Biometric Devices And Recognisation

Shreya Shrimandhar Demapure.[1], Yogita Bharatesh Chougule[2]
[1, 2] Dept of Information technology
[1, 2] Sharad Institute of Technology, Yadrav.

Abstract- *Biometrics refers to the automatic identification of a person based on his physiological / behavioural characteristics. This method of identification is preferred for various reasons; the person to be identified is required to be physically present at the point of identification; identification based on biometric techniques obviates the need to remember a password or carry a token. With the increased use of computers or vehicles of information technology, it is necessary to restrict access to sensitive or personal data. A wide variety of systems requires reliable personal recognition schemes to either confirm or determine the identity of an individual requesting their services. The purpose of such schemes is to ensure that the rendered services are accessed only by a legitimate user and no one else. Examples of such applications include secure access to buildings, computer systems, laptops, cellular phones, and ATMs. In the absence of robust personal recognition schemes, these systems are vulnerable to the wiles of an impostor. Biometric recognition or, simply, biometrics refers to the automatic recognition of individuals based on their physiological and/or behavioural characteristics. By using biometrics, it is possible to confirm or establish an individual's identity based on "who she is," rather than by "what she possesses" (e.g., an ID card) or "what she remembers" (e.g., a password). In this paper, we give a brief overview of the field of biometrics and summarize some of its advantages, disadvantages, strengths, limitations, and related privacy concerns. I*

Keywords*:* Automatic identification, Biometrics, identification, multimodal biometrics, recognition, verification.

I. INTRODUCTION

Biometricis the technical term for body measurements and calculations. It refers to metrics related to human characteristics. Biometrics authentication (or realistic authentication) is used in computer science as a form of identification and It is also used to identify individuals in groups that are under surveillance.

Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. Biometric identifiers are often categorized as physiological versus behavioural characteristics.[Physiological characteristics are related to the shape of the body. Examples include, but are not limited to fingerprint, palm veins, face recognition, DNA, print, hand, recognition, retina and odour/scent. Behavioural characteristics are related to the pattern of behaviour of a person, including but not limited to rhythm, gait, and voice. Some researchers have coined the term behaviometrics to describe the latter class of biometrics.

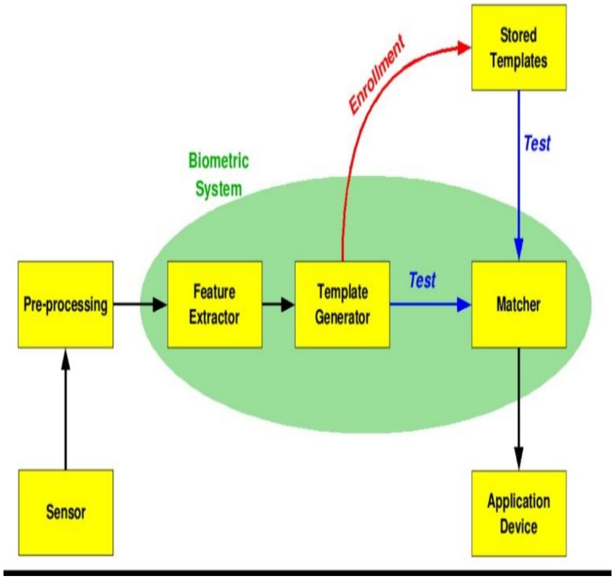
More traditional means of access control include token-based identification systems, such as a driver's license or passport, and knowledge-based identification systems, such as a password or number. Since biometric identifiers are unique to individuals, they are more reliable in verifying identity than token and knowledge-based methods; however, the collection of biometric identifiers raises privacy concerns about the ultimate use of this information.

II. BIOMETRIC FUNCTIONALITY

Many different aspects of human physiology, chemistry or behaviour can be used for biometric authentication. The selection of a particular biometric for use in a specific application involves a weighting of several factors. Jain et al. (1999) identified seven such factors to be used when assessing the suitability of any trait for use in biometric authentication.

