A Comparative Study on Unimodal and Multimodal Biometric Recognition

Md. Morshedul Arefin, Md. Ekramul Hamid

Abstract- Biometrics is one of the recent trends in security, which is mainly used for verification and recognition systems. By using biometrics we confirm a particular person's claimed identity based on particular person's physiological or behavioral characteristics such as fingerprint, face or voice etc. Most biometric systems deployed in real-world applications are unimodal, such as they use a single source of information for authentication (e.g., single fingerprint, face, voice etc.). Some of the limitations imposed by unimodal biometric systems can be overcome by including multiple sources of information for establishing identity. In this paper, it is shown that fingerprint and face recognition can form a good combination for a multimodal biometric system.

Keywords: Biometrics, Identification, Verification, Features, Fusion.

I. 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 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 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), a user name, or a smart card, and the system conducts a one-to-one comparison to determine whether the claim is true or not (e.g., "*Does this biometric data belong to Bob?*").

• In the identification mode, the system recognizes an individual by searching the templates of all the users in the database for a match. Therefore, the system conducts a one-to-many comparison to establish an individual's identity (or fails if the subject is not enrolled in the system database) without the subject having to claim an identity (e.g., "*Whose biometric data is this?*"). Identification is a critical component in *negative recognition* applications where the system establishes whether the person is who she (implicitly or explicitly) denies to be. The purpose of negative recognition is to prevent a single person from using multiple identities [18]. Identification may also be used in positive recognition for convenience (the user is not required to claim an identity). While traditional methods of personal recognition such as passwords, PINs, keys, and tokens may work for positive recognition, negative recognition can only be established through biometrics. Throughout this paper, we will use the generic term *recognition* where we do not wish to make a distinction between verification and identification. The block diagrams of a verification system and an identification system are depicted in Fig. 1; user enrollment, which is common to both of the tasks, is also graphically illustrated.

Identity verification is typically used for *positive recognition*, where the aim is to prevent multiple people from using the same identity [18].

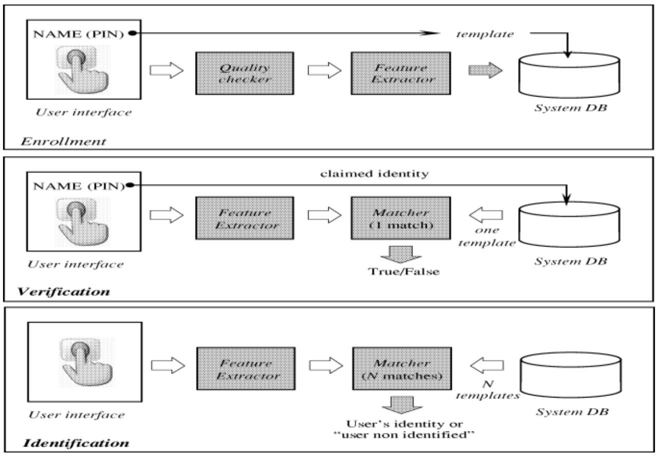

Fig. 1. Block diagrams of enrollment, verification, and identification tasks are shown using the four main modules of a biometric system, i.e., sensor, feature extraction, matcher, and system database

A biometric system is designed using the following four main modules (see Fig. 1).

i) 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.

ii) 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 (local ridge and valley singularities) in a fingerprint image are extracted in the feature extraction module of a fingerprint-based biometric system.

iii) Matcher module, in which the features extracted 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.

Manuscript Received on December 2014.

Md. Morshedul Arefin, Department of Computer Science and Engineering, University of Rajshahi, Bangladesh.
Prof. Dr. Md. Ekramul Hamid, Department of Computer Science and Engineering, University of Rajshahi, Bangladesh.

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.

iv) 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.

• **Ear:** It has been suggested that the shape of the ear and the structure of the cartilaginous 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 nonintrusive 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). While the verification performance of the face recognition systems that are commercially available is reasonable [26], they impose a number of restrictions on how the facial images are obtained, sometimes requiring a fixed and simple background or special illumination. It is questionable whether the face itself, without any contextual information, is a sufficient basis for recognizing a person from a large number of identities with an extremely high level of confidence [21].

• **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 (visible spectrum) photograph. The technology could be used for covert recognition. A thermogram-based system does not require contact and is noninvasive, but image acquisition is challenging in uncontrolled environments, where heat emanating surfaces (e.g., room heaters and vehicle exhaust pipes) are present in the vicinity of the body.

