UNIT I

INTRODUCTION TO BIOMETRICS

Introduction and back ground – biometric technologies – passive biometrics – active biometrics - Biometrics Vs traditional techniques – Benefits of biometrics - Operation of a biometric system– Key biometric processes: verification, identification and biometric matching – Performance measures in biometric systems: FAR, FRR, FTE rate, FTA rate and rate- Need for strong authentication – Protecting privacy and biometrics and policy – Biometric applications

INTRODUCTION AND BACKGROUND

- Biometrics is the science of establishing the identity of an individual based on the physical, chemical or behavioral attributes of the person.
- The relevance of biometrics relies on the accurate determination of an individual's identity in the context of several different applications.
- Examples of these applications include sharing networked computer resources, granting access to nuclear facilities, performing remote financial transactions or boarding a commercial flight.
- The proliferation of web-based services (e.g., online banking) and the deployment of decentralized customer service centers (e.g., credit cards) have further underscored the need for reliable identity management systems that can accommodate a large number of individuals.
- Traditional methods of establishing a person's identity include knowledge-based (e.g., passwords) and token-based (e.g., ID cards) mechanisms, but these surrogate representations of identity can easily be lost, shared, manipulated or stolen thereby compromising the intended security.
- Biometrics offers a natural and reliable solution to certain aspects of identity management by utilizing fully automated or semi-automated schemes to recognize individuals based on their biological characteristics.
- By using biometrics it is possible to establish an identity based on *who you are*, rather than by *what you possess*, such as an ID card, or *what you remember*, such as a password (Figure 1.1).
- In some applications, biometrics may be used to supplement ID cards and passwords thereby imparting an additional level of security. Such an arrangement is often called a dual-factor authentication scheme.

Fig. 1.1 shows the authentication schemes of biometric system:

(a) Traditional schemes use ID cards, passwords and keys to validate individuals and ensure that system resources are accessed by a legitimately enrolled individual.

(b) With the advent of biometrics, it is now possible to establish an identity based on "who you are" rather than by "what you possess" or "what you remember".

The effectiveness of an authenticator (biometric or non-biometric) is based on its relevance to a particular application as well as its robustness to various types of malicious attacks.

O'Gorman lists a number of attacks that can be launched against authentication systems based on passwords and tokens:

a) Client attack (e.g., guessing passwords, stealing tokens)
b)Host attack (e.g., accessing plain text file containing passwords);
c)Eavesdropping (e.g., "shoulder surfing" for passwords);
d)Repudiation (e.g., claiming that token was misplaced);
e)Trojan horse attack (e.g., installation of bogus log-in screen to steal passwords); and
f)Denial of service (e.g., disabling the system by deliberately supplying an incorrect password several times)

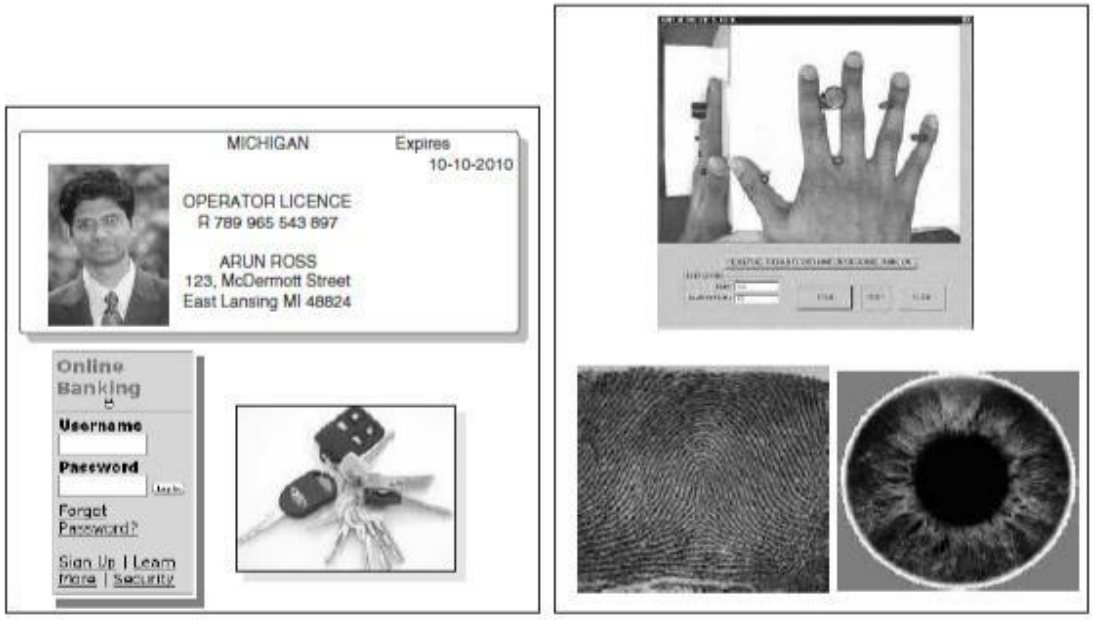


Fig. 1.1 Authentication schemes.

BIOMETRIC TECHNOLOGIES(ACTIVE AND PASSIVE BIOMETRICS)

- Biometrics can be defined by the level of involvement the user needs to provide to be biometrically measured.

- User involvement with a biometric system falls into two categories:

  a. Passive biometrics
  b. Active biometrics

a. Passive Biometrics:

- A passive biometric does not require the user to actively submit to measurement.
- These types of systems are generally referred to as covert.
- They do not require the user to be aware that he/she is being biometrically measured.