- Universality means that every person using a system should possess the trait.
- Uniqueness means the trait should be sufficiently different for individuals in the relevant population such that they can be distinguished from one another.
- Permanence relates to the manner in which a trait varies over time. More specifically, a trait with 'good' permanence will be reasonably invariant over time with respect to the specific matching algorithm.
- Measurability (collectability) relates to the ease of acquisition or measurement of the trait. In addition, acquired data should be in a form that permits subsequent processing and extraction of the relevant feature sets.
- Performance relates to the accuracy, speed, and robustness of technology used (see performance section for more details).

- Acceptability relates to how well individuals in the relevant population accept the technology such that they are willing to have their biometric trait captured and assessed.
- Circumvention relates to the ease with which a trait might be imitated using an artefact or substitute.
- Proper biometric use is very application dependent. Certain biometrics will be better than others based on the required levels of convenience and security. No single biometric will meet all the requirements of every possible application.



The block diagram illustrates the two basic modes of a biometric system. First, in verification(or authentication) mode the system performs a one-to-one comparison of a captured biometric with a specific template stored in a biometric database in order to verify the individual is the person they claim to be. Three steps are involved in the verification of a person. In the first step, reference models for all the users are generated and stored in the model database. In the second step, some samples are matched with reference models to generate the genuine and impostor scores and calculate the threshold. The third step is the testing step. This process may use a smartcard, username or ID number (e.g. PIN) to indicate which template should be used for comparison.

'Positive recognition' is a common use of the verification mode, "where the aim is to prevent multiple people from using the same identity".

Second, in identification mode the system performs a one-to-many comparison against a biometric database in an attempt to establish the identity of an unknown individual. The system will succeed in identifying the individual if the comparison of the biometric sample to a template in the database falls within a previously set threshold. Identification mode can be used either for 'positive recognition' (so that the user does not have to provide any information about the template to be used) or for 'negative recognition' of the person "where the system establishes whether the person is who she (implicitly or explicitly) denies to be”. The latter function can only be achieved through biometrics since other methods of personal recognition such as passwords, PINs or keys are ineffective.

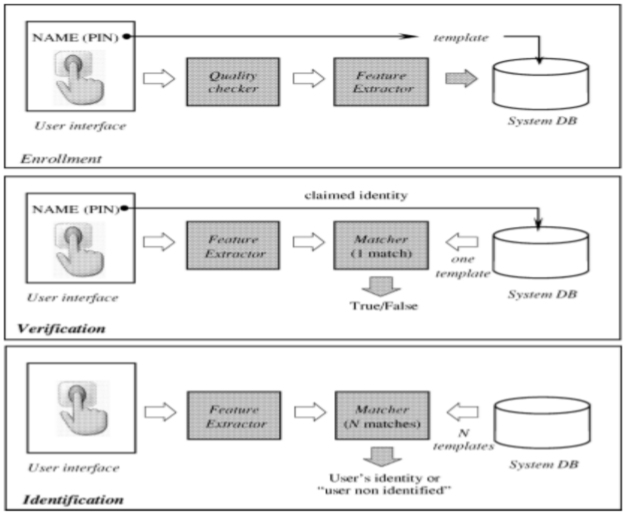
The first time an individual uses a biometric system is called enrolment. During enrolment, biometric information from an individual is captured and stored. In subsequent uses, biometric information is detected and compared with the information stored at the time of enrolment. Note that it is crucial that storage and retrieval of such systems themselves be secure if the biometric system is to be robust. The first block (sensor) is the interface between the real world and the system; it has to acquire all the necessary data. Most of the times it is an image acquisition system, but it can change according to the characteristics desired. The second block performs all the necessary pre-processing: it has to remove artifactsfrom the sensor, to enhance the input (e.g. removing background noise), to use some kind of normalization, etc. In the third block, necessary features are extracted. This step is an important step as the correct features need to be extracted in an optimal way. A vector of numbers or an image with particular properties is used to create a template. A template is a synthesis of the relevant characteristics extracted from the source. Elements of the biometric measurement that are not used in the comparison algorithm are discarded in the template to reduce the file size and to protect the identity of the enrolee[citation needed].

