evolving technology which has been widely used in forensics such as criminal identification and prison security. More recently, it is being seriously considered for adoption in a broad range of civilian applications. *Electronic commerce and electronic banking* are two of the most important and emerging application areas of biometrics due to the rapid progress in electronic transactions. These applications include electronic fund transfers,



face

facial thermogram

fingerprint

hand geometry

hand vein

iris

retinal scan

signature

voice print

Figure 4: Examples of different biometric characteristics [5].

ATM security, check cashing, credit card security, smart cards security, online transactions, *etc*. Currently, there are several large biometric security projects in these areas under development, including credit card security (MasterCard) and smart card security (IBM and American Express). A variety of biometric technologies are now competing to demonstrate their efficacy in these application areas. *The market of physical access control* is currently dominated by token-based technology. However, it is predicted that, with the progress in biometric technology, market share will increasingly shift to biometric techniques. *Information system/computer network security* such as user authentication and access to databases via remote login is another important potential application area for biometrics. It is expected that more and more information systems/computer networks will be secured with biometrics with the rapid expansion of Internet and Intranet. With the introduction of biometrics, *government benefits distribution program* such as welfare disbursement programs will experience substantial savings in deterring multiple claimants. In addition, *customs and immigration*

Forensic	**Civilian**	**Commercial**
Criminal Investigation	National ID	ATM
Corpse identification	Driver's license	Credit card
Parenthood determination	Welfare disbursement	Cellular
	Border crossing	Access control

Table 1: Biometric Applications

initiatives such as *INS* Passenger Accelerated Service System (INSPASS) which permits faster immigration procedures based on hand geometry will greatly increase the operational efficiency. Biometrics-based *national ID systems* provide a unique ID to the citizens and integrate different government services. Biometrics-based *voter and driver registration* provides registration facilities for voters and drivers. Biometrics-based *time/attendance monitoring systems* can be used to prevent any abuses of the current token-based/manual systems.

Biometric Technologies

Currently, there are mainly nine different biometric techniques that are either widely used or are under intensive investigation, including *face, fingerprint, hand geometry, hand vein, iris, retinal pattern, signature, voice-print, and facial thermogram.* Examples of these nine different biometric characteristics are shown in Figure 4.

Face

Facial images are probably the most common biometric characteristic used by humans to make a personal identification. Face recognition is one of the most active area of research with applications ranging from static, controlled mug shot verification to dynamic, uncontrolled face identification in a cluttered background [2]. Face recognition is a non-intrusive technique and people generally do not have any problem in accepting face as a biometric characteristic. During the past 25 years, a substantial amount of research effort has been devoted to face recognition [2]. Approaches to face recognition are typically based on either (i) location and shape of facial attributes such as eyes, eyebrows, nose, lips, chin shape, *etc* [2] and their spatial relationships or (ii) overall (global) analysis of the face image and the decomposition of face into a number of canonical faces. A number of commercial face recognition systems are available [1]. While the performance of these systems is reasonable, it is questionable whether the face itself, without any contextual information, is sufficiently effective to make a personal identification with a high level of confidence. Further, current face recognition systems impose a number of restrictions on how the facial images are acquired (e.g., simple background, uniform and fixed illumination). In order for the face recognition to be widely adopted, they should be automatically (*i*) detect whether there exists a face in the acquired image, (*ii*) locate the face if there is one, and (*iii*) recognize the face from a general viewpoint. These issues highlight some of the difficulties in face recognition.

Facial Thermogram

The underlying vascular system in the human face produces a unique facial signature when heat passes through the facial tissue and is emitted from the skin [10]. Such facial signatures can be captured using an infrared camera, resulting in an image called a face thermogram. It is believed that a face thermogram is unique to each individual and they are not vulnerable to disguises. Even plastic surgery, which does not reroute the flow of blood through the veins, cannot change the formation of the face thermogram. An infrared camera can capture the face thermogram in low/changing ambient light or in the absence of any light at all, which greatly reduces the restrictions on how face thermograms are acquired. Face thermogram is a non-intrusive biometric technique which can verify an identity without contact, without full camera view, and without the cooperation of subjects. It is claimed that face thermogram-based recognition is superior to face recognition using CCD cameras [10]. Although it may be true that face thermograms are unique to each individual, it has not been proven that face thermograms are sufficiently discriminative. Face thermograms depend heavily on a number of factors such as the emotion of the subjects, the body temperature, *etc.* and like face recognition, face thermogram recognition is view-dependent.