- These systems are also seen as being invasive to the user's privacy.
- They are generally used in surveillance applications.
- For use in a surveillance application, a database of known people must be collected and the system then watches for a matching biometric measurement.
- These systems are normally greatly influenced by the environment in which they are used.
- Passive biometrics are more suitable for use in identification systems than in authentication systems.
- Passive biometrics do not normally provide a single result.
- Normally, a set of enrolled people is returned, and a human operator makes the final match.
- Examples of passive biometrics are:
    - ❖ Face
    - ❖ Voice
    - ❖ Gait

b. <u>Active Biometrics:</u>

- An *active biometric* requires the user to actively submit to measurement.
- These types of systems are generally referred to as *overt*.
- They require the user to be aware that he/she is being biometrically measured.
- These systems are seen as being supportive of the user's privacy.
- Active biometrics are generally used in applications that authenticate a user's identity
- They work by the user making a claim about who he/she is.
- The user supplies a user ID or some other unique identifier.
- The user then provides a biometric measurement in support of that claim.
- In this case, there is normally a high level of certainty attained as to the user's identity.
- Active biometrics are not as environmentally dependent as passive biometrics. Examples of active biometrics are:
    - ❖ Fingerprint
    - ❖ Hand geometry

- ❖ Retinal scanning
- ❖ Iris scanning

BIOMETRICS VS TRADITIONAL TECHNIQUES

The most frequently used authentication technologies are passwords and PINs. They secure access to Pcs, networking and application; control entry to secure areas of a building and ATM and debit transaction. Handheld tokens have replaced passwords in some higher security applications.

Passwords, PINs and tokens have a number of problems that call into question their suitability for modern applications particularly high-security applications.

- o Increased Security
- o Increased Convenience
- o Increased Accountability

Increased Security:

- Biometrics can provide a greater degree of security than traditional authentication method .i.e. the resources are accessible to only authorized user.
- Passwords and PINs are easily guessed or compromised tokens can be stolen.
- Many users select obvious words or number of passwords or PIN authentication such that an unauthorized user may be able to break into an account with little effort.
- Long passwords with numbers and symbols are too difficult to remember for most users and rarely enforced.
- By contrast, biometrics data cannot be guessed or stolen. Although some biometric system can be broken under certain conditions, today's biometric systems are highly unlikely to be fooled by a picture of face, an impression of fingerprint or a recording of voice.
- In systems where the biometric authentication releases passwords the user or administrator can create longer and more complex passwords than would be feasible without biometrics.
- Passwords, PINs and tokens can also be shared which increases the chance of malicious activity.
- In many enterprises a common password is shared among administrators and there is no certainity as who is using the password . Based on distinctive characteristics biometric data cannot be shared in this fashion.
- Although there are a number of security issues involved in biometric system that must be addressed through intelligent system design, the level of security provided by most biometrics system far exceeds the security provided by passwords, PINs and tokens.

Increased Convenience:

- One of the reason passwords are kept simple is that they are easily forgotten. As computer users are forced to manage more and more passwords, passwords being forgotten increases unless user choose a universal password, reducing security further. Tokens and cards can be forgotten as well.
- Biometrics are not impossible to forget they can offer much greater convenience than system based on remembering multiple passwords.
- For pc applications in which a user must access multiple resources biometrics can greatly simplify the authentication process.
- Biometric authentication allows for association of higher levels of rights and privileges with a successful authentication.
- Highly sensitive information can more readily available on a biometrically protected network than on protected by passwords.

Increased Accountability:

- Increased awareness of security issues in the enterprise and an customer facing application the need for strong auditing and reporting capabilities has grown more pronounced.
- Using biometrics to secure computers and eliminate phenomena such as buddy punching and provides a high degree of certainity.
- The benefits of security convenience and accountability apply primarily to enterprises, workstation and home users.

BENEFITS OF BIOMETRICS

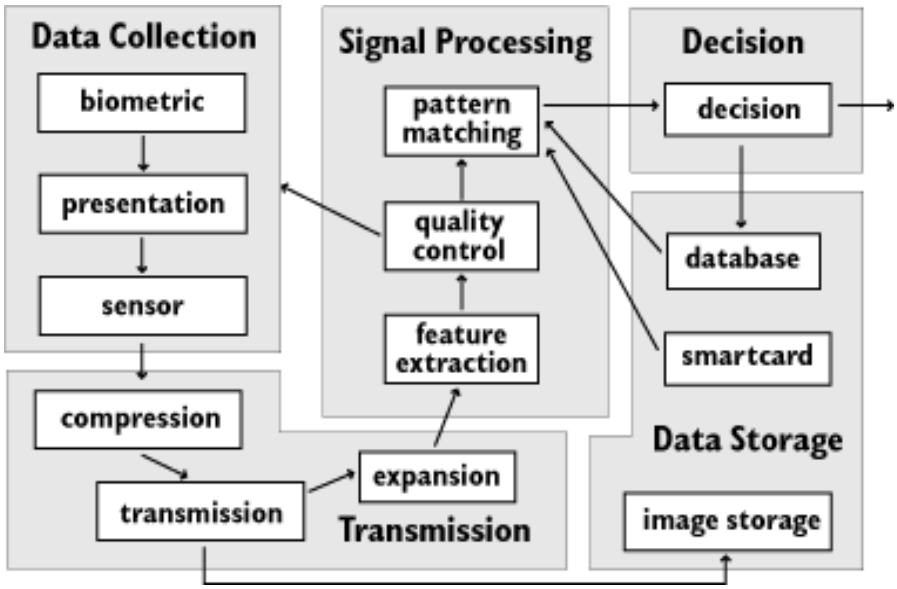
- Relies on the unique biological characteristics of the individuals.
- Allows rapid identification of criminals, combatants or terrorist.
- Enhances the home land security and figure crimes.
- Convenient way to access secure facilities or information system.
- Nothing to remember.
- It Can’t be guessed, Stolen, Shared, lost or forgotten.
- Prevents impersonation protects against identity theft .
- High degree of non repudiation.
- Enhances the privacy protect against unauthorized access to personal information.
- Fraud detection
- Fraud deterrence.
- Increased effectiveness and affordability.

