PAPER *Special Issue on Biometrics*

Biometrics Systems: Anatomy of Performance

Anil Jain[†] *and* **Sharath Pankanti**[††]**,** *Nonmembers*

SUMMARY

An accurate automatic personal identification is critical to a wide range of application domains such as access control, electronic commerce, and welfare benefits disbursement. Traditional personal identification methods (e.g., passwords, and PIN) suffer from a number of drawbacks and are unable to positively identify a person. Biometrics refers to automatic identification of an individual based on her distinct physiological and/or behavioral traits. While biometrics is not an identification panacea, it is beginning to provide very powerful tools for a variety of new applications (e.g., cellular phones, smart cards and international border control) requiring positive identification. This work attempts to summarize important research issues in biometrics.

key words: Biometrics, Face, Fingerprint, Hand Geometry, Identity Theft, Iris, Performance Evaluation, Person Identification, Recognition, Retina, Security, Signature, Verification, Thermograms, Voice.

1. Introduction

Association of identity to an individual is called person identification. The problem of resolving the identity of a person can be categorized into two fundamentally distinct types of problems with different inherent complexities [2]: (i) verification and (ii) recognition. Verification (authentication) refers to the problem of confirming or denying a person's claimed identity (Am I who I claim I am?). Recognition (identification) refers to the problem of establishing a subject's identity (Who am I?). A reliable personal identification is critical in many daily transactions. For example, access control to physical facilities and computer privileges are becoming increasingly important to prevent their abuse. The *identity theft* has assumed an alarming proportion in our society [19], [25]. Consequently, some insurance companies in the United States are offering protection against identity theft and to deter related fraud (e.g., due to stolen credit cards). American Express is issuing "temporary" card numbers so that the customers are more comfortable in using credit cards for e-commerce. Thus, there is an increasing interest in developing inexpensive, reliable, and pervasive [24] personal identification methods in many emerging civilian, commercial, and financial applications (Table 1).

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

Table 1 Biometric Applications [1].

Typically, a person could be identified based on (i) a person's possession ("something that you possess"), e.g., permit physical access to a building to all persons whose identity could be authenticated by possession of a key; (ii) a person's knowledge of a piece of information ("something that you know"), e.g., permit login access to a system to a person who knows the user-id and a password associated with it. Another approach to positive identification is based on identifying physical characteristics of the person. The characteristics could be either a person's physiological traits, e.g., fingerprints, and hand geometry or her behavioral characteristics, e.g., voice and signature. This method of identification of a person based on her *distinctive* physiological/behavioral characteristics (see Fig. 1) is called *biometrics*. Since the biological characteristics can not be forgotten (like passwords) and can not be easily shared or misplaced (like keys), they are generally considered to be a more reliable approach to solving the personal identification problem.

A significant difference between a biometrics-based person identification and other conventional methods of identification is that the conventional methods do not involve any complex pattern recognition and hence they almost always perform accurately as intended by their system designers. On the other hand, a typical biometrics-based system is not perfectly accurate and commits two types of errors. A *false accept* (false positive or false match) refers to identifying an impostor to be a genuine user. A *false reject* (false negative or false non-match) refers to rejecting a genuine user as an impostor. It is desirable to maintain both low false match and low false non-match rates to achieve a high overall accuracy of the system. As the higher speed processors are becoming available at cheaper prices and as the cost of the biometric sensors is dramatically decreasing, we believe that increasing the accuracy of biometrics sys-

Manuscript received September 20, 2000.
Manuscript revised January 31, 2001.

[†]Anil Jain is University Distinguished Professor with Department of Computer Science and Engineering at Michigan State University, E. Lansing, MI, USA. jain@cse.msu.edu

[††]Sharath Pankanti is with IBM T. J. Watson Research Center, Hawthorne, NY, USA. sharat@us.ibm.com

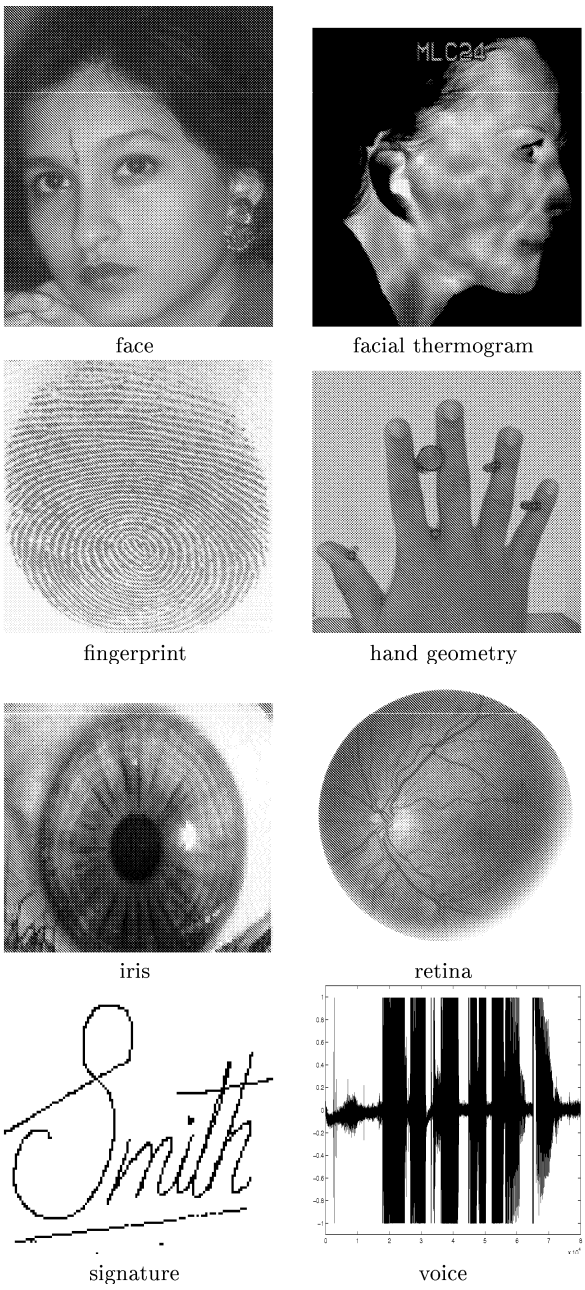

Fig. 1 Examples of biometric characteristics.

tems will become the predominant focus of the system design.