During the enrolment phase, the template is simply stored somewhere (on a card or within a database or both). During the matching phase, the obtained template is passed to a matcher that compares it with other existing templates, estimating the distance between them using any algorithm (e.g. Hamming distance). The matching program will analyse the template with the input. This will then be output for any specified use or purpose (e.g. entrance in a restricted area)[citationneeded]. Selection of biometrics in any practical application depending upon the characteristic measurements and user requirements. In selecting a particular biometric, factors to consider include, performance, social acceptability, ease of circumvention and/or spoofing, robustness, population coverage, size of equipment needed and identity theft deterrence.

The selection of a biometric is based on user requirements and considers sensor and device availability, computational time and reliability, cost, sensor size, and power consumption.

III. PERFORMANCE

Here following are used as performance metrics for biometric systems:



- **False match rate** (FMR, also called FAR = False Accept Rate): the probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percent of invalid inputs that are incorrectly accepted. In case of similarity scale, if the person is an imposter in reality, but the matching score is higher than the threshold, then he is treated as genuine. This increases the FMR, which thus also depends upon the threshold value.
- **False non-match rate** (FNMR, also called FRR = False Reject Rate): the probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percent of valid inputs that are incorrectly rejected.
- **Receiver operating characteristic**or relative operating characteristic (ROC): The ROC plot is a visual characterization of the trade-off between the FMR and the FNMR. In general, the matching algorithm performs a decision based on a threshold that determines how close to a template the input needs to be for it to be considered a match. If the threshold is reduced, there will be fewer false non-matches but more false accepts. Conversely, a higher threshold will reduce the FMR but increase the FNMR. A common variation is the Detection error trade-off *(DET)*, which is obtained using normal deviation scales on both axes. This more linear graph illuminates the differences for higher performances (rarer errors).
- **Equal error rate** or crossover error rate (EER or CER): the rate at which both acceptance and rejection errors are equal. The value of the EER can be easily obtained from the ROC curve. The EER is a quick way to compare the accuracy of devices with different ROC curves. In general, the device with the lowest EER is the most accurate.
- **Failure to enrol rate** (FTE or FER): the rate at which attempts to create a template from an input is unsuccessful. This is most commonly caused by low-quality inputs.
- **Failure to capture rate** (FTC): Within automatic systems, the probability that the system fails to detect a biometric input when presented correctly.
- **Template capacity**: the maximum number of sets of data that can be stored in the system.

IV. COMPARISON OF VARIOUS BIOMETRICS:

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

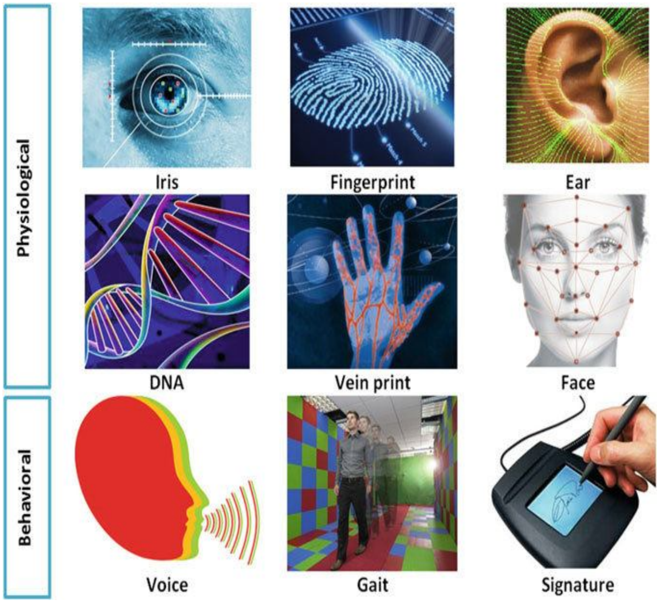


Fig-Different Biometric Modalities.

• **DNA:** Deoxyribonucleic acid (DNA) is the one-dimensional (1–D) ultimate unique code for one's individuality—except for the fact that identical twins have identical DNA patterns. It is, however, currently used mostly in the context of forensic applications for person recognition. Three issues limit the utility of this biometrics for other applications:

1) **Contamination and sensitivity:** it is easy to steal a piece of DNA from an unsuspecting subject that can be subsequently abused for an ulterior purpose;
2) **Automatic real-time recognition issues:** the present technology for DNA matching requires cumbersome chemical methods (wet processes) involving an expert's skills and is not guardroom-linenon-invasive recognition; and
3) **Privacy issues:** information about susceptibilities of a person to certain diseases could be gained from the DNA pattern and there is a concern that the unintended abuse of genetic code information may result in discrimination, e.g., in hiring practices.

