17BEBME5E02 BIOMETRIC SYSTEMS 3 0 0 3 100

OBJECTIVES:

- To understand the technologies of fingerprint, iris, face and speech recognition
- To understand the general principles of design of biometric systems and the underlying trade-offs.
- To recognize personal privacy and security implications of biometrics based identification technology.
- To identify issues in the realistic evaluation of biometrics based systems.

OUTCOMES:

At the end of the course, the student should be able to:

- Demonstrate knowledge engineering principles underlying biometric systems.
- Analyze design basic biometric system applications.

UNIT I INTRODUCTION TO BIOMETRICS 9

Introduction and back ground – biometric technologies – passive biometrics – active biometrics - Biometric systems – Enrollment – templates – algorithm – verification – Biometric applications – biometric characteristics- Authentication technologies –Need for strong authentication - Protecting privacy and biometrics and policy – Biometric applications – biometric characteristics

UNIT II FINGERPRINT TECHNOLOGY 9

History of fingerprint pattern recognition - General description of fingerprints - Finger print feature processing techniques - fingerprint sensors using RF imaging techniques – fingerprint quality assessment – computer enhancement and modeling of fingerprint images – fingerprint enhancement – Feature extraction – fingerprint classification – fingerprint matching

UNIT III FACE RECOGNITION AND HAND GEOMETRY 9

Introduction to face recognition, Neural networks for face recognition – face recognition from correspondence maps – Hand geometry – scanning – Feature Extraction - Adaptive Classifiers - Visual-Based Feature Extraction and Pattern Classification - feature extraction – types of algorithm – Biometric fusion.

UNIT IV MULTIMODAL BIOMETRICS AND PERFORMANCE EVALUATION 9

Voice Scan – physiological biometrics –Behavioral Biometrics - Introduction to multimodal biometric system – Integration strategies – Architecture – level of fusion – combination strategy –training and adaptability – examples of multimodal biometric systems – Performance evaluation- Statistical Measures of Biometrics – FAR – FRR – FTE – EER – Memory requirement and allocation.

UNIT V BIOMETRIC AUTHENTICATION 9

Introduction - Biometric Authentication Methods - Biometric Authentication Systems – Biometric authentication by fingerprint -Biometric Authentication by Face Recognition. -.

Expectation- Maximization theory - Support Vector Machines. Biometric authentication by fingerprint –biometric authentication by hand geometry- Securing and trusting a biometric transaction – matching location – local host - authentication server – match on card (MOC) – Multibiometrics and Two-Factor Authentication

Total : 45

TEXT BOOKS:

S.NO.	Author(s) Name	Title of the book	Publisher	Year of publication
1	James Wayman, Anil Jain, Davide Maltoni	Biometric Systems, Technology Design and Performance Evaluation	Springer	2005
2	S.Y. Kung, S.H. Lin, M.W.Mak	Biometric Authentication: A Machine Learning Approach	Prentice Hall	2005

REFERENCES:

S.NO.	Author(s) Name	Title of the book	Publisher	Year of publication
1	Paul Reid	Biometrics for Network Security	Pearson Education	2004
2	Nalini K Ratha, Ruud Bolle	Automatic fingerprint Recognition System	Springer	2003
3	L C Jain, I Hayashi, S B Lee, U Halici	Intelligent Biometric Techniques in Fingerprint and	CRC Press	1999
4	John Chirillo, Scott Blaul	Implementing Biometric Security	John Wiley	2003
5	Arun A. Ross, Karthik Nanda Kumar, Anil K. Jain	Handbook of Multibiometrics	Springer	2006

KARPAGAM ACADEMY OF HIGHER EDUCATION
COIMBATORE-21
Faculty of Engineering
Department of Biomedical Engineering

LECTURE PLAN

Name of the staff : T.S.BELLIRAJ
Designation : Assistant Professor
Class : III-B.E BME
Subject : Biometric System
Subject code : 17BEBME5E02

Sl.No.	Topics to be covered	Time Duration	Teaching aids
	UNIT-I INTRODUCTION TO BIOMETRICS		
1	Introduction and back ground	01	**R6 (Pg 3-5)**
2	Biometric technologies	01	R7 (Pg 3-7)
3	Passive biometrics & Active biometrics	01	J - 1
4	Biometric systems – Enrollment,templates,algorithm & verification	01	R6 (Pg15-21)
5	Biometric applications	01	R7(Pg 12-13)
6	biometric characteristics	01	R7(Pg 15)
7	Authentication technologies	01	R6 (Pg 3-5)
8	Need for strong authentication	01	T1 (Pg 9-14)
9	Protecting privacy and biometrics and policy	01	T1 (Pg 15)
	UNIT-II FINGERPRINT TECHNOLOGY		
10	History of fingerprint pattern recognition	01	T1 (Pg 21)
11	General description of fingerprints	01	W1
12	Finger print feature processing techniques	01	W1
13	Fingerprint sensors using RF imaging techniques	01	W2
14	Fingerprint quality assessment	01	W3
15	Computer enhancement and modeling of fingerprint images	01	W4
16	Fingerprint enhancement	01	T1 (Pg 33)
17	Feature extraction	01	R7 (Pg 27)
18	Fingerprint classification & fingerprint matching.	01	T1 (41 -43)
	UNIT-III FACE RECOGNITION AND HAND GEOMETRY		
19	Introduction to face recognition	01	R6 (Pg 63)
20	Neural networks for face recognition	01	R6 (Pg 71)
21	Face recognition from correspondence maps	01	T1 (pg 101-107)
22	Hand geometry	01	R6 (Pg 99-106)
23	Scanning & Feature Extraction	01	R6 (Pg 99-106)
24	Adaptive Classifiers	01	R6(Pg 52 – 56)
25	Visual-Based Feature Extraction and Pattern Classification	01	R6(Pg 77 – 82)
26	Feature extraction	01	R6(Pg 77 – 82)
27	Types of algorithm & Biometric fusion.	01	R6(Pg 52 – 56)
	UNIT-IV MULTIMODAL BIOMETRICS AND PERFORMANCE EVALUATION		
28	Voice Scan – physiological biometrics	01	R6 (Pg 87 – 92)

29	Behavioral Biometrics	01	R6 (Pg 99)
30	Introduction to multimodal biometric system & Integration strategies	02	T1 (Pg 271)
31	Architecture – level of fusion & combination strategy	01	W5
32	Training and adaptability – examples of multimodal biometric systems	01	J2
33	Performance evaluation- Statistical Measures of Biometrics – FAR – FRR – FTE – EER Switch level modeling	02	R6 (Pg 33 – 38)
34	Memory requirement and allocation.	01	W5
UNIT-V BIOMETRIC AUTHENTICATION			
35	Introduction - Biometric Authentication Methods	01	W6
36	Biometric Authentication Systems – Biometric authentication by fingerprint	01	T1 (Pg 336)
37	Biometric Authentication by Face Recognition.	01	T1 (Pg 315)
38	Expectation- Maximization theory	01	T1 (Pg 55-56)
39	Support Vector Machines	01	T1 (Pg 55-56)
40	Biometric authentication by Handgeometry	01	W6
41	Securing and trusting a biometric transaction	01	T1 (Pg 9-14)
42	matching location – local host - authentication server – match on card (MOC)	01	W7
43	Multibiometrics and Two-Factor Authentication.	01	T1 (Pg 9-14)

Journal:

J1 – www.jgrcs.info

J2 - International Journal of Research in Advanced Engineering and Technology

Website:

W1- http://www.odec.ca/projects/2004/fren4j0/public_html/fingerprint_patterns.htm
W2- https://link.springer.com/chapter/10.1007/0-387-21685-5_2
W3- https://ieeexplore.ieee.org/document/7475528
W4 - https://link.springer.com/chapter/10.1007/0-387-21685-5_5
W5- https://www.tutorialspoint.com/biometrics/multimodal_biometric_systems
W6 - https://heimdalsecurity.com/blog/biometric-authentication/
W7 - https://www.secureidnews.com/news-item/tech-101-match-on-card-biometrics/

TEXT BOOK

Sl.No.	Author(s)	Title of the Book	Publisher	Year of Publication
1	James Wayman, Anil Jain, Davide Maltoni	Biometric Systems, Technology Design and Performance Evaluation	Springer	2005
2	S.Y. Kung, S.H. Lin, M.W.Mak	Biometric Authentication: A Machine Learning Approach	Prentice Hall	2005

REFERENCES

Sl.No.	Author(s)	Title of the Book	Publisher	Year of Publication
1	Paul Reid	Biometrics for Network Security	Pearson Education	2004
2	Nalini K Ratha, Ruud Bolle	Automatic fingerprint Recognition System	Springer	2003
3	L C Jain, I Hayashi, S B Lee, U Halici	Intelligent Biometric Techniques in Fingerprint and Face Recognition	CRC Press	1999
4	John Chirillo, Scott Blaul	Implementing Biometric Security	John Wiley	2003
5	Arun A. Ross, Karthik Nanda Kumar, Anil K. Jain	Handbook of Multibiometrics	Springer	2006
6	Samir nanavati, Michael Thieme , Raj nanavati	Biometrics , Identity verification iu a networked world	Wiley Computer	2002
7	Anil K.Jain , Patrick Flynn , arun A.Ross	Handbook of Biometrics	springer	2007

Staff In-Charge **HOD/BME**

UNIT 1: INTRODUCTION TO BIOMETRICS

TOPIC: INTRODUCTION AND BACKGROUND

Objective:

To study the introduction and background of biometric technologies

Description:

What is Biometrics?

Biometrics is a technology used to identify, analyze, and measure an individual's physical and behavioral characteristics.

- Identity verification in computer systems is done based on measures like keys, cards, passwords, PIN and so forth. Unfortunately, these may often be forgotten, disclosed or changed.
- A reliable and accurate identification/verification technique may be designed using biometric technologies, which are further based on the special characteristics of the person such as face, iris, fingerprint, signature and so forth.
- This technique of identification is preferred over traditional passwords and PIN-based techniques for various reasons:

- The person to be identified is required to be physically present at the time of identification.
- Identification based on biometric techniques obviates the need to remember a password or carry a token.

- ✓ A biometric system essentially is a pattern recognition system that makes a personal identification by determining the authenticity of a specific physiological or behavioral characteristic possessed by the user.
- ✓ Biometric technologies are thus defined as the "automated methods of identifying or authenticating the identity of a living person based on a physiological or behavioral characteristic."

A biometric system can be either an identification system or a verification (authentication) system; both are defined below.

- **Identification:** One to Many - A comparison of an individual's submitted biometric sample against the entire database of biometric reference templates to determine whether it matches any of the templates.
- **Verification:** One to One - A comparison of two sets of biometrics to determine if they are from the same individual.

1) Biometric authentication requires comparing a registered or enrolled biometric sample (biometric template or identifier) against a newly captured biometric sample (for example, the one captured during a login). This is a three-step process (Capture, Process, Enroll) followed by a Verification or Identification.
2) During Capture, raw biometric is captured by a sensing device, such as a fingerprint scanner or video camera; then, distinguishing characteristics are extracted from the raw biometric sample and converted into a processed biometric identifier record (biometric template).
3) Next is enrollment, in which the processed sample (a mathematical representation of the template) is stored/registered in a storage medium for comparison during authentication.
4) In many commercial applications, only the processed biometric sample is stored. The original biometric sample cannot be reconstructed from this identifier.

BACKGROUND

Many biometric characteristics may be captured in the first phase of processing. However, automated capturing and automated comparison with previously stored data requires the following properties of biometric characteristics:

- **Universal:** Everyone must have the attribute. The attribute must be one that is seldom lost to accident or disease.
- **Invariance of properties:** They should be constant over a long period of time. The attribute should not be subject to significant differences based on age or either episodic or chronic disease.

- **Measurability:** The properties should be suitable for capture without waiting time and it must be easy to gather the attribute data passively.
- **Singularity:** Each expression of the attribute must be unique to the individual. The characteristics should have sufficient unique properties to distinguish one person from any other. Height, weight, hair and eye color are unique attributes, assuming a particularly precise measure, but do not offer enough points of differentiation to be useful for more than categorizing.
- **Acceptance:** The capturing should be possible in a way acceptable to a large percentage of the population. Excluded are particularly invasive technologies; that is, technologies requiring a part of the human body to be taken or (apparently) impairing the human body.
- **Reducibility:** The captured data should be capable of being reduced to an easy-to-handle file.
- **Reliability and tamper-resistance:** The attribute should be impractical to mask or manipulate. The process should ensure high reliability and reproducibility.
- **Privacy:** The process should not violate the privacy of the person.
- **Comparable:** The attribute should be able to be reduced to a state that makes it digitally comparable to others. The less probabilistic the matching involved, the more authoritative the identification.
- **Inimitable:** The attribute must be irreproducible by other means. The less reproducible the attribute, the more likely it will be authoritative.

TOPIC2: BIOMETRIC TECHNOLOGIES

Objective:

To study about biometrics and various biometric technologies.

Description:

What is Biometrics?

- The term "biometrics" is derived from the Greek words bio (life) and metric (to measure).
- Biometric is the most secure and convenient authentication tool.
- It cannot be borrowed, stolen, or forgotten and forging one is practically impossible.

- Biometrics measure individual's unique physical or behavioral characteristics to recognize or authenticate their identity.
- Common physical biometrics includes fingerprints, hand or palm geometry, retina, iris, and facial characteristics.
- Behavioral characters characteristics include signature, voice, keystroke pattern, and gait. Of this class of biometrics, technologies for signature and voice are the most developed.

Biometric technologies:

There are many biometric technologies to suit different types of applications. To choose the right biometric to be highly fit for the particular situation, one has to navigate through some complex vendor products and keep an eye on future developments in technology and standards. Here comes a list of biometrics:

Fingerprints - A fingerprint looks at the patterns found on a fingertip. There are a variety of approaches to fingerprint verification, such as traditional police method, using pattern-matching devices, and things like moire fringe patterns and ultrasonics. This seems to be a very good choice for in-house systems.

Hand geometry - This involves analyzing and measuring the shape of the hand. It might be suitable where there are more users or where user accesses the system infrequently. Accuracy can be very high if desired and flexible performance tuning and configuration can accommodate a wide range of applications. Organizations are using hand geometry readers in various scenarios, including time and attendance recording.

Retina - A retina-based biometric involves analyzing the layer of blood vessels situated at the back of the eye. This technique involves using a low intensity light source through an optical coupler to scan the unique patterns of the retina. Retinal scanning can be quite accurate but does require the user to look into a receptacle and focus on a given point.

Iris - An iris-based biometric involves analyzing features found in the colored ring of tissue that surrounds the pupil. This uses a fairly conventional camera element and requires no close contact

between the user and the reader. Further, it has the potential for higher than average template-matching performance.

Face- Face recognition analyses facial characteristics. It requires a digital camera to develop a facial image of the user for authentication. Because facial scanning needs extra peripheral things that are not included in basic PCs, it is more of a niche market for network authentication. However, the casino industry has capitalized on this technology to create a facial database of scam artists for quick detection by security personal

Signature - Signature verification analyses the way user signs his name. Signing features such as speed, velocity, and pressure are as important as the finished signature's static shape. People are used to signatures as a means of transaction-related identity verification.

Voice - Voice authentication is based on voice-to-print authentication, where complex technology transforms voice into text. Voice biometrics requires a microphone, which is available with PCs nowadays. Voice biometrics is to replace the currently used methods, such as PINs, passwords, or account names. But voice will be a complementary technique for finger-scan technology as many people see finger scanning as a higher authentication form.

Topic3: Active and Passive Biometrics

Objective:

To study about active and passive biometrics also to analyze the difference between them.

Description:

- The use of physiological or behavioral characteristics of a human person through automated technological means to determine or verify the identity of that person.

  Physiological biometrics use algorithms and other methods to define identity in terms of data gathered from direct measurement of the human body.

- Finger print and finger scan, hand geometry, Iris and retina scanning and facial geometry are all examples of physiological biometrics.

Behavioral biometrics is, however, defined by analyzing a specific action of a person. How a person talks, signs their name or types on a keyboard is a method of determining his identity when analyzed correctly.

Biometrics can furthermore also be defined as either passive, or active.

- ✓ Passive biometrics does not require a user's active participation and can be successful without a person even knowing that they have been analyzed.

- ✓ Active biometrics does require person's cooperation and will not work if they deny their participation in the process.

Active Biometrics:

1. All Fingerprint technologies
2. Hand geometry technologies
3. Retina scanning technologies
4. Signature recognition technologies

Passive Biometrics:

1. Voice recognition technologies (limited)
2. Iris recognition technologies (limited)
3. Facial recognition (truly passive)

Difference between Active and Passive biometrics

Passive	Active
Experience: Customers are able to speak naturally with a live agent at the beginning of a call while their identity is being verified seamlessly in the background.	**Experience:** Customers speak a short, fixed passphrase to confirm their identity at the start of a self-service interaction. The passphrase is consistent across the application and can be prompted – eliminating the need for consumer to remember it.
Enrollment: Customers simply speak naturally for less than a minute to create a "voiceprint" that is stored for comparison to in all subsequent live calls**.**	**Enrollment:** Customers repeat a set phrase such as, 'My voice is my password' three times to create a voiceprint that is stored and compared to in all future calls for verification.
Result: Shortens average call durations and creates a positive memorable customer service experience.	**Result:** Customers quickly and easily authenticate, increasing containment within the self-service channel.

