BIOMETRICS

Alok Padole, Anuj Borkute

Abstract— Biometric recognition refers to an automatic recognition of individuals based on feature vector(s) derived from their physiological and/or behavioral characteristic. Biometric recognition systems should provide a reliable personal recognition schemes to either confirmer determine the identity of an individual. Applications of such a system include computer systems security, secure electronic banking, mobile phones, credit cards, secure access to buildings, health and social services. By using biometrics a person could be identified basedon "who she/he is" rather than "what she/he has" (card, token, key) or "what she/he knows" (Password, PIN). In this paper, a brief overview of biometric methods, both Unimodal andMultimodal, and their advantages and disadvantages are presented.

The term "biometrics" is derived from the Greek words bio (life) and metric (to measure). Biometrics refers to the automatic identification of a person based on his/her physiological or behavioral characteristics. This method of identification is preferred over traditional methods involving passwords and PIN numbers for its accuracy and case sensitiveness. A biometric system is essentially a pattern recognition system which makes a personal identification by determining the authenticity of a specific physiological or behavioral characteristic possessed by the user. An important issue in designing a practical system is to determine how an individual is identified. Depending on the context, a biometric system can be either a verification (authentication) system or an identification system. Verification involves confirming or denying a person's claimed identity while in identification, one has to establish a person's identity. Biometric systems are divided on the basis of the authentication medium used. They are broadly divided as identifications of Hand Geometry, Vein Pattern, Voice Pattern, DNA, Signature Dynamics, Finger Prints, Iris Pattern and Face Detection. These methods are used on the basis of the scope of the testing medium, the accuracy required and speed required. Every medium of authentication has its own advantages and shortcomings. With the increased use of computers as vehicles of information technology, it is necessary to restrict unauthorized access to or fraudulent use of sensitive/personal data. Biometric techniques being potentially able to augment this restriction are enjoying a renewed interest.

Index Terms: Biometrics, Multimodal Biometrics, Recognition, Verification, Identification, Security.

1 INTRODUCTION

Since the beginning of civilization, identifying fellow human beings has been crucial to the fabric of human society. Consequently, person identification is an integral part of the infrastructure needed for diverse business sectors such as finance, health care, transportation, entertainment, law enforcement, security, access control, border control, government, and communication. 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 (actually, a card file). Later, the leftover (typically, fragmentary) fingerprints (commonly referred to as *latent's*) 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 (e.g., illegal aliens, security clearance for employees for sensitive jobs, fatherhood determination, forensics, positive identification of convicts and prisoners), it is being increasingly used today to establish person recognition in a large number of civilian applications. What biological measurements qualify to be a biometric? 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 (i.e., a system that employs biometrics for personal recognition), there are a number of other issues that should be considered, including:
- Performance: This 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 (characteristic) in their daily lives;
- Circumvention: This 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,

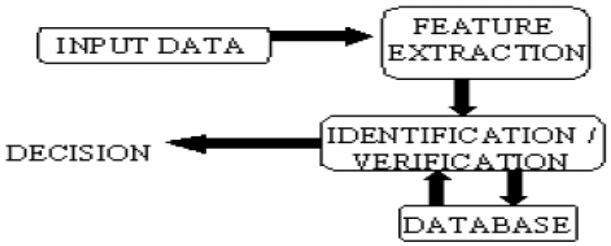
and be sufficiently robust to various fraudulent methods and attacks to the system.

Biometrics is used for two authentication methods (Illustrated in Fig. 1):

• **Identification:** This involves establishing a person's *identity* based *only* on biometric measurements. The comparator matches the obtained biometric with the ones stored in the database bank using a 1:N matching algorithm for identification.

• **Verification:** It involves confirming or denying a person's *claimed identity*. A basic identity (e.g. ID number) is accepted and a biometric template of the subject taken, is matched using a 1:1 matching algorithm to confirm the person's identity.

Fig. 1:



2. TYPES OF BIOMETRICS

Bertillonage: The method consisted of identifying people by taking various body measurements like a person's height, arm length, length and breadth of the head, the length of different fingers, the length of forearms, etc. using calipers. However, the methodology was unreliable as non-unique measurements allowed multiple people to have same results, decreasing the accuracy and hence is no longer used.

Fingerprint Recognition: Involves taking an image of a person's fingertips and records its characteristics like whorls, arches, and loops along with the patterns of ridges, furrows, and minutiae.

Face recognition: technique records face images through a digital video camera and analyses facial characteristics like the distance between eyes, nose, mouth, and jaw edges. These measurements are broken into facial planes and retained in a database, further used for comparison.

