BIOMETRICS

UNIT-1

* Authentication is a fundamental component of human interaction with the computers
* Traditional means of authentication, primarily password and personal Identification Numbers (PIN) have until recently dominated completly and are likely to remain essentially for years to come. However, stronger authentication technologies, capable of providing higher degree of security
* Biometrics are one such strong authentication technology.

Benefits of Biometrics verses Traditional Authentication methods:

* Passwords, PINs have a number of problems that call into question their suitability for modern applications, particularly high security applications such as access to online financial transactions or medical data

1. Increased Security:

Biometrics can provide a greater degree of security than traditional authentication methods i.e., resources are only accessible to authorized users and are kept protected from unauthorized users. Biometrics data cannot be guessed or stored in the same fashion as a password or PIN.

2. Increased Convenience:

One of the reasons passwords are kept simple is that they are easily forgotten.

Biometrics are difficult if not impossible to forget, they can offer much greater convenience than systems based on remembering multiple passwords. Highly sensitive information can more readily be made available on a biometrically protected network than on a one protected by passwords. This can increase user and enterprise convenience, as users can access otherwise protected information without the need of human intervention.

3. Increased Accountability:

Using biometrics to secure computers and facilities eliminates phenomena such as buddy punching and provides a high degree of certainity as to what user accessed what computer at what time. Even if the auditing and reporting capabilities of a system are rarely used, the fact that they exist often server as an effective deterrent

Benefits of Biometrics in Identification System:

In Identification systems, Biometrics can be used for security, convenience and accountability. Especially when they are deployed to a modest number of users. However identification systems are more often deployed in large scale environment.

1. Fraud Detection:

Identification systems are deployed to determine whether a person's biometric information exists more than once in a database. By locating and identifying individuals who who have already registered for a program or service, biometrics can reduce fraud.

2. Fraud Deterrance:

More than fraud detection, fraud deterrance is a primary benefit in large scale identification systems. The presence of biometric identification technology can deter individual from attempting to enroll multiple times in a public benefit systems, then the public agency has saved money and ensured the integrity of records. In the absence of biometrics, there is no effecient way of identifying duplicate applicants or registrants and it is therefore difficult to deter such applications.

Biometrics:

Biometrics is the automated use of physiological or behavioural characterstics to determine or verify identify

Automated Use:

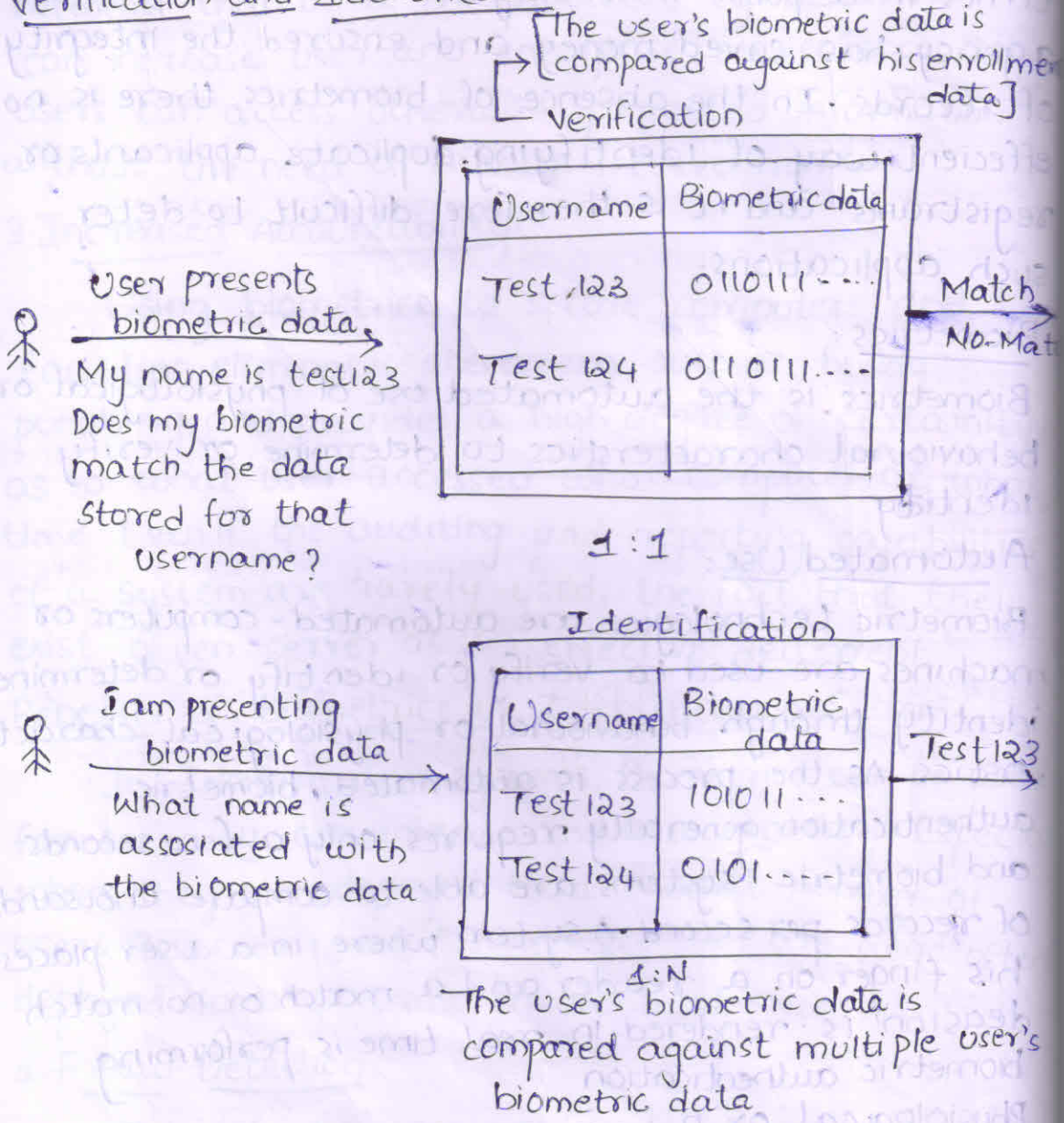
Biometric technologies are automated - computers or machines are used to verify or identify or determine identity through behavioural or physiological charact-erstics. As the process is automated, biometric authentication generally requires only a few seconds and biometric systems are able to compare thousands of records per second. A system where in a user places his finger on a reader and a match or no match decision is rendered in real time is performing biometric authentication

