IJITKM Volume 7 • Number 1 • December 2013 pp. 117-129 (ISSN 0973-4414)

Biometrics Security Concerns

Dr. Chander Kant, Archana Toky
Assistant Professor, Deptt. of computer Science & Appl. K.U. Kurukshetra
Faculty, Deptt. Of Computer Science, Govt. College for women, Hisar
ckverma@rediffmail.com, archanatoky@gmail.com

Abstract
Biometrics is the utilization of biological characteristics (face, iris, and fingerprint) or behavioral traits (signature, voice) for identity verification of an individual. Biometric authentication is gaining popularity as more trustable alternative to password-based security systems as it is relatively hard to be forgotten, stolen, or guessed. On the other hand, biometric data which can uniquely identify a person (e.g. fingerprints, iris patterns) can be used to track individuals, linking many separate databases (where the person has been, what he has purchased etc.), which raises privacy concerns. This paper discusses Biometric System and its working. It also focuses on its vulnerabilities and point of attacks, challenges of the system.
Keywords: biometrics, authentication, verification, validation, recognition.

1. Introduction

Biometrics is the measurement of biological data.[1] The term biometrics is commonly used today to refer to the authentication of a person by analyzing physical characteristics, such as fingerprints, or behavioral characteristics, such as signatures. Since many physical and behavioral characteristics are unique to an individual, biometrics provides a more reliable system of authentication than ID cards, keys, passwords, or other traditional systems. The word biometrics[2] comes from two Greek words and means life measure. Any characteristic can be used as a biometric identifier if (1) every person possesses the characteristic, (2) it varies from person to person, (3) its properties do not change considerably over time, and (4) it can be measured manually or automatically. Physical characteristics commonly used in biometric authentication include face, fingerprints, handprints, eyes, and voice.
Biometric authentication can be used to control the security of computer networks, electronic commerce and banking transactions, and restricted areas in office buildings and factories. It can help prevent fraud by verifying identities of voters and holders of driver's license or visas.

2 Biometric Systems

A *biometric system* is essentially a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database. Depending on the application context, a biometric system may operate either in *verification* mode or *identification* mode (Figure 1) [3]. In the verification mode, the system validates a person's identity by comparing the captured biometric data with his 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. Identity verification is typically used for *positive recognition*, where the aim is to prevent multiple people from using the same identity [3].

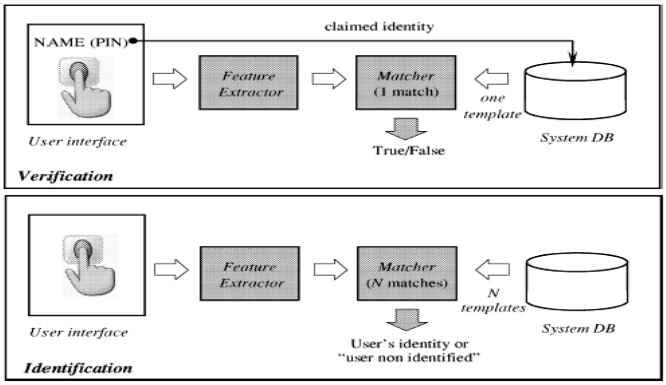

Fig1. Verification and identification tasks of a biometric system

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 [4]. Identification is a critical component in *negative recognition* applications where the system establishes whether the person is who he denies to be. The purpose of negative recognition is to prevent a single person from using multiple identities.

3. Biometrics technologies

A brief description of the commonly used biometrics is given below (Fig. 2).

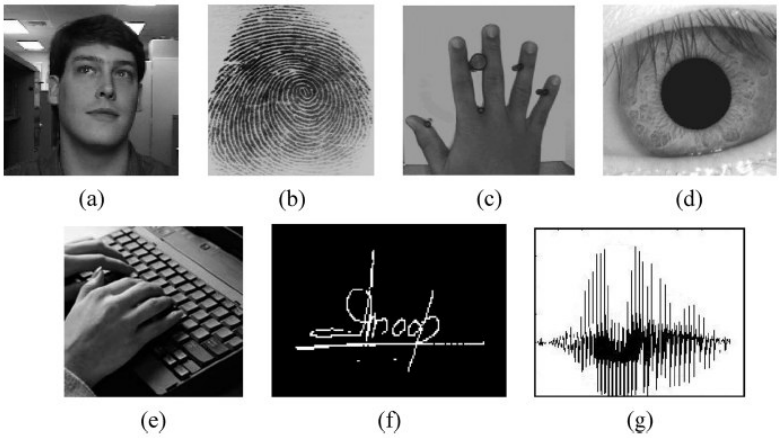

Fig 2- Examples of biometrics a) Face , b) fingerprint c) hand geometry d) iris e) keystroke f) signature and g) voice