Fingerprints

A fingerprint is the pattern of ridges and furrows on the surface of a fingertip. Its formation is determined during the fetal period. Fingerprints of identical twins are different and there is no correlation between the prints on the different fingers of an individual. Fingerprints are one of the most understood and studied biometrics [6]. Humans have used fingerprints for personal identification for centuries and the validity of fingerprint identification has been well-established. With the development of solid state sensors, the marginal cost of incorporating a fingerprint-based biometric system may soon become affordable in many applications. Consequently, fingerprints are expected to lead the biometric applications in the near future. Fingerprints have sufficient information to allow large scale identification. One problem with fingerprint technology is its acceptability by a typical user, because fingerprints have traditionally been associated with criminal investigations and police work. People may feel uncomfortable in using fingerprints in civilian applications. Another problem with fingerprint technology is that automatic fingerprint identification generally requires a large amount of computational resources. Fingerprints of a small fraction of population may be unusable for automatic identification because of genetic, aging, environmental, or occupational reasons.

Hand Geometry

A variety of measurements of the human hand including its shape and lengths and widths of the fingers, *etc.* can be used as biometric characteristics [8]. Hand geometry-based biometric systems have been installed at literally thousands of locations around the world. The technique is very simple, relatively easy to use, and is inexpensive. Operational environmental factors (e.g., dry weather) or individual anamolies (e.g., dry skin) generally have virtually no negative effects on the identification accuracy. It does not appear to be a problem for people to accept this technology. A main disadvantage of this technique is its low discriminative capability – it is very difficult for a hand geometry-based biometric system to achieve a very high identification accuracy especially for a large population. The physical size of a hand geometry-based system is large, which may restrict it from certain applications such as laptop computers. The existing systems may have problems sensing the hand geometry measurements from individuals with limited dexterity (e.g., due to arthritis). Hand geometry information may not remain invariant permanent biometric characteristic over the lifespan of an individual, especially, during the childhood. Different types of rings may pose additional challenges in extracting the correct hand geometry information.

Hand Vein

Hand veins provide a very robust and stable pattern that can be used as a biometric characteristic to make a personal identification [11]. Digitized images of hand vein patterns can be easily captured with an infra-red camera. Hand vein patterns are unique to each individual. It is very difficult to change the formation of the hand vein pattern of an individual by surgery. Thus, hand vein based technique is very efficient in circumventing fraudulent attempts. A hand vein-based biometric system has the potential to achieve a reasonable identification accuracy and people are normally willing to accept it. However, there is no hand vein-based biometric system available that is able to demonstrate its superior capability in conducting automatic personal identification. Like hand geometry, it might be very difficult for a hand vein-based biometric system to achieve a very high identification accuracy. The physical size of a hand vein-based system is large. Hand vein patterns could be obliterated due to medical conditions (e.g., obesity, aging).

Retinal Pattern

The pattern formed by veins beneath the retinal surface in an eye is stable and unique [12]. Digital images of retinal patterns can be acquired by projecting a low-intensity beam of visual or infrared light into the eye and an image of the retina thus illuminated is captured using optics similar to a retinascope. In order that a fixed portion of the retinal vasculature is used for identification, the subject is required to closely gaze into an eye-piece and focus on a predetermined spot in the visual field. Retinal pattern based identification is very accurate. The degree of user cooperation/involvement required in imaging a retina may not be acceptable to the subjects undergoing identification. Retinal scan is currently perceived to be the most secure biometric technique. A large number of retinal scan-based biometric systems have been installed in several highly secure environments (e.g., prisons). The disadvantage of this biometrics is that retinal scanners are expensive.

Iris

Iris is the annular region of eye bounded by pupil and sclera (white of the eye) on either side. Visual texture of iris stabilizes very early (first 2 years) in life and its complex structure carries very distinctive information useful for identification of individuals. Initial available results on accuracy and speed of iris-based identification are extremely promising and point to the feasibility of a large scale identification using iris information. Each iris is unique and even irises of identical twins are different. Iris is more readily imaged than retina. Although the early iris-based identification systems needed a considerable user participation and were expensive, efforts are underway to build more user-friendly and cost effective versions. It remains to be seen how this relatively recently discovered biometric matures and gains public acceptance. It is extremely difficult to surgically tamper iris texture information and it is easy to detect artificial irises (e.g., designer contact lenses) [3].

