A Study of Unimodel Multimodel and Soft Biometric Recognition

Srinivasa Kumar Devireddy[1], K.Siva Nagireddy[2] ,G.Ramaswamy[3], D.Ravikiran[4], P.Sireesha[5],Y.Suresh Babu[6]

[1]Nalanda Institute of Engineering & Technology,Siddharth Nagar, Sattenapalli,Guntur Dt., Andhra Pradesh, India.
[2]Arjun Engineering College,Hyderabad, Andhra Pradesh,India.
[3]St.Mary's College of Engineering & Technology,Hyderabad Andhra Pradesh, India.
[4]Narasaraopet Engineering College,Narasaraopet,Guntur Dt., Andhra Pradesh, India.
[5]SCR College of Engineering,Chilakaluripet,Guntur Dt. Andhra Pradesh, India.
[6]Jagarlamudi Kuppuswamy Chowdary College,Guntur, Andhra Pradesh, India.

ABSTRACT
Reliable personal recognition is critical to many business processes. A wide variety of systems require reliable personal recognition schemes to either confirm or determine the identity of an individual requesting their services. The purpose of such schemes is to ensure that the rendered services are accessed only by a legitimate user, and not anyone else. Examples of such applications include secure access to buildings, computer systems, laptops, cellular phones and ATMs. In the absence of robust personal recognition schemes, these systems are vulnerable to the wiles of an impostor. Biometric recognition, or simply biometrics, refers to the automatic recognition of individuals based on their physiological and/or behavioral characteristics. By using biometrics it is possible to confirm or establish an individual's identity based on "who she is", rather than by "what she possesses" (e.g., an ID card) or "what she remembers" (e.g., a password). In this paper, we give a brief overview of the field of biometrics and summarize some of its advantages, disadvantages, strengths, limitations, and related privacy concerns.

Key words: *Biometrics, Recognition, Verification, Identification, Multimodal Biometrics, soft biometrics*

1. Introduction

Humans have used body characteristics such as face, voice, gait, etc. for thousands of years to recognize each other. Alphonse Bertillon, chief of the criminal identification division of the police department in Paris, developed and then practiced the idea of using a number of body measurements to identify criminals in the mid 19th century. Just as his idea was gaining popularity, it was obscured by a far more significant and practical discovery of the distinctiveness of the human fingerprints in the late 19th century. Soon after this discovery, many major law enforcement departments embraced the idea of first "booking" the fingerprints of criminals and storing it in a database. Later, the leftover fingerprints (commonly referred to as *latents*) at the scene of crime could be "lifted" and matched with fingerprints in the database to determine the identity of the criminals. Although biometrics emerged from its extensive use in law enforcement to identify criminals, it is being increasingly used today to establish person recognition in a large number of civilian applications.

Any human physiological and/or behavioral characteristic can be used as a biometric characteristic as long as it satisfies the following requirements:

- *Universality*: each person should have the characteristic;
- *Distinctiveness*: any two persons should be sufficiently different in terms of the characteristic;
- *Permanence*: the characteristic should be sufficiently invariant (with respect to the matching criterion) over a period of time;
- *Collectability*: the characteristic can be measured quantitatively.

However, in a practical biometric system, there are a number of other issues that should be considered, including:

- *Performance*, which refers to the achievable recognition accuracy and speed, the resources required to achieve the desired recognition accuracy and speed, as well as the operational and environmental factors that affect the accuracy and speed;
- *Acceptability*, which indicates the extent to which people are willing to accept the use of a particular biometric identifier in their daily lives;
- *Circumvention*, which reflects how easily the system can be fooled using fraudulent methods.

A practical biometric system should meet the specified recognition accuracy, speed, and resource requirements, be harmless to the users, be accepted by the intended population, and be sufficiently robust to various fraudulent methods and attacks to the system.

2. Biometric Systems

A *biometric system* is essentially a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template set in

Manuscript received August 5, 2008.
Manuscript revised August 20, 2008.

the database. Depending on the application context, a biometric system may operate either in *verification* mode or *identification* mode:

- In the verification mode, the system validates a person's identity by comparing the captured biometric data with her own biometric template(s) stored system database. In such a system, an individual who desires to be recognized claims an identity, usually via a PIN (Personal Identification Number), a user name, a smart card, etc., and the system conducts a one-to-one comparison to determine whether the claim is true or not. Identity verification is typically used for *positive recognition*, where the aim is to prevent multiple people from using the same identity [26].
- In the identification mode, the system recognizes an individual by searching the templates of all the users in the database for a match. Therefore, the system conducts a one-to-many comparison to establish an individual's identity without the subject having to claim an identity. Identification is a critical component in *negative recognition* applications where the system establishes whether the person is who she (implicitly or explicitly) denies to be. The purpose of negative recognition is to prevent a single person from using multiple identities [26]. Identification may also be used in positive recognition for convenience. While traditional methods of personal recognition such as passwords, PINs, keys, and tokens may work for positive recognition, negative recognition can only be established through biometrics.