TOPIC 4: **Biometric systems Enrollment, template, algorithm and verification**

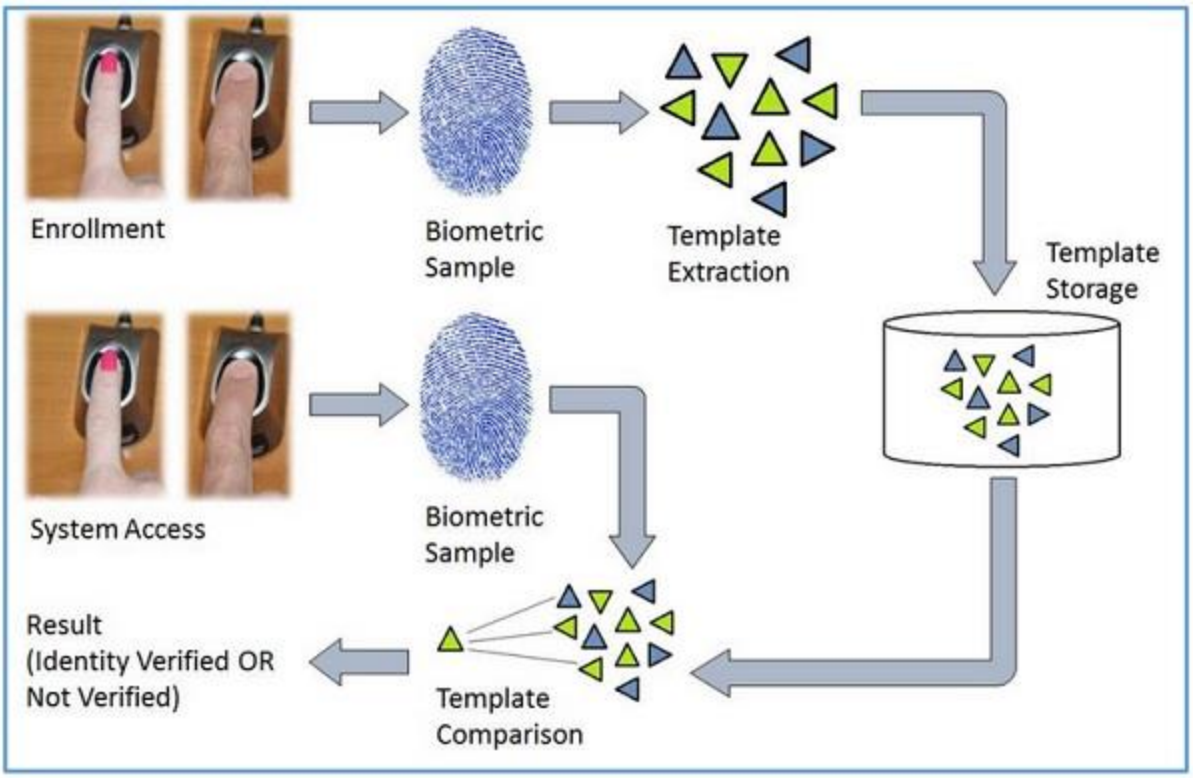
Objective:

To study about the biometric system enrollment, template, algorithm and verification.

Description:

- Biometrics system operates in two phases: enrollment and verification.
- Biometric reference data (also referred to as template) is collected during enrollment and stored in a database or in a portable data carrier such as a smart card or token.
- Verification is the actual usage of the system for the desired purpose. Current biometric data is collected and compared with the reference data.
- The comparison process is an algorithmic approach to determine the probability that two samples stem from the same biometric trait.
- Depending on the outcome, access to the security system is granted or other appropriate actions taken.

BLOCK DIAGRAM OF BIOMETRICS



The block diagram illustrates the two basic modes of a biometric system.

GENERAL WORKING OF A BIOMETRIC SYSTEM

There are four general steps a biometric system takes to perform identification and verification −

- Acquire live sample from candidate. (using sensors)
- Extract prominent features from sample. (using processing unit)
- Compare live sample with samples stored in database. (using algorithms)
- Present the decision. (Accept or reject the candidate.)

The biometric sample is acquired from candidate user. The prominent features are extracted from the sample and it is then compared with all the samples stored in the database. When the input sample matches with one of the samples in the database, the biometric system allows the person to access the resources; otherwise prohibits.

BIOMETRICS TERMINOLOGY

Biometric Template − It is a digital reference of the distinct characteristics that are extracted from a biometric sample.

Candidate/Subject − A person who enters his biometric sample.

Closed-Set Identification − The person is known to be existing in the database.

Enrollment − It is when a candidate uses a biometric system for the first time, it records the basic information such as name, address, etc. and then records the candidate's biometric trait.

False Acceptance Rate (FAR) − It is the measure of possibility that a biometric system will incorrectly identify an unauthorized user as a valid user.

FAR = Number of False Acceptances / Number of Identification Attempts

A biometric system providing **low FAR ensures high security**.

False Reject Rate (FRR) − It is the measure of possibility that the biometric system will incorrectly reject an authorized user as an invalid user.

FRR = Number of False Rejections / Number of Identification Attempts

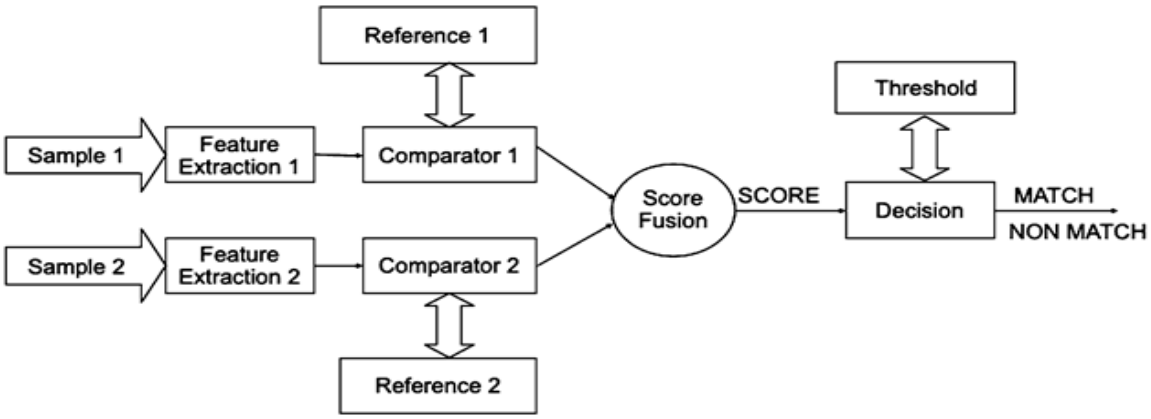
Open-Set Identification − The person is not guaranteed to be existing in the database.

Task − It is when the biometric system searches the database for matching sample.

Biometrics System Algorithm:

- A **biometrics algorithm** is sequence of instructions that tell a biometric system how to solve a particular problem.
- Typically, biometric systems use these sequences of rules to interpret data that has been abstracted from the original source.
- For example, rather than work on fingerprint images directly, biometric systems take from a particular print a set of features that best defines differences between individuals.

- An algorithm will have a finite number of steps and is typically used by the biometric engine to compute whether a biometric sample and template are a match.



- The first time an individual uses a biometric system is called enrollment.
- During the enrollment, biometric information from an individual is captured and stored.
- Biometric information is detected and compared with the information stored at the time of enrollment.
- The first block (sensor) is the interface between the real world and the system; it has to acquire all the necessary data.
- Most of the times it is an image acquisition system, but it can change according to the characteristics desired.
- The second block performs all the necessary pre-processing: it has to remove artifacts from the sensor, to enhance the input (e.g. removing background noise), to use some kind of normalization, etc.
- In the third block necessary features are extracted. This step is an important step as the correct features need to be extracted in the optimal way.
- A vector of numbers or an image with particular properties is used to create a template.
- A template is a synthesis of the relevant characteristics extracted from the source. Elements of the biometric measurement that are not used in the comparison algorithm are discarded in the template to reduce the file size and to protect the identity of the enrollee.
- During the enrollment phase, the template is simply stored somewhere (on a card or within a database or both).

- During the matching phase, the obtained template is passed to a matcher that compares it with other existing templates, estimating the distance between them using any algorithm.
- The matching program will analyze the template with the input. This will then be output for any specified use or purpose (e.g. entrance in a restricted area).
- Selection of biometrics in any practical application depending upon the characteristic measurements and user requirements.
- In selecting a particular biometric, factors to consider include, performance, social acceptability, ease of circumvention and/or spoofing, robustness, population coverage, size of equipment needed and identity theft deterrence.
- Selection of a biometric based on user requirements considers sensor and device availability, computational time and reliability, cost, sensor size and power consumption.

TOPIC 5: BIOMETRIC APPLICATIONS

OBJECTIVE:

To study about the various biometric applications are common to these groups such as physical access, PC/network access, time and attendance, etc.

DESCRIPTION:

Forensic:

The use of biometric in the law enforcement and forensic is more known and from long date, it is used mainly for identification of criminals. In particular, the AFIS (automatic fingerprint identification system) has been used for this purpose. The typical applications are:

- **Identification of criminals-** collecting the evidence in the scene of crime (e.g., fingerprints) it is possible to compare with data of suspects or make a search in the database of criminals.
- **Surveillance** --using cameras one can monitor the very busy places such as stadiums, airports, meetings, etc.

Looking in the crowds for suspect, based on the face recognition biometric, using a images (e.g., mug shots) database of wanted persons or criminals.

Currently there are many cameras monitoring crowds at airports for detecting wanted terrorists.

- **Corrections -**This refers to the treatment of offenders (criminals) through a system of penal incarceration, rehabilitation, probation, and parole, or the administrative system by which these are effectuated.

  Is this cases a biometric system can avoid the possibility of accidentally releasing the wrong prisoner, or to ensure that people leaving the facilities are really visitors and not inmates.

- **Probation and home arrest -** biometric can also be used for post-release programs (conditional released) to ensure the fulfillment of the probation, parole and home detention terms.

Government

There are many application of the biometry in the government sector. An AFIS (automatic fingerprint identification system) is the primary system used for locating duplicates enrolls in benefits systems, electronic voting for local or national elections, driver's license emission, etc. The typical applications are:

- **National Identification Cards -** The idea is to include digital biometric information in the national identification card.

  This is the most ambitious biometric program, since the identification must be performed in a large-scale database, containing hundreds of millions samples, corresponding to the whole population of one country.

  This kind of cards can be used for multiple purposes such as controlling the collection of benefits, avoiding duplicates of voter registration and drivers license emission.

All this applications are primarily based on finger-scan and AFIS technology; however it is possible that facial-scan and iris-scan technology could be used in the future.

- **Voter ID and Elections -** While the biometric national ID card is still in project, in many countries are already used the biometry for the control of voting and voter registration for the national or regional elections.

  During the registration of voter, the biometric data is captured and stored in the card and in the database for the later use during the voting.

  The purpose is to prevent the duplicate registration and voting.

- **Driver's licenses -** In many countries the driver license is also used as identification document, therefore it is important to prevent the duplicate emission of the driver license under different name.

  With the use of biometric this problem can be eliminated.

  However it is important that the data must be shared between states, because in some country such as United States, the license is controlled at the states as opposed to the federal level.

- **Benefits Distribution (social service) -** The use of biometry in benefits distribution prevents fraud and abuse of the government benefits programs.

  Ensuring that the legitimate recipients have a quick and convenient access to the benefits such as unemployment, health care and social security benefits.

- **Employee authentication -** The government use of biometric for PC, network, and data access is also important for security of building and protection of information.

  Below are more detailed this kind of applications also used in commercial sector.

- **Military programs -** the military has long been interested in biometrics and the technology has enjoyed extensive support from the national security community.

Commercial

Banking and financial services represent enormous growth areas for biometric technology, with many deployments currently functioning and pilot project announced frequently. Some applications in this sector are:

- **Account access -** The use of biometric for the access to the account in the bank allows to keep definitive and auditable records of account access by employees and customers. Using biometry the customers can access accounts and employees can log into their workstations.
- **ATMs -** the use of biometric in the ATM transaction allows more security,
- **Expanded Service Kiosks -** A more receptive market for biometrics may be special purpose kiosks, using biometric verification to allow a greater variety of financial transaction than are currently available though standard ATMs.
- **Online banking -** Internet based account access is already widely used in many places, the inclusion of biometric will make more secure this type of transactions from home. Currently, there are many pilot programs using biometric in home banking.
- **Telephony transaction -** Voice-scan biometric can be used to make more secure the telephone-based transactions. In this type of application, when the costumer calls to make a transaction, a biometric system will authenticate the customer's identity based on his or her voice with no need of any additional device.
- **PC/Network access -** The use of biometric log-in to local PCs or remotely through network increase the security of the overall system keeping more protected the valuable information.
- **Physical access -** the biometric is widely used for controlling the access to building or restricted areas.
- **E-commerce -** biometric e-commerce is the use of biometrics to verify of identity of the individual conduction remote transaction for goods or services
- **Time and attendance monitoring -** In this sector the biometrics is used for controlling the presence of the individuals in a determine area. For example for c

Health Care

The main aim of biometrics in health care is to prevent fraud, protect the patient information and control the cell of pharmaceutical products. Some typical applications are:

- **PC/Network Access -** the biometrics are used to control a secure access of the employees to the hospital network, primarily, in order to protect the patient information,
- **Access to personal information -** Using biometrics, the medical patient information may be stored on smart card or secure networks; this will enable the access of the patients to their personal information.
- **Patient identification -** In case of emergency, when a patient does not have identification document and is unable to communicate, biometric identification may be a good alternative to identify.

Travel and Immigration

The application in this sector includes the use of biometrics to identify or verify the identity of individual interacting during the course of travel, with a travel or immigration entity or acting in the capacity of travel or immigration employee. Typical applications are:

- **Air travel -** In many airport are already used a biometric system in order to reduce the inspection processing time for authorized travelers.
- **Border crossing -** The use of biometrics to control the travelers crossing the national or state border is increasing, especially in regions with high volume of travelers or illegal immigrants.
- **Employee access -** Several airport use biometric to control the physical access of employees to secure areas.
- **Passports -** Some country already issues passports with biometric information on a barcode or smart chips. The use of biometrics prevent the emission of multiple passports for the same person and also facilitates the identification at the airports and border controls.

TOPIC 6: BIOMETRIC CHARACTERISTICS AUTHENTICATION TECHNOLOGIES

OBJECTIVE**:**

To study about the biometric characteristics authentication technologies and types of authentication technologies..

DESCRIPTION:

- A biometric characteristic is any distinguishing characteristics of an individual that can be measured and extracted from a biometric sample for the purpose of biometric identification.
- Biometric characteristics may include a fingerprint, signature, voice pattern, ear form, DNA or other distinguishing characteristic.

What is a biometric authentication?

- Biometric Authentication is any process that validates the identity of a user who wishes to sign into a system by measuring some intrinsic characteristic of that user.
- Biometric samples include finger prints, retinal scans, face recognition, voice prints and even typing patterns.
- Biometric authentication is a type of system that relies on the unique biological characteristics of individuals to verify identity for secure access to electronic systems.
- Biometric verification is considered a subset of biometric authentication.
- The biometric technologies involved are based on the ways in which individuals can be uniquely identified through one or more distinguishing biological traits, such as fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves, keystroke dynamics, DNA and signatures.
- Biometric authentication is the application of that proof of identity as part of a process validating a user for access to a system.
- Biometric technologies are used to secure a wide range of electronic communications, including enterprise security, online commerce and banking -- even just logging in to a computer or smartphone.
- Biometric authentication systems compare the current biometric data capture to stored, confirmed authentic data in a database.

- If both samples of the biometric data match, authentication is confirmed and access is granted. The process is sometimes part of a multifactor authentication system.
- For example, a smartphone user might log on with his personal identification number (PIN) and then provide an iris scan to complete the authentication process.

Types of biometric authentication technologies:

Retina scans produce an image of the blood vessel pattern in the light-sensitive surface lining the individual's inner eye.

Iris recognition is used to identify individuals based on unique patterns within the ring-shaped region surrounding the pupil of the eye.

Finger scanning the digital version of the ink-and-paper fingerprinting process, works with details in the pattern of raised areas and branches in a human finger image.

Finger vein ID is based on the unique vascular pattern in an individual's finger.

Facial recognition systems work with numeric codes called face prints, which identify 80 nodal points on a human face.

Voice identification systems rely on characteristics created by the shape of the speaker's mouth and throat, rather than more variable conditions.

The security field uses three different types of authentication:

- Something you know — a password, PIN, or piece of personal information (such as your mother's maiden name)
- Something you have — a card key, smart card, or token (like a Secure ID card)
- Something you are — a biometric.

Of these, a biometric is the most secure and convenient authentication tool. It can't be borrowed, stolen, or forgotten, and forging one is practically impossible.

TOPIC 7: BIOMETRIC CHARACTERISTICS- NEED FOR STRONG AUTHENTICATION

Objective:

To study about the need for strong Authentication and the terms used for strong authentication.

Description:

- Strong authentication is any method of verifying the identity of a user or device that is intrinsically stringent enough to ensure the security of the system it protects by withstanding any attacks it is likely to encounter.
- Strong authentication is a commonly-used term that is largely without a standardized definition. According to the European Central Bank (and the many organizations that follow its guidelines), strong authentication combines at least two mutually-independent factors so that the compromise of one method should not lead to the compromise of the second.
- Additionally, the authentication method must include one non-reusable element, which cannot easily be reproduced or stolen from the Internet.
- The term strong authentication is often used synonymously with two-factor authentication (2FA) or multifactor authentication (MFA).
- However, that usage is misleading because some types of very secure authentication rely on a single authentication factor.

Multi-factor authentication (**MFA**) is a method of computer access control in which a user is only granted access after successfully presenting several separate pieces of evidence to an authentication mechanism – typically at least two of the following categories: knowledge (something they know), possession (something they have), and inherence (something they are).[

Two-factor authentication (also known as **2FA**) is a method of confirming a user's claimed identity by utilizing a combination of *two* different components. Two-factor authentication is a type of multi-factor authentication.

A good example from everyday life is the withdrawing of money from a cash machine; only the correct combination of a bank card (something that the user possesses) and a PIN (personal identification number, something that the user knows) allows the transaction to be carried out.

Three-factor authentication (3FA) is the use of identity-confirming credentials from three separate categories of authentication factors – typically, the knowledge, possession and inherence categories.

Multifactor authentication dramatically improves security. It is unlikely that an attacker could fake or steal all three elements involved in 3FA, which makes for a more secure log in.

What are authentication factors?

The ways in which someone can be authenticated usually fall into three categories known as the factors of authentication, which include:

1. Knowledge factors -- something the user knows, such as a password, PIN or shared secret.

2. Possession factors -- something the user has, such as an ID card, security token or a smartphone.

3. Inherence factors, more commonly called biometrics -- something the user is. These may be personal attributes mapped from physical characteristics, such as fingerprints, face and voice. It also includes behavioral biometrics, such as keystroke dynamics, gait or speech patterns.

Systems with more demanding requirements for security may use location and time as fourth and fifth factors. For example, users may be required to authenticate from specific locations, or during specific time windows.

Multifactor authentication involves two or more independent credentials for more secure transactions.

Authentication factors classically fall into three categories:

- Knowledge factors include things a user must know in order to log in: User names, IDs, passwords and personal identification numbers (PINs) all fall into this category.

- Possession factors include anything a user must have in his possession to log in. This category includes one-time password tokens (OTP tokens), key fobs, smartphones with OTP apps, employee ID cards and SIM cards.
- Inherence factors include any biological traits the user has that are confirmed for log in. This category includes the scope of biometrics such as retina scans, iris scans, fingerprint scans, finger vein scans, facial recognition, voice recognition, hand geometry and even earlobe geometry
- Three-factor authentication is mainly used in businesses and government agencies that require high degrees of security.
- The use of at least one element from each category is required for a system to be considered three-factor authentication -- selecting three authentication factors from two categories qualifies only as two-factor authentication (2FA).
- An additional factor, location, is sometimes employed for four-factor authentication (4FA).

TOPIC 8: PROTECTING AND PRIVACY POLICY IN BIOMETRICS

Objective:

To study about the need for protection and privacy policy in biometrics.