Signature

Each person has a unique style of handwriting. No two signatures of a person are exactly identical; the variations from a typical signature also depend upon the physical and emotional state of a person. Despite the variations in an individuals signatures, a few successful systems for signature-based authentication systems have been designed [7]. The authentication accuracy of signature-based biometric systems is reasonable but does not appear to be sufficiently high to lead to large scale identification. There are two approaches to signature verification: (*i*) static and (*ii*) dynamic. Static signature verification uses only the geometric (shape) features of a signature. Dynamic signature verification uses both the geometric (shape) features and the dynamic features such as acceleration, velocity, and trajectory profiles of the signature. An inherent advantage of a signature-based biometric system is that the signature has been established as an acceptable form of personal identification method and can be "transparently" incorporated into the existing business processes requiring signatures (e.g., credit card transactions). Another advantage of signature is that it is impossible for an impostor to obtain the dynamics information from a written signature.

Speech

The characteristics of human speech are determined by the shape/size of the appendages (e.g., vocal tracts, mouth, nasal cavities, lips) systhesizing the sound [4]. Speech of a person is distinctive but may not contain sufficient information to offer speech-based identification. Speech-based verification could be either a text-dependent verification or a text-independent verification. A text-dependent verification authenticates the identity of an individual based on utterance of a fixed predetermined phrase. A text-independent verification verifies the identity of a speaker independent of the phrase, which is more difficult than a text-dependent verification but offers more protection against fraud. Existing commercial speaker verification systems can achieve a reasonable identification accuracy. Generally, people are willing to accept a speech based biometric system. However, speech-based features are are sensitive to a number of factors such as background noise as well as the emotional and physical state of the speaker. In addition, some people seem to be extraordinarily skilled in mimicking other's voice which may be a reason why speech-based authentication is perceived to be of low-security.

Comparison of Biometric Technologies

Each of the biometric technique reviewed above has its own advantages and disadvantages. A brief comparison of these biometric techniques along seven factors is provided in Table 2.

Table 2: Comparison of Biometric Technologies based on perception of three biometrics experts [5].

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.Thermogram	high	high	low	high	medium	high	high

The applicability of a specific biometric technique depends heavily on the application domain. For example, an authentication application (e.g., access to a nuclear facility) requiring 0.1% FAR and FRR can not be realistically met by speech-based system. No single technique can outperform all the others in all operational environments. In this sense, each biometric technique is *admissible*. For example, it is well known that both the fingerprint technique and the iris scan technique perform much better than the voice print technique in terms of accuracy and speed. However, in a telephone account security application, the voice print technique is preferred, because it can be integrated seamlessly into the existing telephone system. It is expected that the future generations of identification systems will increasingly rely on systems integrating multiple biometrics and technologies to obtain robust performance.

A Case Study

Two primary components of a biometric-based identification system are the feature extraction and matcher. This section summarizes typical steps involved in these two components in case of fingerprint-based authentication system.

The unprocessed input values of the fingerprint images are not invariant over the time of capture and typically, landmark features on a finger, e.g., the fingerprint ridge endings and ridge bifurcations (collectively known as minutiae) are used in a fingerprint-based authentication system. A fingerprint feature extraction system detects the minutiae from the input fingerprint image through a series of complex image processing steps (See Figure 5). The feature vector, typically, consists of a list of the locations and other attributes (e.g., orientation of the ridge) of the minutiae detected in a fingerprint image.

A fingerprint matcher (see Figure 6) takes two fingerprint feature vectors and determines whether the minutiae in the feature vectors originate from the same finger based on the minutiae attributes. The feature vectors can not be directly compared from their original representation as the sensed fingers may be differently aligned with respect to the imaging system. The feature vectors are typically aligned based on, for example, any landmark information in the feature vector. In this particular example (Figure 6(c)), the properties of a segments of ridges adjoining a pair ridge ending minutiae are used to align the feature vectors. The number of "corresponding" minutiae, i.e., minutiae in the close neighborhood of each other with similar attributes constitutes a basis for quantifying likelihood of fingerprint feature vectors originating from the same finger.

Summary

Biometrics refers to automatic identification of a person based on her physiological or behavioral characteristics. It provides a better solution for the increased security requirements of our information society. As biometric sensors continue to become less expensive (and miniaturized), as the negative perception of biometrics as encroachment on individual privacy continue to decline, and as the public realizes that biometrics is actually an effective