VoiceRecognition: Combines physiological and behavioral factors to produce speech patterns that can be captured by speech processing technology. Inherent properties of the speaker like fundamental frequency, nasal tone, cadence, inflection, etc. are used for speech authentication.

Iris recognition: Analyzes features like rings, furrows, and freckles existing in the colored tissue surrounding the pupil. The scans use a regular video camera and works through glasses and contact lenses. The image of the iris can be directly taken by making the user position his eye within the field of a single narrow-angle camera. This is done by observing a visual feedback via a mirror. The isolated iris pattern obtained is then demodulated to extract its phase information.

RetinaRecognition: Technology uses infrared scanning and compares images of the blood vessels in the back of the eye, the choroid vasculature. The eye's inherent isolation and protection from the external environment as an internal organ of the body is a benefit. Retina scan is used in high-end security applications like military installations and power plants.

Signature recognition : Is an instance of writer recognition, which has been accepted as irrefutable evidence in courts of laws. The way a person signs his name is known to be a characteristic of that individual. Approach to signature verification is based on features like number of interior contours and number of vertical slope components. Signatures are behavioral biometric that can change with time, influenced by physical and emotional conditions of the signatories.

Hand Vascular Pattern Identification : uses a non-harmful near infrared light to produce an image of one's vein pattern in their face, wrist, or hand, as veins are relatively stable through one's life. It is a non-invasive, computerized comparison of shape and size of subcutaneous blood vessel structures in the back of a hand.

3. Architecture of a biometric system

Generally speaking, there are two phases in a biometric system (see Fig. 1): a learning phase (enrolment) and a recognition phase (verification). In all cases, the item considered (e.g. finger print or voice) is recorded using a sensor and digital data are then available (a table of pixels, a digital signal, etc.). In most cases the data themselves are not used directly; instead the relevant characteristics are first extracted from the data to form a **template.** This has two advantages: the volume of data to be stored is reduced, and greater anonymity is achieved in data storage (because it is not possible to recover the original signal by referring to these characteristics).

The role of the **learning** module is to create a model of a given person by reference to one or more recordings of the item considered. Most of the models used are statistical models, which make it possible to allow for certain variability in individual data. The **recognition** module enables a decision to be taken. In identification mode, the system compares the measured signal with the various models contained in the data base and selects the model corresponding most closely to the signal. In verification mode, the system will compare the measured signal with just one of the data base models and then authorize the person or reject him. Identification may be a very difficult

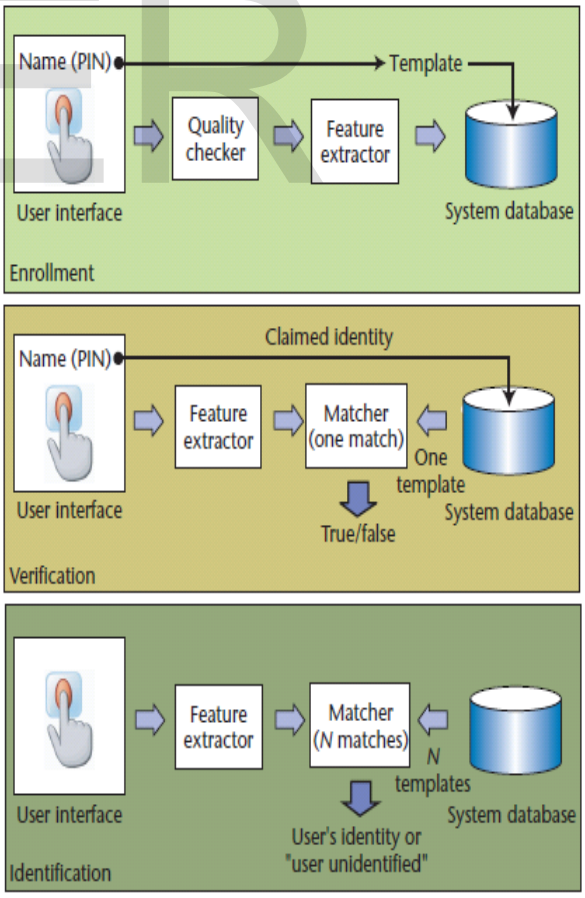
task if the data base contains thousands of individuals. Access time problems then become crucial.