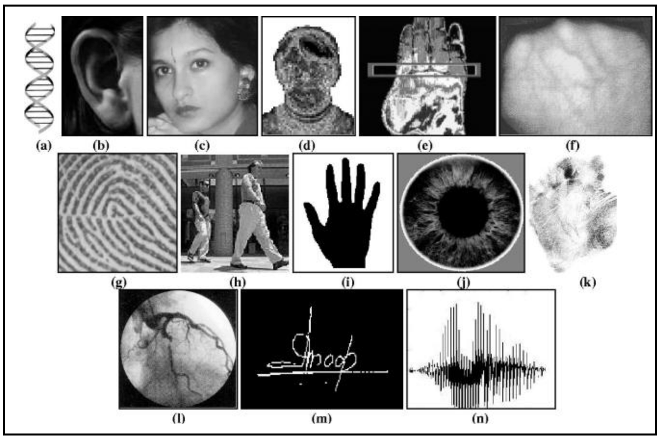

Fig. 2. Examples of biometric characteristics: (a) DNA, (b) ear, (c) face, (d) facial thermogram, (e) hand thermogram, (f) hand vein, (g) fingerprint, (h) gait, (i) hand geometry, (j) iris, (k) palmprint, (l) retina, (m) signature, and (n) voice

• **Fingerprint:** Humans have used fingerprints for personal identification for many centuries and the matching accuracy using fingerprints has been shown to be very high [17]. 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.

• **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. Further, hand geometry information may not be invariant during the growth period of children. In addition, an individual's jewelry (e.g., rings) or limitations in dexterity (e.g., from arthritis), may pose further challenges in extracting the correct hand geometry information.

• **Iris:** The iris is the annular region of the eye bounded by the pupil and the sclera (white of the eye) on either side.

The visual texture of the iris is formed during fetal development and stabilizes during the first two years of life. The 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 (e.g., designer contact lenses). 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.

• **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 [24]. Finally, when using a high-resolution palmprint scanner, all the features of the palm such as hand geometry, ridge and valley features (e.g., minutiae and singular points such as deltas), principal lines, and wrinkles may be combined to build a highly accurate biometric system.

• **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.

• **Signature:** The way a person signs his or 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 biometric that 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 (e.g., vocal tracts, mouth, nasal cavities, and lips) 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 (such as a common cold), and 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.

II. LIMITATIONS OF UNIMODAL BIOMETRIC SYSTEMS

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

A. 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 Fig. 3) resulting in a user being incorrectly rejected.

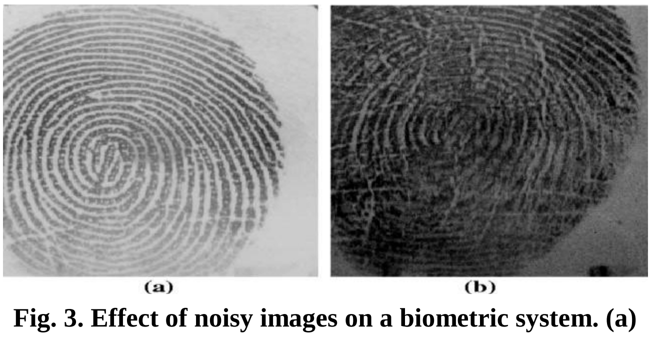

Fig. 3. Effect of noisy images on a biometric system. (a) Fingerprint obtained from a user during enrollment. (b) Fingerprint obtained from the same user during verification after three months. The development of scars or cuts can result in erroneous fingerprint matching results

B. 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 Fig. 4) 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.

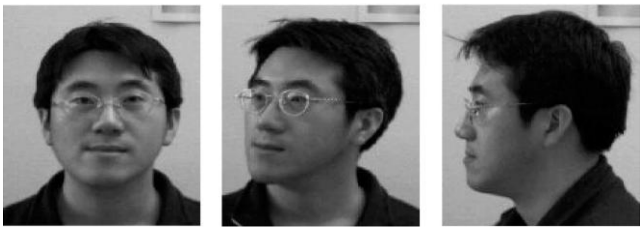

Fig. 4. Intra-class variation associated with an individual's face image. Due to changes in pose, an appearance-based face recognition system will not be able to match these three images successfully, even though they belong to the same individual

C. Inter-class similarities

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.* [21] have shown that the *information content* (number of distinguishable patterns) in two of the most commonly used representations of hand geometry and face are only of the order of and , respectively. Thus, every biometric trait has some theoretical upper bound in terms of its discrimination capability.