• **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 penniform landmark location on the ear. The feature so fanear 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).The most popular approaches to face recognition are based on either:
1) the location and shape of facial attributes such as the eyes, eyebrows, nose, lips and chin, and their spatial relationships, or
2) the overall (global) analysis of the face image that represents a face as a weighted combination of a number of canonical faces. While the verification performance of the face recognition systems that are commercially available is reasonable , they impose a number of restrictions on how the facial images are obtained, sometimes requiring a fixed and simple background or special illumination .These systems also have difficulty in recognizing a face from image captured from two drastically different views and under different illumination conditions. 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. In order for a facial recognition system to work well in practice, it should automatically:

1. detect whether a face is present in the acquired image;
2. locate the face if there is one; and
3. recognize the face from a general viewpoint (i.e., from any pose).

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

• **Fingerprint:** Humans have used fingerprints for personal identification for many centuries and the matching accuracy using fingerprints has been shown to be very high . 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 fatal development. Fingerprints of identical twins are different and so are the prints on each finger of the same person. Today, a fingerprint scanner costs about U.S. $20 when ordered in large quantities and the marginal cost of embedding a fingerprint-based biometric in a system (e.g., laptop computer) has become affordable in a large number of applications.

The accuracy of the currently available fingerprint recognition systems is adequate for verification systems and small- to medium-scale identification systems involving a few hundred users. Multiple fingerprints of a person provide additional information to allow for large-scale recognition involving millions of identities. One problem with the current fingerprint recognition systems is that they require a large amount of computational resources, especially when operating in the identification mode. Finally, fingerprints of a small fraction of the population may be unsuitable for automatic identification because of genetic factors, aging, environmental, or occupational reasons
(e.g., manual workers may have a large number of cuts and bruises on their fingerprints that keep changing).

• **Gait:** Gait is the peculiar way one walks and is a complex patio-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 behavioural 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 does not appear to have any negative effects on the verification accuracy of hand geometry-based systems. The geometry of the hand is not known to be very distinctive and hand geometry-based recognition systems cannot be scaled up for systems requiring identification of an individual from a large population. Further, hand geometry information may not be invariant during the growth period of children. In addition, an individual's jewellery (e.g., rings) or limitations in dexterity (e.g., from arthritis), may pose further challenges in extracting the correct hand geometry information. The physical size of a hand geometry-based system is large, and it cannot be embedded in certain devices like laptops. There are verification systems available that are based on measurements of only a few fingers (typically, index and middle) instead of the entire hand. These devices are smaller than those used for hand geometry, but still much larger than those used in some other biometrics (e.g., fingerprint, face, voice).

• **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 fatal 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 behavioural biometric is not expected to be unique to each individual but it offers sufficient discriminatory information to permit identity verification. Keystroke dynamics is a behavioural 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.

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

• **Palmprint:** The palms of the human hands contain pattern of ridges and valleys much like the fingerprints. The area of the palm is much larger than the area of a finger and, as a result, palmprints are expected to be even more distinctive than the fingerprints. Since palmprint scanners need to capture a large area, they are bulkier and more expensive than the fingerprint sensors. Human palms also contain additional distinctive features such as principal lines and wrinkles that can be captured even with a lower resolution scanner, which would be cheaper . 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.