Table I Comparison of various biometric technologies [2]

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

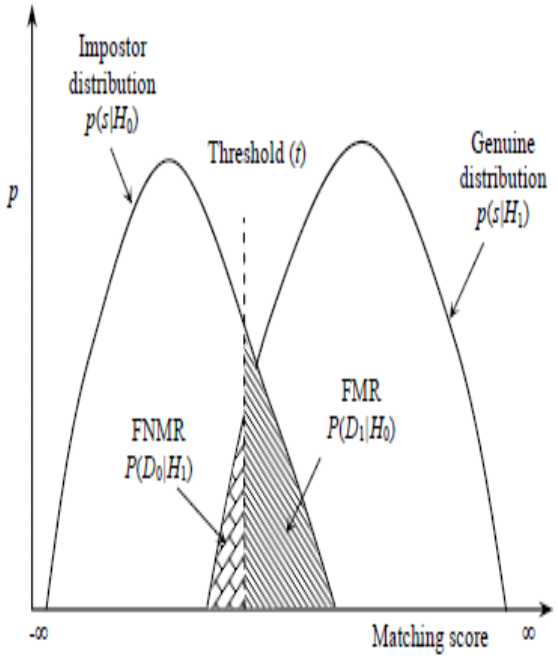
In verification mode, the system validates a person's identity by comparing the captured biometric characteristic with the individual's biometric template, which is presorted in the system database. In such a system, an individual who desires to be recognized claims an identity—usually via a personal identification number (PIN), login name, smart card, or the like—and the system conducts a one-to-one comparison to determine whether the claim is true. The question being answered is, "Is this person Bob?" Identity verification is typically used for positive recognition, where the aim is to prevent multiple people from using the same identity. In identification mode, the system recognizes an individual by searching the entire template database for a match. The system conducts a one-to-many comparison to establish an individual's identity (or fails if the subject is not enrolled in the system database). The question being answered is, "Who is this person?" Identification is a critical component of *negative recognition* applications, in which the system establishes whether the person is who she (implicitly or explicitly) denies being. The purpose of negative recognition is to prevent a single person from using multiple identities. Identification can also be used in positive recognition for convenience (because the user is not required to claim an Identity). While the traditional methods of personal recognition such as passwords, PINs, keys, and tokens work for positive recognition, only biometrics can be used for negative recognition.

Figure 2 contains block diagrams of a verification system and an identification system, both performing the task of user enrollment. The enrollment module registers individuals into the biometric system database. During the enrollment phase, a biometric reader (such as a fingerprint sensor or CCD camera) first scans the individual's biometric characteristic to produce its digital representation. The system generally performs a quality check to ensure that successive stages can reliably process the acquired sample. To facilitate matching, a feature extractor processes the input sample to generate a compact but expressive representation, called a template. Depending on the application, the biometric system might store the template in its central database or record it on a smart card issued to the individual.



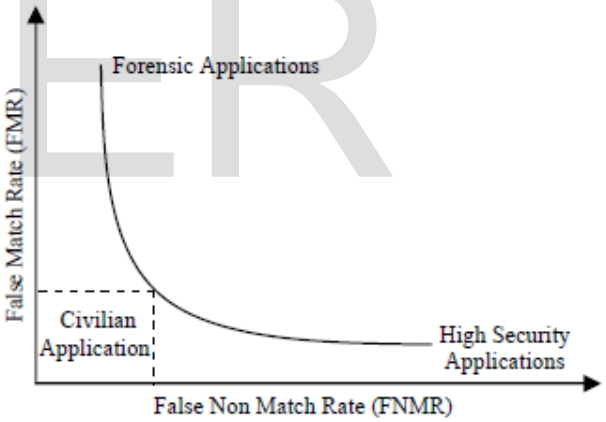
3. Biometric System Errors:

Two samples of the same biometric characteristic from the same person (e.g., two impressions of a user's right index finger) 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, $S(XQ, XI)$ (typically a single number), that quantifies the similarity between the input and the database template representations (XQ and XI, 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* (i.e., belonging to the same person); pairs of biometric samples generating scores lower than t are inferred as *non-mate pairs* (i.e., belonging to different persons). 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 3a).



(a)

Figure 3b Biometric system error rates. (a) FMR and FNMR for a given threshold t are displayed over the genuine and impostor score distributions; FMR is the percentage of non-mate pairs whose matching scores are greater than or equal to t, and FNMR is the percentage of mate pairs whose matching scores are less than t. (b) Choosing different operating points results in different FMR and FNMR. The curve relating FMR to FNMR at different thresholds is referred to as Receiver Operating Characteristics (ROC). Typical operating points of different biometric applications are displayed on an ROC curve. Lack of understanding of the error rates is a primary source of confusion in assessing system accuracy in vendor/user communities alike. 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,



(b)

t (see Figure 3b).