D. 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 Fig. 5). 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.* [1] report the FTE problem in a speaker recognition system.

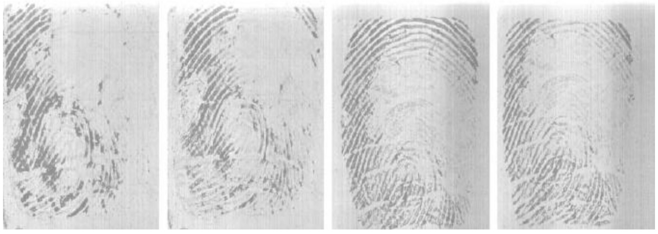

Fig. 5. An example of "failure to enroll" for fingerprints (with respect to a given fingerprint recognition system): four different impressions of a subject's finger exhibiting poor quality ridges due to extreme finger dryness. A given fingerprint system (using a certain sensor and matching algorithm) might not be able to enroll this subject since minutiae and ridge information cannot be reliably extracted

E. 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 [3] and voice [2] 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 [4].

III. 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* [5], are expected to be more reliable due to the presence of multiple, independent pieces of evidence [7]. These systems are also able to meet the stringent performance requirements imposed by various applications [6]. Multimodal biometric systems address the problem of nonuniversality, since multiple traits ensure sufficient population coverage. Further, multimodal biometric systems provide antispoofing 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.

A. 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 serial 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.

B. Levels of Fusion

Multimodal biometric systems integrate information presented by multiple biometric indicators.

The information can be consolidated at various levels. Fig. 6 illustrates the three levels of fusion when combining two (or more) biometric systems. These are as follows.

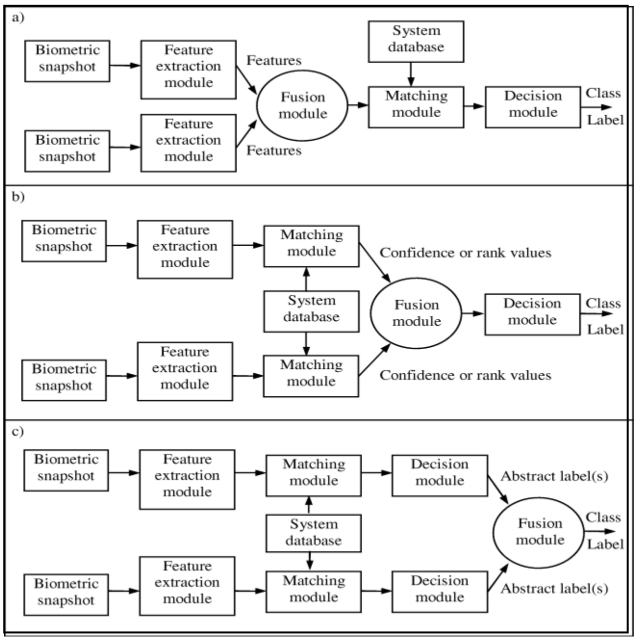

Fig. 6. Different levels of fusion in a parallel fusion mode: (a) fusion at the feature extraction level, and (b) fusion at matching score (confidence or rank) level, and (c) fusion at decision (abstract label) level. In all the three cases, the final class label is "Accept" or "Reject" when the biometric system is operating in the verification mode or the identity of the best matched user when operating in the identification mode. In (c), the intermediate abstract label(s) could be "Accept" or "Reject" in a verification system or a subset of database users in an identification system

I) 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.

ii) 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.

iii) 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 [8] 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 [23]. 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.* [5] theoretically analyzed the improvement in verification accuracy when two biometric characteristics are fused at the matching score level and at the decision level.

C. What to Integrate?

Multimodal biometric systems can be designed to operate in one of the following five scenarios (see Fig. 7).

i) 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.

ii) Multiple biometrics (Multimodal): 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 matches and then fingerprint matching which is slower but more accurate can be used for making the final identification decision).