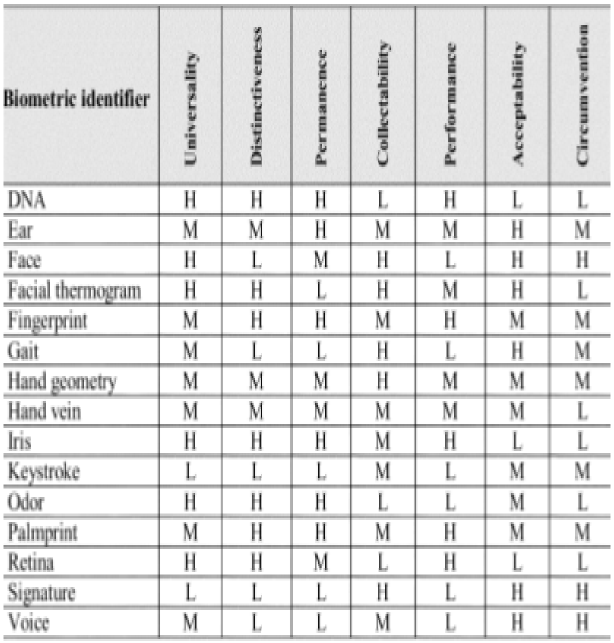
• **Retinal scan:** The retinal vasculature is rich in structure and is supposed to be a characteristic of each individual and each eye. It is claimed to be the most secure biometric since it is not easy to change or replicate the retinal vasculature. The image acquisition requires a person to peep into 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 behavioural 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 thatfool the system.

•**Voice:** Voice is a combination of physiological and behavioural 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 Synthes is of the sound.

These physiological characteristics of human speech are in variant for an individual, but the behavioural 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 fix predetermined phrase. Text-independent voice recognition system recognizes the speaker independent of what she speaks. A text-independent system is more difficult to design than a text-dependent system but offers more protection against fraud. A disadvantage of voice-based recognition is that speech features are sensitive to a number of factors such as background noise. Speaker recognition is most appropriate in phone-based applications but the voice signal over phone is typically degraded in quality by the microphone and the communication channel. The applicability of a specific biometric technique depends heavily on the requirements of the application domain. No single technique can outperform all the others in all operational environments. In this sense, each biometric technique is admissible and there is no optimal biometric characteristic. For example, it is well known that both the fingerprint-based and iris-based techniques are more accurate than the voice-based technique. However, in a tele-banking application, the voice-based technique may be preferred since it can be integrated seamlessly into the existing telephone system.

TABLE I Comparison of various biometric technology . High, medium and low are denoted by H,M and L Respectively



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

V. ADVANTAGES AND DISADVANTAGES OF BIOMETRICS

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

A.Positive Recognition in Commercial Applications The traditional technologies available to achieve a positive recognition include knowledge-based methods (e.g., PINs and passwords) and token-based methods (e.g., keys and cards). Most people set their passwords based on words or digits that they can easily remember, such as names and birthdays of family members, favourite movie or music stars, and dictionary words (a survey of 1200 British office workers in year 2001 found that almost half chose their own name, the name of a pet, or that of a family member as a password; others based their passwords on the names such as Darth Vader and Homer Simpson). Such passwords are easy to crack by guessing or by a simple brute force dictionary attack. Although it is possible, and even advisable, to keep different passwords for different applications and change them frequently, most people use the same password across different applications and never change them. If a single password is compromised, it may result in a breach in security in many applications. For example, a hacker may create a bogus web site that entices users with free air miles if they were to register on the website with a login name and password. The hacker may then try to use the same login name and password to attack the users' corporate accounts, and most likely succeed. Longer passwords are more secure but harder to remember which prompts some users to write them down in accessible locations (e.g., on a "Post-it" note) and hide it under the keyboard. Strong passwords are difficult to remember and result in more help desk calls for forgotten or expired passwords. Cryptographic techniques such as encryption can provide very long passwords (encryption keys) that are not required to be remembered but that are in turn protected by simple passwords, thus defeating their purpose. Further, a hacker needs to break only one password amongallthe employees togain accessto a company'sInternet and thus, a single weak password compromises the overall security of every system that the user has access to. Thus, the security of the entire system is only as good as the weakest password. Finally, when a password is shared with a colleague, there is no way for the system to know who the actual user is. Similarly, there are many problems with possession-based personal recognition. For example, keys and tokens can be shared, duplicated, lost or stolen and an attacker may make a "master" key that may open many locks. It is significantly more difficult to copy, share, and distribute biometrics with as much ease as passwords and tokens. Biometrics cannot be lost or forgotten and online biometrics-based recognition systems require the person to be recognized to be present at the point of recognition. It is difficult to forge biometrics and extremely unlikely for a user to repudiate, for example, having accessed a computer network. Further, all the users of the system have relatively equal security level and one account is no easier to break than any other (e.g., through social engineering methods). Biometrics introduces incredible convenience for the users (as users are no longer required to remember multiple, long and complex frequently changing passwords) while maintaining a sufficiently high degree of security. Let us now consider a brute force attack on a biometric system operating in a verification mode in a commercial application. The chance of success of a brute force attack depends on the matching accuracy of the biometric verification. Let us assume that a certain commercial biometric verification system wishes to operate at 0.001% FMR. At this setting, several biometric systems (e.g., the state-of-the-art fingerprint and iris recognition systems) can easily deliver less than 1% FNMR . An FMR of 0.001% indicates that, if a hacker launches a brute force attack with a large number of different fingerprints, 1 out of 100 000 attempts will succeed on an average. This may be considered equivalent to the security offered by a randomly chosen five-digit PIN (although a brute force attack against a five-digit PIN is guaranteed to succeed in 100 000 attempts and requires only 50 000 attempts, on an average). To attack a biometric-based system, one needs to generate (or acquire) a large number of samples of that biometric (e.g., fingerprints), which is much more difficult than generating a large number of PINs/passwords. Finally, the FMR of a biometric system can