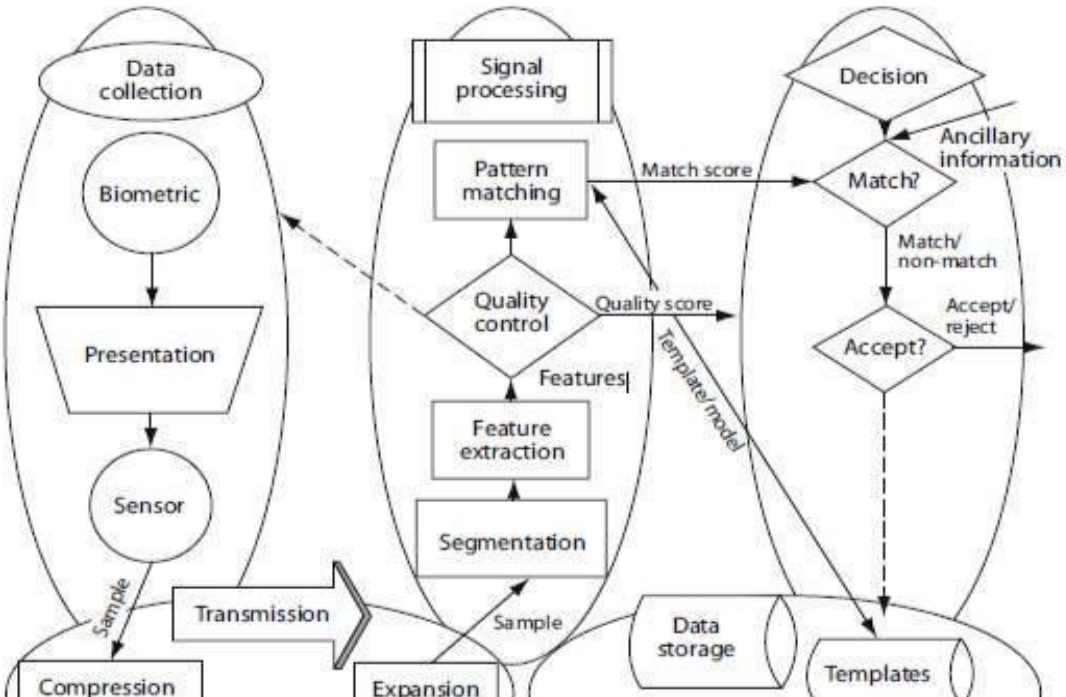
- This is especially critical in applications such as welfare disbursement where an impostor may attempt to claim multiple benefits (i.e., double dipping) under different names.

OPERATION OF BIOMETRIC SYSTEM

The main stages of a biometric system includes:

A. Data Collection
B. Transmission
C. Signal Processing
D. Storage
E. Decision





A. Data Collection:

Biometric systems begin with the measurement of a behavioral/physiological characteristic.

Key to all systems is the underlying assumption that the measured biometric characteristic is both distinctive between individuals and repeatable over time for the same individual.

The problems in measuring and controlling these variations begin in the data collection subsystem.

The user's characteristic must be presented to a sensor.

The presentation of any biometric characteristic to the sensor introduces a behavioral (and, consequently, psychological) component to every biometric method.

This behavioral component may vary widely between users, between applications, and between the test laboratory and the operational environment.

The output of the sensor, which is the input data upon which the system is built, is the convolution of:

(1) the biometric measure;

(2) the way the measure is presented; and

(3) the technical characteristics of the sensor.

Both the repeatability and the distinctiveness of the measurement are negatively impacted by changes in any of these factors.

If a system is to be open, the presentation and sensor characteristics must be standardized to ensure that biometric characteristics collected with one system will match those collected on the same individual by another system.

If a system is to be used in an overt, non-cooperative application, the user must not be able to will fully change the biometric or its presentation sufficiently to avoid being matched to previous records.

B. Transmission:

Some, but not all, biometric systems collect data at one location but store and/or process it at another. Such systems require data transmission.

If a great amount of data is involved, compression may be required before transmission or storage to conserve bandwidth and storage space.

In such cases, the transmitted or stored compressed data must be expanded before further use.

The process of compression and expansion generally causes quality loss in the restored signal, with loss increasing with increasing compression ratio.

The compression technique used will depend upon the biometric signal.

If a system is to be open, compression and transmission protocols must be standardized so that every user of the data can reconstruct the original signal.

Standards currently exist for the compression of fingerprints (Wavelet Scalar Quantization), facial images (JPEG), and voice data (Code Excited Linear Prediction).

C. Signal Processing:

i)Segmentation is the process of finding the biometric pattern within the transmitted signal.

For example, a facial recognition system must first find the boundaries of the face or faces in the transmitted image.

ii)Feature extraction is fascinating. The raw biometric pattern, even after segmentation from the larger signal, contains non-repeatable distortions caused by the presentation, sensor and transmission processes of the system.

These non-controllable distortions and any non-distinctive or redundant elements must be removed from the biometric pattern, while at the same time preserving those qualities that are both distinctive and repeatable.

These qualities expressed in mathematical form are called “features”.

In general, feature extraction is a form of non-reversible compression, meaning that the original biometric image cannot be reconstructed from the extracted features.

In some systems, transmission occurs after feature extraction to reduce the requirement for bandwidth.

iii)After feature extraction, or maybe even before, we will want to check to see if the signal received from the data collection subsystem is of good quality.

If the features “don’t make sense” or are insufficient in someway, we can conclude quickly that the received signal was defective and request a new sample from the data collection subsystem while the user is still at the sensor.

The development of this “quality control” process has greatly improved the performance of biometric systems.

iv)The term “template” is used to indicate stored features.

The features in the template are of the same type as those of a sample.

The term “model” is used to indicate the construction of a more complex mathematical representation capable of generating features characteristic of a particular user.

Models and features will be of different mathematical types and structures.

Models are used in some speaker and facial recognition systems.

Templates are used in fingerprint, iris, and hand geometry recognition systems.

The term “enrollment” refers to the placing of a template or model into the database for the very first time.

The purpose of the pattern matching process is to compare a presented feature sample to the stored data, and to send to the decision subsystem quantitative measure of the comparison.