Mathematically, the errors in a verification system can be formulated as follows. If the
stored biometric template of the user *I* is represented by *XI* and the acquired input for recognition is
represented by *XQ*, then the null and alternate hypotheses are:
*H*0: input *XQ* does not come from the same person as the template *XI*;
*H*1: input *XQ* comes from the same person as the template *XI*.
The associated decisions are as follows:
*D*0: person is not who she claims to be;
*D*1: person is who she claims to be.
The decision rule is as follows: if the matching score $S(XQ, XI)$ is less than the system threshold *t*,
then decide *D*0, else decide *D*1. The above terminology is borrowed from communication theory,
where the goal is to detect a message in the presence of noise. *H*0 is the hypothesis that the received
signal is noise alone, and *H*1 is the hypothesis that the received signal is message plus the noise.
Such a hypothesis testing formulation inherently contains two types of errors:
Type I: false match (*D*1 is decided when *H*0 is true);
Type II: false non-match (*D*0 is decided when *H*1 is true).
FMR is the probability of type I error (also called significance level in hypothesis testing) and FNMR is the probability of type II error:
FMR = $P(D1 \mid H0)$;
FNMR = $P(D0 \mid H1)$.
The expression (1-FNMR) is also called the power of the hypothesis test. To evaluate the accuracy of a fingerprint biometric system, one must collect scores generated from multiple images of the same finger (the distribution $p(S(XQ, XI) \mid H1)$), and scores generated from a number of images from different fingers (the distribution $p(S(XQ, XI) \mid H0)$). Figure 2a graphically illustrates the computation of FMR and FNMR over genuine and impostor distributions:

$$\int_{t}^{\infty} p(S(X, X) \mid H0)\, dS = 0,$$

$$\int_{t}^{\infty} p(S(X, X) \mid H0)\, dS = \text{FMR},$$

$$\int_{-\infty}^{t} p(S(X, X) \mid H1)\, dS = 1 - \text{FNMR}.$$

Besides the above error rates, the failure to capture (FTC) rate and the failure to enroll (FTE) rate are also used to summarize the accuracy of a biometric system. The FTC rate is only applicable when the biometric device has an automatic capture functionality implemented in it and denotes the percentage of times the biometric device fails to capture a sample when the biometric characteristic is presented to it. This type of error typically occurs when the device is not able to locate a biometric signal of sufficient quality (e.g., an extremely faint fingerprint or an occluded face). The FTE rate, on the other hand, denotes the percentage of times users are not able to enroll in the recognition system. There is a tradeoff between the FTE rate and the perceived system accuracy (FMR and FNMR). FTE errors typically occur when the system rejects poor quality inputs during enrollment. Consequently, the database contains only good quality templates and the perceived system accuracy improves. Because of the interdependence among the failure rates and error rates, all these rates (i.e., FTE, FTC, FNMR, FMR) constitute important specifications in a biometric system, and should be reported during performance evaluation.
The accuracy of a biometric system in the identification mode can be inferred using the system accuracy in the verification mode under simplifying assumptions. Let us denote the identification false non-match and false match rates with FNMR*N* and FMR*N*, respectively, where *N* represents the number of identities in the system database (for simplicity, we assume that only a single identification attempt is made per subject, a single biometric template is used for each enrolled user, and the impostor scores between different users are uncorrelated). Then, FNMR*N* ≅ FNMR and FMR*N* = 1-(1-FMR)*N* ≅ N· FMR (the approximation hold good only when N.FMR<0.1).
A detailed discussion on these issues is available in and. If the templates in the database of an identification system have been classified and indexed, then only a portion of the database is searched during identification and this leads to the following formulation of FNMR*N* and FMR*N*:•FNMR*N* = RER+(1-RER)· FNMR, where RER (Retrieval Error Rate) is the probability that the database template corresponding to the searched finger is wrongly discarded by the retrieval mechanism. The above expression is obtained using the following argument: in case the template is not correctly retrieved (this happens with probability RER), the system always generates a false-non match, whereas in case the retrieval returns the right template (this happens with probability (1-RER)), false non-match rate of the system is FNMR. Also, this expression is only an approximation since it does not consider the probability of falsely matching an incorrect template before the right one is retrieved;
FMR*N* = 1-(1-FMR)*N*· *P*; where *P* (also called the *penetration rate*) is the average percentage of database searched during the identification of an input fingerprint.
The accuracy requirements of a biometric system are very much application dependent. For example, in some forensic applications such as criminal identification, one of the critical

design issues is the FNMR rate (and not the FMR): *i.e.*, we do not want to miss identifying a criminal even at the risk of manually examining a large number of potentially incorrect matches generated by the biometric system. On the other extreme, the FMR may be one of the most important factors in a highly secure access control application, where the primary objective is deterring impostors (although we are concerned with the possible inconvenience to the legitimate users due to a high FNMR). There are a number of civilian applications whose performance requirements lie in between these two extremes, where both FMR and FNMR need to be considered. For example, in applications like bank ATM card verification, a false match means a loss of several hundred dollars while a high FNMR may lead to a potential loss of a valued customer. Figure 2b depicts the FMR and FNMR tradeoffs in different types of biometric applications.