A primary objective of this paper is to closely examine the causality of the errors in a typical biometric system from pattern recognition system design perspective [3] and to identify the research challenges related to performance limitations of a biometric system. The rest of this paper is organized as follows. Section 2 presents a summary of basic concepts in pattern recognition system and proposes a framework for studying the performance limitations of a pattern recognition system. Section 3 presents a typical architecture of a biometric system. In Section 4, we summarize functionality of a fingerprint based biometric identity authentication system. We discuss various issues related to the performance limitations of biometrics systems in Sections 5, 6, and 7. In Section 8, we conclude and state remaining issues related to a widespread deployment of biometrics systems.

2. Pattern Recognition System

The design of a pattern recognition system is based on modeling the (i) information that is expected to remain invariant in different instantiations (presentations) of a given entity to be recognized and (ii) information for discriminating the given entity from extraneous entities or from other valid target entities. A typical pattern recognition system simultaneously attempts to capture both the invariance information in the patterns representing the same entities (intraclass variations) as well as the information enabling the discrimination of the patterns representing different entities (interclass variation) in two distinct stages: (a) the raw measurements from the sensor may contain a lot of extraneous information, so the feature extraction stage gleans a representation (or pattern) from the input measurements; (b) the decision-making stage matches the features (or patterns) obtained from the feature extraction stage with the stored prototype or pattern representation. The matching module implements the concept of the (in)variance in the feature space either as distance or similarity score metric: higher distance implies more dissimilarity; bigger scores indicate more similarity. Typically, a matcher rejects/accepts the hypothesis whether the two given patterns belong to the same category. For instance, in a hand geometry based person authentication system, feature extraction module may locate the right index finger from the hand image captured from a camera and determine its length and width to obtain the feature vector (l, w); the associated matcher may use Euclidean norm based distance metric (e.g., $d_i = \sqrt{(l-l_i)^2 + (w-w_i)^2} < T \Rightarrow (l, w) \in \mathcal{C}_i$, where T is a threshold, (l_i, w_i) is a prototypical pattern representing identity class $\mathcal{C}_i$) for identifying the patterns originating from the same hand. Fig. 2 illustrates these concepts in a simple two-dimensional fea-

ture space.

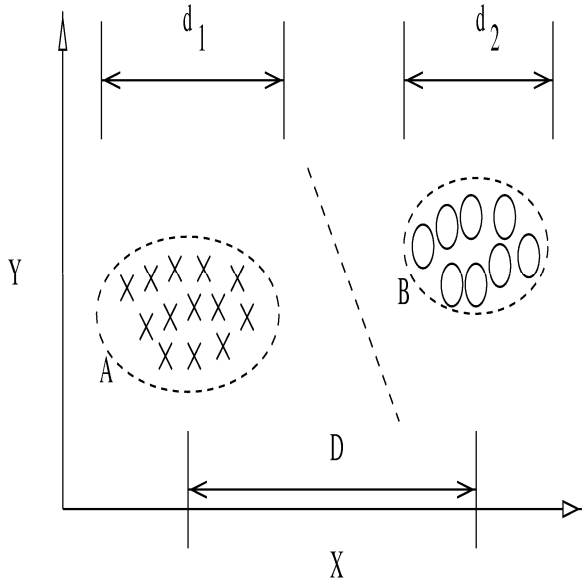

Fig. 2 Two-dimensional feature space of a hypothetical two-class pattern recognition problem. × and ◯ represent various patterns comprising the two classes, A and B, respectively. The boundaries around the patterns indicate the extent of expected variance in the patterns from the same class. d_1 and d_2 are within-class spreads for the two classes; D is the between-class separation. The dashed boundary depicts the class separation. The commonly referred *degrees-of-freedom (dof)* measures total spread in the feature measurements; large *dof* is necessary but not sufficient ingredient for better discriminability.

There are several reasons why a practical pattern recognition system is not perfectly accurate. Here, we attempt to categorize the limitations of the accuracy of a pattern recognition system in three fundamental categories. We will quickly define these limitations below and defer a more detailed exposition of these concepts to a later portion of this paper (Sections 5-7).

Given a sensor acquisition mechanism and the distributions of the sensor measurements from each class, they inherently determine an lower bound on the system error. We will refer to this limit as *information limited behavior* of the system.

The ideal feature extraction system should perfectly model the sensed measurements and should be designed to retain all the invariance and discrimination information in the sensed measurements. A practical feature extraction system is often based on a representation scheme (e.g., due to computational considerations or to avoid the curse of dimensionality) which may not capture all the useful information in the sensed measurements (see Fig. 3). This component of a limitation in a pattern recognition system will be referred to as *representation limited behavior*.

Finally, given a representation scheme, the design of an ideal matcher should perfectly model the invariance relationship in the different patterns from the same class. Again, a practical matcher may not correctly model the invariance relationship. We will refer to this limitation of a practical pattern recognition system as *invariance limited behavior*.

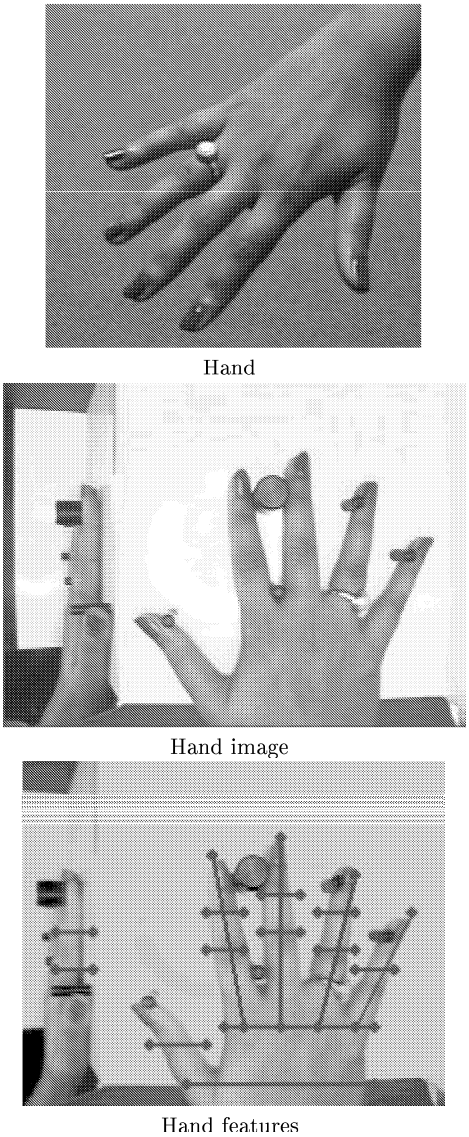

Fig. 3 Biometric trait, sensed signal, and representation.