The signal processing subsystem is designed with the goal of yielding small distances between enrolled models/templates and later samples from the same individual and large distances between enrolled models/templates and samples of different individuals.

D. Storage:

The remaining subsystem to be considered is that of storage.

There will be one or more forms of storage used, depending upon the biometric system.

Templates or models from enrolled users will be stored in a database for comparison by the pattern matcher to incoming feature samples.

For systems only performing “one-to-one” matching, the database may be distributed on smart cards, optically read cards or magnetic stripe cards carried by each enrolled user.

The database will be centralized if the system performs one-to-*N* matching with *N* greater than one, as in the case of identification or “PINless verification” systems.

As *N* gets very large, system speed requirements dictate that the database be partitioned into smaller subsets such that any feature sample need only be matched to the templates or models stored in one partition, or indexed by using an appropriate data structure which allows the templates to be visited in an advantageous order during the retrieval.

If it may be necessary to reconstruct the biometric patterns from stored data, raw (although possibly compressed) data storage will be required.

The biometric pattern is generally not reconstructable from the stored templates or models, although some methods do allow a coarse reconstruction of patterns from templates.

The storage of raw data allows changes in the system or system vendor to be made without the need to re-collect data from all enrolled users.

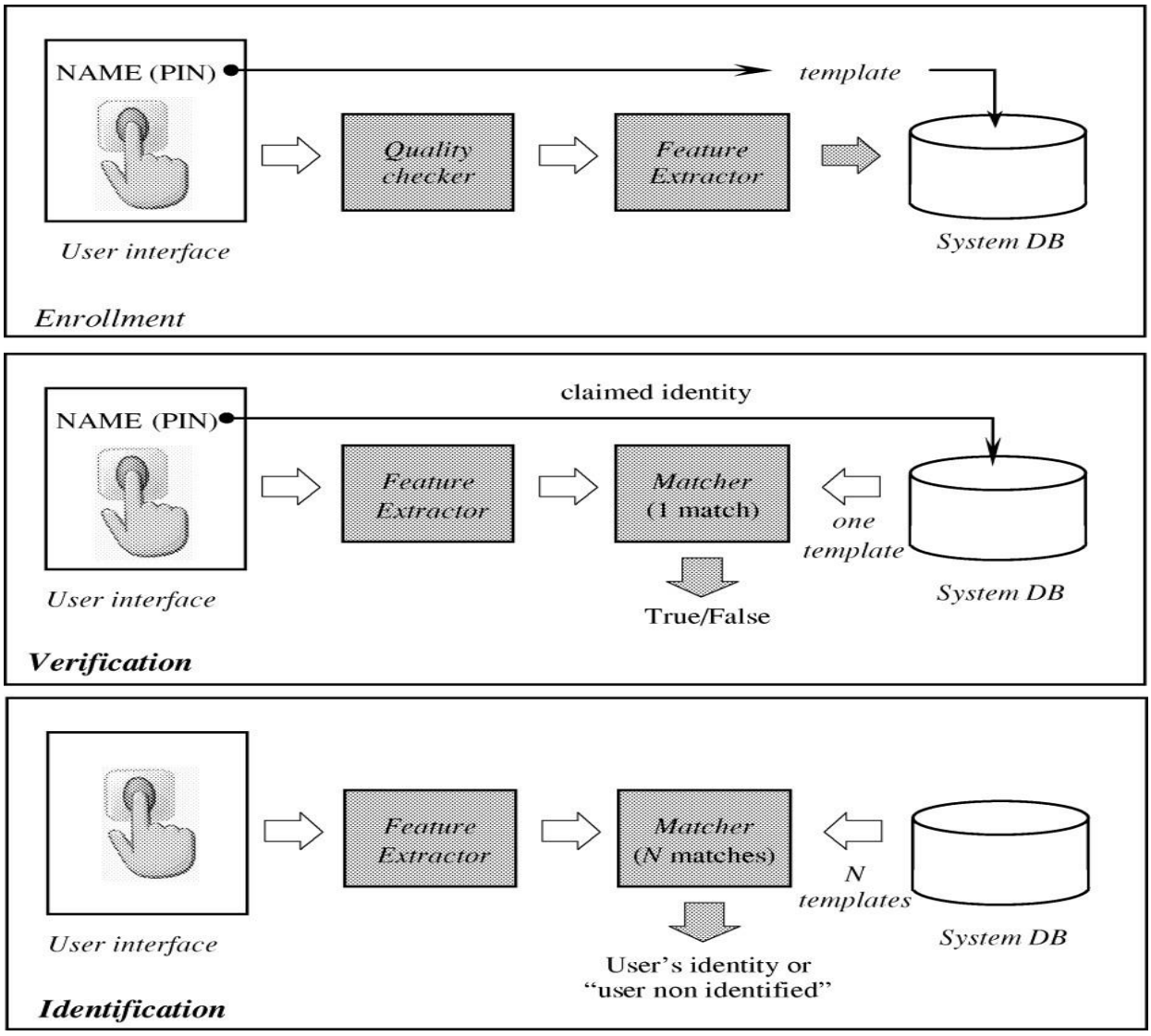
E. Decision:

The decision subsystem implements system policy by directing the database search, determines "matches" or "non-matches" based on the distance or similarity measures received from the pattern matcher, and ultimately makes an "accept/reject" decision based on the system policy.

Such a decision policy could be to reject the identity claim (either positive or negative) of any user whose pattern could not be acquired.

The decision policy employed is a management decision that is specific to the operational and security requirements of the system.

KEY BIOMETRIC PROCESS



VERIFICATION:

Verification system answer the question "Am I who I claim to be?" by requiring that a user claim an identity inorder for a biometric comparison to be performed.

After a user claims an identity he or she provides biometric data which is then compared against his or her enrolled biometric data.

Depending on the type of biometric system, the identity that a user claims might be a windows username, a given name or an ID number; the answer returned by the system is match or not.

Verification systems can contain dozens, thousands or million of biometric record but are always predicted on a user's biometric data.