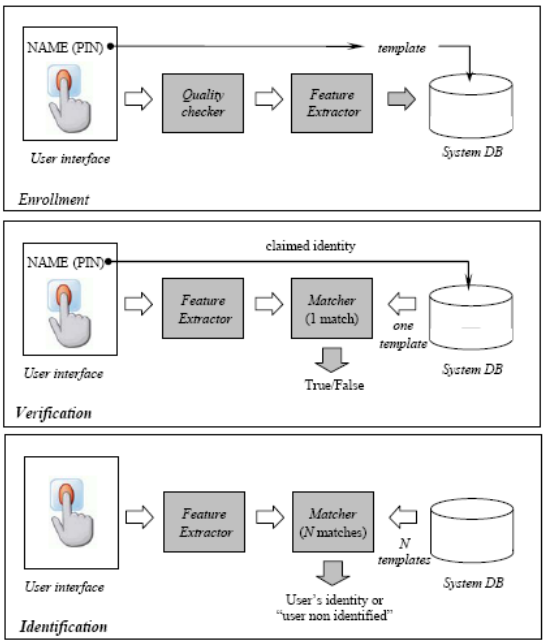

Figure 1. Block diagrams of enrollment, verification and identification

A biometric system is designed using the following four main modules (see Figure 1):

1. Sensor module, which captures the biometric data of an individual. An example is a fingerprint sensor that images the ridge and valley structure of a user's finger.
2. Feature extraction module, in which the acquired biometric data is processed to extract a set of salient or discriminatory features. For example, the position and orientation of minutiae points in a fingerprint image are extracted in the feature extraction module of a fingerprint-based biometric system.
3. Matcher module, in which the features during recognition are compared against the stored templates to generate matching scores. For example, in the matching module of a fingerprint-based biometric system, the number of matching minutiae between the input and the template fingerprint images is determined and a matching score is reported. The matcher module also encapsulates a decision making module, in which a user's claimed identity is confirmed (verification) or a user's identity is established (identification) based on the matching score.
4. System database module, which is used by the biometric system to store the biometric templates of the enrolled users. The enrollment module is responsible for enrolling individuals into the biometric system database. During the enrollment phase, the biometric characteristic of an individual is first scanned by a biometric reader to produce a digital representation of the characteristic. The data capture during the enrollment process may or may not be supervised by a human depending on the application. A quality check is generally performed to ensure that the acquired sample can be reliably processed by successive stages. In order to facilitate matching, the input 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 *smart card* issued to the individual. Usually, multiple templates of an individual are stored to account for variations observed in the biometric trait and the templates in the database may be updated over time.

3. Biometric System Errors

Two samples of the same biometric characteristic from the same person are not exactly the same due to imperfect imaging conditions (e.g., sensor noise and dry fingers), changes in the user's physiological or behavioral characteristics (e.g., cuts and bruises on the finger), ambient conditions (e.g., temperature and humidity) and user's interaction with the sensor (e.g., finger placement).

Therefore, the response of a biometric matching system is the matching score, $S(X_Q, X_I)$, that quantifies the similarity between the input and the database template representations (X_Q and X_I, respectively). The higher the score, the more certain is the system that the two biometric measurements come from the same person. The system decision is regulated by the threshold, *t*: pairs of biometric samples generating scores higher than or equal to *t* are inferred as *mate pairs*; pairs of biometric samples generating scores lower than *t* are inferred as *non-mate pairs*. The distribution of scores generated from pairs of samples from the same person is called the *genuine distribution* and from different persons is called the *impostor* distribution (see Figure 2a).

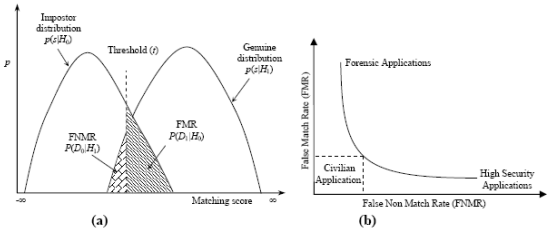

Figure 2. Biometric system error rates.

A biometric verification system makes two types of errors: (i) mistaking biometric measurements from two different persons to be from the same person (called *false match*), and (ii) mistaking two biometric measurements from the same person to be from two different persons (called *false non-match*). These two types of errors are often termed as *false accept* and *false reject*, respectively. There is a trade-off between false match rate (FMR) and false non-match rate (FNMR) in every biometric system. In fact, both FMR and FNMR are functions of the system threshold *t*; if *t* is decreased to make the system more tolerant to input variations and noise, then FMR increases. On the other hand, if *t* is raised to make the system more secure, then FNMR increases accordingly. The system performance at all the operating points (thresholds, *t*) can be depicted in the form of a *Receiver Operating Characteristic* (ROC) curve. A ROC curve is a plot of FMR against (1-FNMR) or FNMR for various threshold values, *t* (see Figure 2b).

4. A Comparison of Various Biometrics

A number of biometric characteristics exist and are in use in various applications (see Figure 3). Each biometric has its strengths and weaknesses, and the choice depends on the application. No single biometric is expected to effectively meet the requirements of all the applications. In other words, no biometric is "optimal". The match between a specific biometric and an application is determined depending upon the operational mode of the application and the properties of the biometric characteristic. A brief introduction of the commonly used biometrics is given below:

DNA: Deoxyribo Nucleic Acid (DNA) is the one-dimensional ultimate unique code for one's individuality - except for the fact that identical twins have identical DNA patterns. It is, however, currently used mostly in the context of forensic applications for person recognition. 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 that can be subsequently abused for an ulterior purpose; (ii) automatic real-time recognition issues: the present technology for DNA matching requires cumbersome chemical methods involving an expert's skills and is not geared for on-line non-invasive recognition; (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, e.g., in hiring practices.

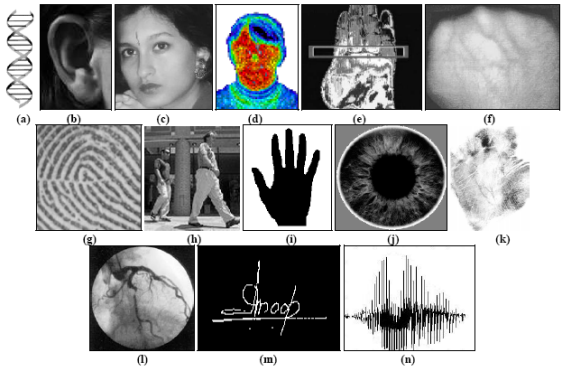

Figure 3. Examples of biometric characteristics

Ear: It has been suggested that the shape of the ear and the structure of the cartilegenous tissue of the pinna are distinctive. The ear recognition approaches are based on matching the distance of salient points on the pinna from a landmark location on the ear. The features of an ear are not expected to be very distinctive in establishing the identity of an individual.