Description:

PRIVACY POLICY:

- Biometric data contains information acquired from individuals, which can be used to identify them.
- This raises issues of privacy and data protection.
- If the biometric data is recorded in a central database, privacy concerns may be higher than for systems where an individual's data is stored only on a card retained by the individual.
- Note however, some biometric applications require a central database for their basic functionality e.g. to check for multiple enrolment attempts.

- Enrolees may be concerned that their biometric data could be used for other purposes than it was originally acquired; for example, face image data might be used for surveillance purposes and fingerprint data checked against forensic databases.
- These concerns are at the heart of many objections to the use of biometrics.
- It is therefore necessary to understand privacy issues in regard to biometric data and biometric systems and to apply to protective safeguards in the deployment of these systems.
- In the UK, the Information Commissioner's Office is responsible for monitoring the use of biometric systems and for requiring that appropriate procedural and technical measures are deployed in accordance with the Data Protection Act.
- The biometric standards community is also addressing these issues and developing a code of good practice for applications.

Information privacy, or **data privacy (or data protection)**, is the relationship between collection and dissemination of data, technology, the public expectation of privacy, and the legal and political issues surrounding them

- ✓ Privacy concerns exist wherever personally identifiable information or other sensitive information is collected, stored, used, and finally destroyed or deleted – in digital form or otherwise.
- ✓ Improper or non-existent disclosure control can be the root cause for privacy issues.
- ✓ Data privacy issues can arise in response to information from a wide range of sources, such as:

- Healthcare records
- Criminal justice investigations and proceedings
- Financial institutions and transactions
- Biological traits, such as genetic material
- Residence and geographic records
- Privacy breach
- Location-based service and geolocation
- Web surfing behavior or user preferences using persistent cookies

- ❖ The challenge of data privacy is to utilize data while protecting individual's privacy preferences and their personally identifiable information.
- ❖ The fields of computer security, data security and information security design and utilize software, hardware and human resources to address this issue.
- ❖ As the laws and regulations related to Privacy and Data Protection are constantly changing, it is important to keep abreast of any changes in the law and continually reassess compliance with data privacy and security regulations

Protecting privacy in information systems:

There are two categories of technology to address privacy protection in commercial IT systems: communication and enforcement.

Policy Communication

- P3P - The Platform for Privacy Preferences. P3P is a standard for communicating privacy practices and comparing them to the preferences of individuals.

Policy Enforcement

- XACML- the Extensible Access Control Markup Language together with its Privacy Profile is a standard for expressing privacy policies in a machine-readable language which a software system can use to enforce the policy in enterprise IT systems.
- EPAL- the Enterprise Privacy Authorization Language is very similar to XACML, but is not yet a standard.
- WS-Privacy - "Web Service Privacy" will be a specification for communicating privacy policy in web services. For example, it may specify how privacy policy information can be embedded in the SOAP envelope of a web service message.

Protecting Privacy on the Internet

- On the internet you almost always give away a lot of information about yourself: Unencrypted e-mails can be read by the administrators of the e-mail server, if the

connection is not encrypted (no https), and also the internet service provider and other parties sniffing the traffic of that connection are able to know the contents.

- Furthermore, the same applies to any kind of traffic generated on the Internet (web-browsing, instant messaging, among others) In order not to give away too much personal information, e-mails can be encrypted and browsing of WebPages as well as other online activities can be done traceless via anonymizers, or, in cases those are not trusted, by open source distributed anonymizers, so called mix nets.

TOPIC 9: BIOMETRIC CHARACTERISTICS

Objective:

To study about the biometric characteristics.

Description:

It is essential to be familiar with the characteristics of biometrics systems in order to better understand how to think objectively about each type and make rational decisions about purchasing and using the technology. Any human anatomical or behavioral trait can be used as a biometric identifier to recognize a person as long as it satisfies the following characteristics:

Distinctiveness: Each person should be sufficiently unique in terms of their biometric traits. This is how well the particular biometric distinguishes people. DNA and fingerprints are among the best.

Permanence: Biometric trait should be invariant (with respect to the matching criterion) over time.

A good biometric system should measure something that changes slowly (if at all) over time. For example, DNA and fingerprints are among the best and hardly change while handwriting and voice may change from time to time.

Collectability: Biometric trait should be measured quantitatively. How easily the biometric can be measured can be significantly important in some applications.

For example, fingerprint biometrics is easy to measure while DNA can be difficult to measure or collect. DNA biometrics might not be ideal for e-passport application.

However, a practical biometric system must consider other issues such as:

Performance: recognition accuracy, speed (throughput), resource requirements and robustness to operational and environmental factors. For example, fingerprint readers are small, compact and accurate while DNA biometrics tend to be costly, slow and labor intensive

Acceptability: The extent to which users are willing to accept the biometric identifier in their daily lives.

For example, Retina scans may make some people uncomfortable when putting their eye really close to something that seems intrusive while photographs of the face for face recognition may appear natural.

Circumvention: ease with which the biometric system can be circumvented by fraudulent methods.

In short, a practical biometric system should have acceptable recognition accuracy and speed with reasonable resource requirements, harmless to the users, accepted by the intended population and sufficiently robust to various fraudulent methods.

Although a number of biometric traits are in use in numerous applications, each biometric trait has its own strengths and weaknesses. The choice is usually dependent on the application because no single trait is expected to effectively meet the requirements of all the applications.

UNIT 2- FINGERPRINT TECHNOLOGY

TOPIC: History of Fingerprint Pattern Recognition

Objective:

To study about the history of fingerprint pattern recognition

Description:

Why Fingerprint Identification?

Fingerprint History:

- Prehistoric picture writing of a hand with ridge patterns was discovered in Nova Scotia. In ancient Babylon, fingerprints were used on clay tablets for business transactions. In ancient China, thumb prints were found on clay seals.
- In 14th century Persia, various official government papers had fingerprints (impressions), and one government official, a doctor, observed that no two fingerprints were exactly alike.
- In 1891, Juan Vucetich, an Argentine Police Official, began the first fingerprint files based on Galton pattern types. At first, Vucetich included the Bertillon system with the files. (see Bertillon below) In 1892, Juan Vucetich made the first criminal fingerprint identification. He was able to identify a woman by the name of Rojas, who had murdered her two sons, and cut her own throat in an attempt to place blame on another.
- Her print was left on a door post, proving her identity as the murderer.

History:

1901- Introduction of fingerprints for criminal identification in England and Wales, using Galton's observations and revised by Sir Edward Richard Henry. Thus began the Henry Classification System, used even today in all English speaking countries.

1902 - First systematic use of fingerprints in the U.S. by the New York Civil Service Commission for testing. Dr. Henry P. Deforest pioneers U.S. fingerprinting.

1903- The New York State Prison system began the first systematic use of fingerprints in U.S. for criminals.

1904 - The use of fingerprints began in Leavenworth Federal Penitentiary in Kansas, and the St. Louis Police Department. They were assisted by a Sergeant from Scotland Yard who had been on duty at the St. Louis Exposition guarding the British Display.

1905 - 1905 saw the use of fingerprints for the U.S. Army. Two years later the U.S. Navy started, and was joined the next year by the Marine Corp.

During the next 25 years more and more law enforcement agencies join in the use of fingerprints as a means of personal identification.

Many of these agencies began sending copies of their fingerprint cards to the National Bureau of Criminal Identification, which was established by the International Association of Police Chiefs.

1918 - It was in 1918 when Edmond Locard wrote that if 12 points (Galton's Details) were the same between two fingerprints, it would suffice as a positive identification. This is where the often quoted (12 points) originated.

Be aware though, there is "NO" required number of points necessary for an identification. Some countries have set their own standards which do include a minimum number of points, but not in the United States.

1924 - In 1924, an act of congress established the Identification Division of the F.B.I.. The National Bureau and Leavenworth consolidated to form the nucleus of the F.B.I. fingerprint files.

1946- By 1946, the F.B.I. had processed 100 million fingerprint cards in manually maintained files; and by 1971, 200 million cards.

With the introduction of AFIS technology, the files were split into computerized criminal files and manually maintained civil files.

Many of the manual files were duplicates though, the records actually represented somewhere in the neighborhood of 25 to 30 million criminals, and an unknown number of individuals in the civil files.

1999- By 1999, the FBI had planned to stop using paper fingerprint cards (at least for the newly arriving civil fingerprints) inside their new Integrated AFIS (IAFIS) site at Clarksburg, WV. IAFIS will initially have individual computerized fingerprint records for approximately 33 million criminals.

2002- Currently now in 2002, paper fingerprint cards are still in use and being processed for all identification purposes.

TOPIC 2: GENERAL DESCRIPTION OF FINGERPRINTS

Objective:

To study about the general description of fingerprints

Description:

It is the most known and used biometrics solution to authenticate people on biometric systems. The reasons for it being so popular are there are ten available sources of biometric and ease of acquisition.

Every person has a unique fingerprint which is composed of ridges, grooves, and direction of the lines. There are three basic patterns of ridges namely, arch, loop, and whorl. The uniqueness of fingerprint is determined by these features as well as minutiae features such as bifurcation and spots (ridge endings).

General Description of Fingerprints

The general classification of fingerprints used today came from the work of Sir Edward Henry, who published his book, Classification and Use of Fingerprints, in 1900. This work forms the basis for modern-day fingerprint forensics. Fingerprints are identified by both macro and micro features. The macro features of a fingerprint include:

- Ridge patterns
- Ridge pattern area
- Core point
- Delta point
- Type lines
- Ridge count

The micro features of a fingerprint are made up of minutia points. Minutia points are classified by:

- Type
- Orientation
- Spatial frequency
- Curvature
- Position

Let's examine the macro features, then the micro features of a fingerprint.

- **Macro Fingerprint Features**

  Macro fingerprint features are, as the name implies, large in size (Figure 1.1). In general, a feature is considered macro if it can be seen unaided by the human eye. The most visible macro feature seen is the ridge pattern. Others can be seen if the print has good ridge/valley definition, the lighting is good, and your eyesight is excellent!

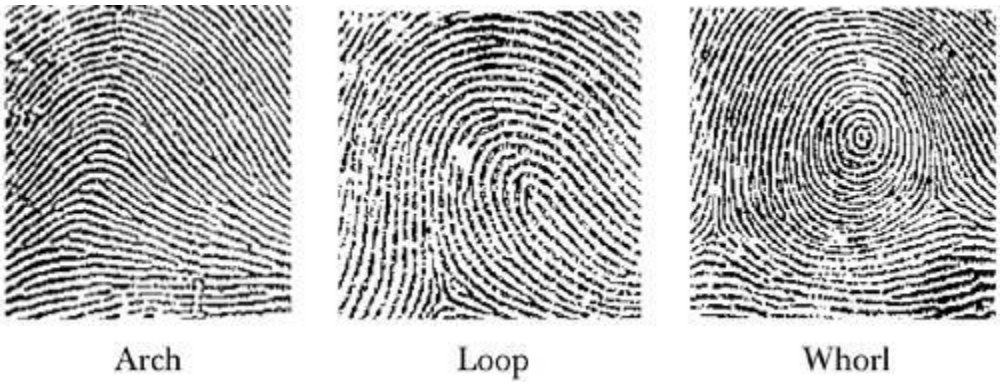


Fig 1.1

Ridge patterns

- Arch" Arches account for approximately 5% of the ridge pattern in a given population. Arches are different from loops in that arches are more open curves. Arches can also form a subgroup called tented arches. In a tented arch, the arch angle is much more obtuse than in a normal arch.
- Loop" Loops account for approximately 60% of the ridge patterns in a given population. Loops may slant left or right, or be presented as a double loop. A double loop has both a left and right loop, conforming to each other's outline.
- Whorl" Whorls account for approximately 35% of the ridge patterns in a given population. Whorls are defined by at least one ridge making a complete circle.

Ridge pattern area

The ridge pattern area is the area in the print where all the macro features are found (Figure 1.2). It is normally defined by diverging ridge flows that form a delta

Fig 1.2

Core point

The core point is found at the center of the finger image (Figure 1.3). It may or may not correspond to the center of the ridge pattern area. It is used as a reference point for measuring other minutia and also during classification. Classification is the organizing of prints based on their ridge pattern

Fig 1.3

Delta point

"The Delta is the point on the first ridge bifurcation, abrupt ending ridge, meeting of two ridges, dot, fragmentary ridge, or any point upon a ridge at or nearest the center of divergence of two type lines, located at or directly in front of their point of divergence. It is a definite fixed point used to facilitate ridge counting and tracing." In Figure 1.4, the delta point has been magnified

Fig 1.4

Type lines

Type lines are the two parallel innermost ridges that define the ridge pattern area. In Figure 1.5, the type lines are the two slightly darker ridge lines in the enlarged section.

Fig 1.5

Ridge count

Ridge count is the number of ridges that intersect a line drawn from a delta to the core. There could be more than one ridge count for each finger image. For each delta in the finger image, there will be a corresponding ridge count between it and the core. In Figure 1.6, the ridge count from the delta to the core is 12 ridges.

Fig 1.6

Micro Fingerprint Features

As the name implies, micro fingerprint features cannot be seen unaided by the human eye. A number of the current fingerprint scanners on the market now have a high enough resolution that pores can be counted. What follows is a description of the minutia that make up the micro features:

- Type
- Orientation
- Spatial frequency
- Curvature
- Position

Type

There are a number of different types of minutia; the common ones are:

- Ridge ending
- Ridge bifurcation
- Ridge divergence
- Dot or island
- Enclosure or lake
- Short ridge

Ridge ending

A ridge ending is a gap in a ridge or a point where a ridge suddenly stops (Figure 1.7).

Fig 1.7

Ridge bifurcation

A ridge bifurcation occurs when a ridge splits into two or more new ridges (Figure 1.8).

Ridge divergence

A ridge divergence occurs when two ridges running parallel suddenly diverge in opposite directions. In Figure 1.9, the two ridges diverge at the point where another ridge has a bifurcation.

Fig 1.8

Fig 1.9

Dot or island

A dot or island occurs when a ridge is short enough to be perceived as a single point (dot) or straight line (island). In Figure 1.10, we can see a group of three dots or islands.

Enclosure or lake

An enclosure (lake) minutia occurs when a ridge bifurcates and then rejoins itself. This then leaves a valley surrounded by the rejoined ridge. In Figure 1.11, the ridge has created two enclosures.

Fig 1.10

Fig 1.11

Short ridge

A short ridge is a ridge of short length, but not so short as to be considered an island or dot. In Figure 1.12, you can see two short ridges and two dots. Notice the short ridges have more of a linear look to them. The dots have more of a circular look to them.

Orientation

Orientation refers to the general direction in which a minutia feature appears to be moving. In Figure 1.13, both scaled areas contain bifurcations, but their orientation is different. The bifurcation in the left-hand enlarged area would have a general slope of approximately 1. The bifurcation in the right-hand enlarged area would have a general slope of -1

Fig 1.12

Fig 1.13

Spatial frequency

Spatial frequency can be viewed as the density of ridges around a given minutia point. In Figure 1.14, the spatial frequency is higher around the island at the top right than the bifurcation at the middle left.

Curvature

Curvature is the rate of change of a ridge's direction. In the above left enlargement in Figure 1.15, the rate of change is lower, as the ridge curves are flatter. In the bottom right enlargement in Figure 5-15, the rate of change is higher, as the ridge curves are tighter.

Position

Position refers to the relative location of the minutia. References are normally made using a Euclidian grid, and having the origin either at the core point or at a delta. In Figure 1.16, the origin has been placed at the core point. The numbers at the end of each axis are at their maximum value. In our example, you can find a bifurcation at (1,-1) and a group of dots at (-1,15)

Fig 1.14

Fig 1.15

Fig 1.16

Fingerprint is one of oldest and most popular recognition technique. Fingerprint matching techniques are of three types −

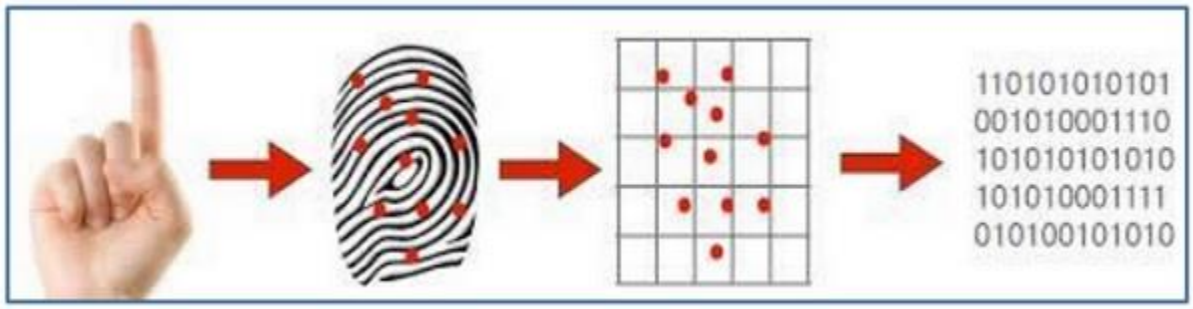
- **Minutiae Based Techniques** − In these minutiae points are found and then mapped to their relative position on finger. There are some difficulties such as if image is of low quality, then it is difficult to find minutiae points correctly. Another difficulty is, it considers local position of ridges and furrows; not global.
- **Correlation Based Method** − It uses richer gray scale information. It overcomes problems of minutiae-based method, by being able to work with bad quality data. But it has some of its own problems like localization of points.

- **Pattern Based (Image Based) Matching** − Pattern based algorithms compare the basic fingerprint patterns (arch, whorl, and loop) between a stored template and a candidate fingerprint.

Applications of Finger Recognition System

- Verification of driver-license authenticity.
- Checking validity of driving license.
- Border Control/Visa Issuance.
- Access control in organizations.

Diagram- Fingerprint Recognition



Merits of Finger Recognition System

- It is the most contemporary method.
- It is most economical method.
- It is highly reliable and secure.
- It works on a small template size, which speeds up the verifying process.
- It consumes less memory space.

Demerits of Finger Recognition System

- Scars, cuts or absence of finger can hinder the recognition process.
- The systems can be fooled by using artificial finger made of wax.

- It involves physical contact with the system.
- They leave the pattern of finger behind at the time of entering sample.

TOPIC3: FINGERPRINT FEATURE PROCESSING TECHNIQUES

Objective:

To study about the fingerprint feature processing techniques.