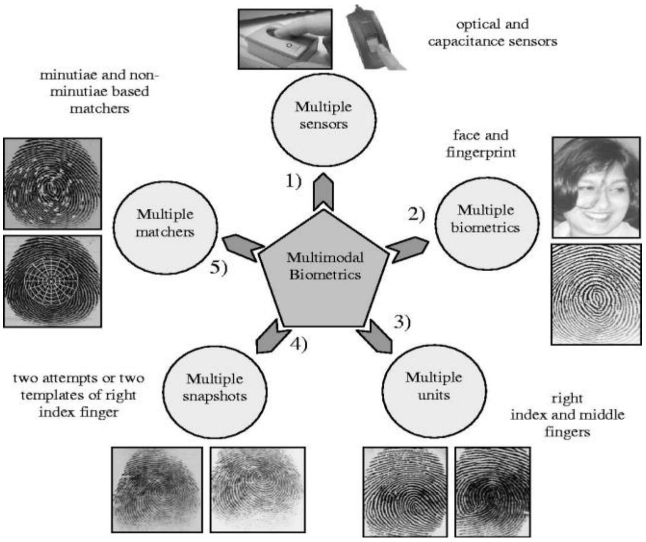

Fig. 7. Various scenarios in a multimodal biometric system

iii) Multiple units of the same biometric (Multi-Sample): fingerprints from two or more fingers of a person may be combined, or one image each of the two irises of a person may be combined.

iv) Multiple snapshots of the same biometric (Multi-Instance): more than one instance of the same biometric is used for the enrollment and/or recognition. For example, multiple impressions of the same finger, multiple samples of the voice, or multiple images of the face may be combined.

v) 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. First, a verification or an identification system can use such a combination scheme to make a recognition decision. Second, an identification system may use such a combination scheme for indexing.

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 (or weakly dependent) 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. In our opinion, scenarios 4 and 5 combine strongly correlated measurements and are expected to result in a smaller improvement in recognition accuracy than scenarios 2 and 3, but they are more cost effective than scenario 2 and more convenient than scenario 3. Scenarios 4 and 5 do require more computational and storage resources than a unimodal biometric system but in principle, different feature extractors and matchers can work in parallel. As a result, the overall response time of the system is limited by the slowest individual feature extractor and/or matcher. Finally, a combination of more than one of these scenarios may also be used.

IV. 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 $S(X_Q, X_I)$ (typically a single number) that quantifies the similarity between the input $(X_Q)$and the template (X_I) representations. 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 *nonmate 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 Fig. 2(a)].

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 nonmatch*). These two types of errors are often termed as *false accept* and *false reject*, respectively. There is a tradeoff between false match rate (FMR) and false nonmatch 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. AROC curve is a plot of FMR against (1-FNMR) or FNMR for various threshold values [see Fig. 2(b)].

Mathematically, the errors in a verification system can be formulated as follows. If the stored biometric template of the user I is represented by X_I and the acquired input for recognition is represented by X_Q , then the null and alternate hypotheses are:

H_0 input X_Q does not come from the same person as the template X_I;

H_1 input X_Q comes from the same person as the template X_I.

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 $S(X_Q, X_I)$ 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 is true H_0);

Type II: false nonmatch (D_0 is decided when H_1 is true).

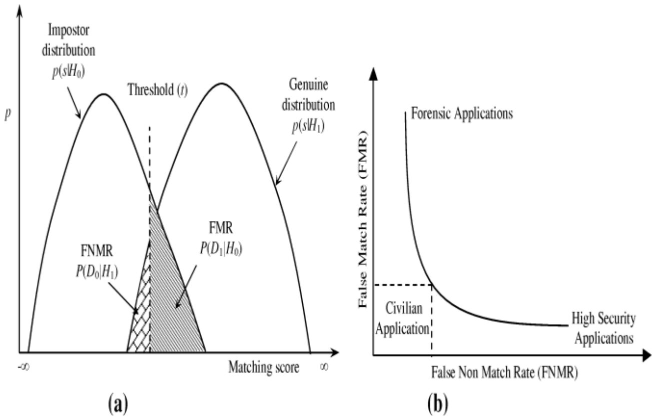

Fig. 8. Biometric system error rates. (a) FMR and FNMR for a given threshold t are displayed over the genuine and impostor score distributions; FMR is the percentage of nonmatch pairs whose matching scores are greater than or equal to t, and FNMR is the percentage of mate pairs whose matching scores 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