1) ***Face****:* Face recognition is a nonintrusive method, and facial images are probably the most common biometric characteristic used by humans to make personal recognition. The applications of facial recognition range from a static, controlled "mugshot" authentication to a dynamic, uncontrolled face identification in a cluttered background. 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 analysis of the face image that represents a face as a weighted combination of a number of canonical faces. While the authentication 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, often requiring a fixed and simple background or special illumination. These systems also have difficulty in matching face images captured from two drastically different views and under different illumination conditions. In order that a facial recognition system works 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; 3) recognize the face from a general viewpoint (i.e., from any pose).

2) ***Fingerprint****:* Humans have used fingerprints for personal identification for many decades and the matching (i.e., identification) 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 fetal development. Fingerprints of identical twins are different and so are the prints on each finger of the same person. The accuracy of the currently available fingerprint recognition systems is adequate for authentication systems involving a few hundred users. Multiple fingerprints of a person provide additional information to allow for large-scale identification 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 the automatic identification because of genetic factors, aging, environmental, or occupational reasons .

3) ***Hand 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 authentication 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 authentication accuracy of hand geometry- based systems. The geometry of the hand is not known to be very distinctive and hand geometry-based recognition systems cannot be scaled up for systems requiring identification of an individual from a large population. Further, hand geometry information may not be invariant during the growth period of children. In addition, an individual's jewelry (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 such as laptops. There are authentication 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 are still much larger than those used in some other biometrics (e.g., fingerprint, face, and voice).

4) ***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 points to the feasibility of large-scale identification systems based on iris information. Each iris is believed to be distinctive and, like fingerprints, even the irises of identical twins are expected to be different. It is extremely difficult to surgically tamper the texture of the iris. Further, the ability to detect artificial irises (e.g., designer contact lenses) has been demonstrated in the literature. 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. While iris systems have a very low false accept rate (FAR) compared to other biometric traits, the false reject rate (FRR) of these systems can be high.

5) ***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 is expected to offer sufficient discriminatory information that permits 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. However, this biometric permits "continuous verification" of an individual over a period of time.

6) ***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 authentication. 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.

7) ***Voice****:* Voice is a combination of physical 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 physical 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 common cold), 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 he or 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 communication channel.

4. How Biometric System works?

Biometric systems convert data derived from behavioral or physiological characteristics into templates, which are used for subsequent matching. This is a multi-stage process whose stages are described below. [6]