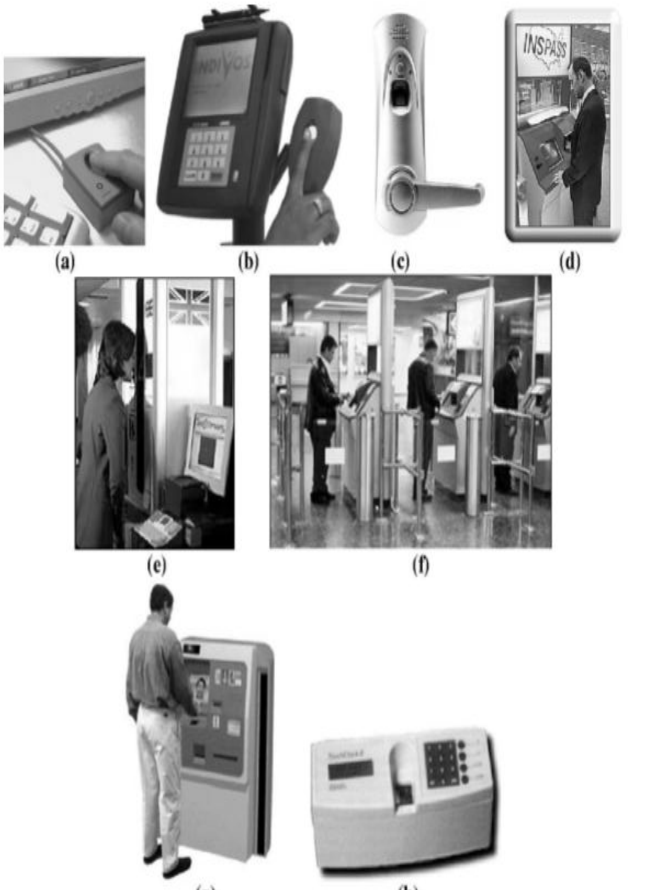


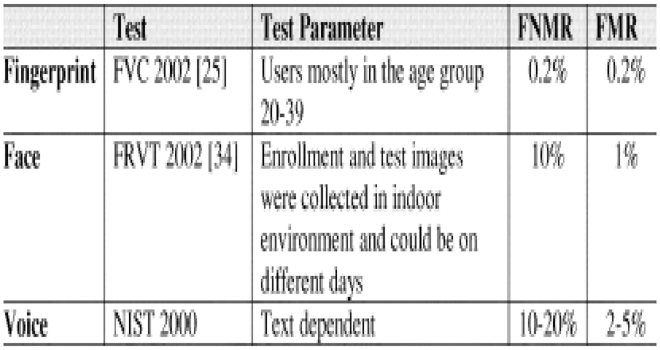
Fig. Examples of biometric application. (a) Fingerprint verification system manufactured by Digital Persona, Inc., is used for computer and network login. (b) Fingerprint-based point of sale (POS) terminal manufactured by Indigos, Inc., that verifies the customers before charging their credit cards and speeds up payment in retail shops, restaurants and cafeterias. (c) Fingerprint-based door lock manufactured by BioThentica Corporation used to restrict access to premises is shown. (d) Immigration and naturalization service accelerated service system (INSPASS), which is installed at major airports in the U.S., is based on hand geometry verification technology developed by Recognition Systems, Inc., and significantly reduces the immigration processing time. (e) Border passage system using iris recognition at London's Heathrow airport. (f) Ben Gurion airport in Tel Aviv (Israel) uses Express Card entry kiosks fitted with hand geometry systems for security and immigration. (g) The Face Pass system from Visage is used in POS verification applications like ATMs, therefore obviating the need for PINs. (h) The Identic Touch Clock fingerprint system is used in time and attendance applications.