Face: Face recognition is a non-intrusive method, and facial images are probably the most common biometric characteristic used by humans to make a personal recognition. The applications of facial recognition range from a static, controlled "mug-shot" verification to a dynamic, uncontrolled face identification in a cluttered background (e.g., airport). The most popular approaches to face recognition are based on either *(i)* the location and shape of facial attributes, such as the eyes, eyebrows, nose, lips, and chin and their spatial relationships, or *(ii)* the

overall (global) analysis of the face image that represents a face as a weighted combination of a number of canonical faces. In order that a facial recognition system works well in practice, it should automatically *(i)* detect whether a face is present in the acquired image; *(ii)* locate the face if there is one; and *(iii)* recognize the face from a general viewpoint (i.e., from any pose).

Facial, hand, and hand vein infrared thermogram: The pattern of heat radiated by human body is a characteristic of an individual and can be captured by an infrared camera in an unobtrusive way much like a regular photograph. The technology could be used for covert recognition. A thermogram-based system does not require contact and is non-invasive, but image acquisition is challenging in uncontrolled environments, where heat emanating surfaces are present in the vicinity of the body. A related technology using near infrared imaging is used to scan the back of a clenched fist to determine hand vein structure. Infrared sensors are prohibitively expensive which is a factor inhibiting wide spread use of the thermograms.

Fingerprint: Humans have used fingerprints for personal identification for many centuries and the matching accuracy using fingerprints has been shown to be very high [25]. A fingerprint is the pattern of ridges and valleys on the surface of a fingertip, the formation of which is determined during the first seven months of fetal development. Fingerprints of identical twins are different and so are the prints on each finger of the same person. Today, a fingerprint scanner costs about US $20 when ordered in large quantities and the marginal cost of embedding a fingerprint-based biometric in a system (e.g., laptop computer) has become affordable in a large number of applications.

Gait: Gait is the peculiar way one walks and is a complex spatio-temporal biometric. Gait is not supposed to be very distinctive, but is sufficiently discriminatory to allow verification in some low-security applications. Gait is a behavioral biometric and may not remain invariant, especially over a long period of time, due to fluctuations in body weight, major injuries involving joints or brain, or due to inebriety. Acquisition of gait is similar to acquiring a facial picture and, hence, may be an acceptable biometric. Since gait-based systems use the video-sequence footage of a walking person to measure several different movements of each articulate joint, it is input intensive and computationally expensive.

Hand and finger geometry: Hand geometry recognition systems are based on a number of measurements taken from the human hand, including its shape, size of palm, and lengths and widths of the fingers. Commercial hand geometry-based verification systems have been installed in hundreds of locations around the world. The technique is very simple, relatively easy to use, and inexpensive. Environmental factors such as dry weather or individual anomalies such as dry skin do not appear to have any negative effects on the verification accuracy of hand geometry-based systems. The geometry of the hand is not known to be very distinctive and hand geometry-based recognition systems cannot be scaled up for systems requiring identification of an individual from a large population. Further, hand geometry information may not be invariant during the growth period of children. In addition, an individual's jewelry or limitations in dexterity, may pose further challenges in extracting the correct hand geometry information. The physical size of a hand geometry-based system is large, and it cannot be embedded in certain devices like laptops. There are verification systems available that are based on measurements of only a few fingers instead of the entire hand.

Iris: The iris is the annular region of the eye bounded by the pupil and the sclera on either side. The visual texture of the iris is formed during fetal development and stabilizes during the first two years of life. The complex iris texture carries very distinctive information useful for personal recognition. The accuracy and speed of currently deployed iris-based recognition systems is promising and point to the feasibility of large-scale identification systems based on iris information. Each iris is distinctive and, like fingerprints, even the irises of identical twins are different. It is extremely difficult to surgically tamper the texture of the iris. Further, it is rather easy to detect artificial irises. Although, the early iris-based recognition systems required considerable user participation and were expensive, the newer systems have become more user-friendly and cost-effective.

Keystroke: It is hypothesized that each person types on a keyboard in a characteristic way. This behavioral biometric is not expected to be unique to each individual but it offers sufficient discriminatory information to permit identity verification. Keystroke dynamics is a behavioral biometric; for some individuals, one may expect to observe large variations in typical typing patterns. Further, the keystrokes of a person using a system could be monitored unobtrusively as that person is keying in information.

Odor: It is known that each object exudes an odor that is characteristic of its chemical composition and this could be used for distinguishing various objects. A whiff of air surrounding an object is blown over an array of chemical sensors, each sensitive to a certain group of compounds. A component of the odor emitted by a human body is distinctive to a particular individual. It is not clear if the invariance in the body odor could be detected despite deodorant smells, and varying chemical composition of the surrounding environment.

Palmprint: The palms of the human hands contain pattern of ridges and valleys much like the fingerprints. The area of the palm is much larger than the area of a finger and as a result, palmprints are expected to be even more distinctive

than the fingerprints. Since palmprint scanners need to capture a large area, they are bulkier and more expensive than the fingerprint sensors. Human palms also contain additional distinctive features such as principal lines and wrinkles that can be captured even with a lower resolution scanner, which would be cheaper [32]. Finally, when using a high resolution palmprint scanner, all the features of the palm such as hand geometry, ridge and valley features, principal lines, and wrinkles may be combined to build a highly accurate biometric system.