Physiological or Behavioural Characterstics:

Biometrics are based on the measurement of distinctive physiological and behavioural characterstics. Finger scan, facial scan, hand scan, Retina scan are considered as physiological biometrics, based on direct measurement of a part of the human body

Voice scan and signature scan are considered as behavioural biometrics, they are based on measuremer and data received derived from an action and therefore indirectly measured characterstics of human body.

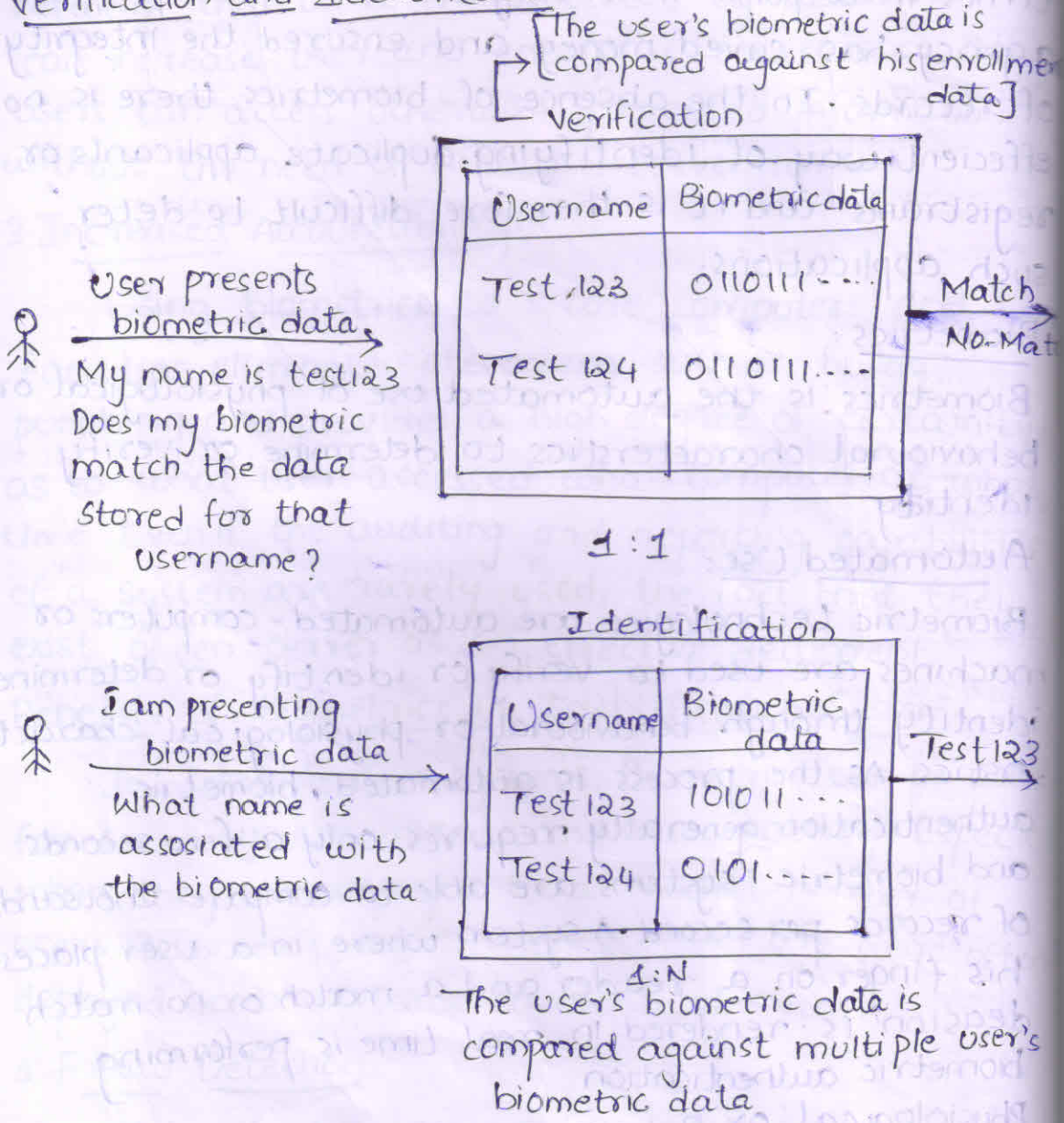
Verification and Identification:



* Verification systems answer the question "Am I who I claimed to be?", by required that a user claim an identity inorder for a biometric comparison to be performed. After a user claims an identity, user provides biometric data which is then compared against his enrolled biometric data

Voice scan and signature scan are considered as behavioural biometrics, they are based on measuremer and data received derived from an action and therefore indirectly measured characterstics of human body.

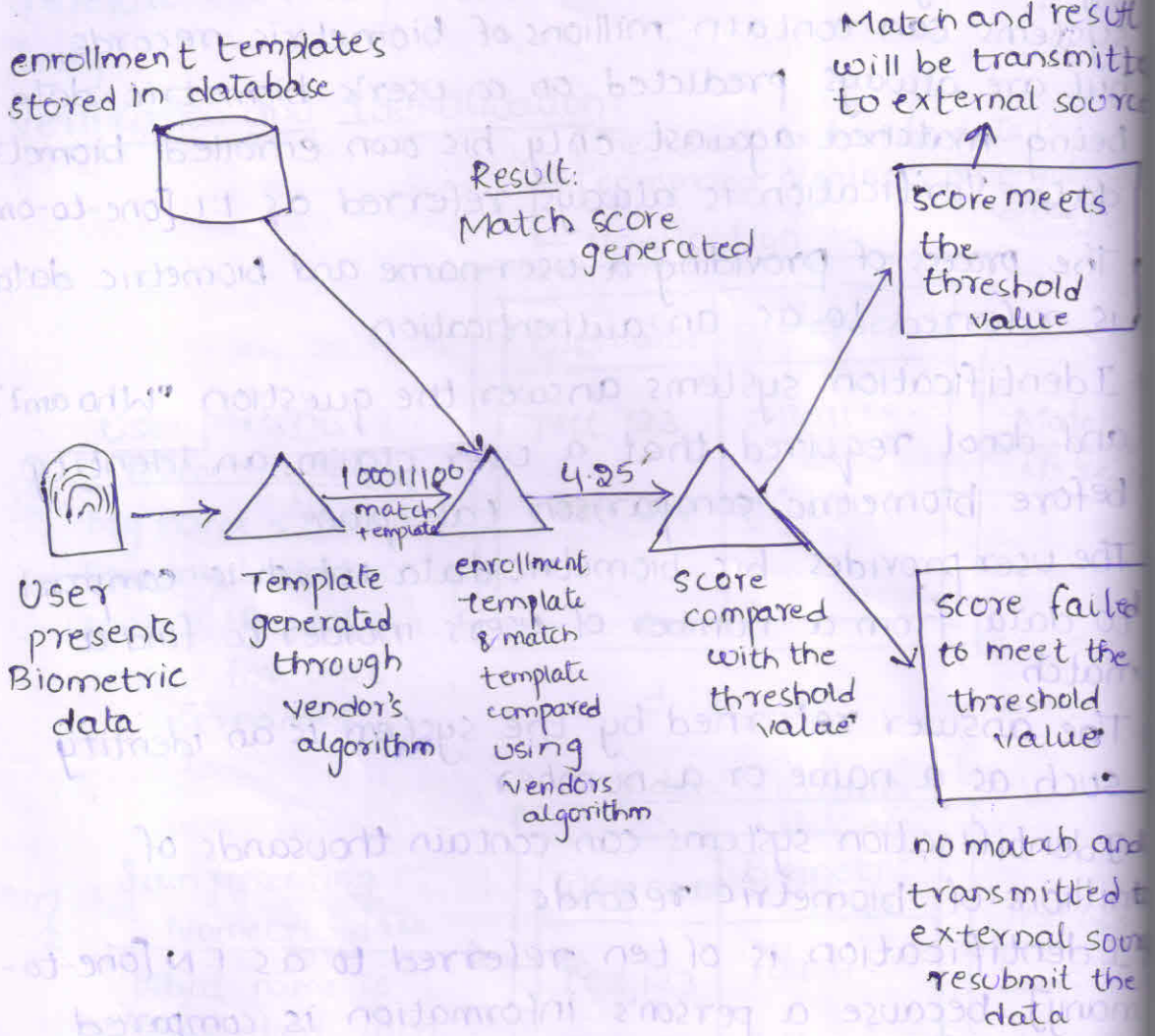
Verification and Identification:



* Verification systems answer the question "Am I who I claimed to be?", by required that a user claim an identity inorder for a biometric comparison to be performed. After a user claims an identity, user provides biometric data which is then compared against his enrolled biometric data

* Depending on the type of biometric system, the identity that a user claims might be a window's username, a given name or an id number, the answer returned by the system is match or no match verification systems can contain millions of biometric records, but are always predicted on a user's biometric data being matched against only his own enrolled biometric data. Verification is always referred as 1:1 [one-to-one]
* The process of providing a user name and biometric data is referred to as an authentication
* Identification systems answer the question "Who am I?" and donot required that a user claim an identity before biometric comparison take place
* The user provides his biometric data which is compared to data from a number of user's inorder to find a match.
* The answer returned by the system is an identity such as a name or a number
* Identification systems can contain thousands of millions of biometric records
* Identification is often referred to as 1:N [one-to-many], because a person's information is compared against multiple records.
* Physical access systems and logical access systems
* How Biometric matching works

Basic process flow Biometric matching:



* A user initially enrolls in biometric systems by providing biometric data, which is converted into a template
* Templates are stored in biometric systems for the purpose of subsequent comparison
* Inorder to be verified or identified after a enrollment, the user provides biometric data, which is converted into a template
* The verification template is compared with one or more enrollment templates.

* The result of a comparison between biometric templates is rendered as a score or confidence level, which is compared to a threshold used for a specific technology, systems user or transaction.
* If the score exceeds the threshold the comparison is a match and that result is transmitted.
* If the score does not meet the threshold, the comparison is not a match and that result is transmitted

Enrollment and Template Creation:

The process by which a users biometric data is initially acquired, accessed, processed and stored in the form of a template for ongoing use in a biometric system is called enrollment.

* Quality enrollment is a critical factor in the long term accuracy of biometric systems. Low quality enrollment may lead to high error rates, including false match rate and false non match rate

Presentation:

After a user provides what ever personal information is required to begin enrollment, such as name or user id, user presents biometric data

Biometric Data:

The biometric data provided by the user is an unprocessed image or recording of a characterstic It is also called as raw Biometric data

* Depending on the biometric system, a user may need to present biometric data several times inorder to enroll
* Enrollment requires the creation of an identifier such as user name or id.

Biometric Technology	Data type
Finger scan	Finger-print image
Voice scan	Voice recording
Face scan	Facial image
Iris scan	Iris image
Retina scan	Retina Image
Hand scan	3-D image of the h (top and sides)
Signature scan	Image of signature

Features Extraction:

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

In voice scan technology, the process includes filter certain frequencies and patterns

In finger scan technology process includes thinning of the ridges to the width of a single pixel.

Templates:

* A template is a small file derived from the distin features of a users biometric data, used to perform biometric matches
* Biometric systems store and compare biometric compares not biometric data
* Most templates occupy 9 bytes to 1 kilo byte
* There is no common biometric template formal- a template created in vendor A's system cann be used through vendor B's system

* Biometric data such as finger prints and facial images cannot be reconstructed from biometric templates
* Biometric templates are generated every time user presents biometric data. To successive placement of a finger on a biometric device generate entirely different templates. This is because of positioning distances, pressures etc.,

Biometric Matching:

The comparision of biometric templates, to determine their degree of similarity or correlation is called matching

Scoring:

A number indicating the degree of similarity or co-relation resulting from the comparison of enrollment and verification template.