Description:

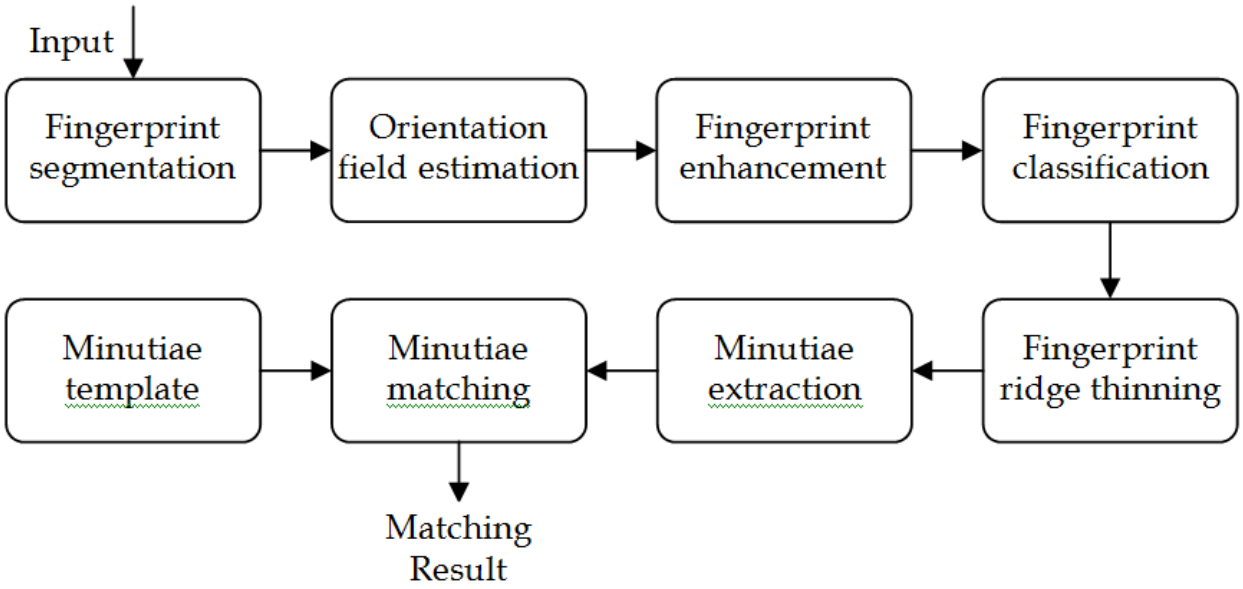
- Fingerprints are the patterns present on a finger. Fingerprint contains complex patterns of stripes, called ridges.
- There exists some gap between the ridges, called valleys. In a fingerprint, the dark lines of the image are called the ridges and the white area between the ridges is called valleys.
- A ridge can spread further in two ways, either it ends or bifurcates into two ridges. The place where ridge ends is called termination or ridge end and where it bifurcates is called bifurcation.
- Minutiae consist of these two basic types, ridge end and bifurcation. These two types of minutiae points are considered as the basic minutiae points.
- Fingerprint recognition proceeds by identifying all the minutiae points and then extracting their features and last is to match the two points.
- Fingerprint Recognition involves three main steps.
- These steps need to be followed so that accurate matching of fingerprints can be performed. These steps involves:-

1. Image Pre-processing
2. Minutiae detection and feature extraction
3. Minutiae Matching

- ✓ Pre-processing is an important step for (Fingerprint Recognition System) FRS. It enhances the quality and produces an image in which minutiae can be detected correctly.
- ✓ The final result of FRS also depends on this step.

- ✓ Minutiae detection and feature extraction step involves refining of the thinned image, detecting the minutiae points and then extracting features from image.

- ✓ The most popular technique of minutiae detection is through the use of the crossing numbers approach.
- ✓ Minutiae matching, the third step involves matching the template image with the input image.
- ✓ Template image is collected during enrolment and saved in the database.
- ✓ During recognition phase, the input image is compared against template image.
- ✓ This phase decides whether the two images are from the same finger or not.



Pre-processing

- ❖ Pre-processing helped enhancing the quality of an image by filtering and removing unnecessary noises.

- ❖ The minutiae based algorithm only worked effectively in 8-bit gray scale fingerprint image.

- ❖ A reason was that an 8-bit gray fingerprint image was a fundamental base to convert the image to 1-bit image with value 0 for ridges and value 1 for furrows.

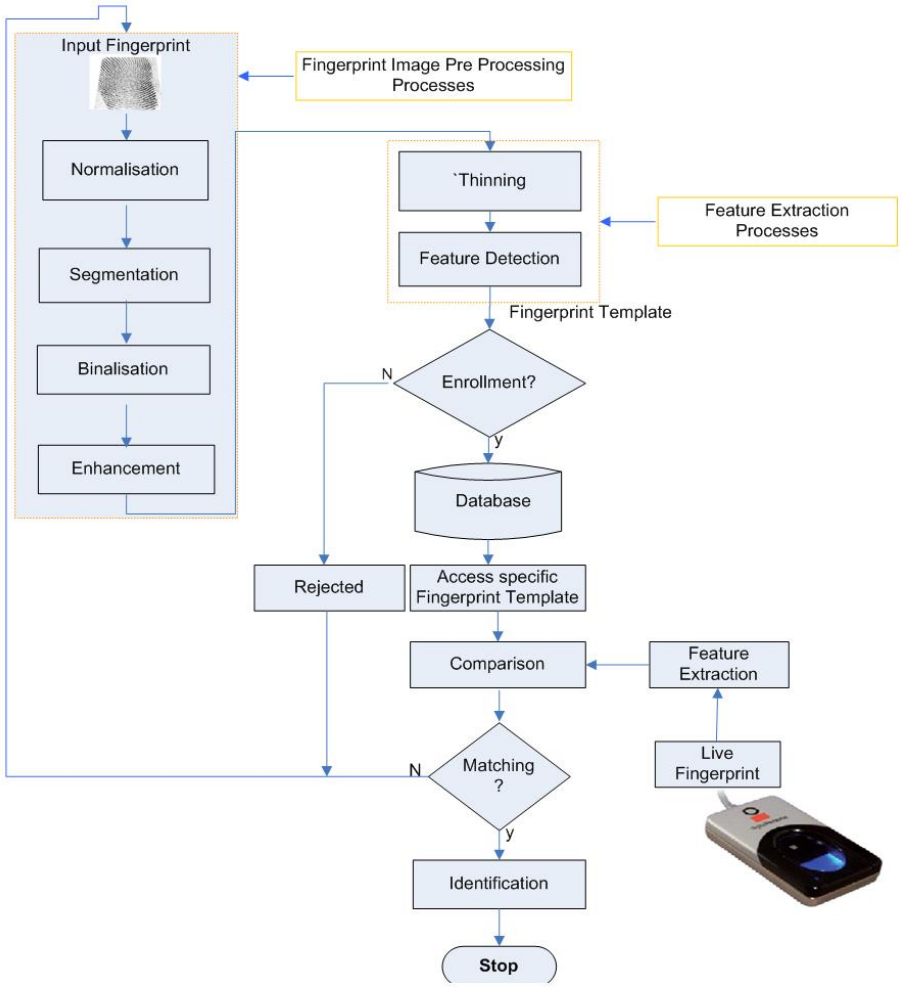
- ❖ As a result, the ridges were highlighted with black color while the furrows were highlighted with white color.
- ❖ This process partly removed some noises in an image and helped enhance the edge detection.
- ❖ Furthermore, there are two more steps to improve the best quality for the input image: minutiae extraction and false minutiae removal.
- ❖ The minutiae extraction was carried out by applying ridge thinning algorithm which was to remove redundant pixels of ridges.
- ❖ As a result, the thinned ridges of the fingerprint image are marked with a unique ID so that further operation can be conducted.
- ❖ After the minutiae extraction step, the false minutiae removal was also necessary.
- ❖ The lack of the amount of ink and the cross link among the ridges could cause false minutiae that led to inaccuracy in fingerprint recognition process.

- ✓ Minutiae-based method is the most popular approach in fingerprint matching.
- ✓ However, most existing methods need to search for the best correspondence of minutiae pairs or use reference points (core and delta points) to estimate the alignment parameters.
- ✓ The problem of lost minutiae or spurious minutiae always occurs during the minutiae detection process. Hence, the corresponding pairs or reference points may not be found under this condition. The minutiae-based fingerprint matching algorithm using phase correlation, defines a new representation called Minutiae Direction Map (MDM). First, we convert minutiae sets into 2D image spaces.
- ✓ Then the transformation parameters are calculated using phase correlation between two MDMs to align two fingerprints to be matched.
- ✓ The similarity of two fingerprints is determined by the distance between two minutiae sets. Our approach does not need to search for the corresponding minutiae pairs. Experimental results show that the proposed approach performed well in matching fingerprint minutiae sets, which greatly improved the economy of storage space.

Fingerprint Processing

The fingerprints captured for biometric use require further processing. This is not the case with those fingerprint capture for security vetting process which does not any process but saved directly into relational database together with personal details.

- Security vetting process requires the total in biometric system, input fingerprint image is processed to skeleton image levels and then features are extracted from the said thinned image.
- Biometrics fingerprint image processing (Digital image processing) stages includes fingerprint capturing, normalisation, segmentation, enhancement, thinning and minutiae extraction as shown in figure below.



Capturing

Fingerprint capturing is the process of input fingerprint image from the optical fingerprint scanner into the computer system.

Normalisation

Normalization operation acts on the input fingerprint image to standardize image pixel intensity values. In this study the research used image brightness normaliser filter (code).

Normalisation is the pre-processing stage in fingerprint template generation and is defined by variance analysis as illustrated in equation 1:

$$N(i,j) = \begin{cases} M_0 + \sqrt{\frac{v_o\,(I(i,j)-M)^2}{v_o}} & \text{if } I(i,j) > M \\ M_0 - \sqrt{\frac{v_o\,(I(i,j)-M)^2}{v_o}} & \text{otherwise} \end{cases} \quad (1)$$

Where:

M and V are the estimated mean and variance of image I (i; j), respectively, and M_0 and V_0 are the desired mean and variance values, respectively.

Segmentation

After normalisation process of fingerprint image I, the segmentation process is performed to separate foreground from the background image.

The study implemented Otsu variance threshold method which assume that the intensity values are different in different fingerprint image and thus within each region represent the corresponding object within the scene, the intensity values are similar . Threshold method was used to extract fingerprint feature from its background by assigning intensity value T (Threshold) as the function f(x,y) for each pixel P. Generally, threshold is expressed as $T = T[x, y, P(x, y), f(x, y)]$ for block Size W×W. Otsu algorithm represents grey image variance. The grey-level variance for a block of size W×W was calculated as shown in equation 2:

$$v(k) = \frac{1}{w^2} \sum_{i=0}^{w-1} \sum_{j=0}^{w-1} (I(i,j) - M(k))^2 \quad (2)$$

Where:

V (k) is the variance for block k, I (i, j) is the grey-level value at pixel (i, j), and M (k) is the mean grey-level value for the block k.

Enhancement

The configuration of parallel ridges and valleys with well-defined frequency and orientation in a fingerprint image provide useful information which helps in removing undesired noise.

Gabor filter was appropriately applied because it has both frequency-selective and orientation-selective properties and have optimal joint resolution in both spatial and frequency domains.

Therefore, it was appropriate to use Gabor filters as band pass filters to remove the noise and preserve true ridge and valley structures .

Binarization

Binarization is the final stage in fingerprint pre-processing stages. It converts a grey level image into a binary image by improving the contrast between the ridges and valleys in a fingerprint image, and consequently facilitates the extraction of Minutiae. Let image I (x, y) represent the intensity value of enhanced grayscale image at pixel position (x, y). Let Tp be the threshold value. In case of fingerprint images Tp represents the imbalance in intensity between the back-ground pixels and ridge pixels. BW(x, y) rep-resent the binary image obtained. BW(x, y) is represented in equation 3 below:

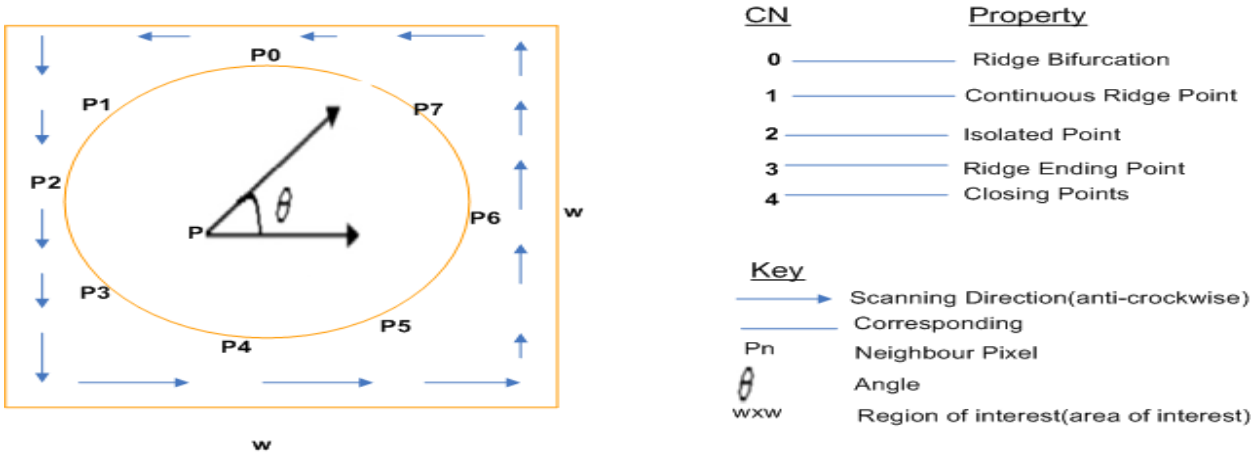
$$BW(x,y) = \begin{cases} 1, & if\ I(x,y) \geq Tp \\ 0, & Otherwise \end{cases} \quad (3)$$

Where:

Pi is the pixel value in neighbourhood of P. The eight neighbourhood pixels are scanned anti-clockwise [11]. The results are shown in figure below.

P_4	P_3	P_2
P_5	P	P_1
P_6	P_7	P_8

The CN for ridge pixel is computed and classified according to the corresponding property value. Ridge pixel values are then classified as ridge ending, crossover, bifurcation, isolated points and crossing points as illustrated in the figure 6.



Enrolment Stage

During enrolment stage, biometric data are obtained, linked with identity, and encoded for storage, retrieval and matching. Fingerprint scanner is used to collect data and verify identities

Identification

Identification is conducted to verify the live scanned fingerprint of an individual from that stored on the database table. The matching algorithm compares a current fingerprint image against the previous enrolled print, checking whether they come from the same finger.

Database Operations

Business logic also contained database operation which is sometimes refers to relational operation. Database procedure or operations is a collection of database tasks defined by end users or application code, for example, a batch job or Extraction algorithm, Transformation, and Loading (ETL) processing. The basic database operation includes insert, update, delete and

search operations were implemented in the study. Other relational database operators employed include Union, Selection and append.

Topic 4: Fingerprint Enhancement:

The basic reason behind the use of fingerprint biometric is that it is the most proven technique to identify the individual. The fingerprint is basically the combination of ridges and valleys on the surface of the finger. The important steps involved in fingerprint recognition using minutiae matching approach are:

1. Image Enhancement

2. Minutiae Extraction

3. Minutiae Matching

1 Image Enhancement

A fingerprint image is corrupted by various kind of noise such as creases, smudges and holes. It is impossible to recover the true ridge/valley structures in the unrecoverable regions; any effort to improve the quality of the fingerprint image in these regions is futile.

Therefore, the reasonable enhancement algorithm is used to improve the clarity of ridges/valley structures of fingerprint images in recoverable regions and to mask out the unrecoverable regions.

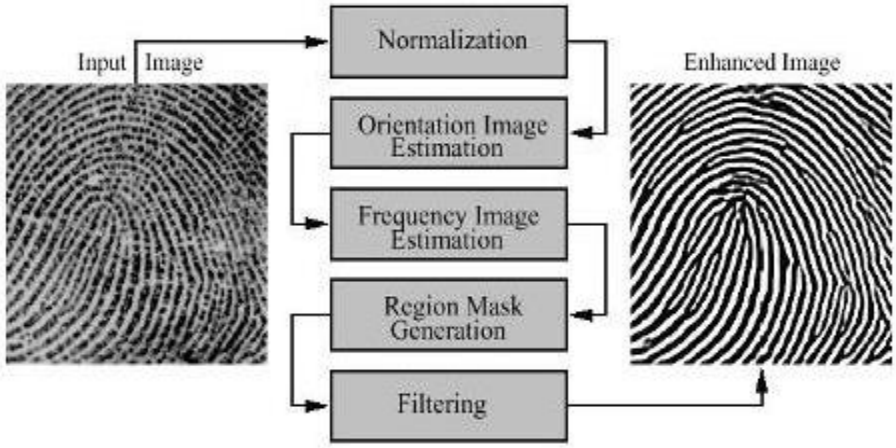


Figure 1 Different Steps of Image Enhancement

Te main steps of the algorithm include (shown in Figure 1):

1) Normalization: An input fingerprint image is normalized so that it has a pre-specified mean and variance.

2) Local orientation estimation: The orientation image is estimated from the normalized input fingerprint image.

3) Local frequency estimation: The frequency image is computed from the normalized input fingerprint image and the estimated orientation image.

4) Region mask estimation: The region mask is obtained by classifying each block in the normalized input fingerprint image into a recoverable or unrecoverable block.

5) Filtering: A bank of Gabor filters which is tuned to local ridge orientation and ridge frequency is applied to the ridge-and-valley pixels in the normalized input fingerprint image to obtain an enhanced fingerprint image.

2 Minutiae Extraction

- The enhanced fingerprint image is binarized and submitted to the thinning algorithm which reduces the ridge thickness to one pixel wide.
- The skeleton image is used to extract minutiae points which are the points of ridge endings and bifurcations.
- The most commonly employed method of minutiae extraction is the Crossing Number (CN) concept.
- This method involves the use of the skeleton image where the ridge flow pattern is eight-connected.
- The minutiae are extracted by scanning the local neighborhood of each ridge pixel in the image using a 3x3 window.
- The CN value is then computed, which is defined as half the sum of the differences between pairs of adjacent pixels in the eight-neighborhood. Using the properties of the CN the ridge pixel can then be classified as a ridge ending, bifurcation or non-minutiae point.
- For example, a ridge pixel with a CN of one corresponds to a ridge ending, and a CN of three corresponds to a bifurcation.