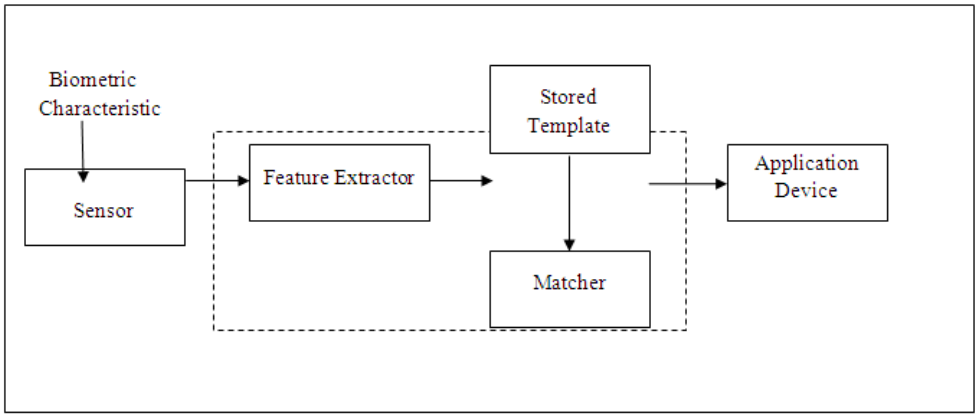

Fig 1. Working of Biometric System

Enrollment - The process whereby a user's initial biometric sample or samples are collected, assessed, processed, and stored for ongoing use in a biometric system. Enrollment takes place in both 1:1 and 1:N systems. If users are experiencing problems with a biometric system, they may need to re-enroll to gather higher quality data.
Submission - The process whereby a user provides behavioral or physiological data in the form of biometric samples to a biometric system. A submission may require looking in the direction of a camera or placing a finger on a platen. Depending on the biometric system, a user may have to remove eyeglasses, remain still for a number of seconds, or recite a pass phrase in order to provide a biometric sample.
Acquisition device – The hardware used to acquire biometric samples. The following acquisition devices are associated with each biometric technology:

Technology	*Acquisition Device*
Fingerprint	Desktop peripheral, PCMCIA card, mouse, chip or reader embedded in keyboard
Voice recognition	Microphone, telephone
Facial recognition	Video camera, PC camera, single-image camera
Iris-scan	Infrared-enabled video camera, PC camera
Retina-scan	Proprietary desktop or wall-mountable unit
Hand geometry	Proprietary wall-mounted unit
Signature-scan	Signature tablet, motion-sensitive stylus
Keystroke-scan	Keyboard or keypad

Biometric sample - The identifiable, unprocessed image or recording of a physiological or behavioral characteristic, acquired during submission, used to generate biometric templates. Also referred to as biometric data. The following sample types are associated with each biometric technology:

Technology	*Biometric Sample*
Fingerprint	Fingerprint image
Voice recognition	Voice recording
Facial recognition	Facial Image
Iris-scan	Iris Image
Retina-scan	Retina Image
Hand geometry	3-D image of top and sides of hand and fingers
Signature-scan	Image of signature and record of related dynamics measurements
Keystroke-scan	Recording of characters typed and record of related dynamics measurements

Feature extraction - The automated process of locating and encoding distinctive characteristics from a biometric sample in order to generate a template. The feature extraction process may include various degrees of image or

sample processing in order to locate a sufficient amount of accurate data. For example, voice recognition technologies can filter out certain frequencies and patterns, and fingerprint technologies can thin the ridges present in a fingerprint image to the width of a single pixel. Furthermore, if the sample provided is inadequate to perform feature extraction, the biometric system will generally instruct the user to provide another sample, often with some type of advice or feedback.

The manner in which biometric systems extract features is a closely guarded secret, and varies from vendor to vendor. Common physiological and behavioral characteristics used in feature extraction include the following:

Technology	*Feature Extracted*
Fingerprint	Location and direction of ridge endings and bifurcations on fingerprint
Voice recognition	Frequency, cadence and duration of vocal pattern
Facial recognition	Relative position and shape of nose, position of cheekbones
Iris-scan	Furrows and striations in iris
Retina-scan	Blood vessel patterns on retina
Hand-scan	Height and width of bones and joints in hands and fingers
Signature-scan	Speed, stroke order, pressure, and appearance of signature
Keystroke-scan	Keyed sequence, duration between characters

Template – A comparatively small but highly distinctive file derived from the features of a user's biometric sample or samples, used to perform biometric matches. A template is created after a biometric algorithm locates features in a biometric sample. The concept of the template is one of biometric technology's defining elements, although not all biometric systems use templates to perform biometric matching: some voice recognition system utilizes the original sample to perform a comparison.

Depending on when they are generated, templates can be referred to as enrollment templates or verification templates. **Enrollment templates** are created upon the user's initial interaction with a biometric system, and are stored for usage in future biometric comparisons. **Verification templates** are generated during subsequent verification attempts, compared to the stored template, and generally discarded after the comparison. Multiple samples may be used to generate an enrollment template – facial recognition, for example, will utilize several facial images to generate an enrollment template. Verification templates are normally derived from a single sample – a template derived from a single facial image can be compared to the enrollment template to determine the degree of similarity.

Just as the feature extraction process is a closely held secret, the manner in which information is organized and stored in the template is proprietary to biometric vendors. Biometric templates are not interoperable – a template generated in vendor A's fingerprint system cannot be compared to a template generated in vendor B's fingerprint system.