Threshold:

A threshold is a predefined number, generally choosen by a system administrator, which establishes the degree of co-relation necessary for a comparison to be beemed a match

Decision:

The result of the comparison between the score and the threshold is a decision

Accuracy of Biometric systems:

The key performance matrics in Biometrics are false match rate (FMR), false non-match Rate (FNMR) failure to enroll rate (FTE)

1) False Match Rate (FMR):

A biometric solutions false match rate is the probability that a user template will be incorrectly judged to be a match for a differe users template

false match may occur because two people have similar enough biometric characterstic. It is al called as false acceptance rate

FMR can be reduced by adjusting threshold tha adjust thresholds that adjust the level of correction necessary for two templates to be judges a match.

2) False Non-Match Rate (FNMR):

* A biometric solution FNMR is the probabilit that user template will be incorrectly judged to not match users enrollment template

* Authorized user is locked out of a system, incom denied access to a facility or resource. It is also called false rejection rate

The factors affecting FNMR are

1) Changes in user's biometric data
2) changes in how a user presents biometric da
3) changes in the environment in which data presented

Failure to Enrollment (FTE):

A system failure to enroll rate represents the probability that a given user will be unable to enroll in a biometric system

FTE is occured when user's have insufficiently distinctive or replicable biometric data or when the design of the biometric solution is such that providing consistant data is difficult

Derived Metrics:

There are another two metrics used to reflect the overall occurancy capabilities of a biometric technology. These metrics are generated from analysis and comparison of FNMR, FTE.

1) Equal Error Rate (EER):

It is also called as cross over rate. It is the rate at which the FNMR is equal to the FMR i.e., it represents the accuracy level at which likelyhood of a false match is the same as the likelyhood of a false non-match.

2) Ability to verify Rate (ATV)

A more valued to derived metrics is the ability to verify rate. ATV is a combination of FTE and FNMR and indicates the overall percentage of users who will be capable of authenticating on a daily basis

$$ATV = (1 - FTE)(1 - FNMR)$$

This metric can be thought of as representing a group of users who cannot enroll along with users falsely rejected by the system. High ATV rate will makes for a more effective system

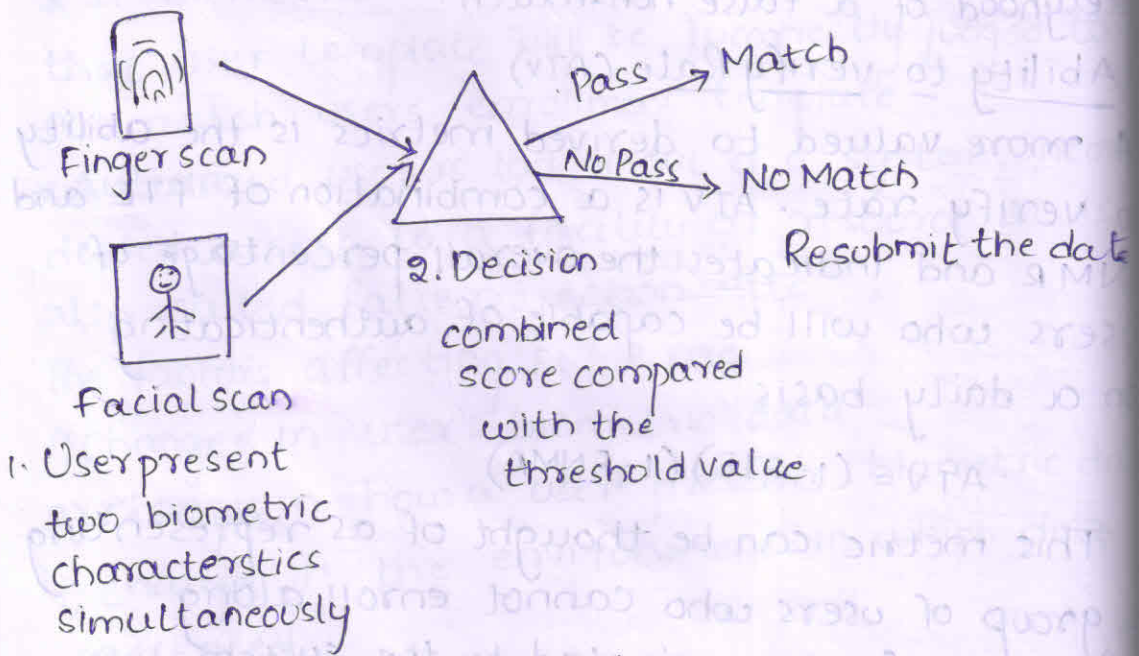
Layered Biometrics:

Layered Biometric solutions are those that requ the submission of more than one biometric characte for verification, such as finger scan and voice scan or finger scan and facial scan. These solutions are seen as a method of reducing FMR [False Match Rate], FNMR [false Non Matching Rate] [Error Rates] There are two types of Layered Biometrics

1) Parallel Layered Biometrics
2) Serial Layered Biometrics

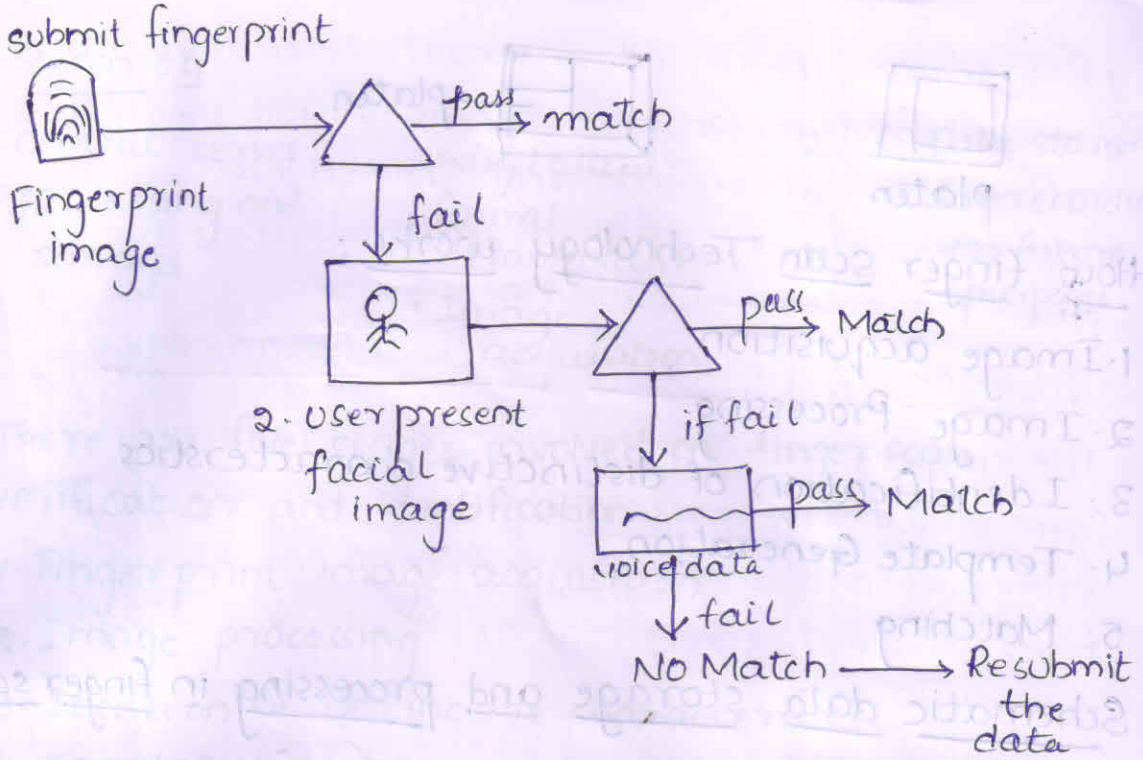
1. Parallel Layered Biometrics:

Parallel Layered solutions required that the us submit multiple biometrics in a single authentica



2. Serial Layered Biometrics:

Serial layered solutions combine the result o two or three seperate authentication process to authentication users. Serial layered user interaction might consist of verification on fingerscan, their facial scan then voice scan



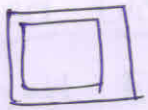
Finger scan Technology:

Finger scan Technology utilises distinctive features of the finger print to identify or verify the individuals identity.

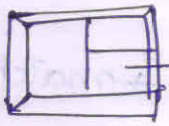
Finger scan systems comprise acquisition hardware, image processing components, template generation and matching components and storage components

The surface on which finger is placed is called a platen also called as a scanner

* Depending on the type of finger scan technology used areas of contact between the finger print on the platen are measured through chip based cameras through ultrasonic imaging or through changes in capacitive fields generated by the finger
* These measurements are converted to digital code
* A platen attached to a small printed circuit board, along with a standard connector that allows digitized information to be transmitted to the peripheral or standalone device



platen



How finger scan Technology works:

1. Image acquisition
2. Image Processing
3. Identification of distinctive characterstics
4. Template Generation
5. Matching