4.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. It is clear that there is plenty of scope for improvement in biometrics.

Researchers are not only addressing issues related to reducing error rates, but they are also looking at ways to enhance the usability of biometric systems.

Biometric systems that operate using any single biometric characteristic have the following limitations:

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 (e.g., accumulation of dirt on a fingerprint sensor) or unfavorable ambient conditions (e.g., poor illumination of a user's face in a face recognition system). Noisy biometric data may be incorrectly matched with templates in the database (see Figure 5) resulting in a user being incorrectly rejected.

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 , or when sensor characteristics are modified (e.g., by changing sensors - the sensor interoperability problem) during the verification phase. As another example, the varying psychological makeup of an individual might result in vastly different behavioral traits at various time instances.

Test Parameter FNMR FMR

Fingerprint FVC 2002 [25] Users mostly in the age group 20-39
0.2% 0.2%

Face FRVT 2002 [34] Enrollment and test images were collected in indoor environment and could be on different days
10% 1%

Voice NIST 2000 Text dependent 10-20% 2-5%

3. 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 .Thus, there is a failure to enroll (FTE) rate associated with using a single biometric trait. It has been empirically estimated that as much as 4% of the population may have poor quality fingerprint ridges that are difficult to image with the currently available fingerprint sensors and result in FTE errors. den Os et al. report the FTE problem in a speaker recognition system.

4. 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 and voice are used. However, physical traits are also susceptible to spoof attacks. For example, it has been demonstrated that it is possible (although difficult and cumbersome and requires the help of a legitimate user) to construct
artificial fingers/fingerprints in a reasonable amount of time to circumvent a fingerprint
verification system .

Figure 4. Effect of noisy images on a biometric system. (a) Fingerprint obtained from a user during enrollment. (b) Fingerprint obtained from the same user during verification after three months. The development of scars or cuts can result in erroneous fingerprint matching results.

Figure 5. Intra-class variation associated with an individual's face image. Due to change in pose, an appearance-based face recognition system will not be able to match these 3 images successfully, even though they belong to the same individual.

Figure 6. An example of "failure to enroll" for fingerprints (with respect to a given fingerprint recognition system): four different impressions of a subject's finger exhibiting poor quality ridges due to extreme finger dryness. A given fingerprint system (using a certain sensor and matching algorithm) might not be able to enroll this subject since minutiae and ridge information cannot be reliably extracted.

5. Multimodal Biometric Systems :

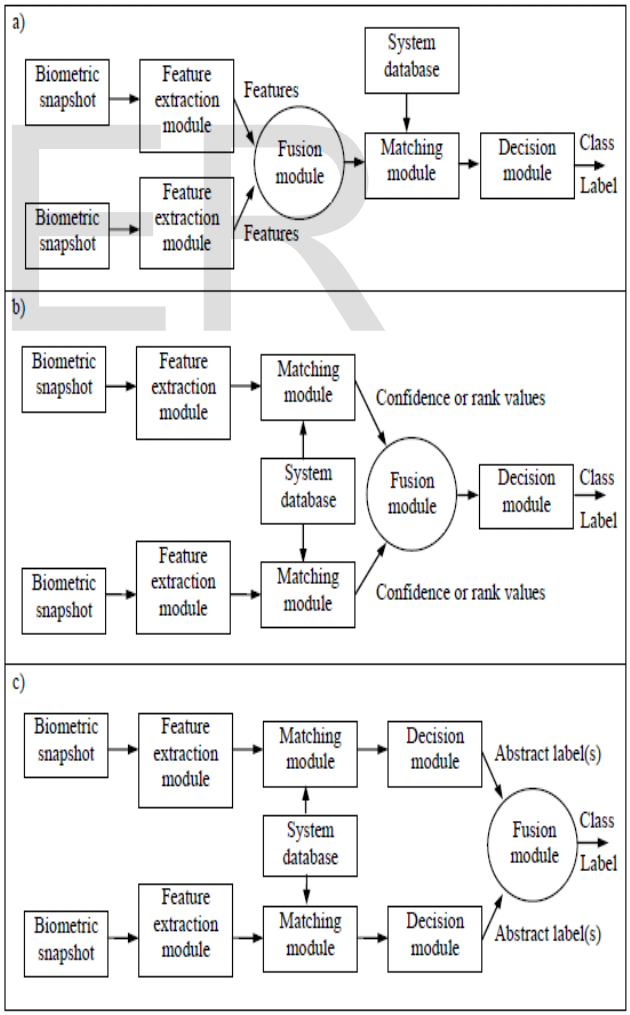
Some of the limitations imposed by unimodal biometric systems can be overcome by using multiple biometric modalities (such as face and fingerprint of a person or multiple fingers of a person). Such systems, known as *multimodal biometric systems*, are expected to be more reliable due to the presence of multiple, independent pieces of evidence. These systems are also able to meet the stringent performance requirements imposed by various applications . 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 (e.g., right index and right middle fingers, in that order), 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.