Retinal scan: The retinal vasculature is rich in structure and is supposed to be a characteristic of each individual and each eye. It is claimed to be the most secure biometric since it is not easy to change or replicate the retinal vasculature. The image acquisition 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. Retinal vasculature can reveal some medical conditions, e.g., hypertension, which is another factor deterring the public acceptance of retinal scan based biometrics.

Biometric Identifier	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
DNA	H	H	H	L	H	L	L
Ear	M	M	H	M	M	H	M
Face	H	L	M	H	L	H	H
Facialthermogram	H	H	L	H	M	H	L
Fingerprint	M	H	H	M	H	M	M
Gait	M	L	L	H	L	H	M
Hand geometry	M	M	M	H	M	M	M
Hand vein	M	M	M	M	M	M	L
Iris	H	H	H	M	H	L	L
Keystroke	L	L	L	M	L	M	M
Odor	H	H	H	L	L	M	L
Palmprint	M	H	H	M	H	M	M
Retina	H	H	M	L	H	L	L
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

Table 1. Comparison of various biometric technologies

Signature: The way a person signs her name is known to be a characteristic of that individual. Although signatures require contact with the writing instrument and an effort on the part of the user, they have been accepted in government, legal, and commercial transactions as a method of verification. Signatures are a behavioral biometricthat change over a period of time and are influenced by physical and emotional conditions of the signatories. Signatures of some people vary substantially: even successive impressions of their signature are significantly different. Further, professional forgers may be able to reproduce signatures that fool the system.

Voice: Voice is a combination of physiological and behavioral biometrics. The features of an individual's voice are based on the shape and size of the appendages that are used in the synthesis of the sound. These physiological characteristics of human speech are invariant for an individual, but the behavioral part of the speech of a person changes over time due to age, medical conditions, emotional state, etc. Voice is also not very distinctive and may not be appropriate for large-scale identification. A text-dependent voice recognition system is based on the utterance of a fixed predetermined phrase. A text-independent voice recognition system recognizes the speaker independent of what she speaks. A text-independent system is more difficult to design than a text-dependent system but offers more protection against fraud. A disadvantage of voice-based recognition is that speech features are sensitive to a number of factors such as background noise. Speaker recognition is most appropriate in phone-based applications but the voice signal over phone is typically degraded in quality by the microphone and the communication channel.

A brief comparison of the above biometric techniques based on seven factors is provided in Table 1.

5. Applications of Biometric Systems

The applications of biometrics can be divided into the following three main groups:

Commercial applications such as computer network login, electronic data security, e-commerce, Internet access, ATM, credit card, physical access control, cellular phone, PDA, medical records management, distance learning, etc.

Government applications such as national ID card, correctional facility, driver's license, social security, welfare-disbursement, border control, passport control, etc.

Forensic applications such as corpse identification, criminal investigation, terrorist identification, parenthood determination, missing children, etc.

Figure 4. Examples of biometric applications.

Traditionally, commercial applications have used knowledge-based systems (e.g., PINs and passwords), government applications have used token-based systems (e.g., ID cards and badges), and forensic applications have relied on human experts to match biometric features. Biometric systems are being increasingly deployed in large scale civilian applications (see Figure 4). The Schiphol Privium scheme at the Amsterdam airport, for example, employs iris scan cards to speed up the passport and visa control procedures [4]. Passengers enrolled in this scheme insert their card at the gate and look into a camera; the camera acquires the image of the traveler's eye and processes it to locate the iris, and compute the Iriscode [5]; the computed Iriscode is compared with the data residing in the card to complete user verification. Thus, biometric systems can be used to enhance user convenience while improving security.

6.Advantages and Disadvantages of Biometrics

Let us now examine the advantages and disadvantages of biometrics in two groups of applications: the commercial positive recognition applications that may work either in the verification or the identification modes, and the government and forensic negative recognition applications that require identification.

6.1 Positive Recognition in Commercial Applications

The traditional technologies available to achieve a positive recognition include knowledge-based methods (e.g., PINs and passwords) and token-based methods (e.g., keys and cards). Most people set their passwords based on words or digits that they can easily remember, such as names and birthdays of family members, favorite movie or music stars, and dictionary words. Such passwords are easy to crack by guessing or by a simple brute force dictionary attack. Although it is possible, and even advisable, to keep different passwords for different applications and change them frequently, most people use the same password across different applications and never change them. If a single password is compromised, it may result in a breach in security in many applications Longer passwords are more secure but harder to remember which prompts some users to write them down in accessible locations and hide it under the keyboard. Strong passwords are difficult to remember and result in more Help Desk calls for forgotten or expired passwords. Cryptographic techniques such as encryption can provide very long passwords that are not required to be remembered but that are in turn protected by simple passwords, thus defeating their purpose. Finally, when a password is shared with a colleague, there is no way for the system to know who the actual user is. Similarly, there are many problems with possession-based personal recognition. For example, keys and tokens can be shared, duplicated, lost or stolen and an attacker may make a "master" key that may open many locks. It is significantly more difficult to copy, share, and distribute biometrics with as much ease as passwords and tokens. Biometrics cannot be lost or forgotten and online biometrics-based recognition systems require the person to be recognized to be present at the point of recognition. It is difficult to forge biometrics and extremely unlikely for a user to repudiate. Further, all the users of the system have relatively equal security level and one account is no easier to break than any other. Biometrics introduces incredible convenience for the users while maintaining a sufficiently high degree of security.

6.2. Negative Recognition in Government and Forensic Applications

In negative recognition applications such as employee background checking and preventing terrorists from boarding airplanes, the personal recognition is required to be performed in the identification mode.
Traditional personal recognition tools such as passwords and PINs are not at all useful for negative recognition applications. While biometric systems may not yet be extremely accurate to support large-scale identification applications, they are the only choice for negative recognition applications. Other negative recognition applications such as background checks and forensic criminal identification are also expected to operate in semi-automatic mode and their use follows a similar cost-benefit analysis.