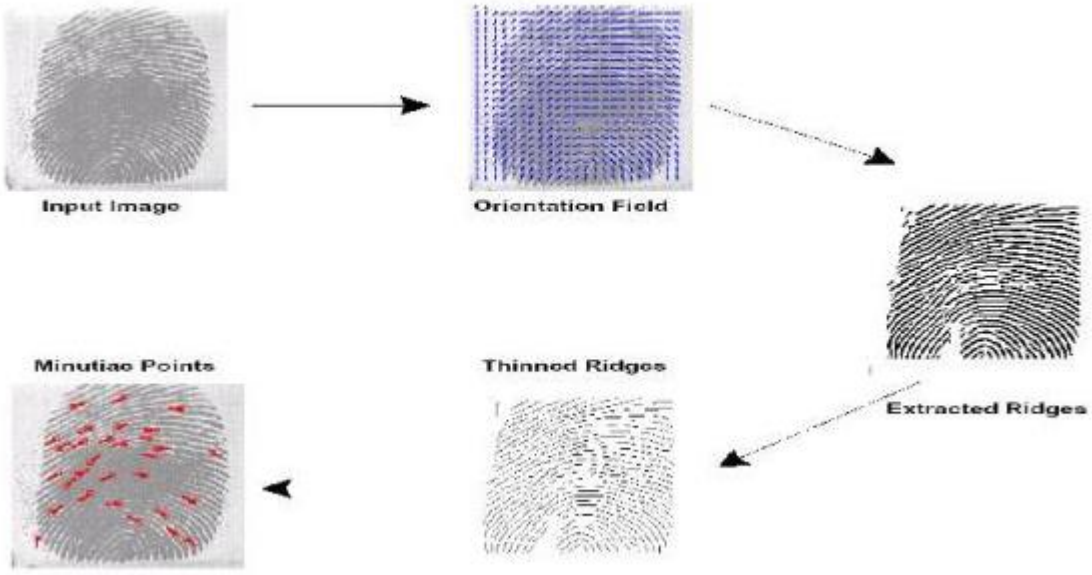


Figure 2 Steps involved in Minutiae Matching

Matching

Minutiae is extracted from the database and query fingerprints and then stored as points in the two dimensional plane. In minutia based matching, the idea is to find the alignment between the template and the input minutiae sets with the maximum number of minutiae pairings.

Strengths of fingerprint recognition

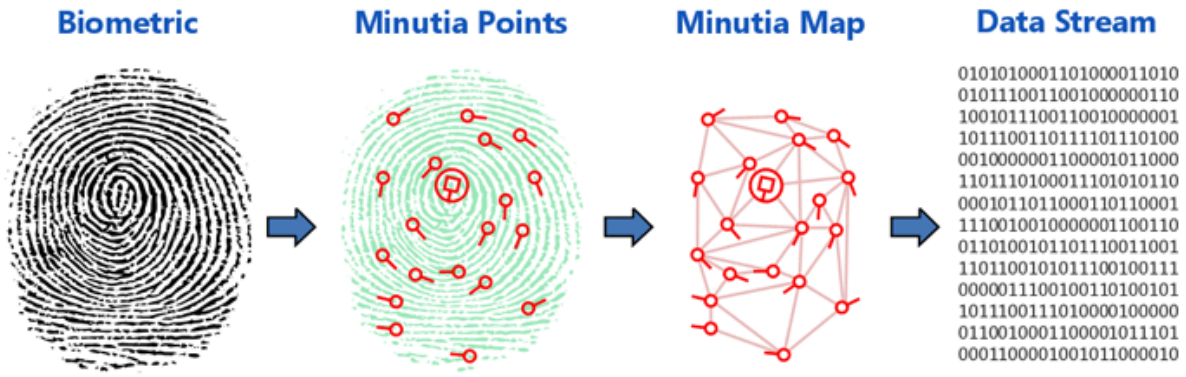
1. Fingerprint recognition is a widely accepted biometric modality and is excellent for background checks. It has found numerous applications in the areas of law enforcement and government forensics such as the AFIS database.
2. For populations that have a low incidence of "outliers", fingerprint biometric has a relatively low false rejection rate and false acceptance rate. This however may not be the case for large groups or groups that have race and gender variations.
3. Fingerprint solutions are provided by a wide range of vendors.
4. Fingerprint technology has the ability to enroll multiple fingers

TOPIC: FINGERPRINT FEATURE EXTRACTION

DESCRIPTION

How Biometric Matching Works

- Biometric matching uses templates to convert an image of a biometric trait, such as a fingerprint or iris image, into a searchable set of data. This process is known as the minutia extraction process.
- For a fingerprint image, points of interest–such as where fingerprint ridges end, converge, or split–are marked by an algorithm or human fingerprint examiner.
- These points are then mapped in relation to the center of the fingerprint. The resulting map of minutia points is simply a set of coordinates that computers can quickly search using matching algorithms that return scores that indicate how closely sets of data match.
- If the score is above an established threshold, the fingerprints are determined to be from the same finger.



Fingerprint matching is the last step in Automatic Fingerprint Identification System (AFIS). Fingerprint matching techniques can be classified into three types:

- Correlation-based matching,
- Minutiae-based matching, and
- Non-Minutiae feature-based matching.

Minutiae-based matching is the most popular and widely used technique, being the basis of the fingerprint comparison.

Proposed matching algorithm

Any Fingerprint Identification System (FIS) has two phases, fingerprint enrolment and fingerprint matching (identification or verification).

Enrolment phase

Above shows the steps of the enrolment phase of the proposed matching algorithm, which is divided into the following steps:

1. Get the core point location of the fingerprint to be enrolled after applying enhancement process.
2. Extract all minutiae from the fingerprint image.
3. From output data of step2, get the minutiae locations (x, y coordinates) together with their type: type1 for termination minutiae and type2 for bifurcation minutiae.

1. Construct tracks of 10 pixels wide centred at the core point.
2. In each track, count the number of minutiae of type 1 and the number of minutiae of type 2.
3. Construct a table of two columns, column 1 for type1 minutiae and column 2 for type2 minutiae, having number of rows equal to number of found tracks.
4. In the first row, record the number of minutiae of type 1 found in the first track in the first column, and the number of minutiae of type 2 found in the first track in the second column.
5. Repeat step 7 for the remaining tracks of the fingerprint, and then store the table in the database.

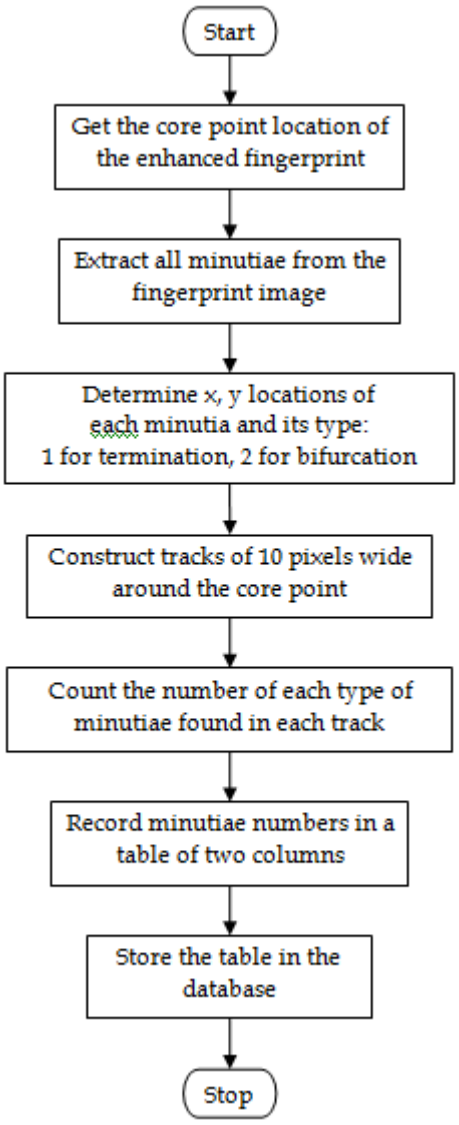
This enrolment phase will be repeated for all prints of the same user's fingerprint. The number of prints depends on the application requirements at which the user registration takes place., there

are 8 prints for each fingerprint. So, eight enrolments will be required for each user to be registered in the application. Finally, eight tables will be available in the database for each user.

Verification phase

For authenticating a user, verification phase should be applied on the user's fingerprint to be verified at the application. Fig. below shows the steps of the verification phase of the proposed matching algorithm, which is divided into the following steps:

1. Capture the fingerprint of the user to be verified.
2. Apply the steps of enrolment phase, described in section 3.1, on the captured fingerprint to obtain its minutiae table T.
3. Get all the minutiae tables corresponding to the different prints of the claimed fingerprint from the database.
4. Get the absolute differences, cell by cell, between minutiae table T and all minutiae tables of the claimed fingerprint taken from the database, now we have eight difference tables.
5. Get the summations of all cells in each of column 1 (type 1) and column 2 (type2) for each difference table, now we have sixteen summations.
6. Get the geometric mean of the eight summations of type1 columns (gm1), and the geometric mean of the eight summations of type 2 columns (gm2).
7. Check: if gm1<= threshold1 and gm2<=threshold2 then the user is genuine and accept him; else the user is imposter and reject him.



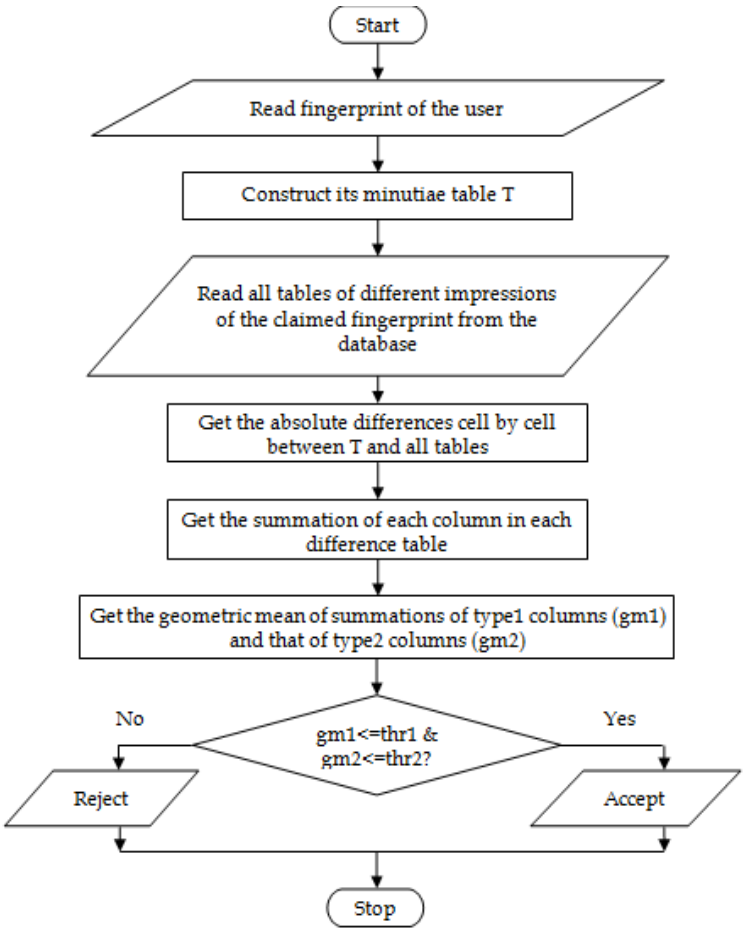
Advantages of the proposed matching algorithm

The proposed minutiae-based matching algorithm has the following advantages:

1. Since all cells in each minutiae table, representing the fingerprint in database, contain *just* the number of minutiae of type1 or type2 in each track around the core point of the fingerprint, neither position (x or y) nor orientation (θ) of the minutiae is considered; the algorithm is *rotation* and *translation invariant*.

2. The numbers of minutiae to be stored in the database *need less storage* than traditional minutiae-based matching algorithms which store position and orientation of each minutia. Experiments show that nearly 50% reduction in storage size is obtained.
3. Matching phase itself *takes less time* which, as will be shown in following sections, reaches 0.00134 sec.

4. Implementation of the proposed matching algorithm



UNIT 4

TITLE: MULTIMODAL BIOMETRICS AND PERFORMANCE EVALUATION

TOPIC 1: Voice Scan physiological biometrics

DESCRIPTION:

Voice Recognition System

Voice recognition biometric modality is a combination of both physiological and behavioral modalities. Voice recognition is nothing but sound recognition. It relies on features influenced by

- **Physiological Component** − Physical shape, size, and health of a person's vocal cord, and lips, teeth, tongue, and mouth cavity.
- **Behavioral Component** − Emotional status of the person while speaking, accents, tone, pitch, pace of talking, mumbling, etc

- Voice biometrics and voice verification systems can be used to verify a person's claimed identity or to identify a particular person
- Voice Recognition is also called Speaker Recognition. At the time of enrollment, the user needs to speak a word or phrase into a microphone. This is necessary to acquire speech sample of a candidate.
- The electrical signal from the microphone is converted into digital signal by an Analog to Digital (ADC) converter.
- It is recorded into the computer memory as a digitized sample.
- The computer then compares and attempts to match the input voice of candidate with the stored digitized voice sample and identifies the candidate.

Voice Recognition Modalities

- Voice scan measures the sound waves of human speech
- User talks to a microphone a passphrase.
- Voice print is compared to a previous one

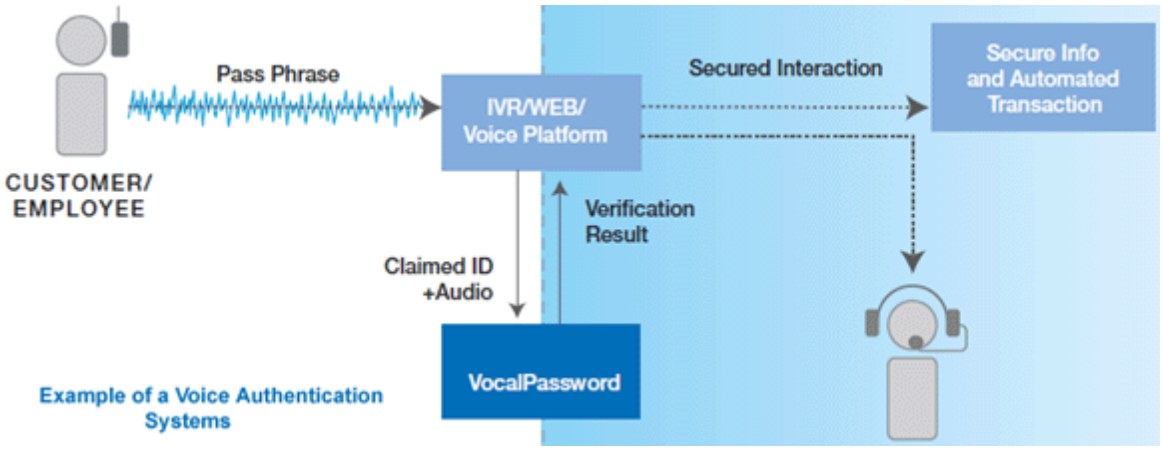
- There are two variants of voice recognition − speaker dependent and speaker independent.
- Speaker dependent voice recognition relies on the knowledge of candidate's particular voice characteristics.
- This system learns those characteristics through voice training (or enrollment).

- The system needs to be trained on the users to accustom it to a particular accent and tone before employing to recognize what was said.
- It is a good option if there is only one user going to use the system.

Speaker independent systems are able to recognize the speech from different users by restricting the contexts of the speech such as words and phrases.

These systems are used for automated telephone interfaces.

- They do not require training the system on each individual user.
- They are a good choice to be used by different individuals where it is not required to recognize each candidate’s speech characteristics.



Secured Access

Difference between Voice and Speech Recognition

Speaker recognition and Speech recognition are mistakenly taken as same; but they are different technologies. Let us see, how

Speaker Recognition (Voice Recognition)	Speech Recognition
The objective of voice recognition is to recognize WHO is speaking.	The speech recognition aims at understanding and comprehending WHAT was spoken.
It is used to identify a person by analyzing its tone, voice pitch, and accent.	It is used in hand-free computing, map, or menu navigation.

Merits of Voice Recognition

- It is easy to implement.

Demerits of Voice Recognition

- It is susceptible to quality of microphone and noise.
- The inability to control the factors affecting the input system can significantly decrease performance.
- Some speaker verification systems are also susceptible to spoofing attacks through recorded voice.

Applications of Voice Recognition

- Performing telephone and internet transactions.
- Working with Interactive Voice Response (IRV)-based banking and health systems.
- Applying audio signatures for digital documents.
- In entertainment and emergency services.
- In online education systems.

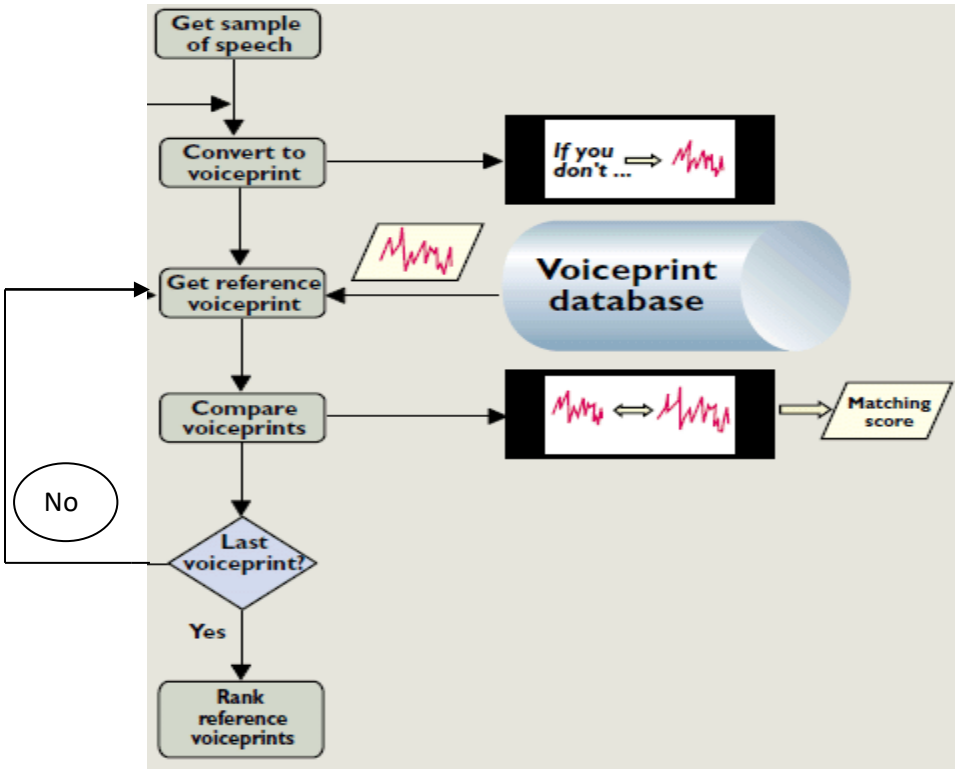
FEATURES:

- Two main factors make a voice unique, the physiological component known as the voice tract and a behavioral component known as the voice accent.