5.1 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. This serves as an indexing scheme in an identification system. 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. This is in contrast to a parallel mode of operation where information from multiple traits is used simultaneously to perform recognition. This difference is crucial. In the cascade operational mode, the various biometric characteristics do not have to be acquired simultaneously. 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.

5.2 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 (somewhat) 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. The new feature vector has a higher dimensionality and represents a person's identity in a different (and hopefully, more discriminating) feature space. Feature reduction techniques may be employed to extract a small number of salient features from the larger set of features.

2. Fusion at the matching score (confidence or rank) 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 (abstract label) level: Each biometric system makes its own recognition decision based on its own feature vector. A majority vote scheme 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. 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. This is because the feature representation conveys the richest information compared to the matching score of a matcher, while the abstract labels contain the least amount of information about the decision being made.

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. Further, the multimodal system may not have access to the feature values of individual modalities because of their proprietary nature. In such cases, integrations at the matching score or decision levels are the only options. This is also reflected in the nature of research dedicated to multimodal biometric systems: very few published papers report results on a combination at the feature level. Hong et al. theoretically analyzed the improvement in verification accuracy when two biometric characteristics are fused at the matching
score level and at the decision level.

5.3 What to Integrate?

Multimodal biometric systems can be designed to operate in one of the following five scenarios (see Figure 9).

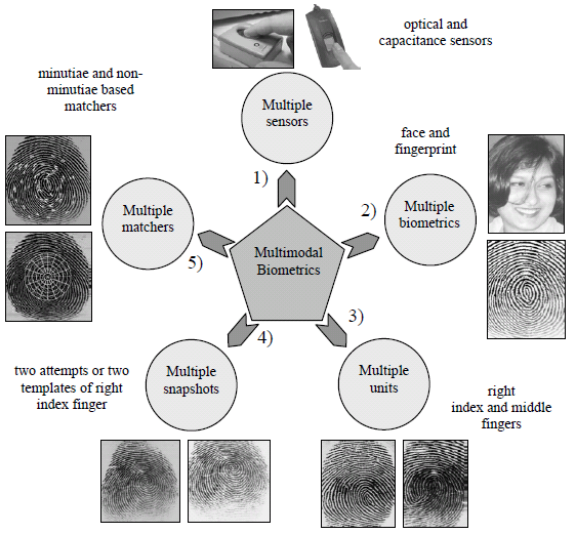
1. *Multiple sensors*: the information obtained from different sensors for the same biometric are combined. For example, optical, solid-state, and ultrasound based sensors are available to capture fingerprints.

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 (e.g., face matching which is typically fast but not very accurate can be used for retrieving the top *M* matches and then fingerprint matching which is slower but more accurate can be used for making the final identification decision).

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.

5. *Multiple representations and matching algorithms for the same biometric*: this involves combining different approaches to feature extraction and matching of the biometric characteristic. This could be used in two cases. Firstly, a verification or an identification system can use such a combination scheme to make a recognition decision. Secondly, an identification system may use such a combination scheme for indexing.