Verification is often referred to as 1:1. The process of providing a username and biometric data is referred to as authentication.

The system validate a person's identity by comparing template with his or her own biometric templates stored in the system database.

An individual claims an identity usually via personal identification number(PIN) a username or smartcard.

The system conducts a one to one comparison to determine whether the claim is true or not.

PC and network security generally employ verification system and verification system are generally faster and more accurate than identification system.

Identity verification is typically used for positive recognition. The aim is to prevent multiple people using the same identity.

IDENTIFICATION:

Identification systems answer the question "Who am I?" and do not require that a user claim an identity before biometric comparisons take place. The user provides his/her biometric data which is compared to data from a number of users in order to find a match. The answer returned by the system is an identity such as a name or ID number.

Identification systems can contain dozens, thousands or millions of biometric records. Identification is often referred to as 1:N because a person's biometric information is compared against multiple records.

The system recognises an individual by searching the templates of all the users in the database for a match.

The system conducts a one to many (1:N) comparison to establish an individual's identity.

Identification is a critical component in negative recognition application where the system establishes whether the person is who he/she denies to be.

The purpose of negative recognition is to prevent single person from using multiple identities.

Negative recognition can only be established through biometrics.

Positive identification system are designed to find a match for a user's biometric information is a database of biometric information.

Only certain biometric technologies are capable of performing identification, including finger, iris and retina scan. Large scale benefits program generally utilize identification system.

ENROLLMENT:

The process by which a user's biometric data is initially acquired, assessed, processed and stored in the form of a template for ongoing use in a biometric system is called enrolment.

Subsequent verification and identification attempts are conducted against the template generated during enrolment.

Enrollment takes place in both 1:1 and 1:N systems, although the way a user enroll may vary substantially from system to system.

Quality enrolment is a critical factor in the long term accuracy of biometric systems.

Low quality enrollments may lead to high error rates including falsme match rates and false non match rate.

PRESENTATION:

After a User provides whatever personal Information is requested to begin enrolment such as name or user id he or she presents biometric data.

Presentation is the process by which a user provides biometric data to an acquisition device- the hardware used to collect biometric data.

Presentation of biometric data can value as little as one second or more than one minute.

BIOMETRIC DATA:

The biometric data used provide is an unprocessed image or recording of a characteristics.

This unprocessed data is also referred to as raw biometric data or a biometric sample.

Biometric system do not store biometric data system use data for template creation.

The enrolment process may also gather data from more than one finger or create multiple enrollment templates.

Enrollment requires the creation of an identifier such as username or ID.

FEATURE EXTARCTION:

The automated process of locating and encoding distinctive characteristics from biometric data inorder to generate a template is called feature extraction.

It take places during enrollment and verification anytime a template is created.

This process includes filtering and optimization of images and data inorder to accurately local features.

BIOMETRIC MATCHING:

The comparison of biometric template to determine their degree of similarity or correlation is called matching. The process of matching biometric templates result in a score, which is compared against a threshold.

i) If score >threshold – result is a match
ii) If score<threshold- result is a non-match.

The matching process involves the comparison of s verification template with the enrollment template. The following steps are involved in matching

1. Scoring
2. Threshold
3. Decision

SCORING: Biometrics match/non match decisions are based on a source- a number indicating the degree of similarity or correlation resulting from the comparison of enrollment and verification template.

Biometric system utilizes proprietary algorithms to process templates and generate scores. There is no standard scales used for biometric scoring.

Scoring is a critical biometric concept and accounts for many of the strength and some of the weakness of biometric system.

THRESHOLD: Once a score is generated, it is compared to the verification attempts threshold.

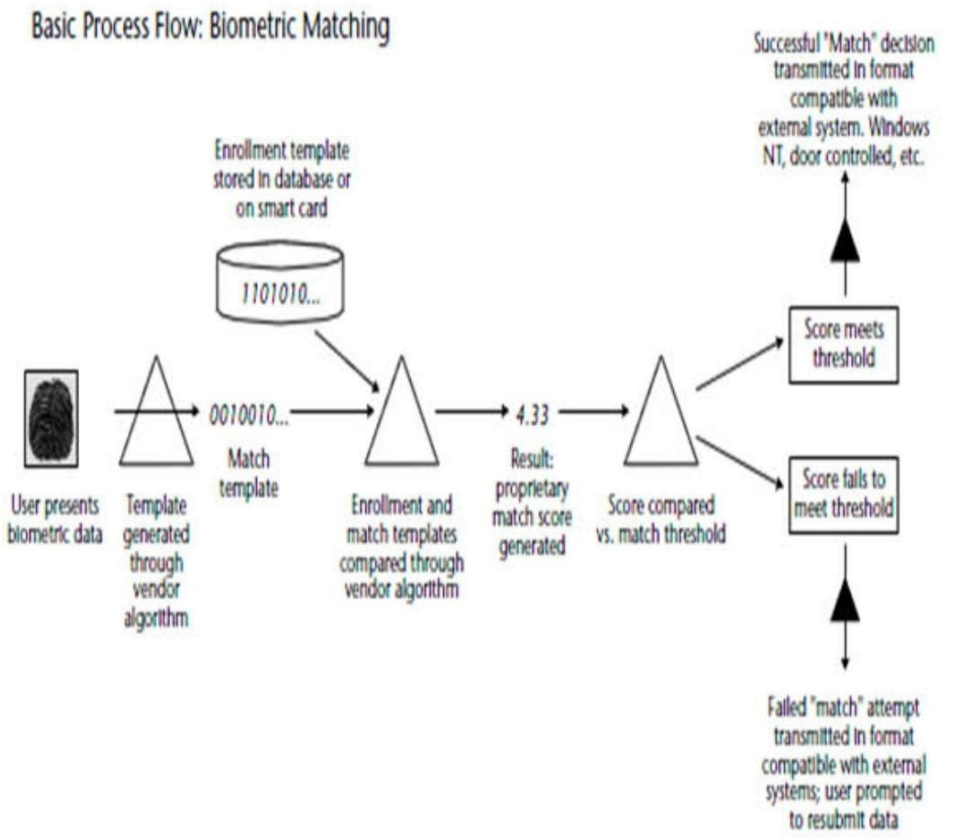
A threshold is a predefined number chosen by a system administrator which established the degree of correlation necessary for a comparison to be deemed a match.