These above mentioned inherent limitations of a practical pattern recognition system result in classification errors. The resulting performance can be characterized in several ways. Fig. 4 depicts a characterization of the performance of a hypothetical system (note that metric has changed from the distance metric in Fig. 2 to similarity): the distributions of the matching scores of patterns from the same class (genuine distribution, G1) and from different classes (impostor distribution, I1). The scores constituting genuine distribution are, on an average, higher than those from the impostor distribution. The two shaded regions together indicate the inherent minimum total error rate of the system.

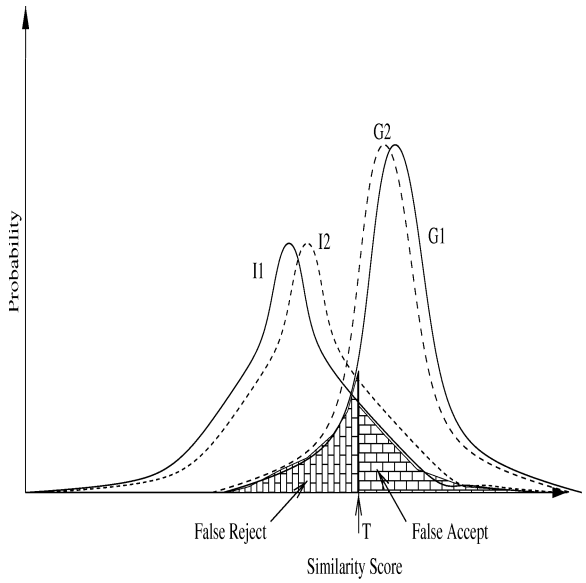

Fig. 4 Probability distributions of the genuine scores and impostor scores, G1 and I1, respectively, determine the performance of the system. False accept and false reject rates are controlled by the system operating threshold, T. G2 and I2 depict the shifts in the distributions predominantly due to invariance and representation limitations, respectively.

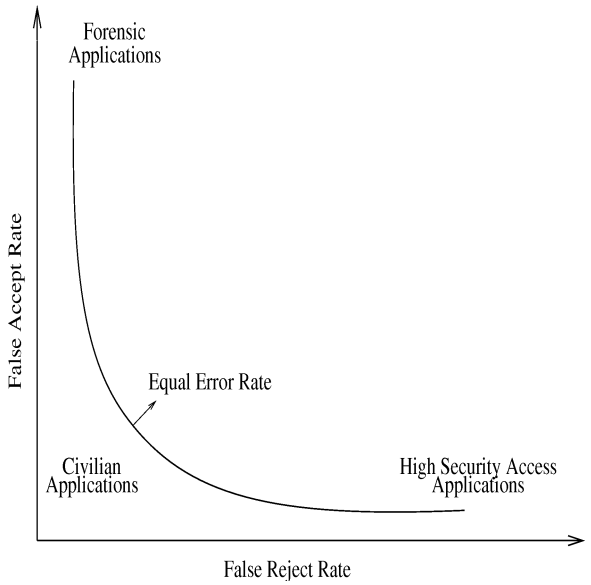

Fig. 5 Receiver operating characteristics (ROC) curve of a system illustrates false reject rate and false acceptance rate of a matcher at all operating points (threshold, T). Each point on an ROC defines FRR and FAR for a given matcher operating at a particular threshold. High security access applications are concerned about break-ins and hence operate the matcher at a point on ROC with a small FAR. Forensic applications desire to catch a criminal even at the expense of examining a large number of false accepts and hence operate their matcher at a high FAR. Civilian applications attempt to operate their matchers at the operating points with both, low FRR and low FAR [2].

One could eliminate dependence on the threshold altogether in Fig. 4 and the system performance can be represented directly in terms of the false positive and false negative error rates. This representation is called receiver operating characteristics (ROC). Fig. 5 shows a hypothetical ROC and typical operating points for different biometrics applications. Fig. 6 shows effects of difference system limitations on the performance.

3. Biometrics System Architecture

A typical biometric system architecture (Fig. 7) reflects essentially a pattern recognition system architecture: it typically acquires the pattern using sensors, a representation of the acquired input is extracted using a feature extraction algorithm, and finally, a decision is made based on the input representation(s) and the pattern representations previously stored in the system. The system primarily consists of two modules: enrollment (training) and authentication (recognition).

The function of enrollment module is same as a "training" or "learning" module in a pattern recognition system. It enrolls or associates identities of persons being enrolled with representations of their biometric measurements. When the biometric signal and the user name of a person to be enrolled are fed to the enrollment module, a feature (e.g., fingerprint minutiae) extraction algorithm is first applied to the biometric signal (e.g., fingerprint images) and a representation of the biometrics features or patterns (e.g., minutiae patterns) are extracted and stored in the system database.

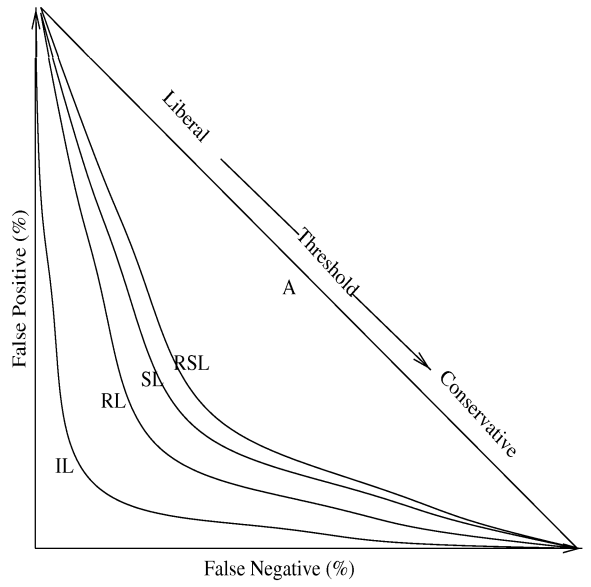

Fig. 6 Effect of imperfect representation space and similarity metric on system accuracy. Curves A, RSL, SL, RL, IL denote ROCs derived from a hypothetical arbitrary decision (A), representation and similarity limited (RSL), similarity limited (SL), representation limited (RL), and information limited (IL) systems, respectively. When an ROC is aligned with X- and Y-axes, it represents a perfect matcher.