- Combining both of these makes it nearly impossible to imitate another person's voice exactly which makes the voice a great characteristic for biometric technology

- Voice recognition mainly focuses on the vocal tract since it is a unique characteristic of a physiological trait and works well in physical access control for users.
- This type of system is easy to install and requires minimal equipment that includes microphones, telephones or PC microphones.
- Because the performance of users can vary slightly, they are asked to repeat a short passphrase or a sequence of numbers or sentences so the system can analyze the voice most accurately.
- A downside is that unauthorized users can record another user's voice and run it through the verification process to gain access control to the system.
- To prevent this, a voice recognition system will ask users to repeat random phrases provided by the system during the verification phase

Outline:



TOPIC 2: Behavioral Biometrics

Description: Behavioral Modalities

- ❖ Behavioral biometrics pertains to the behavior exhibited by people or the manner in which people perform tasks such as walking, signing, and typing on the keyboard.
- ❖ Behavioral biometrics modalities have higher variations as they primarily depend on the external factors such as fatigue, mood, etc.
- ❖ This causes higher FAR and FRR as compared to solutions based on a physiological biometrics.

1. Gait Recognition

- ✓ Gait is the manner of a person's walking. People show different traits while walking such as body posture, distance between two feet while walking, swaying, etc., which help to recognize them uniquely.
- ✓ A gait recognition based on the analyzing the video images of candidate's walk. The sample of candidate's walk cycle is recorded by Video. The sample is then analyzed for position of joints such as knees and ankles, and the angles made between them while walking.
- ✓ A respective mathematical model is created for every candidate person and stored in the database. At the time of verification, this model is compared with the live sample of the candidate walk to determine its identity.

Merits of Gait Recognition System

- It is non-invasive.
- It does not need the candidate's cooperation as it can be used from a distance.
- It can be used for determining medical disorders by spotting changes in walking pattern of a person in case of Parkinson's disease.

Demerits of Gait Recognition System

- For this biometric technique, no model is developed with complete accuracy till now.

- It may not be as reliable as other established biometric techniques.

Application of Gait Recognition System

- It is well-suited for identifying criminals in the crime scenario.

2. Signature Recognition System

- ❖ In this case, more emphasis is given on the behavioral patterns in which the signature is signed than the way a signature looks in terms of graphics.
- ❖ The behavioral patterns include the changes in the timing of writing, pauses, pressure, direction of strokes, and speed during the course of signing.
- ❖ It could be easy to duplicate the graphical appearance of the signature but it is not easy to imitate the signature with the same behavior the person shows while signing.
- ❖ This technology consists of a pen and a specialized writing tablet, both connected to a computer for template comparison and verification. A high quality tablet can capture the behavioral traits such as speed, pressure, and timing while signing.

1. During enrollment phase, the candidate must sign on the writing tablet multiple times for data acquisition.
2. The signature recognition algorithms then extracts the unique features such as timing, pressure, speed, direction of strokes, important points on the path of signature, and the size of signature. The algorithm assigns different values of weights to those points.
3. At the time of identification, the candidate enters the live sample of the signature, which is compared with the signatures in the database.

Constraints of Signature Recognition System

- To acquire adequate amount of data, the signature should be small enough to fit on tablet and big enough to be able to deal with.
- The quality of the writing tablet decides the robustness of signature recognition enrollment template.

- The candidate must perform the verification processes in the same type of environment and conditions as they were at the time of enrollment. If there is a change, then the enrollment template and live sample template may differ from each other.

Merits of Signature Recognition System

- Signature recognition process has a high resistance to imposters as it is very difficult to imitate the behavior patterns associated with the signature.
- It works very well in high amount business transactions. For example, Signature recognition could be used to positively verify the business representatives involved in the transaction before any classified documents are opened and signed.
- It is a non-invasive tool.
- We all use our signature in some sort of commerce, and thus there are virtually no privacy rights issues involved.
- Even if the system is hacked and the template is stolen, it is easy to restore the template.

Demerits of Signature Recognition System

- The live sample template is prone to change with respect to the changes in behavior while signing. For example, signing with a hand held in plaster.
- User need to get accustomed of using signing tablet. Error rate is high till it happens.

Applications of Signature Recognition System

- It is used in document verification and authorization.

3. Keystroke Recognition System

During the World War II, a technique known as Fist of the Sender was used by military intelligence to determine if the Morse code was sent by enemy or ally based on the rhythm of typing. These days, keystroke dynamics the easiest biometric solution to implement in terms of hardware.

This biometric analyzes candidate's typing pattern, the rhythm, and the speed of typing on a keyboard. The **dwell time** and **flight time** measurements are used in keystroke recognition.

Dwell time − It is the duration of time for which a key is pressed.

Flight time − It is the time elapsed between releasing a key and pressing the following key.

- The candidates differ in the way they type on the keyboard as the time they take to find the right key, the flight time, and the dwelling time.
- Their speed and rhythm of typing also varies according to their level of comfort with the keyboard.
- Keystroke recognition system monitors the keyboard inputs thousands of times per second in a single attempt to identify users based on their habits of typing.

There are two types of keystroke recognition −

- **Static** − It is one time recognition at the start of interaction.
- **Continuous** − It is throughout the course of interaction.

Application of Keystroke Dynamics

- Keystroke Recognition is used for identification/verification. It is used with user ID/password as a form of **multifactor authentication**.
- It is used for surveillance. Some software solutions track keystroke behavior for each user account without end-user's knowledge. This tracking is used to analyze if the account was being shared or used by anyone else than the genuine account owner. It is used to verify if some software license is being shared.

Merits of Keystroke Recognition System

- It needs no special hardware to track this biometric.
- It is a quick and secure way of identification.
- A person typing does not have to worry about being watched.
- Users need no training for enrollment or entering their live samples.

Demerits of Keystroke Recognition System

- The candidate's typing rhythm can change between a number of days or within a day itself because of tiredness, sickness, influence of medicines or alcohol, change of keyboard, etc.
- There are no known features dedicated solely to carry out discriminating information.

TOPIC 3: INTRODUCTION TO MULTIMODAL BIOMETRIC SYSTEM

DESCRIPTION:

All the biometric systems we discussed till now were unimodal, which take single source of information for authentication. As the name depicts, multimodal biometric systems work on accepting information from two or more biometric inputs.

A multimodal biometric system increases the scope and variety of input information the system takes from the users for authentication.

Why Multimodal Biometrics is required?

The unimodal systems have to deal with various challenges such as lack of secrecy, non-universality of samples, extent of user's comfort and freedom while dealing with the system, spoofing attacks on stored data, etc.

Some of these challenges can be addressed by employing a multimodal biometric system.

There are several more reasons for its requirement, such as −

- Availability of multiple traits makes the multimodal system more reliable.
- A multimodal biometric system increases security and secrecy of user data.
- A multimodal biometric system conducts fusion strategies to combine decisions from each subsystem and then comes up with a conclusion. This makes a multimodal system more accurate.

- If any of the identifiers fail to work for known or unknown reasons, the system still can provide security by employing the other identifier.
- Multimodal systems can provide knowledge about "liveliness" of the sample being entered by applying liveliness detection techniques. This makes them capable to detect and handle spoofing.

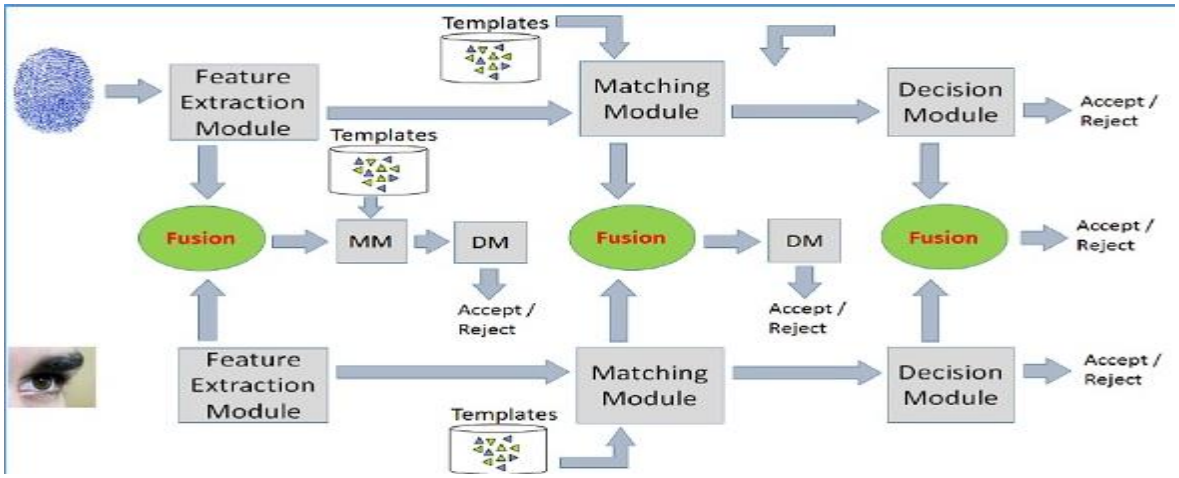
Working of Multimodal Biometric System

Multimodal biometric system has all the conventional modules a unimodal system has −

- Capturing module
- Feature extraction module
- Comparison module
- Decision making module

In addition, it has a fusion technique to integrate the information from two different authentication systems. The fusion can be done at any of the following levels −

- During feature extraction.
- During comparison of live samples with stored biometric templates.
- During decision making.



The multimodal biometric systems that integrate or fuse the information at initial stage are considered to be more effective than the systems those integrate the information at the later stages. The obvious reason to this is, the early stage contains more accurate information than the matching scores of the comparison modules.

Fusion Scenarios in Multimodal Biometric System

Within a multimodal biometric system, there can be variety in number of traits and components. They can be as follows −

- Single biometric trait, multiple sensors.
- Single biometric trait, multiple classifiers (say, minutiae-based matcher and texture-based matcher).
- Single biometric trait, multiple units (say, multiple fingers).
- Multiple biometric traits of an individual (say iris, fingerprint, etc.).

These traits are then operated upon to confirm user's identity.

Design Issues with Multimodal Biometric Systems

You need to consider a number of factors while designing a multimodal biometric system

- Level of security you need to bring in.
- The number of users who will use the system.
- Types of biometric traits you need to acquire.
- The number of biometric traits from the users.
- The level at which multiple biometric traits need integration.
- The technique to be adopted to integrate the information.
- The trade-off between development cost versus system performance.

TOPIC 4: Integration strategies

Description:

NEED FOR BIOMETRICS INTEGRATION

- Unimodal biometric systems suffer many drawbacks problem of noisy data, intra class variation, improper, User sensor adjustment, interclass similarities insufficient population coverage and spoof attacks.
- These problems lead to higher false rejection Rate (FRR) and false Acceptance Rate FAR).
- Unimodal biometric system may not be able to achieve 100% performance. Multi biometric systems are comparatively found to be more reliable due to integration of multiple, independent biometrics information.
- Moreover, they help in resolving various problems encountered by Unimodal biometric systems. They indexing or filtering of large biometric databases and are robust to noise, provide universal coverage and improve matching accuracy.
- Further, when two or more modalities are used for authentication, it becomes difficult to spoof the biometric system.
- Experiments have shown that the accuracy of multimodality can reach 100% and its performance is far better than Unimodal identification

INTEGRATIONLEVEL'S

Information integration in a multi biometric system can be done at four different levels

A. Integration at feature extraction level:

- Feature sets extracted from biometric traits are integrated and the combined feature vector thus obtained is passed to the matching module.

B Image level integration

- Each image representation in bit form is integrated to obtain a single bit sequence representing the final image

C.Matching score level

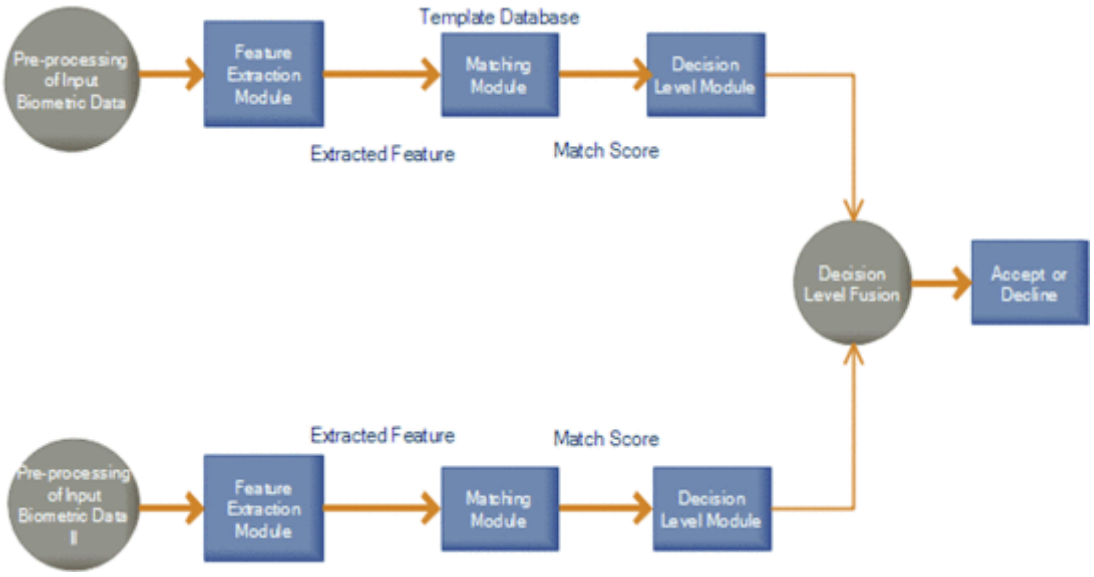
- Matching score values, representing the similarities between biometric information obtained and the already stored biometric templates for each modality are combined.
- Applying fusion at this level is preferred as it is easy to obtain and combine matching scores.

D. Decision level

- Separate authentication process is carried out for each biometric modality and the decisions taken by individual systems are integrated to obtain the final result.
- Integration at this level is supposed to be rigid because of availability of limited information.

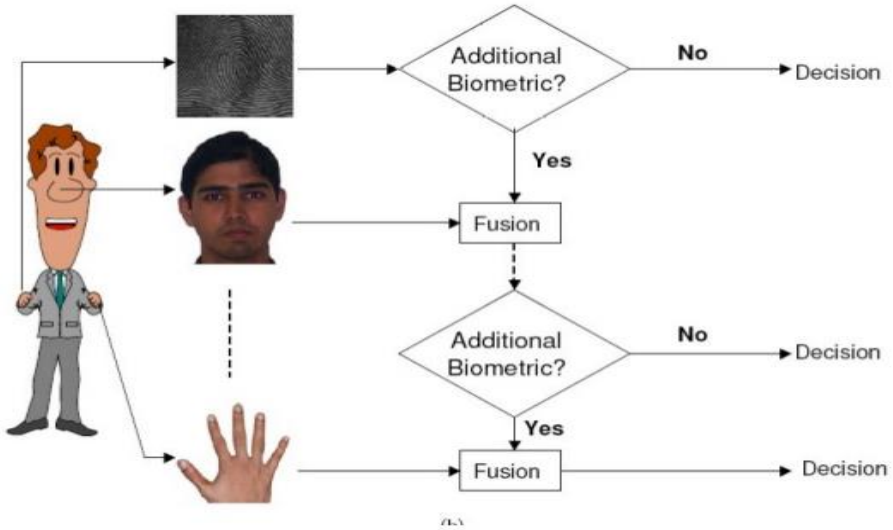
- Integrating information at an early stage is believed to be more effective since the feature set contains more information about the input data.
- An effective fusion scheme is the key to a successful multi biometric system. Fusion rules must be chosen according to the type of application, biometric traits to be used and the level of fusion.
- Different matching algorithms and several rules are then applied to the Information obtained for reaching at a decision.

TOPIC 5: Architecture of Multimodal biometrics

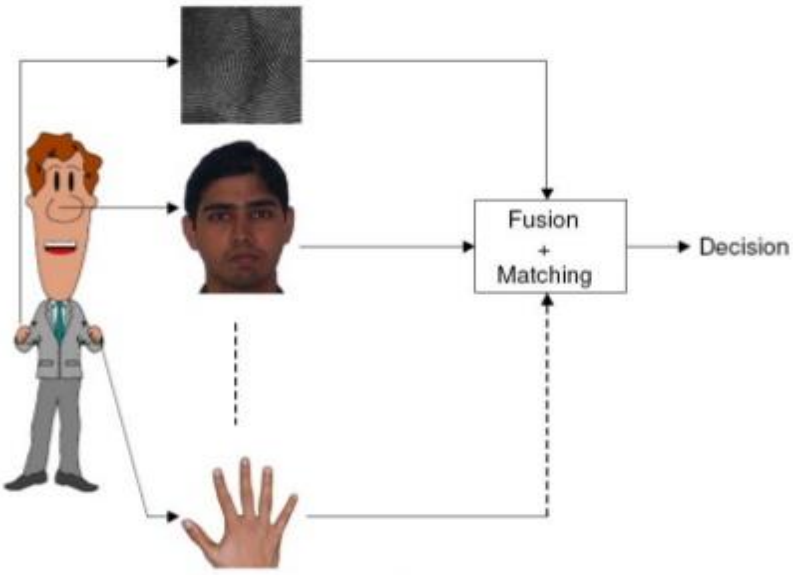


Architecture

- Architecture of a multimodal biometric system refers to the sequence in which the multiple cues are acquired and processed.
- Two types
  1) serial
  2)parallel
- Serial Architecture: In the serial or cascade architecture, the processing of the modalities takes place sequentially and the outcome of one modality affects the processing of the subsequent modalities. Ex: bank ATMs
- Parallel Architecture :In the parallel design, different modalities operate independently and their results are combined using an appropriate fusion scheme. Ex: in military



Serial



Parallel Architecture

TOPIC 6: LEVEL OF FUSION

Levels of fusion

- Broadly categorized into 2 types
  - a) **fusion prior to matching**
  - b) **fusion after matching**
- In Fusion prior to matching integration of information can take place either at the sensor level or at the feature level.
- Sensor level:: Sensor level fusion can be done only if the multiple cues are either instances of the same biometric trait obtained from multiple compatible sensors or multiple instances of the same biometric trait obtained using a single sensor,ex: 3D model of face.
- In sensor level fusion, the multiple cues must be compatible and the correspondences between points in the data must be known in advance.
- It may not be possible to integrate face images obtained from cameras with different resolutions

- Feature level: When the feature vectors are homogeneous (e.g., multiple fingerprint impressions of a user's finger), a single resultant feature vector can be calculated as a weighted average of the individual feature vectors.
- When the feature vectors are non-homogeneous (e.g., feature vectors of different biometric modalities like face and hand geometry), we can concatenate them to form a single feature vector. features vectors must be compatible.
- Integration at the feature level is difficult to achieve in practice because of the following reasons:

  (i) The relationship between the feature spaces of different biometric systems may not be known.

  (ii) Concatenating two feature vectors may result in a feature vector with very large dimensionality leading to the 'curse of dimensionality' problem.