Biometric decision-making is frequently misunderstood. For the vast majority of technologies and systems, there is no such thing as a 100% match, though systems can provide a very high degree of certainty. The biometric decision-making process is comprised of various components, as indicated below.

Matching - The comparison of biometric templates to determine their degree of similarity or correlation. A match attempt results in a score that, in most systems, is compared against a threshold. If the score exceeds the threshold, the result is a match; if the score falls below the threshold, the result is a non-match.

Biometric comparisons take place when proprietary algorithms process biometric templates. These algorithms manipulate the data contained in the template in order to make valid comparisons, accounting for variations in placement, background noise, etc. Without the vendor algorithm, there is no way to compare biometric templates – comparing the bits which comprise the templates does not indicate if they came from the same user. The bits must be processed by the vendor as a precondition of comparison .

The matching process involves the comparison of the match template, created upon sample submission, with the reference template(s) already on file. In **1:1 verification systems**, there is generally a single match template matched against a reference template. In **1:N identification systems**, the single match template can be matched against dozens, thousands, even millions of reference templates.

In most systems, reference and match templates should never be identical. An identical match is an indicator that

some sort of fraud is taking place, such as the resubmission of an intercepted or otherwise compromised template.
Score – A number indicating the degree of similarity or correlation of a biometric match. Traditional verification methods – passwords, PINs, keys, and tokens - are binary, offering only a strict yes/no response. This is not the case with most biometric systems. Nearly all biometric systems are based on matching algorithms that generate a score subsequent to a match attempt. This score represents the degree of correlation between the match template and the reference template. There is no standard scale used for biometric scoring: for some vendors a scale of 1-100 might be used, others might use a scale of –1 to 1; some vendors may use a logarithmic scale and others a linear scale. Regardless of the scale employed this verification score is compared to the system's threshold to determine how successful a verification attempt has been.

Incidentally, many systems return a score during enrollment, referred to as an enrollment score or quality score. This score refers to how successful the extraction process was at finding distinctive features in the biometric sample. If the sample was rich in information, there will likely be a high enrollment score. This score is not used in the matching process, but might be used to determine whether a user can enroll successfully. A low quality score may indicate that the user cannot be reliable verified.

Threshold - A predefined number, often controlled by a biometric system administrator, which establishes the degree of correlation necessary for a comparison to be deemed a match. If the score resulting from template comparison exceeds the threshold, the templates are a "match" (though the templates themselves are not identical).

When a biometric system is set to low security, the threshold for a successful match is more forgiving than when a system is set to high security.

Decision – The result of the comparison between the score and the threshold. The decisions a biometric system can make include match, non-match, and inconclusive, although varying degrees of strong matches and non-matches are possible. Depending on the type of biometric system deployed, a **match** might grant access to resources, a **non-match** might limit access to resources, while **inconclusive** may prompt the user to provide another sample.

One of the most interesting facts about most biometric technologies is that unique biometric templates are generated every time a user interacts with a biometric system. As an example, two immediately successive placements of a finger on a biometric device generate entirely different templates. These templates, when processed by a vendor's algorithm, are recognizable as being from the same person, but are not identical. In theory, a user could place the same finger on a biometric device for years and never generate an identical template.

Therefore, for most technologies, there is simply no such thing as a 100% match. This is not to imply that the systems are not secure – biometric systems may be able to verify identify with error rates of less than 1/100,000 or 1/1,000,000. However, claims of 100% accuracy are misleading and are not reflective of the technology's basic operation.

5. Biometrics Challenges :

Here we categorize the fundamental barriers of biometrics into four main categories :
(a) Accuracy (b) Scale (c) Security (d) Privacy.

a) Accuracy

The critical promise of the ideal biometrics is that when a biometric identifier sample is presented to the biometric system, it will offer the correct decision. Unlike password or token-based system, a practical biometric system does not make perfect match decisions and can make two basic types of errors: (i) False Match: the biometric system incorrectly declares a successful match between the input pattern and a non-matching pattern in the database or the pattern associated with an incorrectly claimed identity (ii) False Non-match: the biometric system incorrectly declares failure of match between the input pattern and a matching pattern in the database (identification/screening) or the pattern associated with the correctly claimed identity (verification).

b) Scale

How does the number of identities in the enrolled database affect the speed performance of the system? In the case of verification systems, the size of the database does not really matter since it essentially involves a 1:1 match. In the case of large scale identification and screening systems containing a total of N identities, sequentially performing N

1:1 matches is not effective (see Table 1); there is a need for efficiently scaling the speed of the system with an increase in the size of the database.