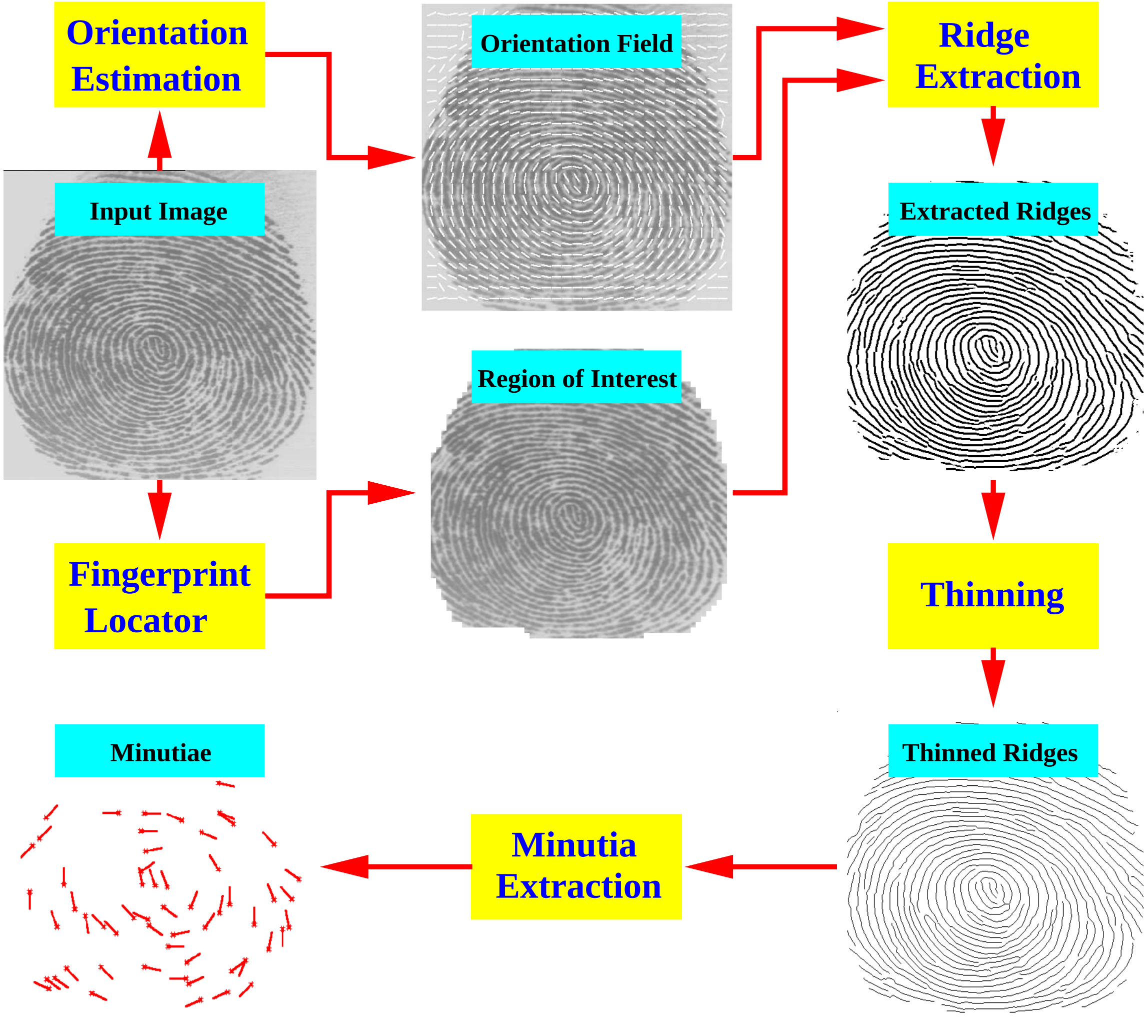
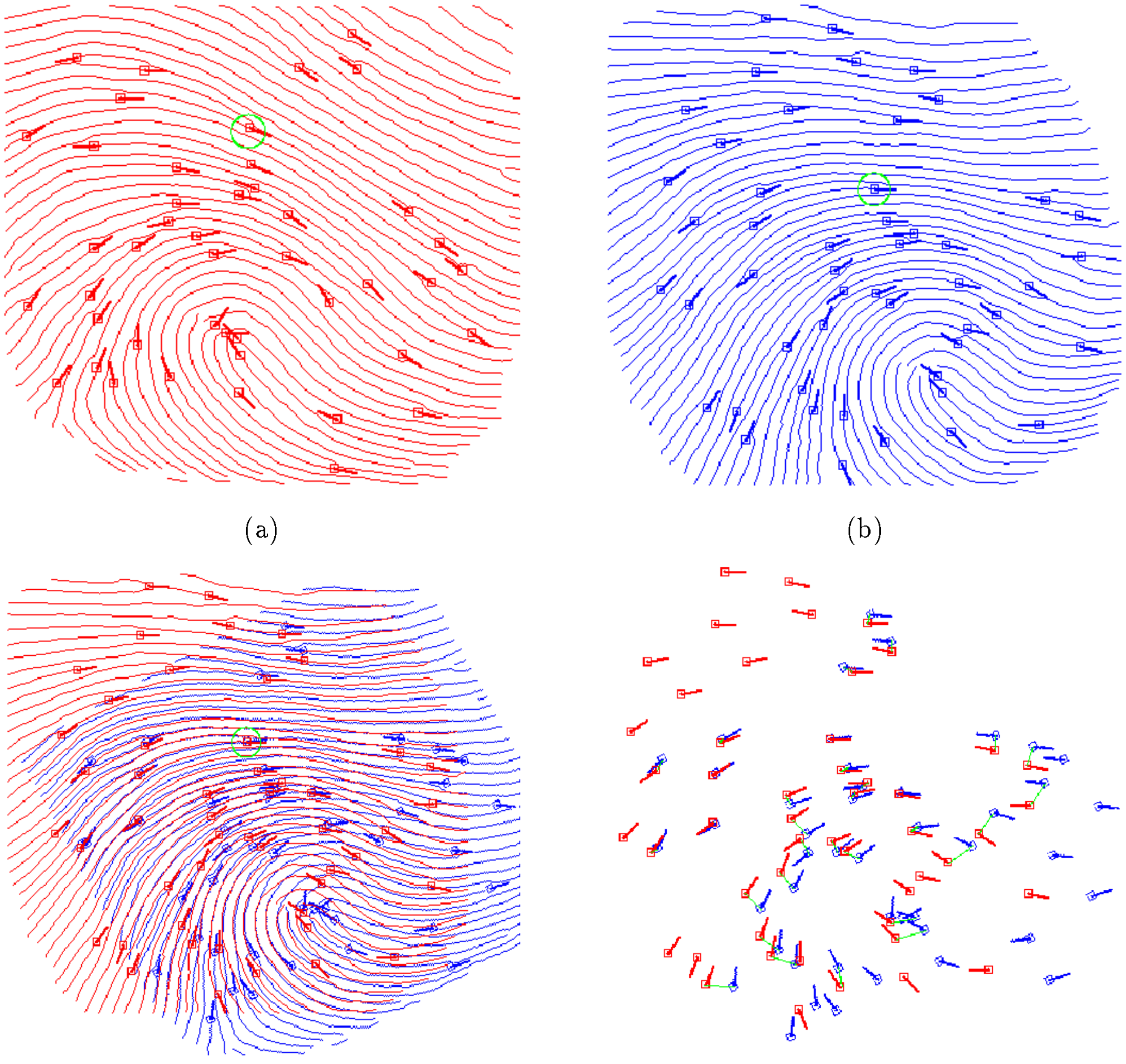