- **Fusion after matching**: categories into

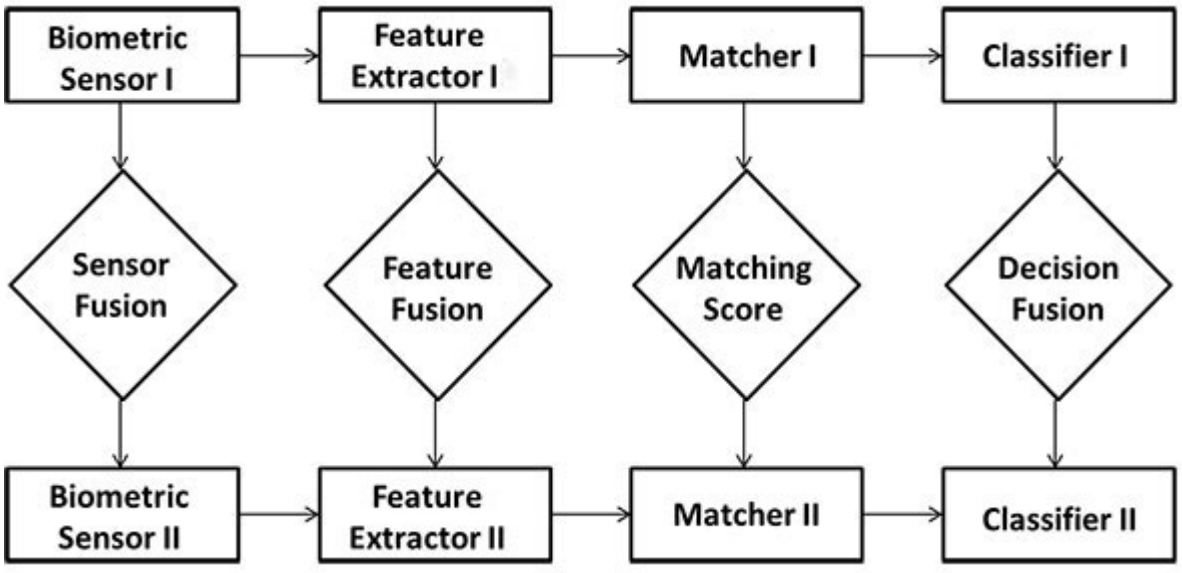
1) Dynamic classifier selection scheme: chooses the results of that classifier which is most likely to give the correct decision for the specific input pattern.

2)Abstract or decision level: can take place when each biometric matcher individually decides on the best match based on the input presented to it. Methods like **majority voting**,**And** rule **Or** rule can be used to arrive at the final decision.

3)Rank level:When the output of each biometric matcher is a subset of possible matches sorted in decreasing order of confidence, the fusion can be done at the *rank level*.so rank is assigned from highest to lowest level.

Fusion in multimodal biometric systems

- We use more than one biometric modality in multimodal biometric systems and hence we have more than one decision channels.
- Thus arises the need to design a mechanism which can combine the classification outcome from each biometric channel and this mechanism is known as biometric fusion.
- This fusion combines the measurements from different biometric attributes to enhance the strengths and decrease the weaknesses of the individual measurements.
- Fusion can be used to address a number of issues faced in implementation of biometric systems such as accuracy, efficiency, robustness, applicability and universality.
- There are various levels of fusing the biometric traits which can be used to increase robustness of the multimodal biometric system.
- They are sensor level fusion, feature level fusion, matching score level fusion and decision level fusion.



Sensor level fusion

- In sensor level fusion, we fuse the biometric traits coming from different sensors such as fingerprint scanner, iris scanner, video camera etc. to form a merged biometric trait and process.

Feature level fusion

- In feature level fusion, signals coming from different biometric channels are first processed after which the feature vectors are extracted separately from each biometric trait.
- The feature vectors are then combined to form a composite feature vector using a specific fusion algorithm and then used for further classification.
- In feature level fusion, some reduction techniques need to be used in order to select only the useful features.
- Features contain richer information of biometric traits as compared to matching score or decision of matcher and thus fusion at the feature level provides better recognition results.
- It has also been observed that feature level fusion provides more accuracy when the features of different biometric modalities are compatible with each other.

Matching score level fusion

- In this fusion level, the feature vectors are processed separately rather than combining them. Then an individual matching score is found and based on the accuracy of each biometric channel, we then fuse the matching level to find a composite matching score which will be used for classification.
- We can use various techniques such as logistic regression, highest rank, Bayes rule, mean fusion etc. to combine match scores.
- In addition to this, another important aspect of this fusion is the normalization of scores acquired from different modalities.
- We can use techniques such as Min-max, z-score, piecewise linear etc. to achieve normalization of the match scores. Matching score level fusion has lesser complexity than the other fusion levels and hence it is widely used.

Decision level fusion

- In decision level fusion, each biometric trait is first pre-classified separately.
- The individual biometric trait is first captured and then features are extracted from the captured trait. The traits are classified as either accept or reject based on these extracted features.

- The final classification is obtained by combining the outputs of different modalities.

Topic 7: Performance evaluation

Description

Criteria for Effective Biometric System

There are seven basic criteria for measuring effectiveness of a biometric system −

- **Uniqueness** − It determines how uniquely a biometric system can recognize a user from a group of users. It is a primary criterion.
- **Universality** − It indicates requirement for unique characteristics of each person in the world, which cannot be reproduced. It is a secondary criterion.
- **Permanence** − It indicates that a personal trait recorded needs to be constant in the database for a certain time period.
- **Collectability** − It is the ease at which a person's trait can be acquired, measured, or processed further.
- **Performance** − It is the efficiency of system in terms of accuracy, speed, fault handling, and robustness.
- **Acceptability** − It is the user-friendliness, or how good the users accept the technology such that they are cooperative to let their biometric trait captured and assessed.
- **Circumvention** − It is the ease with which a trait is possibly imitated using an artifact or substitute.

Biometric System Performance

Biometric system manufacturers claim high system performance which is practically difficult to achieve in actual operating environments. The possible reasons are, tests conducted in controlled environment setups, limitations on hardware, etc.

For example, a voice recognition system can work efficiently only in quiet environment, a facial recognition system can work fine if lighting conditions are controlled, and candidates can be trained to clean and place their fingers properly on the fingerprint scanners.

However, in practice, such ideal conditions may not be available in the target operating environment.

Performance Measurements

The performance measurements of a biometric system are closely tied to False Reject Rate (FRR) and False Accept Rate (FAR).

FRR is also known as **Type-I error** or False Non Match Rate (FNMR) which states the likelihood of a legitimate user being rejected by the system.

FAR is referred to as **Type-II error** or False Match Rate (FMR) which states the likelihood of a false identity claim being accepted by the system.

An ideal biometric system is expected to produce zero value for both FAR and FRR. Means it should accept all genuine users and reject all fake identity claims, which is practically not achievable.

FAR and **FRR** are inversely proportional to each other. If FAR is improved, then the FRR declines. A biometric system providing **high FRR ensures high security**. If the FRR is too high, then the system requires to enter the live sample a number of times, which makes it less efficient.

The performance of current biometrics technologies is far from the ideal. Hence the system developers need to keep a good balance between these two factors depending on the security requirements.

False Acceptance Rate (FAR)

- The FAR is the frequency that a **non authorized** person is **accepted** as authorized.
- Because a false acceptance can often lead to damages, FAR is generally a security relevant measure.
- FAR is a non-stationary statistical quantity which does not only show a personal correlation, it can even be determined for each individual biometric characteristic (called personal FAR).

False Rejection Rate (FRR)

- The FRR is the frequency that an **authorized** person is **rejected** access.
- FRR is generally thought of as a comfort criteria, because a false rejection is most of all annoying.
- FRR is a non-stationary statistical quantity which does not only show a strong personal correlation, it can even be determined for each individual biometric characteristic (called personal FRR).

Failure To Enrol rate (FTE, also FER)

- The FER is the proportion of people who fail to be enrolled successfully.
- FER is a non-stationary statistical quantity which does not only show a strong personal correlation, it can even be determined for each individual biometric characteristic (called personal FER).

  Those who are enrolled yet but are mistakenly rejected after many verification/identification attempts count for the Failure To Acquire (FTA) rate.
- FTA can originate through temporarily not measurable features ("bandage", non-sufficient sensor image quality, etc.).
- The FTA usually is considered within the FRR and need not be calculated separately, see also FNMR and FMR.

False Identification Rate (FIR)

- The False Identification Rate is the probability in an identification that the biometric features are falsely assigned to a reference.
- The exact definition depends on the assignment strategy; namely, after feature comparison, often more than one reference will exceed the decision threshold.

Equal Error Rate, or EER

- It is the measure of the likelihood that the biometric security system has the FAR equal to the FRR. This is a very important measure for any biometrics system.
- The reason why this can occur will be discussed in later articles.

Topic 8: Memory Requirement and allocation

Description:

As new processors continuously improve the performance of embedded systems, the processor-memory gap widens and memory presents a major bottleneck in both storage area and energy consumption.

In this section, we will introduce a memory analysis method, and several optimization techniques are implemented based on the analysis result.

There are three kinds of memory they are;

- Fixed memory
- Stack memory
- Heap memory

➢ **Fixed address memory:**

- Executable code
- Global variables
- Constant structures that don't fit inside a machine instruction. (constant arrays, strings, floating points, long integers etc.)
- Static variables.
- Subroutine local variable in non-recursive languages (e.g. early FORTRAN).

➢ **Stack memory:**

Local variables for functions, whose size can be determined at call time.

Information saved at function call and restored at function return:

- Values of called arguments
- Register values:
  - Return address (value of PC)
  - Frame pointer (value of FP)
  - Other registers
- Static link (to be discussed)

➢ **Heap memory:**

- Structures whose size varies dynamically (e.g. variable length arrays or strings).
- Structures that are allocated dynamically (e.g. records in a linked list).
- Structures created by a function call that must survive after the call returns.

Issues:

- Allocation and free space management

- Deallocation / garbage collection

Memory Analysis Methodology:

- When a program is running, the memory module is divided into two parts: program segment and data segment, which includes a heap and a stack.
- The heap starts from the bottom of the program segment and increases when the latest reserved block is beyond its range.
- Whenever there is dynamic memory allocation, a block of memory is reserved for later use. When a memory free happens, the specific memory block is returned to the memory pool.
- On the other hand, the stack pointer position changes when a function call is executed or returned.
- Generally, the stack and the heap grow and shrink in opposite direction.
- A collision of stack and heap implies a fatal error state.
- At any particular moment, the memory usage of the system is determined by the sum of the size of program, heap and stack as shown in Equation

$$M(total) = M(program)+M(heap)+M(stack)\ldots\ldots\ldots\ldots\ldots\ldots(1)$$

By inserting the memory trace agents in the program where memory usage changes can happen, we get the position of the heap bottom and the stack pointer dynamically during the program running time.

Taking program size into consideration, a dynamic memory usage trace map is generated. From this trace map, we can get information about the overall memory requirement as well as the memory bottleneck of the application.

Topic 9: Training and Adaptability and types of algorithm

Description:

What Is Machine Learning?

- Machine learning is a core sub-area of artificial intelligence as it enables computers to get into a mode of self-learning without being explicitly programmed.
- When exposed to new data, computer programs are enabled to learn, grow, change, and develop by themselves.

- Training *set* while a *test set* and *validation set* are used for evaluating whether the discovered relationships hold. More formally, a **training set** is a set of data used to discover potentially predictive relationships.
- A **test set** is a set of data used to assess the strength and utility of a predictive relationship.
- Test and training sets are used in intelligent systems, machine learning, genetic programming and statistics.

These can be defined as:

- Training set: A set of examples used for learning, that is to fit the parameters [i.e., weights] of the classifier.
- Validation set: A set of examples used to tune the hyper parameters [i.e., architecture, not weights] of a classifier, for example to choose the number of hidden units in a neural network.
- Test set: A set of examples used only to assess the performance [generalization] of a fully-specified classifier

Types of Learning

- **Supervised (inductive) learning**
  - Training data includes desired outputs
- **Unsupervised learning**
  - Training data does not include desired outputs
- **Semi-supervised learning**
  - Training data includes a few desired outputs
- **Reinforcement learning**
  - Rewards from sequence of actions.

UNIT 5

TITLE: BIOMETRIC AUTHENTICATION

TOPIC 1: INTRODUCTION TO BIOMETRIC AUTHENTICATION

DESCRIPTION:

Biometric Authentication is any process that validates the identity of a user who wishes to sign into a system by measuring some intrinsic characteristic of that user.

Biometric samples include finger prints, retinal scans, face recognition, voice prints and even typing patterns.

- ✓ Biometric authentication is a security process that relies on the unique biological characteristics of an individual to verify that he is who is says he is.
- ✓ Biometric authentication systems compare a biometric data capture to stored, confirmed authentic data in a database.
- ✓ If both samples of the biometric data match, authentication is confirmed.
- ✓ Typically, biometric authentication is used to manage access to physical and digital resources such as buildings, rooms and computing devices

AUTHENTICATION METHODS:

- **Face recognition**

  Among the various biometric identification methods, face recognition is one of the most flexible, working even when the subject is unaware of being scanned.

  It also shows promise as a way to search through masses of people who spent only seconds in front of a "scanner" - that is, an ordinary digital camera. Face recognition systems work by systematically analyzing specific features that are common to everyone's face - the distance between the eyes, width of the nose, position of cheekbones, jaw line, chin and so forth.

  These numerical quantities are then combined in a single code that uniquely identifies each person.

- **Fingerprint identification**

  Fingerprints remain constant throughout life. In over 140 years of fingerprint comparison worldwide, no two fingerprints have ever been found to be alike, not even those of identical twins.
- Good fingerprint scanners have been installed in PDAs like the iPaq Pocket PC; so scanner technology is also easy.
- Might not work in industrial applications since it requires clean hands. Fingerprint identification involves comparing the pattern of ridges and furrows on the fingertips, as well as the minutiae points (ridge characteristics that occur when a ridge splits into two, or ends) of a specimen print with a database of prints on file.
- **Hand geometry biometrics**

  Hand geometry readers work in harsh environments, do not require clean conditions, and forms a very small dataset.
- It is not regarded as an intrusive kind of test. It is often the authentication method of choice in industrial environments.
- **Retina scan**

  There is no known way to replicate a retina. As far as anyone knows, the pattern of the blood vessels at the back of the eye is unique and stays the same for a lifetime.
- However, it requires about 15 seconds of careful concentration to take a good scan. Retina scan remains a standard in military and government installations.
- **Iris scan**

  Like a retina scan, an iris scan also provides unique biometric data that is very difficult to duplicate and remains the same for a lifetime.
- The scan is similarly difficult to make (may be difficult for children or the infirm). However, there are ways of encoding the iris scan biometric data in a way that it can be carried around securely in a "barcode" format. (See the SF in the News article Biometric Identification Finally Gets Started for some detailed information about how to perform an iris scan.)
- **Signature**

  A signature is another example of biometric data that is easy to gather and is not

physically intrusive. Digitized signatures are sometimes used, but usually have insufficient resolution to ensure authentication.

- **Voice analysis**
  Like face recognition, voice biometrics provide a way to authenticate identity without the subject's knowledge.
- It is easier to fake (using a tape recording); it is not possible to fool an analyst by imitating another person's voice.

Topic 2: Biometric authentication by fingerprint

Description:

Introduction to Fingerprint Authentication

- This type of identification technology is more reliable, secure and efficientand uses human physiological processes and behaviors to identifying users' ID.
- This biometric-security system is human-oriented system and is more accurate than the traditional password-based systems.
- This authentication is used in many of the online transactions, confidential financial dealings, industries, offices, institutes, colleges and security access control systems.

    - Fingerprints form a unique identification pattern for humans, which consist of a pattern of ridges on fingers that helps to grip things by hand.
    - Fingerprint scanner is the heart of this automated authentication system which is responsible for the acquisition of images based on the patterns of ridges and valleys of human fingers, and then matching them with the pre-stored patterns.
    - It consists of sensors that are optical, ultrasonic, thermal, capacitive, etc., but mostly optical and capacitance scanning methods are used.
    - These sensors generate top quality images of finger ridges and valleys by overriding inconsistent and irregular designs of the scanned image.
    - These scanners consist of Analog to digital converters which process the analog electric signals to produce digital representation of the image.
    - When we press the finger on a fingerprint scanner, it collects the signals, processes the image and extracts minutiae information of the finger.

- Subsequently a processing unit or host acquires this ID information and store it in a fingerprint database.

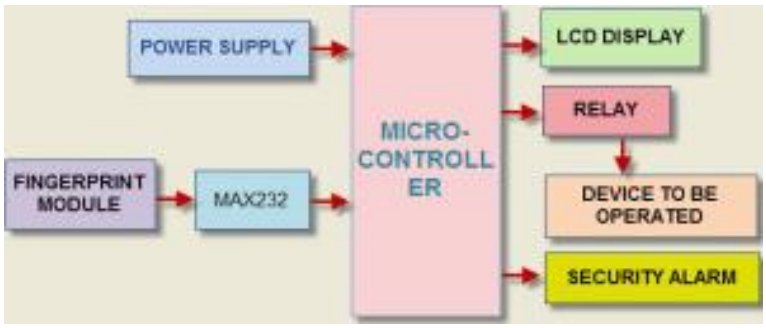
During login, the storage unit compares the pre-stored data and displays appropriate information. For image processing, the digital signal processor or PC is very expensive, but FPGA based hardware is advantageous due to its processing speed, low cost, flexibility and portability.

This type of authentication uses special algorithms to compare such fingerprint IDs for effective retrieval of information. For minimizing the power consumption, these systems often get into sleep mode and become active only during fingerprints recognizing mode.

Fingerprint Authentication and Controlling System of Devices Using Microcontroller

This type of authentication or identification system is a simple and low-cost system and can be easily implemented with the use of a basic 8051 microcontroller.

In this system, the device monitoring and control is performed at a high-level security by authenticating user fingerprints.



Block Diagram of Fingerprint Authentication and Controlling System

- ✓ The operation of this security system can be easily understood with the above block diagram that consists of power supply, a microcontroller, fingerprint, MAX232, LCD display, relay and alarm blocks.
- ✓ These blocks' operation is performed from left to right wherein the power supply block gives entire power to the circuit, and the fingerprint module gives the input

to the microcontroller, and then the microcontroller processes the data and correspondingly drives the buzzer, LCD and relay to operate the loads.