Table1 Performance for commonly used biometric technologies.

	Authentication	Large Scale ID throughput	Screening throughput
Finger	10 msec	1/min	>1/sec
Face	90 µsec	0.66/min	22/sec
Iris	<1 µsec	> 1/sec	> 2000/sec

Typical approaches to scaling include using multiple hardware units and coarse pattern classification (e.g., first classifying a fingerprint into major classes such as Arch, Tented Arch, Whorl, Left loop and Right loop). Both these approaches do not perform well in practice. Using hardware linearly proportional to the database size is not feasible. Therefore, in large scale applications, the throughput issues are also critical in screening applications.

c) Security

The integrity of biometric systems, i.e., assuring that the input biometric sample was indeed presented by its legitimate owner, and the system really matched the input pattern with genuinely enrolled pattern samples, is crucial. While there are a number of ways a executor may attack a biometric system , there are usually two very serious criticisms against biometric technology that have not been addressed satisfactorily: (i) biometrics are not secrets and (ii) enrolled biometric templates are not revocable. The first fact implies that the attacker has a ready knowledge of the information in the legitimate biometric identifier and, therefore, could fraudulently inject it into the biometric system to gain access. The second fact implies that when biometric identifiers have been "compromised", the legitimate user has no recourse to revoking the identifiers to switch to another set of uncompromised identifiers. We believe that the knowledge of biometric identifier(s) does not necessarily imply the ability of the attacker to inject the identifier measurements into the system. The challenge then is to design a secure biometric system that will accept only the legitimate presentation of the biometric identifiers without being fooled by the doctored or spoofed measurements injected into the system.

d) Privacy

A reliable biometric system provides an undeniable proof of identity of the person. Consequently, the users have two concerns: Will the undeniable proof of biometrics-based access be used to track the individuals that may breach upon an individual's right to privacy? Will the biometric data be harmed for an unintentional purpose, e.g., will the fingerprints provided for access control is matched against the fingerprints in a criminal database? How would one ensure and assure the users that the biometric system is being used only for the intended purpose and none other? The problem of designing information systems whose functionality is verifiable at their deployed instantiation is very difficult. Perhaps, one needs to devise a system that meticulously records authentication decisions and the people who accessed the logged decisions using a biometric-based access control system. Such a system can automatically generate alarms to the users upon observing a suspicious pattern in the system administrator's access of users' logs. One promising research direction may be biometric cryptosystems - generation of cryptographic keys based on biometric samples.

6. Biometric Performance Metrics:

The following are used as performance metrics for biometric systems:[4]

- **False Accept Rate or False Match Rate (FAR or FMR)**: 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 which are incorrectly accepted.
- **False Reject Rate or False Non-Match Rate (FRR or FNMR)**: 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 which are incorrectly rejected.
- **Receiver Operating Characteristic or Relative Operating Characteristic (ROC)**: The ROC plot is a visual characterization of the trade-off between the FAR and the FRR. In general, the matching algorithm performs a decision based on a threshold which 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 less false non-matches but more false accepts. Correspondingly, a higher threshold will reduce the FAR but increase the FRR. A common variation is the *Detection error trade-off (DET),* which is obtained using normal deviate 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 accept and reject 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 most accurate.
- **Failure To Enroll 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 which can be stored in the system.

7. A comparison of biometrics technologies

The table below compares the performance of various biometrics technologies with one another in seven categories of evaluation:

- **Universality** describes how commonly a biometric trait occurs in each individual.
- **Uniqueness** is how well the biometric distinguishes one individual from another.
- **Permanence** measures how well a biometric resists aging.
- **Collectability** explains how easy it is to acquire the biometric for measurement.
- **Performance** indicates the accuracy, speed, and robustness of the system capturing the biometric.
- **Acceptability** indicates the degree of approval of a technology by the public in everyday life.
- **Circumvention** is how easy it is to fool the authentication system.