The authentication module is similar to "recognition" or "testing" module in a pattern recognition system. It authenticates the identity of the person who intends to access the system. The person to be authenticated indicates his/her identity and presents his/her biometric measurement to the system; the biometric sensor captures the input biometric signal; features extracted from the captured biometric signal are matched against the person's representation stored in the system database to verify the identity claim made by the person. An identification system determines the identity associated with the biometric measurement without the user having to lay claim to an identity.

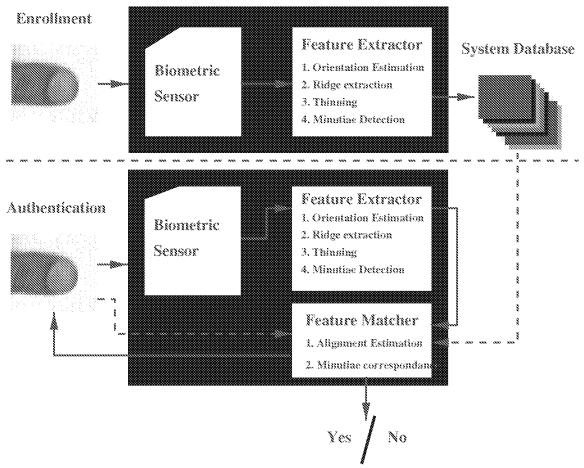

Fig. 7 Architecture of an automatic identity authentication system.

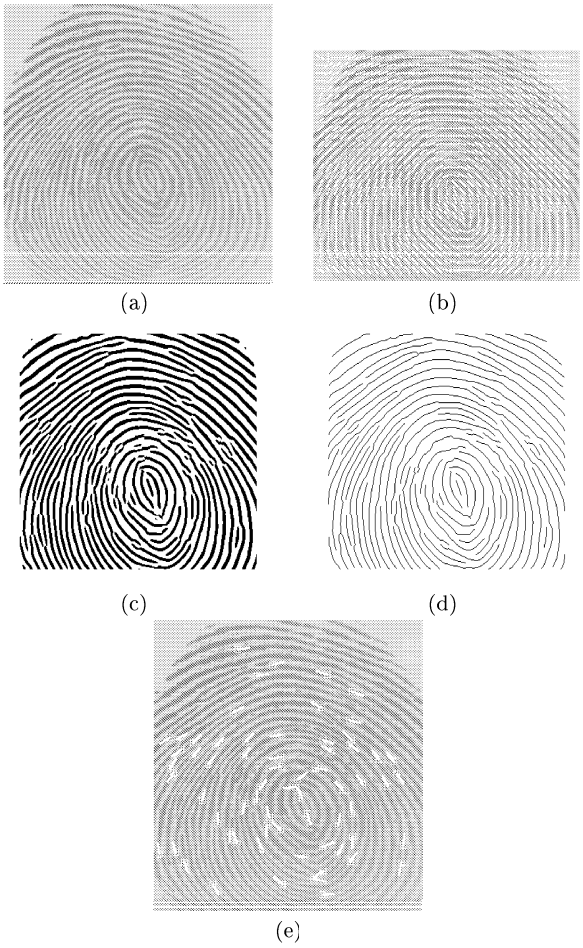

Fig. 8 Steps in fingerprint feature extraction [17]. (a) Input fingerprint image; (b) Orientation estimation for input Image; (c) ridges; (d) thinned ridges; (d) minutiae set overlaid on the input image.

4. An Example: Fingerprint Matching System

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

The unprocessed input gray values of the fingerprint images are not invariant over the time of capture and are susceptible to noise. Therefore, landmark features on a finger, e.g., the fingerprint ridge endings and ridge bifurcations (collectively known as minutiae), are used in a fingerprint-based authentication system. The feature extraction system detects the minutiae from the input image through a series of image processing steps (see Figures 8(a)-(e)). The feature vector typically consists of a list of the locations and other attributes (e.g., orientation of the ridge at a given minutia position) of the minutiae detected in a fingerprint image.

Given two feature vectors, a fingerprint matcher (see Figure 9) determines whether the minutiae in the feature vectors represent the same finger. Since the sensed fingers may be differently aligned with respect

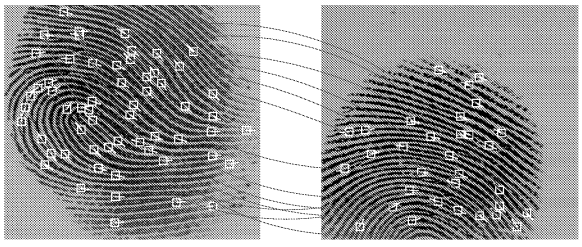

Fig. 9 Fingerprint feature matching [17].

to their respective imaging system, the two feature vectors cannot be directly compared and the feature vectors need to be *aligned*. The feature vectors are typically aligned based on, for example, some landmark information in the feature vector. In Figure 9, the properties of the ridge associated with minutiae are used to align the feature vectors. Once the feature vectors are aligned and overlaid, the number of "corresponding" minutiae (minutiae in sufficiently close proximity with each other and with similar attributes) constitutes a ba-

sis for quantifying the likelihood of fingerprint feature vectors representing the same finger. If the similarity score based on corresponding minutiae is higher than a predetermined threshold, the identities associated with the two feature vectors are said to be the same.

5. Quantifying Information Limited Behavior

One of the most fundamental questions one would like to ask about any *practical* biometric system is: what is the inherent discriminable information available in the input signal. Unfortunately, these questions are, if at all, have been answered in a very limited way for most biometrics modalities. An underlying reason for the lack of research in this area is that it is an ill-formulated problem in information theoretic sense. For instance, it is not always possible to define what an *ideal* matcher ("Turing Test") should decide if presented with very obliterated biometric measurements from a single biometric entity.

In addition, irreproducible and extraneous modulations of the sensed physiological or behavioral traits obfuscate the invariant and discriminatory information (Fig. 10). For instance, manual work, accidents etc. inflict injuries to the finger, thereby changing the ridge structure of the finger either permanently or semi-permanently. This may introduce additional spurious minutiae. There may be, in extreme cases, different portions/regimes of the biometric signal captured at the input which may offer only a limited opportunity for making a reliable identification decision. The act of sensing itself, especially for the modalities requiring contact as well as modalities using adverse/imperfect imaging conditions (e.g., non-standard environment [9]) adds noise to the image. For example, residues leftover from the previous fingerprint capture may restrict the reliability of decision-making. For instance, a recent large scale study reports that as many as 4% of the input fingerprint livescan images were not useful for personal authentication [9].