7. Limitations of Unimodal Biometric Systems

The successful installation of biometric systems in various civilian applications does not imply that biometrics is a fully solved problem. Table 2 presents the state-of-the-art error rates of three popular biometric traits. Biometric systems that operate using any single biometric characteristic have the following limitations:

Figure 5. Effect of noisy images

1. Noise in sensed data: The sensed data might be noisy or distorted. A fingerprint with a scar, or a voice altered by cold are examples of noisy data. Noisy data could also be the result of defective or improperly maintained sensors or unfavorable ambient conditions. Noisy biometric data may be incorrectly matched with templates in the database (see Figure 5) resulting in a user being incorrectly rejected.

Figure 6. Intra-class variation associated with an individual's face image.

2. Intra-class variations: The biometric data acquired from an individual during authentication may be very different from the data that was used to generate the template during enrollment, thereby affecting the matching process. This variation is typically caused by a user who is incorrectly interacting with the sensor (see Figure 6), or when sensor characteristics are modified during the verification phase.

3. Distinctiveness: While a biometric trait is expected to vary significantly across individuals, there may be large inter-class similarities in the feature sets used to represent these traits. This limitation restricts the discriminability provided by the biometric trait. Golfarelli et al. [29] have shown that the *information content* in two of the most commonly used representations of hand geometry and face are only of the order of 10^5 and 10^3, respectively.

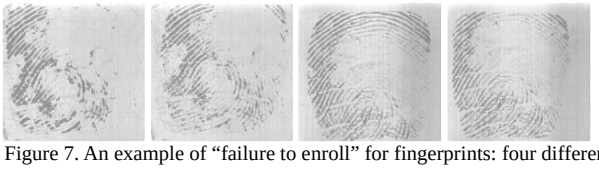

Figure 7. An example of "failure to enroll" for fingerprints: four different impressions of a subject's finger exhibiting poor quality ridges due to extreme finger dryness.

4. Non-universality: While every user is expected to possess the biometric trait being acquired, in reality it is possible for a subset of the users to not possess a particular biometric. A fingerprint biometric system, for example, may be unable to extract features from the fingerprints of certain individuals, due to the poor quality of the ridges (see Figure 7). Thus, there is a failure to enroll (FTE) rate associated with using a single biometric trait.

5. Spoof attacks: An impostor may attempt to spoof the biometric trait of a legitimate enrolled user in order to circumvent the system. This type of attack is especially relevant when behavioral traits such as signature [9] and voice [8] are used. However, physical traits are also susceptible to spoof attacks.

6.

Biometric	Test	Test Parameter	FNMR	FMR
Finger Print	FVC 2002 [25]	Users mostly in the age group 20-39	0.2%	0.2%
Face	FRVT 2002 [34]	Enrollment & test images were collected in indoor environment and could be on different days	10%	1%
Voice	NIST 2000	Text dependent	10-20%	2-5%

Table 2: State-of-the-art error rates associated with fingerprint, face, and voice biometric systems [6].

8. Multimodal Biometric Systems

Some of the limitations imposed by unimodal biometric systems can be overcome by using multiple biometric modalities (such as face and fingerprint of a person or multiple fingers of a person). Such systems, known as *multimodal biometric systems* [12], are expected to be more reliable due to the presence of multiple, independent pieces of evidence [14]. These systems are also able to meet the stringent performance requirements imposed by various applications [13]. Multimodal biometric systems address the problem of non-universality, since multiple traits ensure sufficient population coverage. Further, multimodal biometric systems provide anti-spoofing measures by making it difficult for an intruder to simultaneously spoof the multiple biometric traits of a legitimate user. By asking the user to present a random subset of biometric traits, the system ensures that a "live" user is indeed present at the point of data acquisition. Thus, a challenge-response type of authentication can be facilitated using multimodal biometric systems.

8.1 Modes of Operation

A multimodal biometric system can operate in one of three different modes: serial mode, parallel mode, or

hierarchical mode. In the serial mode of operation, the output of one biometric trait is typically used to narrow down the number of possible identities before the next trait is used. For example, a multimodal biometric system using face and fingerprints could first employ face information to retrieve the top few matches, and then use fingerprint information to converge onto a single identity. Further, a decision could be arrived at without acquiring all the traits. This reduces the overall recognition time. In the hierarchical scheme, individual classifiers are combined in a treelike structure.

8.2 Levels of Fusion

Multimodal biometric systems integrate information presented by multiple biometric indicators. The information can be consolidated at various levels. Figure 8 illustrates the three levels of fusion when combining two (or more) biometric systems. These are

1. Fusion at the feature extraction level: The data obtained from each biometric modality is used to compute a feature vector. If the features extracted from one biometric indicator are independent of those extracted from the other, it is reasonable to concatenate the two vectors into a single new vector, provided the features from different biometric indicators are in the same type of measurement scale.
2. Fusion at the matching score level: Each biometric matcher provides a similarity score indicating the proximity of the input feature vector with the template feature vector. These scores can be combined to assert the veracity of the claimed identity. Techniques such as weighted averaging may be used to combine the matching scores reported by the multiple matchers.
3. Fusion at the decision level: Each biometric system makes its own recognition decision based on its own feature vector. A majority vote scheme [15] can be used to make the final recognition decision.

The integration at the feature extraction level assumes a strong interaction among the input measurements and such schemes are referred to as *tightly coupled* integrations [31]. The *loosely coupled* integration, on the other hand, assumes very little or no interaction among the inputs and integration occurs at the output of relatively autonomous agents, each agent independently assessing the input from its own perspective. It is generally believed that a combination scheme applied as early as possible in the recognition system is more effective. For example, an integration at the feature level typically results in a better improvement than at the matching score level. However, it is more difficult to perform a combination at the feature level because the relationship between the feature spaces of different biometric systems may not be known and the feature representations may not be compatible.