Table 2 Comparison of various biometric technologies

Biometrics	Univer-sality	Unique-ness	Perma-nence	Collect-ability	Perfor-mance	Accept-ability	Circum-vention
Face	H	L	M	H	L	H	L
Fingerprint	M	H	H	M	H	M	H
Hand Geometry	M	M	M	H	M	M	M
Keystroke Dynamics	L	L	L	M	L	M	M
Hand vein	M	M	M	M	M	M	H
Iris	H	H	H	M	H	L	H
Retina	H	H	M	L	H	L	H
Signature	L	L	L	H	L	H	L
Voice	M	L	L	M	L	H	L
Facial Thermogram	H	H	L	H	M	H	H
DNA	H	H	H	L	H	L	L

H=High, M=Medium, L=Low

Each system is ranked as low, medium, or high in each category. A low ranking indicates poor performance in the evaluation criterion, whereas a high ranking indicates very good performance.

The chart shows that iris scanning has a high rating in practically every category, but a low rating in acceptability, perhaps because people may be hesitant to look into an eye scanner. On the other hand, signature receives a high rating in acceptability but a low rating in most other categories, probably because signatures can be forged.

7. Factors Cause Biometric Systems to Fail?

Biometric system performance varies according to sample quality and the environment in which the sample is being submitted. While it is not possible to definitely state if a biometric submission will be successful, it is possible to locate factors that can reduce affect system performance [7].

Biometrics Deformations

Fingerprint

- Cold finger
- Dry/oily finger
- High or low humidity
- Angle of placement
- Pressure of placement
- Location of finger on platen (poorly placed core)
- Cuts to fingerprint
- Manual activity that would mar or affect fingerprints (construction, gardening)

Voice recognition

- Cold or illness that affects voice
- Different enrollment and verification capture devices
- Different enrollment and verification environments (inside vs. outside)
- Speaking softly
- Variation in background noise
- Poor placement of microphone / capture device
- Quality of capture device

Facial recognition

- Change in facial hair
- Change in hairstyle
- Lighting conditions
- Adding/removing glasses
- Change in weight
- Change in facial aspect (angle at which facial image is captured)

Iris-scan

- Too much movement of head or eye
- Glasses
- Colored contacts

Retina-scan

- Too much movement of head or eye
- Glasses

Hand geometry

- Jewelry
- Change in weight
- Bandages
- Swelling of joints

Signature-scan

- Signing too quickly
- Different signing positions (e.g., sitting vs. standing)

In addition, for many systems, an additional strike occurs when a long period of time has elapsed since enrollment or since one's last verification. If significant time has elapsed since enrollment, physiological changes can complicate verification. If time has elapsed since a user's last verification, the user may have "forgotten" how he or she enrolled, and may place a finger differently. For the most part, a single strike will probably not materially affect the performance of a given system. However, as you have more and more strikes for a given submission, your chances of a successful verification diminish.

These strikes do not include inherent characteristics such as age, ethnicity, or gender, which can also affect system accuracy. The performance of many biometric systems varies for specific populations.

8. Are Biometric Systems Difficult to Use?

Biometrics are much easier to use than one might expect. Here is a brief technology-by-technology summary of how one interacts with biometric systems.

Fingerprint. When prompted, the user gently places his or her finger on a postage-stamp sized optical or silicon surface. This surface, known as a platen, is built into a peripheral device, mouse, keyboard, or PCMCIA card. The user generally must hold the finger in place for 1-2 seconds, during which automated comparison and matching takes place. After a successful match, the user has access to programs, files, or resources. Typical verification time from "system ready" prompt: 2-3 seconds.

Facial recognition. User faces the camera, preferably positioned within 24 inches of the face. Generally, the system will locate one's face very quickly and perform matches against the claimed identity. In some situations, the user may need to alter his facial aspect slightly to be verified. Typical verification time from "system ready" prompt: 3-4 seconds.

Voice recognition. User positions him or herself near the acquisition device (microphone, telephone). At the prompt, user either recites enrollment pass phrase or repeats pass phrase given by the system. Typical verification time from "system ready" prompt: 4-6 seconds.