be arbitrarily reduced for higher security at the cost of increased inconvenience to the users that results from a higher FNMR. Note that a longer PIN or password also increases the security while causing more inconvenience in remembering and correctly typing them. Certain commercial applications would like to operate the biometric system in an identification mode instead of the verification mode for the added convenience of not requiring the users to claim an identity. Usually, speed is perceived as the biggest problem in scaling up an identification application. However, the fact is that the identification accuracy scales even worse than the speed. Consider an identification application with 10 000 users. We can certainly find a combination of a fast fingerprint matching algorithm and special purpose hardware capable of making an identification in a few seconds. On the other hand, a matching algorithm with a verification FMR of 0.001% will have an identification of ! This implies that an impostor has a good chance of gaining access to the system by simply using all of the ten fingers on her two hands. Therefore, while small- to medium-scale commercial applications (e.g., a few hundred users) may still use single biometric identification, the only obvious solution for building a highly accurate identification system for large scale applications appears to be multimodal biometric systems . For example, a system may combine face and fingerprint of a person or fingerprints from multiple fingers of a person for recognition. Finally, in commercial applications, addition or replacement of existing personal recognition methods with biometrics-based solutions should be based on a cost-benefit analysis. For example, is the installation and maintenance cost of a biometric-based computer login system less than the currently used password system? Note that, according to the Gartner Group, between 20% and 50% of all help desk calls are for password resets. Forrester Research states that the average help desk labour cost for a single password reset is about US $38.

B. Negative Recognition in Government and Forensic Applications In negative recognition applications such as employee background checking and preventing terrorists from boarding airplanes, the personal recognition is required to be performed in the identification mode. As mentioned earlier, achieving the same accuracy in an identification system as in a verification system is a much harder problem due to the large number of comparisons that are required to be performed. Consider that airport authorities are looking for the FBI’s 100 most wanted criminals (database size of 100) and the state-of-the-art fingerprint verification system operates at 1% FNMR and 0.001% FMR, i.e., if this system was deployed as a verification system, the system would fail to match the correct users 1% of the time and erroneously verify wrong users 0.001% of the time. Let us consider the outcome of the same system when deployed as an identification system. While the identification will still be 1%, the identification FNMR$_N$ will be ~100*0.001%=0.1% . This means that, while the system has a 99% chance of catching a criminal, it will produce large number of false alarms (e.g., assuming that 200 000 people may use a major U.S. airport in a day, the system will produce 200 false alarms!). Further, if faces are used instead of fingerprints for the identification (face recognition may be preferred for an airport application because faces can be acquired covertly), the number of misses and false alarms will be considerably higher, given the rather poor accuracy of face identification systems, especially in environments with cluttered background and varying lighting conditions. Although multimodal biometric systems can significantly improve the identification accuracy, exclusively relying on automatic biometric systems for negative identification may be unfeasible. Traditional personal recognition tools such as passwords and PINs are not at all useful for negative recognition applications. While biometric systems may not yet be extremely accurate to support large-scale identification applications, they are the only choice for negative recognition applications. Further, if operated in a semi-automatic mode where a human expert examines all the alarms generated by the system for the final decision, biometric systems can be quite effective. For example, if 100 airport security agents are required to manually match every person at an airport against the FBI’s 100 most wanted, only five agents may be required to take a closer look at the 200 alarms generated daily by the biometric system. We need to understand that, in such semi-automatic applications, the biometric system only generates an alarm that calls for a closer (manual) examination of the individual and an alarm does not directly translate into catching a terrorist. In fact, the trade-off between the FMR and FNMR rates in a biometric system is no different from that in any detection system, including the metal detectors already in use at all the airports Other negative recognition applications such as background checks and forensic criminal identification are also expected to operate in semi-automatic mode and their use follows a similar cost-benefit analysis. For example, in a latent search, an automatic fingerprint identification system (AFIS) is typically used by law enforcement agencies only to narrow down the number of fingerprints matches to be performed by a human expert from a few million to a few hundred. A forensic expert always makes the final decision. In our opinion, use of biometrics in negative recognition applications does not infringe upon the civil liberties of individuals since, if you are not in the “criminal database” already, the recognition system does not keep a record of you (does not remember you). However, appropriate legislation is required to protect the abuse of such systems.