FMR is the probability of type-I error (also called significance level in hypothesis testing) and FNMR is the probability of type-II error as

$$FMR = P(D_1|H_0)$$

$$FNMR = P(D_0|H_1).$$

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 $p(S(X_Q, X_I)|H_1)$, and scores generated from a number of images from different fingers (the distribution $p(S(X_Q, X_I)|H_0)$. Fig. 8(a) graphically illustrates the computation of FMR and FNMR over genuine and impostor distributions

$$FMR = \int_t^{\alpha} p(S(X_Q, X_I)|H_1)dS$$

$$FNMR = \int_t^{-\alpha} p(S(X_Q, X_I)|H_1)dS.$$

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 nonmatch 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, $FNMR_N \cong FNMR$ and $FMR_N = 1-(1-FMR)^N \cong N.FMR$ (the approximations hold good only when $N.FMR < 0.1$). A detailed discussion on these issues is available in [17] and [19]. 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 nonmatch 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 [20].
- $FMR_N = 1 - (1 - FMR)^{N.P}$, 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. Fig. 8(b) depicts the FMR and FNMR tradeoffs in different types of biometric applications.

V. EXAMPLES OF MULTIMODAL BIOMETRIC SYSTEMS

Multimodal biometric systems have received much attention in recent literature. Brunelli *et al.* [9] 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.* developed a statistical framework based on Bayesian statistics to integrate information presented by the speech (text-dependent) and face data of a user [10]. Hong *et al.* combined face and fingerprints for person identification [6]. 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 Fig. 9).

Kumar *et al.* combined hand geometry and palmprint biometrics in a verification system [25]. A commercial product called BioID [11] 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 [22]. General strategies for combining multiple classifiers have been suggested in [12] and [13]. All the approaches presented in [12] (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 [14] 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, [15]–[16]).

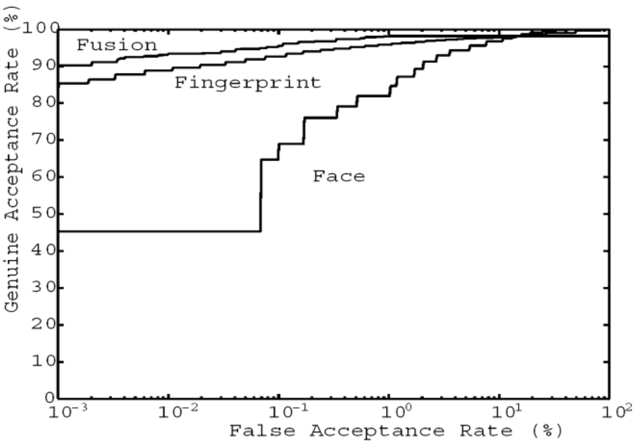

Fig. 9. An improvement in matching accuracy is obtained when face recognition and fingerprint recognition systems are combined in an identification system developed by Hong and Jain [6]

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 or two fingers of a person) Fig. 9. 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 [6]. is expected to result in a better improvement in performance than a combination of correlated modalities (e.g., different impressions of the same finger or different fingerprint matchers). 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.