Schematic data storage, and processing in finger s systems:

Scenario 1:			
Device level Processing and storage	• 1 • 2 • 3 • 4 • 5	• receives the decision • Transmitted to central server	• Data sto for reco for futu purposes
Scenario 2:			
Device level processing and local PC storage	1 2 3 4	• storage of template • Matching • Decision transmitives	• Data sto for record for futu purpos
Scenario 3			
local PC processing and Storage	Image acqui-sition	2 3 4 5	Data stor for recordi for futu purpose

Scenario 4:

central server processing and storage

- image indigitalized format transmitted
- Image acquisition

2 Data stored
3 for recording
4 for future
5 purposes

There are five stages involved in finger scan verification and identification

1. Finger print image acquisition
2. Image processing
3. Location of Distinctive characterstics
4. Template Creation
5. Template Matching

* Each vendor's process may differ slightly from the sequence described

1. Image Acquisition:

Image quality is measured in Dots Per Inch (DPI). More dots for inch means a high resolution image. Today's Finger scan peripherals can acquire images of 500 DPI the standard for Forensic-quality Finger Printing. Finger print quality can vary substantially from person-to-person and from finger-to-finger. Inorder to acquire finger print image user require to keep his/her finger on the platen. In image acquisition that can effect a system's accuracy and performance is the size of the platen

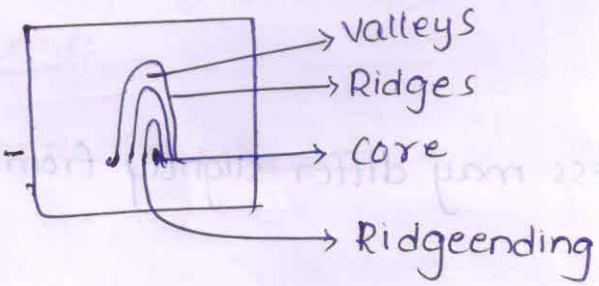
2. Image Processing:

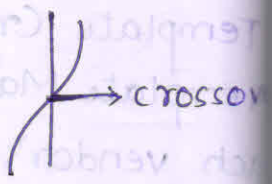
Once a high quality image is acquired, it must be converted to a usable format. Image processing includes eliminate gray areas from the image by converting the fingerprint images gray pixels

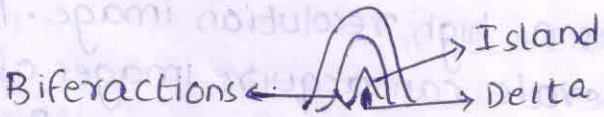
to black and white, which results thick black rid
(raised part of finger print) contrasted to whit
valleys. The ridges are then thinned from
approximately 5-8 pixels in width down to a sin
pixel, for precise location of features

3. Location of Distinctive feature Characterstics:

The finger print comprises ridges and valleys t
form distinctive patterns, such as swirls, loops
arches. Most finger prints have a core, a cen
point around which swirls, loops or arches ar
curved.







Fingerprint ridges and valleys are characterse
discontinuties and irregularities known as minutiae
these are the distinctive features on which most
fingerprint scan technology are based. There are
many types of minutia, the most common being
ridge endings and biferactions. Depending on the
size of the platen a typical fingerscan image
produce between 10-15 minutiaes

4. Template Creation:

Vendor's use algorithm to simplify map finger pr

minutae. Information used when mapping minutae can improved the location and angle of a minutae point, the type and quality of minutae and the distance and position of minutae relative to core.

5. Template Matching:

Finger scan templates can range in size from 200 bytes to 1000 bytes. These generates cannot be manually read and simply performing a bit-to-bit comparision of two fingerscan templates will not determine whether they are from the same person But vendor algorithms are required to process templates and to determine the correlation between the two

Competing fingerscan Technologies:

There are three leading technologies in the finger scan industry

1. Optical Technology
2. Silicon Technology
3. Ultra-scan Technology

1. Optical Technology:

The user places a finger on a coated platen, built of hard coated plastic or coated glass. A camera registers the image of the fingerprint against a coated glass or plastic platen, upon which the digitized ridges and valleys appear as black, grey and white lines

Strengths:

1. Reliable over
2. Is resistant to electrostatic discharge
3. Is fairely inexpensive
4. Can provide resolutions upto 500DPI

Weaknessess:

1. Size, the platen must be of sufficient surface
2. Depth to capture quality images

2. Silicon Technology:

* It uses a silicon as a platen. The silicon sen acts as one plate of a capacitor and the finger becomes the other plate
* Silicon Technologies can use active capacitance, generates a small field that extends beyond surface of the platen and reads to the live la of skin, which measures upto point of contact

Strengths:

1. High quality image
2. Lower cost

Weakness:

Silicon's Durability

3. Ultra - sound Technology:

It is the least frequently used technology. Ultrasound devices transmit inaudible acoustic waves to the finger, generating images by measuring the impedance between the finge the platen and air. Ultrasound devices are more capable of penetrating dust and resid A limitation of the technology is the need f a larger acquisition device due to the machi involved in ultra sonic imaging.