Figure 5: Feature extraction process starting from fingerprint image to extraction of the features called "minutiae", which are endings and birfurcations of fingerprint ridges [6].



(a)

(b)

(c)

(d)

Figure 6: Results of applying the matching algorithm to an input minutiae set and a template; (a) input minutiae set; (b) template minutiae set; (c) alignment result based on the minutiae marked with green circles; (d) matching result where template minutiae and their correspondences are connected by green lines [6].

strategy for protection of privacy/fraud, this technology is likely to be used in almost every transaction needing authentication of personal identities.

References

[1] *Biometrics Consortium Homepage.* http://www.biometrics.org, 1998.

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

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

[4] S. Furui, Recent Advances in Speaker Recognition", Pattern Recognition Letters, 18:859-872, 1997.

[5] A. K. Jain, R. Bolle, and S. Pankanti (eds.). *Biometrics: Personal Identification in Networked Society.* Kluwer, New York, (to appear) 1998.

[6] A. K. Jain, L. Hong, S. Pankanti, and R. Bolle. An identity-authentication system using fingerprints. *Proceedings IEEE*, 85(9):1365–1388, 1997.

[7] V. Nalwa. Automatic on-line signature verification. *Proceedings IEEE*, 85(2):213–239, 1997.

[8] *Recognition System Homepage.* http://www.recogsys.com/, 1998.

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

[10] TRS. *Technology Recognition Systems Homepage.* http://www.betac.com/trs/, 1998

[11] *Veincheck Homepage.* http://innotts.co.uk/*sim*joerice/, 1998.

[12] R. B. Hill, “Apparatus and method for identifying individuals through their retinal vasculature patterns,” US Patent No. 4109237, 1978.