REFERENCES

1. E. d. Os, H. Jongebloed, A. Stijsiger, and L. Boves, “Speaker verification as a user-friendly access for the visually impaired,” in *Proc. Eur. Conf. Speech Technology*, Budapest, Hungary, 1999, pp. 1263–1266.
2. A. Eriksson and P. Wretling, “How flexible is the human voice? A case study of mimicry,” in *Proc. Eur. Conf. Speech Technology*, Rhodes, 1997, pp. 1043–1046.
3. W. R. Harrison, *Suspect Documents, Their Scientific Examination*. Chicago, IL: Nelson-Hall, 1981.
4. T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, “Impact of artificial gummy fingers on fingerprint systems,” *Proc. SPIE*, vol. 4677, pp. 275–289, Feb. 2002.
5. L. Hong, A. K. Jain, and S. Pankanti, “Can multibiometrics improve performance ?,” in *Proc. AutoID’99*, Summit, NJ, Oct. 1999, pp. 59–64.
6. L. Hong and A. K. Jain, “Integrating faces and fingerprints for personal identification,” *IEEE Trans. Pattern Anal. Machine Intell.*, vol. 20, pp. 1295–1307, Dec. 1998.
7. L. I. Kuncheva, C. J.Whitaker, C. A. Shipp, and R. P.W. Duin, “Is independence good for combining classifiers?,” in *Proc. Int. Conf. Pattern Recognition (ICPR)*, vol. 2, Barcelona, Spain, 2001, pp. 168–171.
8. Y. A. Zuev and S. Ivanon, “The voting as a way to increase the decision reliability,” in *Proc. Foundations of Information/Decision Fusion with Applications to Engineering Problems*,Washington, DC, Aug. 1996, pp. 206–210.
9. R. Brunelli and D. Falavigna, “Person identification using multiple cues,” *IEEE Trans. Pattern Anal. Machine Intell.*, vol. 12, pp. 955–966, Oct. 1995.
10. E. S. Bigun, J. Bigun, B. Duc, and S. Fischer, “Expert conciliation for multimodal person authentication systems using bayesian statistics,” in *Proc. Int. Conf. Audio and Video-Based Biometric Person Authentication (AVBPA)*, Crans-Montana, Switzerland, Mar. 1997, pp. 291–300.
11. R. W. Frischholz and U. Dieckmann, “Bioid: A multimodal biometric identification system,” *IEEE Comput.*, vol. 33, pp. 64–68, 2000.
12. T. K. Ho, J. J. Hull, and S. N. Srihari, “Decision combination in multiple classifier systems,” *IEEE Trans. Pattern Anal. Machine Intell.*, vol. 16, pp. 66–75, Jan. 1994.
13. J. Kittler, M. Hatef, R. P. W. Duin, and J. Matas, “On combining classifiers,” *IEEE Trans. Pattern Anal. Machine Intell.*, vol. 20, pp. 226–239, Mar. 1998.
14. S. Prabhakar and A. K. Jain, “Decision-level fusion in fingerprint verification,” *Pattern Recognit.*, vol. 35, no. 4, pp. 861–874, 2002.
15. U. Dieckmann, P. Plankensteiner, and T. Wagner, “Sesam: A biometric person identification system using sensor fusion,” *Pattern Recognit. Lett.*, vol. 18, no. 9, pp. 827–833, 1997.
16. S. Ben-Yacoub, Y. Abdeljaoued, and E. Mayoraz, “Fusion of Face and Speech Data for Person Identity Verification,” IDIAP, Martigny, Switzerland, Res. Paper IDIAP-RR 99–03, 1999.
17. D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, “FVC2002: Fingerprint verification competition,” in *Proc. Int. Conf. Pattern Recognition (ICPR)*, Quebec City, QC, Canada, Aug. 2002, pp. 744–747.
18. J. L. Wayman, “Fundamentals of biometric authentication technologies,” *Int. J. Image Graphics*, vol. 1, no. 1, pp. 93–113, 2001.
19. (2002) Best Practices in Testing and Reporting Performance of Biometric Devices, Version 2.01. U. K. Biometric Work Group (UKBWG). [Online]. Available: http://www.cesg.gov.uk/technology/biometrics/
20. R. Cappelli, D. Maio, and D. Maltoni, “Indexing fingerprint databases for efficient 1:N matching,” in *Proc. 6th Int. Conf. Control Automation Robotics and Vision*, 2000.
21. M. Golfarelli, D. Maio, and D. Maltoni, “On the error-reject tradeoff in biometric verification systems,” *IEEE Trans. Pattern Anal. Machine Intell.*, vol. 19, pp. 786–796, July 1997.
22. A. K. Jain and A. Ross, “Learning user-specific parameters in a multibiometric system,” in *Proc. Int. Conf. Image Processing (ICIP)*, Rochester, NY, Sept. 2002, pp. 57–60.
23. J. Clark and A. Yuille, *Data Fusion for Sensory Information Processing Systems*. Boston, MA: Kluwer, 1990.
24. D. Zhang and W. Shu, “Two novel characteristic in palmprint verification: Datum point invariance and line feature matching,” *Pattern Recognit.*, vol. 32, no. 4, pp. 691–702, 1999.
25. A. Kumar, D. C. Wong, H. C. Shen, and A. K. Jain, “Personal verification using palmprint and hand geometry biometric,” presented at the 4th Int. Conf. Audio- andVideo-based Biometric Person Authentication, Guildford, U.K., June 9–11, 2003.
26. P. J. Philips, P. Grother, R. J.Micheals, D. M. Blackburn, E. Tabassi, and J. M. Bone. FRVT 2002: Overview and Summary. [Online]. Available: http://www.frvt.org/FRVT2002/documents.htm