Finger scan Strengths:

Finger scan Technology has a number of advantages over other technologies

1. Proven Technology capable of high levels of accuracy:

* The fingerprint has long been recognised as a highly distinctive feature identifier - classification, analysis and study of finger prints have existed for decades
* Strong finger scan solutions are capable of processing thousands of users without allowing a false match and can verify nearly one hundred percent of users with one or two placements of a finger
* Many finger scan solutions can be deployed in applications where both security and convenience are primary drives.

2. Range of Deployment Environments:

Reduced size and power requirements along with finger scan resistance to environmental changes such as background, lighting and temperature, allow the technology to be deployed in a range of logical and physical access environments. There are more finger scan solutions in the biometric market place than all other technologies combined

3. Easy-to-use devices:

The act of placing a finger on a device is largely intuitive and can be grasped with

little training. Many other biometric technol require complex user-system interactions. Fi scan devices are generally designed such tha placement is an easily repeatable process

4. Ability to enroll multiple fingers:

Most people can enroll upto ten fingers in a biometric system gives finger scan advantages security and flexibility. Allowing a user to verify with one or several enrolled fingers reduces the likelihood of a user being falsel rejected

Fingerscan Weaknesses:-

1. Inability to enroll some users:

A small percentage of users are unable to en in many finger scan systems. Certain demograp groups have lower quality fingerprints and mo difficult to enroll them. Elderly population manua labourers and some asian population are more likely to be unable to enroll in some fingerscan systems

2. Performance Deterioration over time:

Although the finger print is a stable physiologic characterstic, daily wear can cause the perfor of some finger scan technologies to drop drasti users who work with hands are likely to see increased error rates over time

3. Assosiation with forensic applications:

Finger scan technologies similarity to forensic finger printing causes some percentage of users discomfort. Privacy advocates fear that

fingerscan data collected for a specific purpose may be used for forensic applications.

4. Need to deploy specialized devices:

Inorder for fingerscan to become a pervasive biometric solution, devices must be present on desktops, at points of sale, at protected door ways and at any location where authentication is required

Types of algorithms used for interpretation:

We need to know which types of algorithms are used to know what constitutes a finger print and how it can be imaged etc..

The following categories of algorithms are used

1) Minutia-based algorithm
2) Pattern-based algorithm
3) Hybrid-based algorithm

1) Minutia-based algorithm:

Vendors who choose to use minutia based algorithms will need to provide the highest quality image possible. Minutia based templates are relatively smaller than pattern based templates. For minutia based finger print algorithm, only a small part of the finger image is required for verification As such it is ideal to have as much minutia as possible in the finger image area. Since just a portion of the minutia is required for verificatio it would be ideal to use this algorithms where space restriction impact the use and deployment of biometrics. A good imager for a minutia-based algorithm would be one that takes a high quality image has a large enough capture window for the relative core of finger image to be imaged

2. Pattern-based algorithms:

Pattern-based algorithms use both the mic macro features of a finger print. When the macro features are utilised, the size of the required for authentication, when compared the size of the image needed for minutia requirements these types of algorithms tend fast and have a larger template size.

They also required more of the image are be present during verification. A good ima for pattern-based matching algorithms is that has a high quality camera and a la enough scanning surface to capture the im macro details.

3. Hybrid-based Algorithm:

A hybrid algorithm uses the best features fro minutia based algorithms and those from patte based matching. This algorithm is a good all- algorithm, giving a good trade off between t accuracy of the minutia algorithm and speed the pattern based recognition. A high quality optical sensor is best for these types of a It would offer a large enough image area, w very good quality for the images. The hybrid algorithm takes longer to enroll because of t use of both minutia and character based recognization. Once these has occured, the matching is actually faster than the minut based algorithm

If:

- Template size is important
- The relative speed difference between minutia based and pattern based algorithms are negligable
- The application does not require high throughput,

→ then minutia base algorithm would work best

If:

- template size is not important
- relative speed difference is sufficiently meaning full
- The application has high throughput then

→ pattern based algorithm would work best

If:

- template size is not important
- faster matching is required
- the application has high throughput then

→ Hybrid based algorithm will work best