5.4 Examples of Multimodal Biometric Systems

Multimodal biometric systems have received much attention

in recent literature. Brunelli et al. 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 develop a statistical framework based on Bayesian statistics to integrate information presented by the speech (text-dependent) and face data of a user. Hong et al. combined face and fingerprints for person identification. 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 .Kumar et al. combined hand geometry and palm print biometrics in a verification system. A commercial
product called Bio ID uses voice, lip motion and face features of a user to verify identity. Jain and Ross improved the performance of a multimodal biometric system by learning user-specific parameters .General strategies for combining multiple classifiers have been suggested in and . All the approaches presented in (the highest rank method, the Borda count method and logistic regression) attempt to reduce or re-rank a given set of classes. These techniques are thus relevant to the identification problem in which a large number of classes (identities) are present. Prabhakar and Jain showed, in the context of a fingerprint verification system, that combining multiple matchers, multiple enrollment templates, and multiple fingers of a user can
significantly improve the accuracy of a fingerprint verification system. They also argue that selecting matchers based on some "goodness" statistic may be necessary to avoid performance degradation when combining multiple biometric modalities. There is a large amount of literature available on the various combination strategies for fusing multiple biometric modalities using the matching scores (see for example It is well known that independence of modalities plays a very important role in the amount of improvement when combining multiple biometric modalities. A carefully designed combination scheme, that has been trained and tested on a large amount of data, is expected to perform better than the best of the individual ingredient modalities. A combination of uncorrelated modalities (e.g., fingerprint and face, two fingers of a person, etc.) is expected to result in a better improvement in performance than a combination of correlated modalities (e.g., different impressions of the same finger, different fingerprint matchers, etc.). Further, a combination of uncorrelated modalities can significantly reduce the failure to enroll rate as well as provide more security against "spoofing". On the other hand, such a combination requires the users to provide multiple identity cues, which may cause inconvenience. Additionally, the cost of the system increases because of the use of multiple sensors (e.g., when combining fingerprints and face). The convenience and cost factors remain the biggest barriers in the use of such multimodal biometrics systems in civilian applications. We anticipate that high security applications, large-scale identification systems, and negative identification applications will increasingly use multimodal biometric systems, while small-scale low-cost commercial applications will probably continue striving to improve unimodal biometric systems.

6. 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 (e.g., face and face thermo grams) 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. For example, if a person is identified each time she makes a purchase, information about where this person shops and what she buys can be simply collected and used by telemarketers to invade her privacy. The issue of privacy becomes more serious with biometric-based recognition systems because biometric characteristics may provide additional information about the background of an individual. For example, retinal patterns may provide medical information about diabetes or high blood pressure in an individual. A health insurance company may use this information in an unethical way for economic gains by denying benefits to a person determined to be of high risk. More importantly, people fear that biometric identifiers could be used for linking personal information across different systems or databases.

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. For example, if a person loses a credit card and an adversary finds it, then the credit history of this person is compromised. But, if the credit card could be used only when the user supplies her biometric characteristics (such as in a smartcard containing the user' biometric data), then the user is protected. Biometrics can also be used to limit access to personal information. For instance, a biometric-based patient information system can reliably ensure that access to medical records is available only to the patient and authorized medical personnel. Nevertheless, many people are uneasy about the use of their personal biological

characteristics in corporate or government recognition systems. To alleviate these fears, companies and agencies that operate biometric systems have to assure the users of these systems that their biometric information remains private and is used only for the expressed purpose for which it was collected. Legislation is necessary to ensure that such information remains private and that its misuse is appropriately punished.
Most of the commercial biometric systems available today do not store the sensed physical characteristics in their original form but, instead, they store a digital representation (a template) in an encrypted format. This serves two purposes. First, the actual physical characteristic cannot be recovered from the digital template thus ensuring privacy and secondly, the encryption ensures that only the designated application can use this template.

7. 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, ecommerce,
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.
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. 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; the computed Iriscode is compared with the data residing in the card to complete user verification. A similar scheme is also being used to verify the identity of Schiphol airport employees working in high-security areas. Thus, biometric systems can be used to enhance user convenience while improving security.

8. 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 (e.g., exclusive knowledge or possession). It is, thus, obvious that any system assuring reliable personal recognition must necessarily involve a biometric component. This is not, however, to state that biometrics alone can deliver reliable personal recognition component. In fact, a sound system design will often entail incorporation of many biometric and non-biometric components (building blocks) to provide reliable personal recognition. Biometric-based systems also have some limitations that may have adverse implications for the security of a system. 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. Security is a risk management strategy that identifies, controls, eliminates, or minimizes uncertain events that may adversely affect system resources and information assets. The security level of a system depends on the requirements (threat model) of an application and the cost-benefit analysis. In our opinion, properly implemented biometric systems are effective deterrents to perpetrators.
There are a number of privacy concerns raised about the use of biometrics. A sound tradeoff between security and privacy may be necessary; collective accountability/acceptability
Standards can only be enforced through common legislation. Biometrics provides tools to enforce accountable logs of system transactions and to protect an individual's right to privacy.
As biometric technology matures, there will be an increasing interaction among the market, technology, and the applications. This interaction will be influenced by the added value of the technology, user acceptance, and the credibility of the service provider. It is too early to predict where and how biometric technology would evolve and get embedded in which applications. But it is certain that biometric-based recognition will have a profound influence on the way we conduct our daily business.