Threshold can vary from user to user, from transaction to transaction and from verification attempts to verification attempts.

Systems can be either highly secure or not secure at all depends on their threshold settings.

DECISION: The result of the comparison between score and the threshold is a decision. The decision of biometric system can make include match, non match and inconclusive. Although varying degrees of strong matches and non matches are possible.

In most systems enrollment and verification template should never be identical. An identical match is an indicator to some sort of fraud is taking place such as the resubmission of a intercepted or otherwise compromised template.



PERFORMANCE MEASURE IN BIOMETRIC SYSTEM/ACCURACY ESTIMATION IN BIOMETRIC SYSTEM

The key performance metrics in biometrics are

1. False Match Rate(FMR)
2. False Non-Match Rate(FMR)
3. Failure To Enroll Rate (FTER)

Analysis of all three metrics is necessary to assess the performance of a specific technology.

FALSE MATCH RATE (FMR):

The first metric that comes to mind when thinking about biometric system is FMR.

A biometric solution's FMR is the probability that a user's template will be incorrectly judged to be a match for different user's template.

FMR describes the likelihood of an imposter beating a biometric system by being matched as someone other than him or herself.

False matches may occur between two people have similar enough biometric characteristics- a fingerprint, a voice or a face that the system finds a high degree of correlation between the user's template.

FMR can be reduced by adjusting threshold that adjust the level of correlation necessary for two templates to be judged a match.

The FMR is often referred to as the False Acceptance Rate(FAR).

The term false acceptance rate assumes that the result of a successful match is that the user is accepted into a building, an application, or a resource, which is often the case.

In many systems, false match rate is the most critical accuracy metric.

When securing entry to a weapons facility, a bank vault, or a high-ranking system administrator's account, it is imperative that imposters be kept out.

Also, as biometrics move increasingly into the public eye, solutions designed to provide high security must be perceived as relatively impervious to false match imposters.

If biometrics are seen as being susceptible to imposters, they will become the target of attacks and lose credibility in the eyes of potential deployers.

An imposter break-in will certainly be a more attention-getting event than other failings of a biometric system.

However, false match rate must always be balanced with false nonmatch rate and failure-to-enroll rate; these metrics have often been overlooked in the biometric industry but can be even more important to a biometric system's overall operation than false match rate.

FAR=Total false acceptance/Total False Attempts

FALSE NON-MATCH RATE (FMR):

A biometric solution's False Non-Match Rate is the probability that a user's template will be incorrectly judged to not match his or her enrolment templates.

In most cases, a False Non-Match Rate means that an authorized user is locked out of a system is correctly denied access to a facility or resource.

A solution's False Non-Match Rate is often referred to as False Rejection Rate(FRR).

False nonmatches occur because there is not a sufficiently strong correlation between a user's verification and enrollment templates. This can be attributed to the following

- Changes in a user's biometric data
- Changes in how a user presents biometric data
- Changes in the environment in which data is presented

FAR=Total false rejection/Total True Attempts

In most biometric applications, particularly those involving employees, the vast majority of verification attempts will be genuine.

As a result, high false nonmatch rates can be as damaging to an enterprise as high false match rates.

When users are falsely nonmatched and denied access to resources, the result is lost productivity, frustrated users, and an increased burden on help desk or support personnel.

Biometric vendors have traditionally focused on limiting false match rates, but a disproportionate focus on FMR reduction can lead to unacceptably high false nonmatch rates.

The FM and FNM error are measured in terms of False Positive Identification Rate(FPIR) and False Negative Identification Rate(FNIR) respectively.

The overall accuracy can be illustrated by Receiver Operation Characteristics(ROC) which shown as the dependence of FRR and FAR at all thresholds.

When these parameter changes FAR and FRR may yield the same value which is called Equal Error Rate.

EER is where FAR=FRR

Crossover=1:X ; where X=round(1/EER)

FAILURE TO ENROLL RATE (FTER):

A system's failure-to-enroll (FTE) rate represents the probability that a given user will be unable to enroll in a biometric system.

FTEs occur when users have insufficiently distinctive or replicable biometric data or when the design of the biometric solution is such that providing consistent data is difficult.

High failure-to-enroll rates can be particularly problematic for a biometric system, as users unable to enroll must verify through another biometric technology or authentication method. In order to define a failure-to-enroll, one must first define enrollment.

As it happens, the process differs significantly from technology to technology and from device to device. Both physiological and behavioral biometrics are subject to failures-to-enroll.

Finger-scan systems may require between one and six high quality presentations of a single fingerprint, and may require that a user enroll two fingers for an enrollment to be complete. Iris-scan systems can require between one and four images captured per iris.

Voice-scan systems may require that a passphrase be recited three times or that a string of numbers be repeated for 30 to 40 seconds.

Facial-scan enrollment may require the capture of a handful of images, may be based on duration of image capture, or may take place through a static image.

The only common element of these varied enrollment processes is the result: A user's information is eventually stored in some type of database or file for future comparisons.

More so than for false match and nonmatch rates, a system's FTE rate is dependent on system design, training, and ergonomics—not necessarily on the underlying biometric data.

Improvements in system design and enrollment process can reduce a system's FTE rate from 10 percent to 1 percent, without any changes to the core biometric processes.

The impact of FTE differs for individual and institutional users. For individuals unable to enroll in a biometric system or device designed for personal use, inability to enroll may be frustrating, but they will still have recourse to standard authentication.

For institutions offering biometric authentication to customers, FTE becomes a customer service issue and will lead to disgruntled customers.

However, even this is not insurmountable—it is unlikely that an institution will penalize nonbiometric users, so recourse to alternate authentication is still an option.