Further, since the discriminability is closely coupled with the composition of the target population, it is also important to know if and how the invariant biometric information is related to the genetic constitution of the individual. It would be interesting to know if and how a given biometric measurement is related to other biometric measurements of the same person (e.g., right index and left index fingers).

A related secondary issue concerns the individual variations in the inherent discriminable information: some individuals may have very distinct deep voice or peculiar faces while others may have very uncharacteristic voice or face. Inherent discriminatory capabilities of the input signal are especially important because rejection is not a valid option in positive personal identification. It is a common misconception that the performance of a biometric system can be arbitrarily improved with impunity by "rejecting" the undesirable patterns, e.g., removing the problematic people from the system. It is claimed that these people can be handled by either non-biometrics based exceptional processing schemes or handled by "manual" processing. However, both these solutions are problematic. In the first approach, we re-introduce the problems inherent in the possession- and knowledge-based techniques for personal identification which is not desirable, e.g., the possessions can be misplaced and exclusive knowledge can be forgotten. The second approach decreases the efficiency of the system and leaves the system more open to *collusion/coercion* attack. Most importantly, the "reject" option often proves to be the most vulnerable security threat to biometrics based access control systems. Thus, a biometrics system can not rely on "reject" option which typically simplifies the design of a practical pattern recognition system. In other words, a biometrics based system should make every attempt to enroll/process/recognize inputs associated with *all* identities in the population.

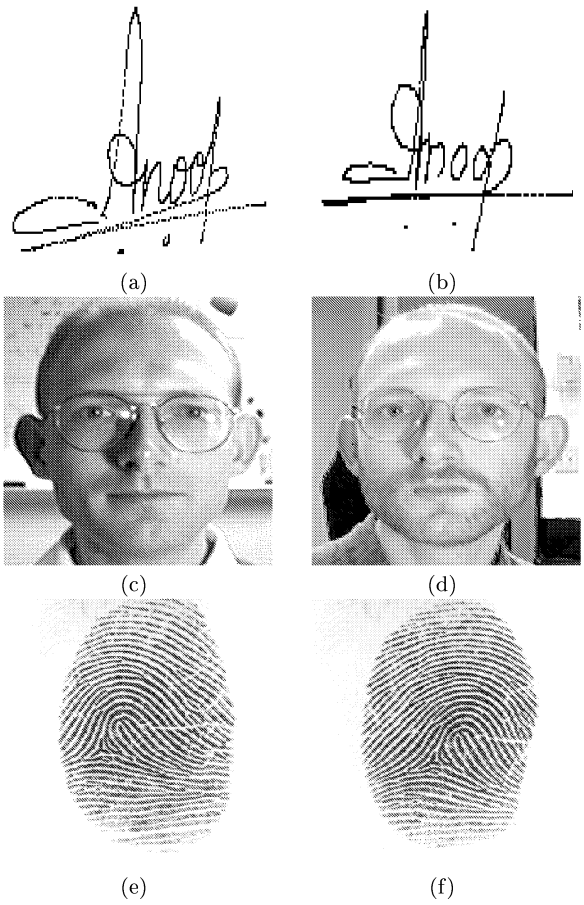

Fig. 10 Inherent signal and signal presentation variability. (a), (b) Variations in signatures of a person; (c), (d) facial variations; (e), (f) fingerprints of the same finger.

The biometric signal capacity has direct implica-

tions to the system design. Inherent signal limitations may suggest a better sensor, temporal/spatial fusion of multiple sensors, or modalities (see Fig. 12). In some contexts, it may also indicate a better system engineering to promote consistent acquisition through a constrained or user-friendly user interface. In other applications, when the validity of the biometric signal is suspect (e.g., due to circumvention issues), system integration with integrity sensors (e.g., liveness detection for fingers) may be indicated. On the other hand, the excess signal capacity may suggest a method of delimiting the signal bandwidth for either individual privacy or efficiency reasons.

The inherent signal capacity issue is of enormous complexity as it involves modeling both the composition of the population as well as interaction between the behavioral and physiological attributes at different scales of time and space. Nevertheless, a first order approximation to the answers to these questions will have a significant bearing on the acceptance of biometrics into our society as well as determining the upper bounds on scalability of the system deployment.

6. Modeling Representation Space

Design of a feature extraction subsystem is based on an implicit or an explicit model of the representation of the input signal and what component of the signal is useful for recognizing patterns.

For reasons of efficiency, parsimony, or expediency, the system designer may have designed the internal representation models that are inadequate to accommodate the signal complexity. For instance, the representation models which are solely based on human intuition and are not justified based on their invariance information, tend to show a preponderance towards terse symbolic descriptions and are impoverished to describe the entire richness of the information in the signal. Consequently, in systems based on a poor choice of representation models, the extraction of the structural details, especially, when the input measurements do not conform to the representation model assumptions, may result in a brittle feature extraction.

For instance, minutia based fingerprint authentication systems may model an ideal fingerprint image as smoothly flowing patterns of uniformly placed ridges and valleys. Such a fingerprint model would be appropriate if sensed ridges are indeed uniformly in contact with the sensor. However, the dryness of the skin, skin disease, sweat, dirt, and humidity in the air, all confound the situation resulting in a non-ideal contact situation: some parts of the ridges may not come in complete contact with the sensor and regions representing some valleys may come in contact with the sensor. This results in "noisy" low contrast images, leading to either spurious minutiae or missing minutiae. A less serious problem is the poor implementation of the representation extraction algorithms that introduces unnecessary measurement errors and inconsistent biases. For instance, a simplistic minutiae extraction algorithm may perturb the location and orientation estimates of the reported minutiae from their gray scale counterparts.

Even before confronting with the issues of signal representation, it is first necessary to determine how to locate the useful portion of the signal. This "segmentation" functionality is integral to all practical pattern recognition systems (see Fig. 11). In some systems, instead of passing a yes/no judgment, the signal is associated with a continuous *quality* variable. Modeling all possible scenarios of signal/noise situations and robustly extracting the signal is often challenging in practice.