9. Discussion and Conclusions :

Any system assuring reliable person recognition must necessarily involve a biometric component. Because of the unique person identification potential provided by biometrics, they have and will continue to provide useful value by deterring crime, identifying criminals, and eliminating fraud. At the same time, we are mindful of the need to provide controls to the problem of "function creep", creating systems that do not threaten basic rights to privacy and anonymity, and substantiate the business case for system deployment.

Biometrics is one of the important and more interesting pattern recognition application with its associated unique legal, political and business challenges.

While this work emphasizes the open fundamental problems in biometrics, this should not be construed to imply that the existing biometric technology is not useful. In fact, there are a large number of biometric solutions that have been successfully deployed to provide useful value in practical applications. For example, the hand geometry system has served as good access control solution in many deployments such a university dorms, building entrance, time/place applications .

AFIS systems have been providing terrific value to the society by using a good integration of automatic and manual processes. The scope of this paper is intended to expand the frontiers of the state of the art biometric technology performance for their effective widespread deployment.

It needs to be emphasized that an emerging technology such a biometrics, is typically confronted with unrealistic performance expectations and not fairly compared with existing alternatives (e.g., passwords) that we have resigned to tolerate. A successful biometric solution does not have to be 100% accurate or secure. A particular application demands a *satisfactory* performance justifying the additional investments needed for the biometric system; the system designer can exploit the application context to engineer the system to achieve the target performance levels.

In this work, we have explored the fundamental roadblocks for widespread adoption of biometrics as means of automatic person identification: effective and efficient pattern recognition; ensuring system integrity, system application integrity and return on investment. From pure pattern recognition perspective, the large scale identification and screening applications are the two most challenging problems – today we cannot solve them no matter how many resources we throw at them. We really need to understand the effective representation space and the invariance properties much more clearly. From system perspective, both security and privacy are open problems with no clear satisfactory solutions on the horizon, and cost savings need to be more thoroughly documented. It appears that surmounting these roadblocks will pave the way not only for inclusion of biometrics into mainstream applications but also for other pattern recognition applications.

The recognition problems have historically been very elusive and have been underestimated in terms of the effort needed to arrive at a satisfactory solution.

Additionally, since humans seem to recognize people with high accuracy, biometrics has incorrectly been perceived to be an easy problem. There is no substitute to research, realistic performance evaluations and standardization efforts facilitating the cycle of build-test-share for transforming the technology into business solutions.

Making the "business case" for biometrics has proved difficult for many reasons: (i) the business value of "security" and "deterrence" is always difficult to quantify, regardless of technology; (ii) fraud rates and costs of long standing business systems (e.g., PINS and passwords) are not well understood; (iii) total costs for biometrics systems have not been well documented or reported. Many recent media reports have been critical of biometric systems on the issue of return on investment but in the view of the authors, too little research has been done on this issue to reach any firm, general conclusions.

Research funding in biometrics is negatively impacted by the lack of substantiated cost savings or increased productivity. It is hard to justify funding for additional research in basic pattern matching algorithm development when the potential financial return is not immediately apparent. Biometrics is an ideal area for computer scientists to work closely with management scientists and business specialists to develop methods for assessing long term financial returns attributable to

deployed systems. We believe that the insistence on "return of investment" (ROI) issues is premature because there is *no* substitute to biometrics for effective positive identification; we strongly believe, development of reliable identity infrastructure is critical to effective functioning of the society and this infrastructure will have to necessarily involve biometrics. We, as a community, have a responsibility to chalk-out viable development of this emerging technology without encroaching on the fundamental rights of human beings. Considering the wide scope of the resultant societal impact, we believe, this responsibility needs to be substantially stimulated and shouldered by sustained and substantial R&D investment from the government agencies worldwide.

Considering the recent mandates of several governments for the nationwide use of biometrics in delivering crucial societal functions, there is a need to act with a sense of urgency. Pattern recognition systems have never been tried at such large scales nor have they dealt with such a wide use of sensitive personal information. As pattern recognition researchers, it is a great opportunity and challenge for us to make a difference in our society while engaged in the work that we love to do.

10. 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 Publishers, 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 Conference 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, Criminology and Police Science*, Vol.50, pp. 585-590, 1962.