Iris-scan. User positions him or herself near the acquisition device (peripheral or standalone camera). User centers eye on device so he or she can see the eye's reflection. Depending on the device, the user is between 2-18 inches away. Capture and verification are nearly immediate. Typical verification time from "system ready" prompt: 3-5 seconds.

Retina-scan. User looks into a small opening on a desktop or wall-mounted device. User holds head very still, looking at a small green light located within the device. Typical verification time from "system ready" prompt: 10-12 seconds.

Hand geometry. User places hand, palm-down, on an 8 x 10 metal surface with five guidance pegs. Pegs ensure that fingers are placed properly, ensure correct hand position. Typical verification time from "system ready" prompt: 2-3 seconds.

Signature-scan. User positions himself to sign on tablet (if applicable). When prompted, user signs name in tablet's capture area. Typical verification time from "system ready" prompt: 4-6 seconds.

Keystroke-scan. User types his or her password or pass phrase. Typical verification time from "system ready" prompt: 2-3 seconds.

9. Biometric System Security

The security ensured by the deployed biometric systems can itself be compromised. A number of studies have analyzed the likelihood of such security breaches and potential approaches to counter these vulnerabilities. The general analysis of a biometric system for vulnerability assessment determines the extent to which an impostor can compromise the security offered by the biometric system.

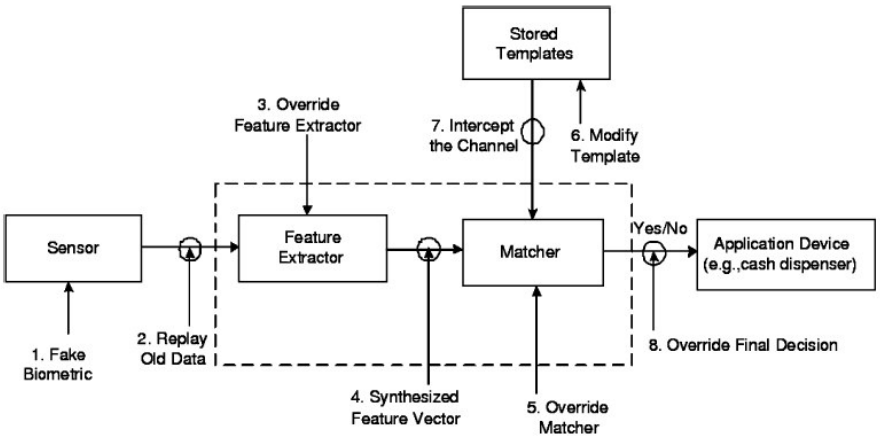

Fig 4- Typical attack points in a biometric system .[1]

The potential points of an adversary attack on the biometric system as shown in fig 4. While many of these attacks are applicable to any information system, the attacks using fake *biometric* and template modification are unique to

biometrics systems. We briefly discuss the characteristics of such attacks, which need to be effectively thwarted in biometrics systems.[4

(i) **Sensor level attack:** A *fake* biometric sample can be presented at the sensor to gain access.A fake biometric can be generated by covertly acquiring the biometric characteristics of a genuine user, e.g. lifting fingerprint impressions from objects touched by persons.

(ii) **Replay attack:** It is possible for an adversary to intercept or acquire a digital copy of the stored biometric sample and replay this signal bypassing the biometric sensor .

(iii) **Trojan Horse1 attack:** The feature extractor can be replaced by a program which generates the desired feature set.

(iv) **Spoofing the features:** The feature vectors generated from the biometric samples are replaced by the set of synthetically generated (fake) features. 1 Virus program(s) that hide within a set of unauthorized access to a hacker seemingly useful software programs to facilitate

(v) **Attack on matcher:** The matcher can also be subjected to a Trojan Horse attack that always produces high (or low) match scores irrespective of which user presents the biometric at the sensor.

(vi) **Attack on template:** The template generated during the user enrolment/registration can be either locally stored or at some central location. This type of attack can either modify the stored template or replaces it with a new template.

(vii) **Attack on communication channel:** The data being transferred through a communication channel can be intercepted for malicious reasons and then modified and inserted back into the system.