FTE can be a major problem in internal, employee-facing deployments. In this environment, high failure-to-enroll rates are directly linked to increased security risks and increased system costs.

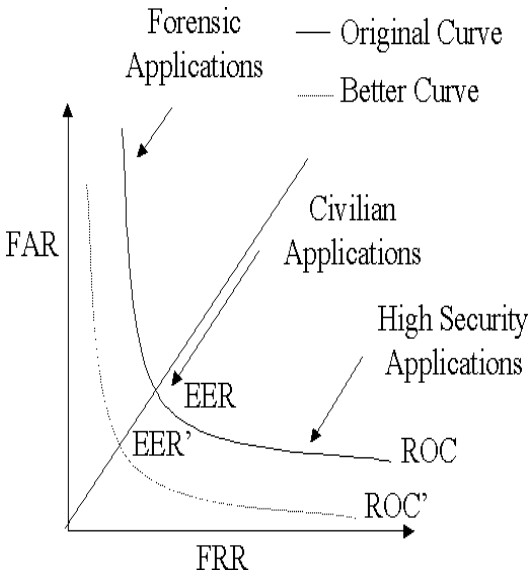
Consider a biometric network authentication system.Deploying a technology with a 2 percent FTE rate to 1,000 users means that approximately 20 users will be unable to verify biometrically.

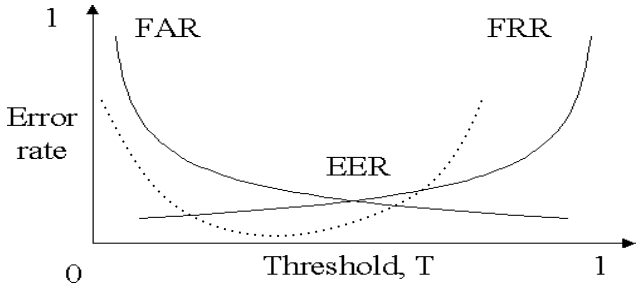
These FTE users will need to be authenticated in some fashion. If they revert to password authentication, then there are 20 accounts on the network that are just as susceptible to compromise as before biometrics were deployed.

Furthermore, the remnants of a password system are still in place, meaning that an infrastructure must be in place for password maintenance and changes.

Ability to verify ATV= 1-[1-FTE][1-FRR]

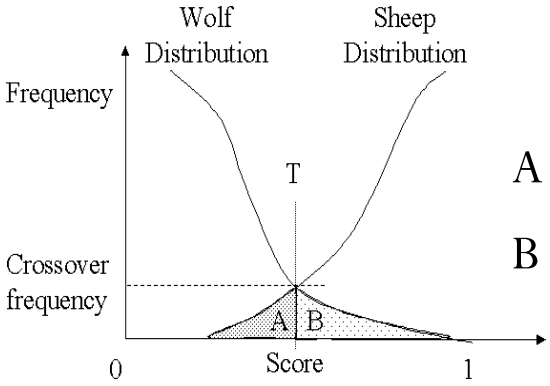
RECEIVER OPERATING CURVE **THRESHOLD ANALYSIS**





FAR AND FRR VS THRESHOLD

DISTRIBUTION ANALYSIS



A = False Rejection

B = False Acceptance

NEED FOR STRONG AUTHENTICATION

Frequency of security breaches (i.e. Twitter, Evernote, LinkedIn) have IT departments paying closer attention to authentication.

Ubiquity of mobile devices is not only increasing the number of online apps that users need to log in to, but also increasingly becoming the device of choice for assisting in authentication. According to Allan, in the past few years, the popularity of phone-as-a token solutions has overtaken one-time password hardware tokens in terms of new and refreshed deployments.

Enhanced methods of authentication have "morphed from traditional tokens to USB devices to smart cards to fingerprint readers, soft tokens and scanning devices." Contextual authentication, based on analytics of behavior patterns and device patterns, is growing in importance and more vendors are offering it with their core user authentication products. Additionally, there is an increased interest

in using biometrics for a higher level of assurance with improved user experience, including form factors like typing rhythm, voice recognition, face topography and iris structure.

Move to cloud-delivered user authentication services is becoming more widely adopted and having the most traction among small and mid-sized businesses and industries where TCO is a more significant consideration. Gartner predicts that by 2017, more than 50% of enterprises will choose cloud-based services – up from less than 10% today.

PROTECTING PRIVACY AND BIOMETRICS POLICY

Unlike more common forms of identification, biometric measures contain no personal information and are more difficult to forge or steal.

1. Biometric measures can be used in place of a name or Social Security number to secure anonymous transactions.

2. Some biometric measures (face images, voice signals and "latent" fingerprints left on surfaces) can be taken without a person's knowledge, but cannot be linked to an identity without a pre-existing invertible database.

3. A Social Security or credit card number, and sometimes even a legal name, can identify a person in a large population. This capability has not been demonstrated using any single biometric measure.

4. Like telephone and credit card information, biometric databases can be searched outside of their intended purpose by court order. Unlike credit card, telephone or social security numbers, biometrics characteristics changes from one measurement to the next.

5. Searching for personal data based on biometric measures is not as reliable or efficient as suing better identifiers, like legal name or social security number.

6. Biometric measures are not always secret, but are sometimes publicly observable and cannot be revoked if compromised.

Privacy and discrimination:

It is possible that data obtained during biometric enrollment may be used in ways for which the enrolled individual has not consented. For example, most biometric features could disclose physiological and/or pathological medical conditions (e.g., some fingerprint patterns are related to chromosomal diseases, iris patterns could reveal genetic sex, hand vein patterns could reveal vascular diseases, most behavioral biometrics could reveal neurological diseases, and so). Moreover, second generation biometrics, notably behavioral and electro-physiologic biometrics (e.g., based on electrocardiography, electroencephalography, electromyography), could be also used for emotion detection.

There are three categories of privacy concerns:

1. Unintended functional scope: The authentication goes further than authentication, such as finding a tumor.
2. Unintended application scope: The authentication process correctly identifies the subject when the subject did not wish to be identified.
3. Covert identification: The subject is identified without seeking identification or authentication, i.e. a subject's face is identified in a crowd.