TABLE II State-Of-The-Art error rate associated with fingerprints ,face, and voice biometric systems .Note that

the accuracy estimates of biometric systems are dependent on a number of test conditions.



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

VI. CONCLUSION

Biometric Systems have already proved successful both on the technical level and as a reservoir of expertise. On the technical level, they have replaced the manual method of identification which are infeasible. It can be seen that fingerprint-based biometrics system is reliable, accurate and serves as a means of security with high performance.Current electronic security systems, which rely primarily on personal identification to ensure that a client is an authorized user of a system, have a common vulnerability: the verification can be duplicated which can be nearly eliminated using biometrics. Biometrics can be used by various organizations to increase security levels and protect their data and patents. Biometrics although interdisciplinary, it is not the eventual choice of the masses due to its high cost and legal considerations like privacy issues. The merit of biometrics is proven by endeavors of the G8 countries to apply it to prevent forgery of passports and other travel documents as part of their fight against terrorism. Without doubt the age of biometrics is here and the technology will directly affect everyone over the next few years.

VII. ACKNOWLEDGEMENT

Reliable personal recognition is critical to many business processes. Biometrics refers to automatic recognition of an individual based on her behavioral and/ orphysiological characteristics. The conventional knowledge-based and token-based methods do not really provide positive personal recognition because they rely on surrogate representations of the person's identity (e.g., exclusive knowledge or possession). It is thus obvious that any system assuring reliable personal recognition must necessarily involve a biometric component. This is not, however, to state that biometrics alone can deliver reliable personal recognition component. In fact, a sound system design will often entail incorporation of many biometric and nonbiometric components (building blocks) to provide reliable personal recognition. Biometric-based system Sal so have some limitations that may have adverse implications for the security of a system. While some of the limitations of biometrics can be overcome with the evolution of biometric technology and a careful system design, it is important to understand that foolproof personal recognition systems simply do not exist and perhaps, never will. Security is a risk management strategy that identifies, controls, eliminates, or minimizes uncertain events that may adversely affect system resources and information assets. These crudity level of a system depends on the requirements (threat model) of an application and the cost-benefit analysis. In our opinion, properly implemented biometric systems are effective deterrents to perpetrators. There are a number of privacy concerns raised about the use of biometrics. A sound trade-off between security and privacy may be necessary; collective accountability/acceptability standards can only be enforced through common legislation. Biometrics provides tools to enforce accountable logs of system transactions and to protect an individual's right to privacy. As biometric technology matures, there will be an increasing interaction among the market, technology, and the applications. This interaction will be influenced by the added value of the technology, user acceptance, and the credibility of the service provider. It is too early top predict where and how biometric technology would evolve and get embedded in which applications. But it is certain that biometric-based recognition will have a profound influence on the way we conduct our daily business.

REFERENCES

[1] Anil K. Jain, Fellow, Arun Ross, Member, and Salil Prabhakar,"An Introduction to Biometric Recognition," in IEEE, vol. 14, no. 1,pp.1-20, January 2004.

[2] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: Security andprivacyconcerns," IEEE Security PrivacyMag., vol.1, no. 2, pp. 33–42, 2003.

[3] D. Maltoni,D. Maio,A.K. Jain, and S. Prabhakar,HandbookofFingerprint Recognition. New York: Springer-Verlag, 2003.

[4] A. K. Jain, R. Bolle, and S. Pankanti, Eds., Biometrics: Personal Identification in Networked Society. Norwell, MA: Kluwer, 1999.