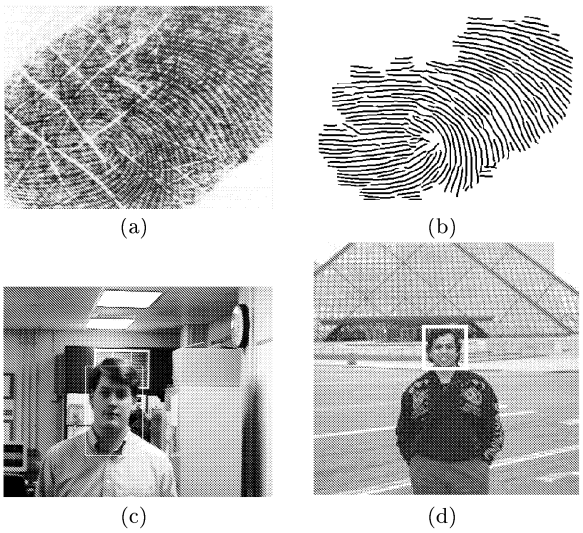

Fig. 11 Face and finger detection. (a) Input finger image; (b) recoverable finger region [15]; (c) indoor face detection; (d) outdoor face detection.

A surprisingly large number of biometric systems use rather simple representation models either borrowed from human intuition, manual identification systems, or allied research areas. Note that representation models based on legacy human-centric biometric matching systems (e.g., criminal/forensic AFIS) do not necessarily lead to optimal performance. Further, representation models for a biometric system borrowed from a closely allied pattern recognition area may not necessarily imply their propriety for person identification. For instance, even after 30 years of speaker verification research, some experts believe that the features inherited from the speech recognition research may not be appropriate for speaker verification and there is a need to take a fresh look at radically new voice features over a longer time segment of the speech signal [8]. In any event, biometrics field needs to focus on new and more sophisticated frameworks for representation and feature extraction. For instance, a recent research in "artificial life" stipulates that different characteris-

tic animal motions (e.g., gaits) represent different local minima in an energy optimizing procedure animals adopt to learn ambulation [7]. The emerging human genome and morphology research may similarly reflect on better representation models for different physiological biometric signals.

Another reason for enriched representation models is to broaden the scope of biometrics-based systems to an exciting set of emerging applications commonly known as affective computing [4]–[6]: systems and methods for detecting "humanly" attributes of the user and for responding in a human-centric way. The biometric signal may allow an interesting interplay with the humanly signal to permit a reciprocal interaction with the affective subsystem: the input biometric signal may communicate the human component (e.g., face image) to the affective system and the affective component (e.g., facial expression) may provide interesting context for the personal identification subsystem (e.g., is the person presenting biometric signal under duress?). Increasing terrorist threats warrant applications identifying not only the known terrorists but the persons undertaking "suspicious" activities. It is our fair guess that as the application demand for both user-specific individualization and user communication functionality grows, the biometrics will become integral (and interacting) components of larger and more comprehensive systems. We already see this trend in integration of speaker verification and speech recognition functionalities; there will be more applications of similar nature offered in the future. In all such integrated communication-cum-recognition systems, a richer representation of the input signal will permit a more human-centric computer interfaces. Thus, there is a need for more enriched data-driven models (e.g., Jain et al. [18]) and their vocabulary, especially, in behavioral biometrics and for more graceful methods for recovering these models from the input signals. As the biometrics systems become more complex, there will be an emergent need to automatically learn the optimal representations and adapt the internal models to the changing external environment (and enrollment).

7. Implementing Representational Invariance

The decisions made by the practical matchers can be brittle or unreliable due to two major reasons: (i) the building blocks of the systems are processing the input acquisitions in a way that cannot tolerate mistakes; (ii) the overall invariance relationship is not computed in way that degrades gracefully with deterioration of signal-to-noise ratio.

Prevalent system design is typically sequential: the results of information processed in each component are typically passed to the next component. This type of system design lays emphasis on somewhat rigid adherence to "expected" inputs and outputs of each component of the system. Consequently, degradation of performance in one component is sufficient to degrade the performance of the entire system. Note also that the traditional decomposition of the system design into feature extraction and matcher components also does not allow efficient passage of all the information necessary for making the invariance decisions. An integrated flow of information within the system (e.g., [23]) would allow a more effective performance of the entire system. Also, as alluded earlier, biometric systems will be increasingly interacting with diverse and novel applications. As systems become complex, it will be tedious and humanly impossible to model various components of the system and their interactions.

Invariant Transformation	**Accommodates**
Rigid	rotation, translation, spurious minutiae insertion/deletion
Similarity	and scaling
Elastic	and smoothly varying non-linear distortion
Topological	and arbitrary topological distortions

Table 2 Different invariance relationships used by matchers in fingerprint domain.

Often, how overall invariance relationship is decomposed into component similarity relationship among the features makes a significant difference in its performance. For instance, in biometric sensors which necessitate contact, such as fingerprints, the act of sensing distorts the measurements. Determined by the pressure and contact of the finger on the sensor, the three-dimensional shape of the finger gets mapped onto the two-dimensional surface of the sensor. Typically, this mapping (elastic distortion) function is uncontrolled and results in a large variance in the mapped fingerprint images across the impressions. In such situations, recovering invariance (distortion) from the parsimonious representations of the fingerprint (e.g., minutiae) is a challenging task. Efforts to find invariance (Table 2) in the representations are further stymied when the features extracted from noisy measurements violate the modeling assumptions mentioned earlier. Given the same invariant transformation (say, rigid transformation), there is a significant improvement in performance when the similarity is computed based on pose clustering using triplets of minutiae [22] (as opposed to similarity computed based on pose clustering using the entire set of minutiae).

One of the problems peculiar to biometrics is that the number of categories (e.g., identities) could be huge. For instance, in a country-wide ID system, the number of categories could be in millions. Further, the number of categories is ever changing depending upon the enrollment process. Both, the large and varying category size poses a number of challenges for scaling the matcher in terms of accuracy and speed.

One additional limitation of the existing biomet-

ric matchers is that they realize the models of the spatio-temporal inter-relationships (e.g., representation plasticity) in the human biometric signal in a very restricted way. For instance, there is very little work done on establishing the inter-relationship between the voice model of a healthy speaker and that of the same speaker with common cold [21]. Similarly, implementing restrictive invariance models of face limits the performance of a typical face recognition system because of aging, and changing styles of facial hair. It is not clear what models of biometric identifier plasticity will be adequate as well as robust in a practical system.