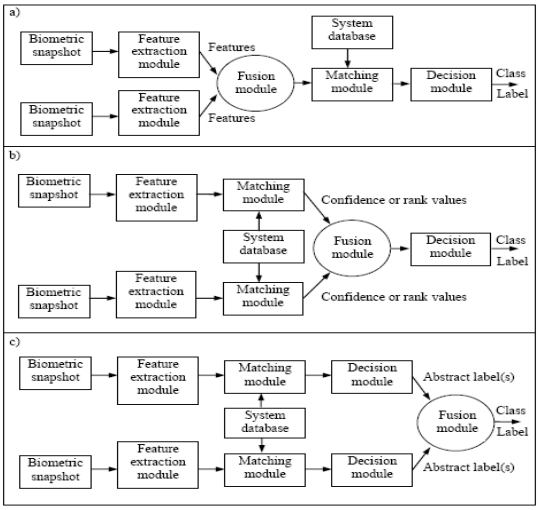

Figure 8. Different levels of fusion in a parallel fusion mode: a) fusion at the feature extraction level; b) fusion at matching score level; c) fusion at decision level.

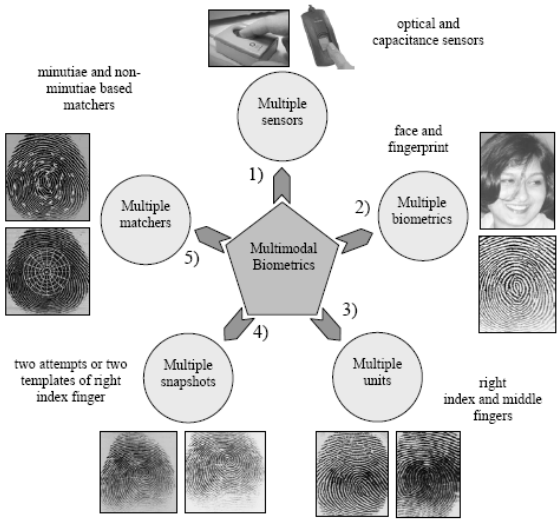

Figure 9.Various Scenarios in a multimodal biometric system

8.3 What to Integrate?

Multimodal biometric systems can be designed to operate in one of the following five scenarios.

1. Multiple sensors: the information obtained from different sensors for the same biometric are combined. For example, optical, solid-state, and ultrasound based sensors are available to capture fingerprints.
2. Multiple biometrics: multiple biometric characteristics such as fingerprint and face are combined. These systems will necessarily contain more than one sensor with each sensor sensing a different biometric characteristic. In a verification system, the multiple biometrics are typically used to improve system accuracy, while in an identification system the matching speed can also be

improved with a proper combination scheme
3.Multiple units of the same biometric: fingerprints from two or more fingers of a person may be combined, or one image each from the two irises of a person may be combined.
4.Multiple snapshots of the same biometric: more than one instance of the same biometric is used for the enrollment and/or recognition. For example, multiple impressions of the same finger, or multiple samples of the voice, or multiple images of the face may be combined.

In scenario 1, multiple sensors are used to sense the same biometric identifier while scenario 2 uses multiple sensors to sense different biometric identifiers. An example of scenario 1 may be the use of multiple cameras mounted to capture different views of a person's face. An example of scenario 2 is the use of a camera for capturing face and an optical sensor to capture a fingerprint. While scenario 1 combines moderately independent information, scenarios 2 and 3 combine independent information and are expected to result in a much larger improvement in recognition accuracy. However, this improvement comes at the cost of inconvenience to the user in providing multiple cues and a longer acquisition time. In scenario 4, only a single input may be acquired during recognition and matched with several stored templates acquired during the one-time enrollment process; alternatively, more data acquisitions may be made at the time of recognition and used to consolidate the matching against a single/multiple template. Scenario 5 combines different representation and matching algorithms to improve the recognition accuracy. Finally, a combination of more than one of these scenarios may also be used.

8.4 Examples of Multimodal Biometric Systems

Multimodal biometric systems have received much attention in recent literature. Brunelli et al. [16] describe a multimodal biometric system that uses the face and voice traits of an individual for identification. Their system combines the matching scores of five different matchers operating on the voice and face features, to generate a single matching score that is used for identification. Bigun et al. develop a statistical framework based on Bayesian statistics to integrate information presented by the speech (text-dependent) and face data of a user [17]. Hong et al. combined face and fingerprints for person identification [13]. Their system consolidates multiple cues by associating different confidence measures with the individual biometric matchers and achieved a significant improvement in retrieval time as well as identification accuracy (see Figure 10). Jain and Ross improved the performance of a multimodal biometric system by learning user-specific parameters [30].

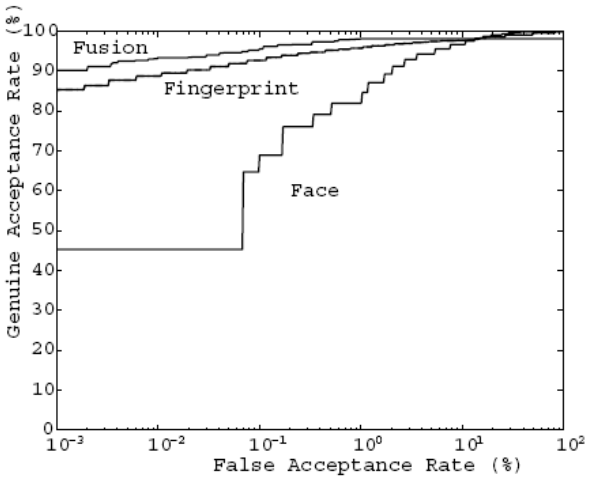

Figure 10. An improvement in matching accuracy is obtained when face recognition and fingerprint recognition systems are combined in an identification system developed by Hong and Jain [13].