BIOMETRIC APPLICATIONS

The operational goals of biometric applications are just as variable as the technologies: some systems search for known individuals; some search for unknown individuals; some verify a claimed identity; some verify an unclaimed identity; and some verify that the individual has no identity in the system at all.

And the application environments can vary greatly – outdoors or indoors, supervised or unsupervised, with people trained or not trained in the use of the acquisition device.

To make sense out of all of the technologies, application goals and environments, systematic method of approach is needed – taxonomies of uses and applications.

A Taxonomy of Uses:

A biometric system can be designed to test one of only two possible hypotheses: (1) that the submitted samples are from an individual known to the system; or (2) that the submitted samples are from an individual not known to the system.

Applications to test the first hypothesis are called "positive identification" systems (verifying a positive claim of enrollment), while applications testing the latter are "negative identification" systems (verifying a claim of no enrollment).

All biometric systems are of one type or the other. This is the most important distinction between systems, and controls potential architectures, vulnerabilities and system error rates.

Positive	Negative
To prove I am someone known to the system	To prove I am not someone known to the system
To prevent multiple users of a single identity	To prevent multiple identities of a single user
Comparison of submitted sample to single claimed template – "one-to-one" under the most common system design	Comparison of submitted sample to all enrolled templates – "one-to-many"
A "false match" leads to "false acceptance"	A "false match" or a "failure to acquire" leads to a "false rejection"
A "false non-match" or a "failure to acquire" leads to a "false rejection"	A "false non-match" leads to a "false acceptance"
Alternative identification methods exist	No alternative methods exist
Can be voluntary	Must be mandatory for all
Spoofed by submitting someone else's biometric measures	Spoofed by submitting no or altered measures

Table 1.1 summarizes the differences between the positive and negative identification

A Taxonomy of Application Environments:

Accurate characterization of the operational environment is primary in selecting the best biometric technology and in predicting the system's operational characteristics.

A proposed operational environment is analysed by differentiating applications based on partitioning into six categories beyond the "positive" and "negative" applications.

i) Overt Versus Covert:

The first partition is "overt/covert".

If the user is aware that a biometric identifier is being measured, the use is overt.

If unaware, the use is covert.

Almost all conceivable access control and non-forensic applications are overt.

Forensic applications can be covert.

ii) Habituated Versus Non-Habituated:

The second partition, “habituated/non-habituated”, applies to the intended users of the application.

Users presenting a biometric trait on a daily basis can be considered habituated after a short period of time.

Users who have not presented the trait recently can be considered “non-habituated”.

If all the intended users are “habituated”, the application is considered a “habituated” application.

If all the intended users are “non-habituated”, the application is considered “non-habituated” application.

In general, all applications will be “non-habituated” during the first week of operation, and can have a mixture of habituated and non-habituated users at any time thereafter.

iii) Attended Versus Non-Attended:

A third partition is “attended/unattended”, and refers to whether the use of the biometric device during operation will be observed and guided by system management.

Non-cooperative applications will generally require supervised operation, while cooperative operation may or may not.

Nearly all systems supervise the enrollment process, although some do not.

iv) Standard Versus Non-Standard Environment:

A fourth partition is “standard/non-standard operating environment”.

If the application will take place indoors at standard temperature (20 °C), pressure (1 atm), and other environmental conditions, particularly where lighting conditions can be controlled, it is considered a “standard environment” application.

Outdoor systems, and perhaps some unusual indoor systems, are considered “non-standard environment” applications.

v) Public Versus Private:

A fifth partition is “public/private”.

Will the users of the system be customers of the system management (public) or employees (private)?

Clearly, attitudes toward usage of the devices, which will directly affect performance, vary depending upon the relationship between the end-users and system management.

vi) Open Versus Closed:

A sixth partition is “open/closed”.

Will the system be required, now or in the future, to exchange data with other biometric systems run by other management?

For instance, some US state social services agencies want to be able to exchange biometric information with other states.

If a system is to be open, data collection, compression and format standards are required.

A closed system can operate perfectly well on completely proprietary formats. This list is open, meaning that additional partitions might also be appropriate. We could also argue that not all possible partition permutations are equally likely or even permissible.

Applications of Biometrics:

The need for reliable user authentication techniques has increased in the wake of heightened concerns about security, and rapid advancements in networking, communication and mobility.

Thus, biometrics is being increasingly incorporated in several different applications.

These applications can be categorized into three main groups (see Table 1.2):

FORENSICS	GOVERNMENT	COMMERCIAL
Corpse identification	National ID card	ATM
Criminal investigation	Drivers license; voter registration	Access control; computer login
Parenthood determination	Welfare disbursement	Mobile phone
Missing children	Border crossing	E-commerce; Internet; banking; smart card

Table 1.2 Authentication solutions employing biometrics can be used in a variety of applications which depend on reliable user authentication mechanisms.

1. Commercial applications such as computer network login, electronic data security, e-commerce, Internet access, ATM or credit card use, physical access control, mobile phone, PDA, medical records management, distance learning, etc.
2. Government applications such as national ID card, managing inmates in a correctional facility, driver's license, social security, welfare-disbursement, border control, passport control, etc.
3. Forensic applications such as corpse identification, criminal investigation, parenthood determination, etc..

CHARACTERISTICS OF BIOMETRICS

UNIVERSALITY- each person should have the characteristics
UNIQUENESS-only 2 persons should be sufficiently different in terms of the characteristics.
PERMANENCE (ROBUST)- the characteristic should be sufficiently invariant over a period of time.
COLLECTABILITY (MEASURABILITY)- the characteristics can be measured quantitatively.
PERFORMANCE-related to the accuracy, speed and robustness of technology used.
ACCEPTABILITY-indicates the extent to which people are willing to accept the use of a particular biometric identifier in their daily lives.
CIRCUMVENTION- reflects how easily the system can be fooled using fraudulent methods.