As with the representation models, a sophisticated biometric system should be able to learn complex invariance relationships and adapt them to various changing extrinsic/intrinsic conditions, constraints, and contexts. For a variety of reasons, biometric systems will use an integrated approach to accommodate and exploit a spectrum of situations (see Fig. 12). Multiple biometrics can alleviate several practical problems. For instance, although a biometric identifier is supposed to be *universal* (each person in the target population should possess it), in practice, no biometric identifier is truly universal. Similarly, the biometric identifiers are not always available for sensing or measurement. That is, a small fraction of the target population may possess biometric identifiers which are not easily quantifiable by the given biometric system. For instance, a small fraction of the population may possess fingerprints which are not easily captured by the representations (features) adopted by a given system. Consequently, the authentication system can not handle this fraction of population based on that particular biometric identifier. Further, different biometrics may not be acceptable to different sections of the target population. In highly secure systems, reinforcement of evidence from multiple independent biometric identifiers offers increasingly irrefutable proof of the identity of the authorized person. The assumptions of universality, collectability, acceptability, and integrity are more realistically accommodated when the personal authentication is based on information from several biometric identifiers. More research is necessary in the multibiometrics area to obtain an understanding of the complex design issues in a large system with interacting components.

Due to various constraints in the design of practical biometric systems, a designer has at her disposition only a limited number of training samples per identity and is confronted with finding the best possible generalization of the samples. Following Vapnik's [13] principle of "best possible design for the problem at hand", the designer would like to use any methodology for exploiting biometrics domain-specific frameworks to arrive at the optimal decision boundaries. Early results [10], [11], [14] show that the general purpose methodologies based on combining multiple classifiers, on support vector machines [12], on maximum likelihood transformations, are applicable to the biometric domain. However, it remains to be seen if additional constraints can be imposed based on strategies specifically related to biometrics domain (e.g., plasticity models mentioned above) to achieve a better performance.

Finally, it is important that the new methods of signal acquisition, representation, and invariance be realistically and objectively assessed. Our current understanding of the performance evaluation facilitates a comparative assessment of the candidate solutions on a given particular dataset (e.g., [16]) but does not permit us to objectively predict the system performance in the real world. Neither do we have the capability of objectively describing the existing databases nor any means of quantifying/comparing their complexities independent of a fully implemented matching system. Acquisition of these capabilities will indicate a level of understanding of the data that will instill end-user trust and acceptance of the system.

8. Conclusions

Our society has come a long way since its inception in small primitive tribes where every person in a community knew every other member of the community and need for mechanisms for personal identification was superfluous. Growing desire for more cost effective methods for identification (e.g., it is estimated that resetting forgotten passwords costs about US $50 per person per year) and rampant prevalent identity fraud are two significant reasons for an increased demand for automatic personal identification. Automatic personal identification using distinctive physiological or behavioral traits, called biometrics, is a necessary ingredient for delivering a positive, reliable, and irrefutable identification. This paper outlines some of the challenges and research issues related to performance of biometrics based person identification system.

An issue as (or perhaps, even more) important as performance of the biometrics system is its social acceptance. The biometric information about a user could be fraudently acquired and/or be possibly used for the purposes for which it was not originally sought (e.g., tracking user movements or investigating crimes). People are also afraid of having to defend themselves from the consequences of erroneous identification decisions e.g., due to insufficiently secure biometric systems accepting fraudulent inputs masquerading as genuine biometric measurements (e.g. fake fingers) of enrolled users. Finally and most importantly, the concept of automatic personal identification is perceived as dehumanizing by many individuals. Addressing the cross-disciplinary research issues related to personal identification and system security/integrity may enhance public trust in the biometric technology which, in fact, has a great potential for protecting individual privacy.

Recently, it has been speculated that an alterna-

tive method of personal identification may be based on silicon chip transponders implanted into the bodies of human beings [20]. Certainly, these technologies are more attractive in terms of their identification performance, mutability of their signature, and their capacity to enable the user to remain anonymous at his will. However, it is for sure that they will be perceived more intrusive and would suffer from an inconvenient enrollment. It, then, remains to be seen in the years to come, whether we would prefer to engineer biometric systems recognize us in a natural way, to engineer our bodies so that they are more easily identifiable by the machines, or to engineer a system in between the two extremes. An answer to this question will be based on how the biometric systems will be perceived by our society.

Acknowledgments

Authors wish to thank Prof. David Maltoni of Biometrics Systems Laboratory, University of Bologna, Cesana, Italy and Rien-Lien Hsu, Dan Gutchess, Salil Prabhakar, and Arun Ross of Pattern Recognition and Image Processing Laboratory, Michigan State University, East Lansing for their assistance and valuable suggestions in the manuscript revisions which substantially improved this presentation. We are grateful to Andrew Senior, IriScan Inc., Eyedentify Inc., and Mikos Ltd. who have provided the face (Figs. 10(c) and (d)), iris, thermogram, and retina images, respectively. Thanks to Kluwer Academic for granting us permission to reprint Figs. 5, 10(c), and 10(d).

References

[1] A. K. Jain, L. Hong and S. Pankanti, "Biometrics: Promising Frontiers for Emerging Identification Market", *Comm. ACM*, pp. 91-98, Feb. 2000.

[2] A. K. Jain, R. Bolle, S. Pankanti (eds.), Biometrics: Personal Identification in Networked Society, Kluwer Academic, December 1998.

[3] A. K. Jain, P. W. Duin, and J. Mao, Statistical Pattern Recognition, IEEE Transactions Pattern Analysis and Machine Intelligence, Vol. 22, No. 1, Jan. 2000. pp. 4-37.

[4] R. Picard, Affective Computing. MIT Press: Cambridge. 1997.

[5] W. Ark, C. C. Dryer, and D. Lu, The emotion mouse. In H.-J. Bullinger and J. Zielgler (Eds.) Human-Computer Interaction: Ergonomics and User Interfaces, Volume 1 of the Proceedings of the 8th International Conference on Human-Computer Interaction, Lawrence Erlbaum Associates, Pub: Mahwah, New Jersey, 818-823.

[6] R.C. Johnson, Computer Program Recognizes Facial Expressions. EE Times, www.eetimes.com, April 5, 1999.

[7] D. Terzopoulos, X. Tu, R. Grzeszczuk, Artificial Fishes with Autonomous Locomotion, Perception, Behavior, and Learning in a Simulated Physical World, Artificial Life IV: Proc. Fourth International Workshop on the Synthesis and Simulation of Living Systems, Cambridge, MA, July 1994, pp. 17-27.

[8] S. Furui, Recent Advances in Speaker Recognition, Proceedings of Audio- and Video-Biometric Person Authentication AVBPA'97, Crans-Montana, Switzerland, March 12-14, 1997, Springer-Verlag, Berlin, J. Bigun, G. Chollet and G. Borgefors (eds.), pp. 237–252.