8.5 Soft Biometric Feature Extraction

Any trait that provides some information about the identity of a person, but does not provide sufficient evidence to exactly determine the identity can be referred to as soft bio-metric trait. Figure 11 shows some examples of soft biometric traits. Soft biometric traits are available and can be extracted in a number of practical biometric applications. For example, demographic attributes like gender, ethnicity, age, eye color, skin color, and other distinguishing physical marks such as scars can be extracted from the face images used in a face recognition system.

Figure 11. Examples of soft biometric traits.

The pattern class of fingerprint images (right loop, left loop, whorl, arch, etc.) is another example of soft trait. Gender, accent, and perceptual age of the speaker can be inferred in a voice recognition system. Eye color can be easily found from iris images. However, automatic and reliable extraction of soft biometric traits is a difficult task.

In this section, we present a survey of the techniques that have been proposed in the literature for extracting soft biometric information and briefly describe our system for determining height, gender, ethnicity, and eye color. Several researchers have attempted to derive gender, ethnicity, and pose information about the users from their face images. Gutta et al. proposed a mixture of experts consisting of ensembles of radial basis functions for the classification of gender, ethnic origin, and pose of human faces. Their gender classifier (male vs female) had an accuracy of 96%, while their ethnicity classifier (Caucasian, South Asian, East Asian, and African) had an accuracy of 92%. These results were reported on good quality face images from the FERET database that had very little expression or pose changes.

Based on the same database, Moghaddam and Yang showed that the error rate for gender classification can be reduced to 3.4% by using an appearance-based gender classifier that uses non-linear support vector machines. Automatic age determination is a more difficult problem than gender and ethnicity classification. Buchanan et al. have studied the differences in the chemical composition of fingerprints that could be used to distinguish children from adults. Kwon and Lobo presented an algorithm for age classification from facial images based on cranio-facial changes in feature-position ratios and skin wrinkle analysis. They attempted to classify users as “babies”, “young adults”, or “senior adults”. However, they did not provide any classification accuracy.

The weight of a user can be measured by asking him to stand on a weight sensor while providing the primary biometric. The height of a person can be estimated from a sequence of real-time images. For example, Su-Kim et al. used geometric features like vanishing points and vanishing lines to compute the height of an object.

9. Social Acceptance and Privacy Issues

Human factors dictate the success of a biometric-based identification system to a large extent. The ease and comfort in interaction with a biometric system contribute to its acceptance. For example, if a biometric system is able to measure the characteristic of an individual without touching, such as those using face, voice, or iris, it may be perceived to be more user-friendly and hygienic. Additionally, biometric technologies requiring very little cooperation or participation from the users may be perceived as being more convenient to users. On the other hand, biometric characteristics that do not require user participation can be captured without the knowledge of the user, and this is perceived as a threat to privacy by many individuals. The very process of recognition leaves behind trails of private information. On the positive side, biometrics can be used as one of the most effective means for protecting individual privacy. In fact, biometrics ensures privacy by safeguarding identity and integrity.

10. Summary

Reliable personal recognition is critical to many business processes. Biometrics refers to automatic recognition of an individual based on her behavioral and/or physiological characteristics. The conventional knowledge-based and token-based methods do not really provide positive personal recognition because they rely on surrogate representations of the person’s identity. It is, thus, obvious that any system assuring reliable personal recognition must necessarily involve a biometric component. While some of the limitations of biometrics can be overcome with the evolution of biometric technology and a careful system design, it is important to understand that *foolproof* personal recognition systems simply do not exist and perhaps, never will. The security level of a system depends on the requirements of an application and the cost-benefit analysis. In our opinion, properly implemented biometric systems are effective deterrents to perpetrators.

References:

[1] S. Prabhakar, S. Pankanti, and A. K. Jain, “Biometric Recognition: Security and Privacy Concerns”, *IEEE Security and Privacy Magazine*, Vol. 1, No. 2, pp. 33-42, 2003.

[2] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition,Springer, NY, 2003.

[3] A. K. Jain, R. Bolle, and S. Pankanti (editors), Biometrics: Personal Identification in Networked Society, Kluwer Academic Pubs, 1999.

[4] CNN World News, “Schiphol Backs Eye Scan Security”, March 27 2002. Available at http://www.cnn.com/2002/WORLD/europe/03/27/schiphol.security/.

[5] J. Daugman, “Recognizing Persons by Their Iris Patterns”, In A. K. Jain, R. Bolle, and S. Pankanti, editors, Biometrics: Personal Identification in a Networked Society, pp. 103-121, Kluwer Academic Publishers, 1999.

[6] L. O'Gorman, “Seven Issues With Human Authentication Technologies”, *Proc. of Workshop on Automatic Identification Advanced Technologies (AutoID)*, pp. 185-186, Tarrytown, New York, March 2002.

[7] E. d. Os, H. Jongebloed, A. Stijsiger, and L. Boves, “Speaker Verification as a User-Friendly Access for the Visually Impaired”, *Proc. of the European Conference on Speech Technology*, pp. 1263-1266, Budapest, 1999.

[8] A. Eriksson and P. Wretling, “How Flexible is the Human Voice? A Case Study of Mimicry”, *Proc. Of the European Conf on Speech Technology*, pp. 1043-1046, Rhodes, 1997.

[9] W. R. Harrison, Suspect Documents, Their Scientific Examination, Nelson-Hall Publishers,1981.