(viii) **Attack on decision module:** The final decision generated by the biometric system can be overridden by a Trojan Horse program. A biometric matcher is typically only a part of a larger information and security management system. Therefore, the non-biometric modules in the overall system can also introduce some security flaws. An example is the iris-based access control system in a New Jersey School. Sometimes, a user will prop the door open, so anyone can enter the school, bypassing the security offered by the biometric module.

10. Conclusion and future work

Biometrics is one of the important and more interesting pattern recognition applications with its associated unique challenges. There are a large number of biometric solutions that have been successfully deployed to provide useful value in practical applications. The scope of this paper is intended to expand the popularity of biometric technology. A successful biometric solution does not have to be 100% accurate or secure. As biometric technology matures, there will be an increasing interaction among the market, technology, and the applications. This interaction will be influenced by the added value of the technology, user acceptance, and the credibility of the service provider. It is too early to predict where and how biometric technology would evolve and get embedded in which applications. But it is certain that biometric-based recognition will have a profound influence on the way we conduct our daily business. The researches in various fields are making this recognition system more strong and usable in daily life and will soon replace other authentication systems.

References

[1] A. K. Jain, "Biometrics", in *The World Book Encyclopedia* .

[2] K. Jain, A. Ross and S. Pankanti, "Biometrics: A Tool for Information Security", IEEE Transactions on Information Forensics and Security Vol. 1, No. 2, pp. 125-143, June 2006.

[3] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*. Springer- Verlag, 2003.

[4] A. K. Jain, Arun Ross and U. Uludag "Biometrics Template security: Challenges and solutions" in *Proc. of* European Signal Processing Conference September 2005.

[5] N. Ratha, J. H. Connell, and R. M. Bolle, "An analysis of minutiae matching strength," in *Proc. Audio and Video-based Biometric Person Authentication (AVBPA)*,pp. 223–228, (Halmstad, Sweden), June 2001.

[6] www.biometricsinfo.org

[7] R. Cappelli, R. Erol, D. Maio, and D. Maltoni, "Synthetic fingerprint-image generation," in *Proc. Int'l. Conf. Pattern Recognition (ICPR)*, vol. 3, pp. 475–478,(Barcelona, Spain), September 2000.

[8] K. Jain and A. Kumar, "Biometrics of Next Generation: An Overview", to appear in *Second Generation Biometrics* (E. Mordini and D. Tzovaras, Eds.), Springer, 2010.

[9] "Improving Biometric Security Using Cryptography", International Journal of Advance Research in Computer Engineering, ISSN 0974-4320, Vol-I, PP 33-38,Jan-Dec 2007.

[10]"Secure Online Business: Exploring the Security Threats to E-Commerce", International journal of Intelligent Information Processing, ISSN 0973-3892, Vol-I, PP 1-8, Jan-Dec 2007.
[11]"Challenges in Biometrics" proceeding of the International Conference on Emerging trends in Computer Science & IT organized by AL-FALAH School of Engineering & Tech, Faridabad, PP 69-77, 23 Apr 2008.
[12]"Role of Biometrics in Modern Business" in the proceeding of national seminar on "Emerging Challenges in Commerce and Management" organized by Govt. College , Karnal, 18-19 Mar 2008.
[13] www.griaulebiometrics.com
[14] A. K. Jain, S. Pankanti, S. Prabhakar, L. Hong, A. Ross, and J. L. Wayman, "Biometrics: A Grand Challenge", *Proc. International Conference on Pattern Recognition (ICPR)* , vol. II, pp. 935-942, Cambridge, UK, Aug. 2004
[15] U. Uludag, S. Pankanti, S. Prabhakar and A. K. Jain, " Biometric Cryptosystems: Issues and Challenges", *Proc. the IEEE, Special Issue on Multimedia Security for Digital Rights Management,* vol. 92, no. 6, pp. 948-960, June 2004.
[16] "Biometrics Recognition System: An Introduction" in the proceeding of national seminar on convergence of IT and Management organized by TIMT, Yamuna Nagar,24 Nov 2007.
[17]"Challenges in Biometrics: proceeding of the International Conference on Emerging trends in Computer Science & IT organized by AL-FALAH school of Engineering & Tech, Faridabad, PP69-77, 23 Apr 2008.