[9] J. L. Wayman, Fundamentals of Biometric Technology, www.engr.sjsu.edu/biometrics/publications.html.

[10] P. J. Phillips, Support Vector Machines Applied to Face Recognition, In Advances in Neural Information Processing Systems 11, MIT Press, pp. 803-809, 1999.

[11] A. K. Jain, S. Prabhakar and S. Chen, Combining Multiple Matchers for a High Security Fingerprint Verification System, Pattern Recognition Letters, Vol 20, No. 11-13, pp. 1371-1379, 1999.

[12] V. N. Vapnik, Statistical Learning Theory, John Wiley & Sons, New York, 1998.

[13] V. N. Vapnik, Estimation of Dependencies Based on Empirical Data, Springer-Verlag, Berlin, 1982.

[14] U. V. Chaudhari and S. H. Maes, Pattern Specific Maximum Likelihood Transformations and Speaker Recognitionn with Sparse Training Data, July 1999 (in press).

[15] L. Hong, Automatic Personal Identification Using Fingerprints, *PhD Thesis*, Department of Computer Science and Engineering, Michigan State University, 1998.

[16] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, *FVC2000:* Fingerprint Verification Competition, 15th IAPR International Conference on Pattern Recognition, Barcelona, Spain, Sep. 3-7, 2000. http://bias.csr.unibo.it/fvc2000/

[17] A. Jain, L. Hong, S. Pankanti, and R. Bolle, On-line Identity-Authentication System using Fingerprints, *Proceedings of IEEE (Special Issue on Automated Biometrics)*, vol. 85, pp. 1365–1388, September 1997.

[18] A. K. Jain, S. Prabhakar, L. Hong and S. Pankanti, "Filterbank-based Fingerprint Matching", IEEE Transactions on Image Processing, Vol. 9, No.5, pp. 846-859, May 2000.

[19] A. Adiga, "The Theft of Your Identity", Financial Times, Friday, September 8, 2000, p3.

[20] M. McGinity, "Body of Technology", Comm. of ACM, Vol. 43, No. 9, Sep. 2000. pp 17–19.

[21] R. G. Tull, J. C. Rutledge, J. J. Mahler, Female alaryngeal speech enhancement for improved speaker identification using linear predictive synthesis, ASA 129th Meeting - Washington, DC, May 30-Jun 06, 1995

[22] R. S. Germain, A. Califano, S. Colville, Fingerprint matching using transformation parameter clustering, IEEE Computational Science and Engineering, 4(4), Oct-Dec, 1997, pp 42–49.

[23] D. Maio and D. Maltoni, Direct gray-scale minutiae detection in fingerprints, IEEE Transactions on Pattern Analysis and Machine Intelligence, 19(1), Jan. 1997. pp. 27-40.

[24] K, Uchinda, "Fingerprint-based User-friendly Interface and Pocket-PID for mobile Authentication", 15th IAPR International Conference on Pattern Recognition, Barcelona, Spain, Sep. 3-7, 2000. Vol. 4, pp. 205 - 209.

[25] US Full Committee hearing on "Identity Theft Prevention Act", Sep. 13, 2000. http://www.house.gov/banking/91300wit.htm.

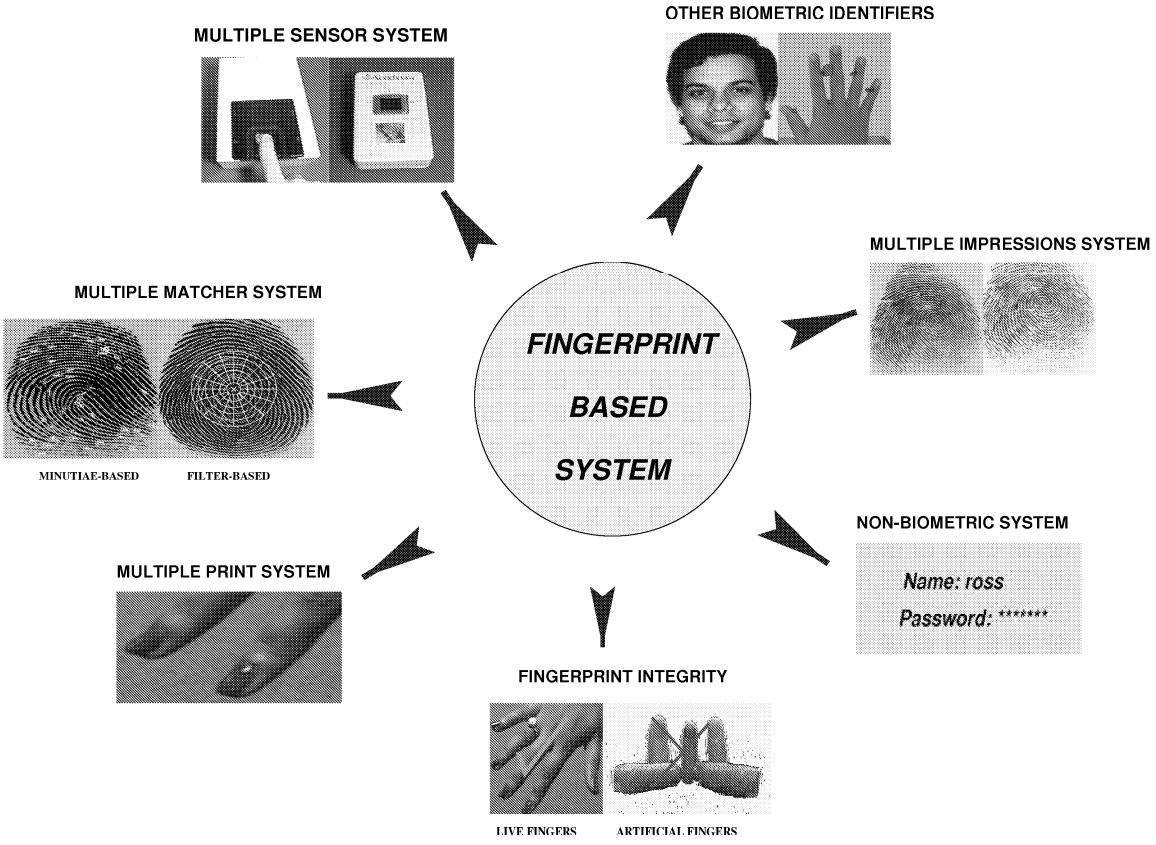

Fig. 12 Multiple choices for integration in a fingerprint based system. An example for each choice is shown.