[10] D. A. Black, “Forgery Above a Genuine Signature”, *Journal of Criminal Law*, Vol.50, pp. 585-590, 1962.

[11] T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, “Impact of Artificial Gummy Fingers on Fingerprint Systems”, *Proc. SPIE*, Vol. 4677, pp. 275-289, San Jose, USA, Feb 2002.

[12] L. Hong, A. K. Jain, and S. Pankanti, “Can Multibiometrics Improve Performance?”, *Proc. AutoID'99*, pp. 59-64, Summit(NJ), USA, Oct 1999.

[13] L. Hong and A. K. Jain, “Integrating Faces and Fingerprints for Personal Identification”, *IEEE Trans. on Pattern Analysis and Machine Intel*, Vol. 20, No. 12, pp. 1295-1307, Dec 1998.

[14] L. I. Kuncheva, C. J. Whitaker, C. A. Shipp, and R. P. W. Duin, “Is Independence Good for Combining Classifiers?”, *Proc. Int.l Conference on Pattern Recognition (ICPR)*, Vol. 2, pp. 168-171, Barcelona, Spain, 2001.

[15] Y. A. Zuev and S. Ivanon, "The Voting as a Way to Increase the Decision Reliability.*Foundations of Information/Decision Fusion with Applications to Engg Prob*, pp.206-210, Washington D.C., USA, August 1996.
[16] R. Brunelli and D. Falavigna, "Person Identification Using Multiple Cues", *IEEE Trans. On Pattern Analysis and Machine Intelligence*, Vol. 12, No. 10, pp. 955-966, Oct 1995.
[17] E. S. Bigun, J. Bigun, B. Duc, and S. Fischer, "Expert Conciliation for Multimodal Person Authentication Systems using Bayesian Statistics", Proc. *Internl Conference on Audioand Video-Based Biometric Person Authent(AVBPA)*, pp. 291-300, Crans-Montana,Switzerland, Mar 1997.
[18] R. W. Frischholz and U. Dieckmann, "Bioid: A Multimodal Biometric Identification System", *IEEE Computer*, Vol. 33, No. 2, pp. 64-68, 2000.
[19] T. K. Ho, J. J. Hull, and S. N. Srihari, "Decision Combination in Multiple Classifier Systems", *IEEE Trans. on Pattern Anals and Machine Intell*, Vol. 16, No. 1, pp. 66-75, Jan 1994.
[20] J. Kittler, M. Hatef, R. P. W. Duin, and J. Matas, "On Combining Classifiers", *IEEE Trans. on Pattern Analysis and Machine Intelligence*, Vol. 20, No. 3, pp. 226-239, Mar 1998.
[21] S. Prabhakar and A. K. Jain, "Decision-level Fusion in Fingerprint Verification", *Pattern Recog*, Vol. 35, No. 4, pp. 861-874, 2002.
[22] U. Dieckmann, P. Plankensteiner, and T. Wagner, "Sesam: A Biometric Person Idfication System Using Sensor Fusion", *Pattern Recog Letters*, Vol. 18, No. 9, pp. 827-833, 1997.
[23] P. Verlinde and G. Cholet, "Comparing Decision Fusion Paradigms Using k-NN Based Classifiers, Decision Trees and Logistic Regression in a Multi-Modal Identity Verification Application", *Intl Conf. on Audio and Video-Based Biometric Person Authentication (AVBPA)*, pp. 188-193, Washington D.C., USA, March 1999.
[24] S. Ben-Yacoub, Y. A.jaoued, and E. Mayoraz, "Fusion of Face and Speech Data for Person Identity Verification", Research Paper IDIAP-RR 99-03, IDIAP, CP 592, 1920 Martigny, Switzerland, Jan 1999.
[25] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, "FVC2002", *Proc. Intl. Conf on Pattern Recognition (ICPR)*, pp.744-747, Quebec City, Canada, August 2002.
[26] J. L. Wayman, "Fundamentals of Biometric Authentication Technologies", *InternationalJournal of Image and Graphics*, Vol. 1, No. 1, pp. 93-113, 2001.
[27] United Kingdom Biometric Work Group (UKBWG), "Best Practices in Testing and Reporting Performance of Biometric Devices, Version 2.01", August 2002,
[28] R. Cappelli, D. Maio and D. Maltoni, "Indexing Fingerprint Databases for Efficient 1:N Matching", *Proc. Intern Conf on Control Automation Robotics and Vision (6th)*, 2000.
[29] M. Golfarelli, D. Maio and D. Maltoni, "On The Error-Reject tradeoff in Biometric Verification Systems", *IEEE trans. on Pattern Analysis and Machine Intelligence*, Vol.19,No.7, pp. 786-796, July 1997.
[30] A. K. Jain and A. Ross, "Learning User-specific Parameters in a Multibiometric System",Proc. International Conference on Image Processing (ICIP), Rochester, New York, September22-25, 2002.
[31] J. Clark and A. Yuille, Data Fusion for Sensory Information Proc. Systems, Kluwer Acad Pub., Boston, 1990.
[32] D. Zhang and W. Shu, "Two Novel Characteristic in Palmprint Verification: Datum Point Invariance and Line Feature Matching", *Pattern Recog*, Vol. 32, No. 4, pp. 691-702,1999.
[33] A. Kumar, D. C. Wong, H. C. S, and A. K. Jain, "Personal Verification using Palmprint and Hand Geometry Biometric", *4th Inll Conf. on Audio- and Video-based Biometric Person Authen*, Guildford, UK, June 9-11, 2003.
[34] P.J. Philips, P. Grother, R. J. Micheals, D. M. Blackburn, E. Tabassi, and J. M. Bone, "FRVT2002:Overview and Summary ", available from http://www.frvt.org/FRVT2002/documents.htm