Circuit Operation

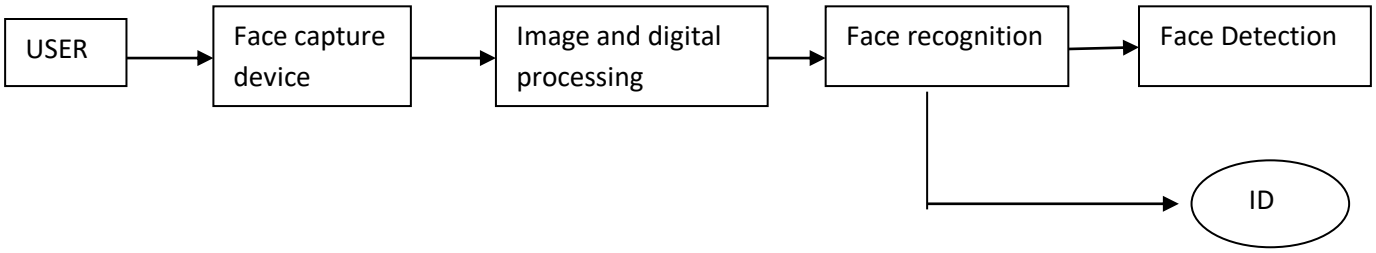
- In this circuit, for powering the entire circuit, mains AC supply at 230V is stepped down to 12V AC, rectified to DC, filtered and regulated to circuit operating range 5V. This power block is not given in the above circuit for not making a whole circuit complex.
- For required operation by user like identifying, adding and deleting finger, an appropriate switch has to be pressed. For certain button pressing, the microcontroller processes the fingerprint images.
- When a person presses the finger on fingerprint scanner, it gives high and low-logic digital signals to the microcontroller after pressing switch2. This controller is programmed in such a way that it stores the digital data.
- When the switch1 is pressed, again it ask for fingerprint scanning; if this data matches with the previously stored fingerprint data, it generates an output signal to the transistor and also displays the information on the LCD display.
- If the transistor is activated, it automatically energizes the relay coil, and thus the relay gets operated and the corresponding device is turned on. This also gives an alarm from a buzzer upon authenticating the fingerprint.
- It is also possible to delete the scanned finger by pressing the switch3, and also, if any unauthorized person tries to access the device, this system gives an alarm. This system can be implemented at homes since it is affordable to generate home alarm system.

Topic 3: Biometric Authentication by Face Recognition

Description:

1. Model

- ✓ The following figure describes an access control system base on face authentication. In this model, each user has an account and a corresponding ID in the Face Database.
- ✓ On a user logging in the system, Face Authentication will use face recognition technologies to analyze and determine his ID as well as his permissions on the system.

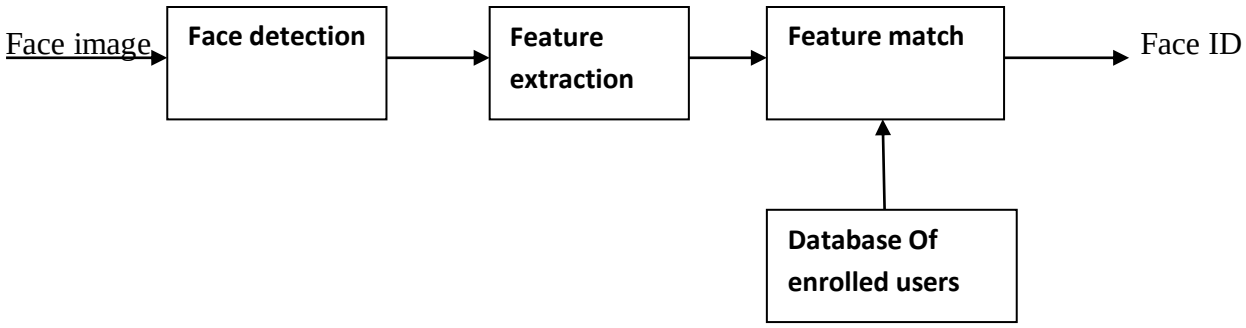


Access Control System Based on Face Authentication Model

- This model can be applied to access control systems where the number of people is small; for example, user accounts in an operating system, members of an office or a family.
- When receiving a request, an access control system based on face authentication must find out exactly whether the person requesting is a client or an impostor.
- Right after that, it decides whether to accept the login or to treat him/her as an impostor and cry out "access denial"
- In order for Face Authentication to satisfy all the security issues that an access control system asks for, the face recognition algorithms in operation must be almost completely exact

Face Recognition Model

As you can see from the diagram below, face recognition requires a wide range of technologies Face recognition systems in general, and access control systems based on face authentication in particular, use a “learning” mechanism to collect data on facial characteristics if users. Hence, the first important point to care about in a face recognition model is the Face Database storing this information



When the system finishes scanning a video or photo of a user’s face, the digitalized information will go through these following modules one after another:

- Face Detection: locating the face in the photo or video and removing unnecessary details on the background.

- Feature Extraction: extracting facial characteristics needed for recognition.

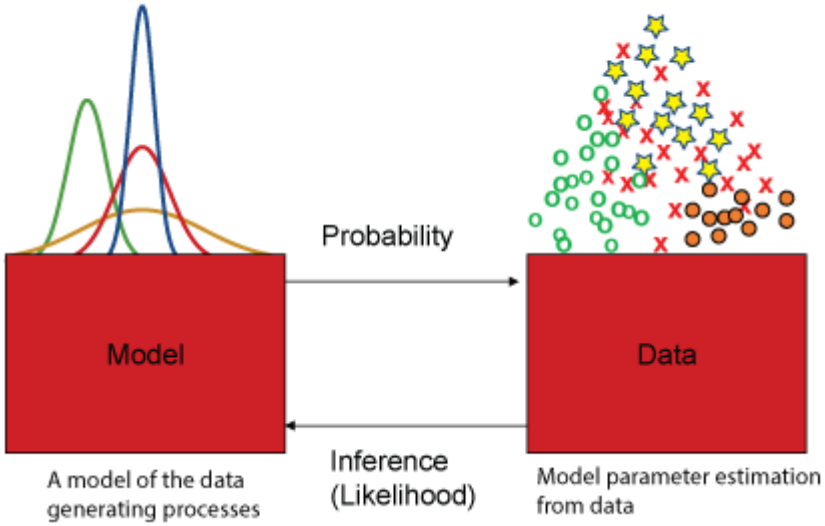
- Feature Match: comparing scanned information with database to decide if it matches some user's face. If the face matched, the ID of the corresponding is returned.

Most of present researches try to create an Automatic Face Recognition model. The hardest part of it is how to get best biometric information on the faces. Therefore, Feature Extraction is the most important module of the system. In the next section, we will focus on basic algorithms used for extracting facial characteristics

Topic4: Expectation-maximization (EM) theory

Description:

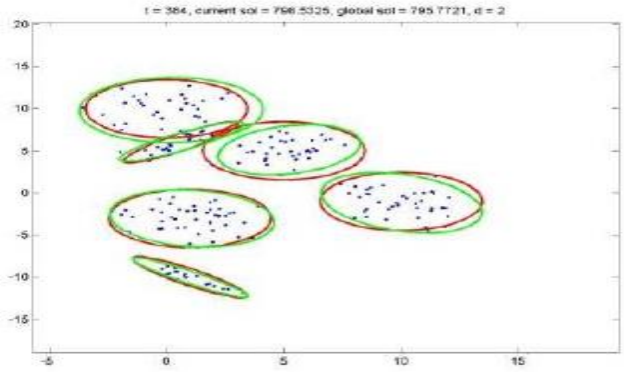
- In statistics an expectation–maximization (EM) algorithm is an iterative method to find maximum likelihood or maximum a posteriori (MAP) estimates of parameters in statistical models, where the model depends on unobserved latent variables.
- The EM iteration alternates between performing an expectation (E) step, which creates a function for the expectation of the log-likelihood evaluated using the current estimate for the parameters, and maximization (M) step, which computes parameters maximizing the expected log-likelihood found on the *E* step.
- These parameter-estimates are then used to determine the distribution of the latent variables in the next E step.



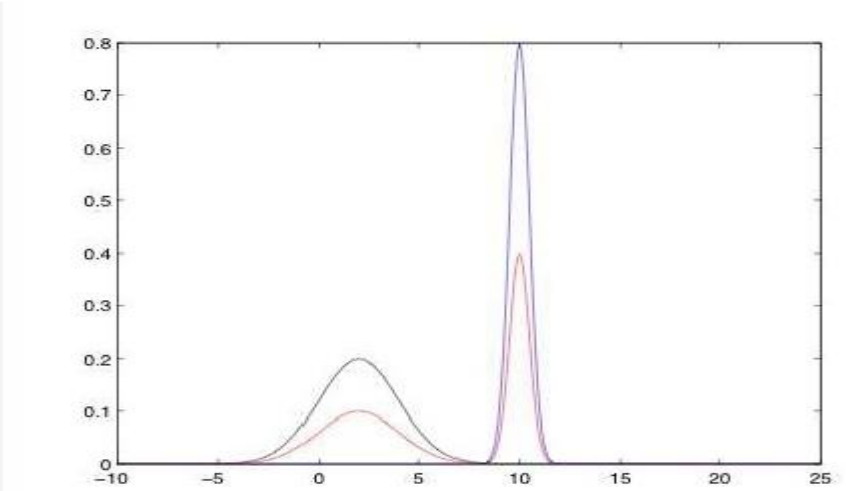
Expectation-maximization (EM) algorithm

Gaussian Mixture Models

- Rather than identifying clusters by "nearest" centroids
- Fit a Set of *k* Gaussians to the data
- Maximum Likelihood over a mixture model



GMM example



$f_0(x) = N(x; 2, 2)$ $f_1(x) = N(x; 10, .5)$

$\pi = [.5 \quad .5]^T$

Mixture Models

- Formally a Mixture Model is the weighted sum of a number of pdfs where the weights are determined by a distribution, π

$$p(x) = \pi_0 f_0(x) + \pi_1 f_1(x) + \pi_2 f_2(x) + \ldots + \pi_k f_k(x)$$

where $\sum_{i=0}^{k} \pi_i = 1$

$$\boxed{p(x) = \sum_{i=0}^{k} \pi_i f_i(x)}$$

Gaussian Mixture Models

- GMM: the weighted sum of a number of Gaussians where the weights are determined by a distribution, π

$$p(x) = \pi_0 N(x|\mu_0, \Sigma_0) + \pi_1 N(x|\mu_1, \Sigma_1) + \ldots + \pi_k N(x|\mu_k, \Sigma_k)$$

$$\text{where } \sum_{i=0}^{k} \pi_i = 1$$

$$\boxed{p(x) = \sum_{i=0}^{k} \pi_i N(x|\mu_k, \Sigma_k)}$$

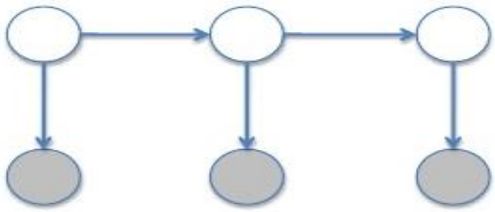
Graphical Models with unobserved variables

- What if you have variables in a Graphical model that are **never** observed?
  - Latent Variables
- Training latent variable models is an unsupervised learning application

Hidden Markov model (HMM)

Latent Variable HMMs

- We can cluster sequences using an HMM with unobserved state variables



- We will train latent variable models using Expectation Maximization

Latent Variable Representation

- We can represent a GMM involving a latent variable

$$p(x) = \sum_{i=0}^{k} \pi_i N(x|\mu_k, \Sigma_k) = \sum_z p(z)p(x|z)$$

$$p(z) = \prod_{k=1}^{K} \pi_k^{z_k} \qquad p(x|z) = \prod_{k=1}^{K} N(x|\mu_k, \Sigma_k)^{z_k}$$

- What does this give us?

Maximum Likelihood over a GMM

- As usual: Identify a likelihood function

$$\ln p(x|\pi,\mu,\Sigma) = \sum_{n=1}^{N} \ln \left\{ \sum_{k=1}^{K} \pi_k N(x_n|\mu_k,\Sigma_k) \right\}$$

- And set partials to zero…

Maximum Likelihood of a GMM

- Optimization of means.

$$\ln p(x|\pi,\mu,\Sigma) = \sum_{n=1}^{N} \ln \left\{ \sum_{k=1}^{K} \pi_k N(x_n|\mu_k,\Sigma_k) \right\}$$

$$\frac{\partial \ln p(x|\pi,\mu,\Sigma)}{\partial \mu_k} = \sum_{n=1}^{N} \frac{\pi_k N(x_n|\mu_k,\Sigma_k)}{\sum_j \pi_j N(x_n|\mu_j,\Sigma_j} \Sigma_k^{-1}(x_k - \mu_k) = 0$$

$$= \sum_{n=1}^{N} \tau(z_{nk}) \Sigma_k^{-1}(x_k - \mu_k) = 0$$

$$\boxed{\mu_k = \frac{\sum_{n=1}^{N} \tau(z_{nk}) x_n}{\sum_{n=1}^{N} \tau(z_{nk})}}$$

MLE of a GMM

$$\mu_k = \frac{\sum_{n=1}^{N} \tau(z_{nk}) x_n}{N_k}$$

$$\Sigma_k = \frac{1}{N_k} \sum_{n=1}^{N} \tau(z_{nk})(x_k - \mu_k)(x_k - \mu_k)^T$$

$$\pi_k = \frac{N_k}{N}$$

$$N_k = \sum_{n=1}^{N} \tau(z_n k)$$

EM for GMMs

- Initialize the parameters
  - Evaluate the log likelihood
- Expectation-step: Evaluate the responsibilities
- Maximization-step: Re-estimate Parameters
  - Evaluate the log likelihood
  - Check for convergence

EM for GMMs

- E-step: Evaluate the Responsibilities

$$\tau(z_{nk}) = \frac{\pi_k N(x_n|\mu_k, \Sigma_k)}{\sum_{j=1}^{K} \pi_j N(x_n|\mu_j, \Sigma_j)}$$

General form of EM

- Given a joint distribution over observed and latent variables: $p(X, Z|\theta)$
- Want to maximize: $p(X|\theta)$

1. Initialize parameters θ^{old}
2. E Step: Evaluate:

$$p(Z|X, \theta^{old})$$

3. M-Step: Re-estimate parameters (based on expectation of complete-data log likelihood)

$$\theta^{new} = \text{argmax}_\theta \sum_Z p(Z|X, \theta^{old}) \ln p(X, Z|\theta)$$

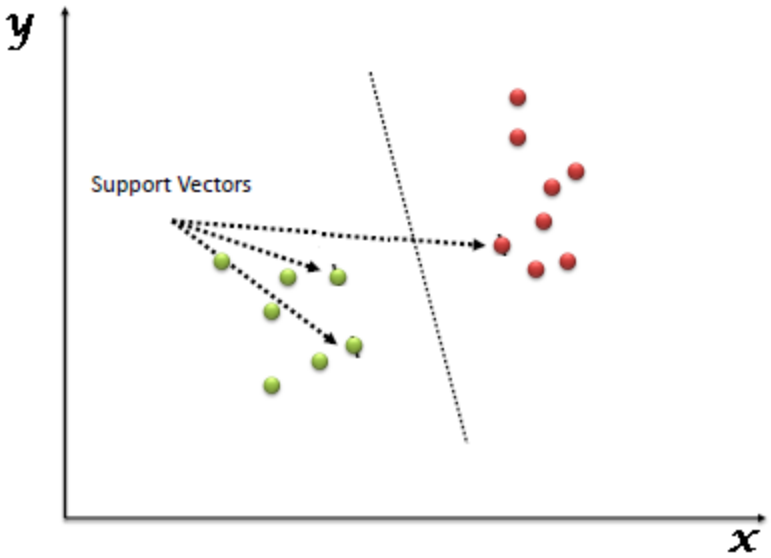
4. Check for convergence of params or likelihood

Topic 5: Support Vector Machines

Description:

What is Support Vector Machine?

- "Support Vector Machine" (SVM) is a supervised machine learning algorithm which can be used for both classification and regression challenges.
- However, it is mostly used in classification problems. In this algorithm, we plot each data item as a point in n-dimensional space (where n is number of features you have) with the value of each feature being the value of a particular coordinate.
- Then, we perform classification by finding the hyper-plane that differentiate the two classes very well (look at the below snapshot).



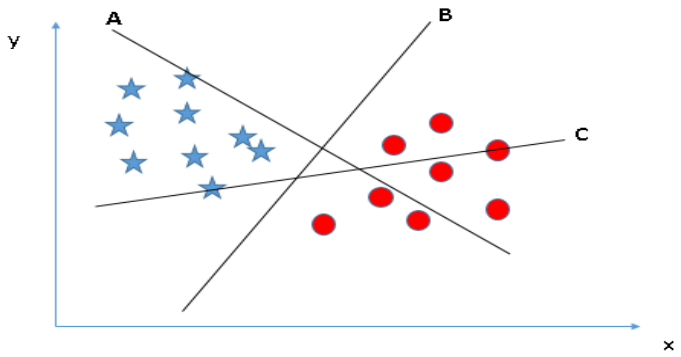
Support Vectors are simply the co-ordinates of individual observation. Support Vector Machine is a frontier which best segregates the two classes (hyper-plane/ line).

How does it work?

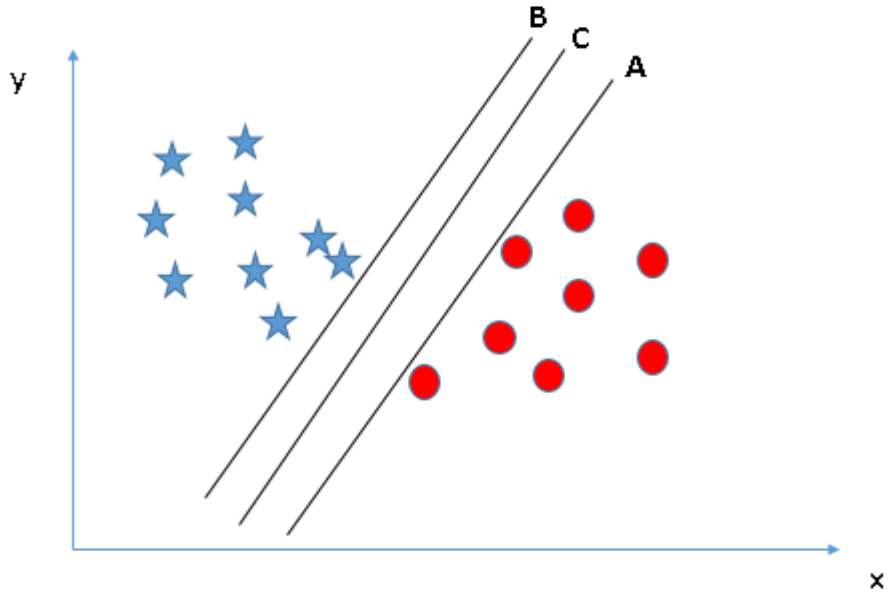
Above, we got accustomed to the process of segregating the two classes with a hyper-plane. Now the burning question is "How can we identify the right hyper-plane?". Don't worry, it's not as hard as you think!

Let's understand:

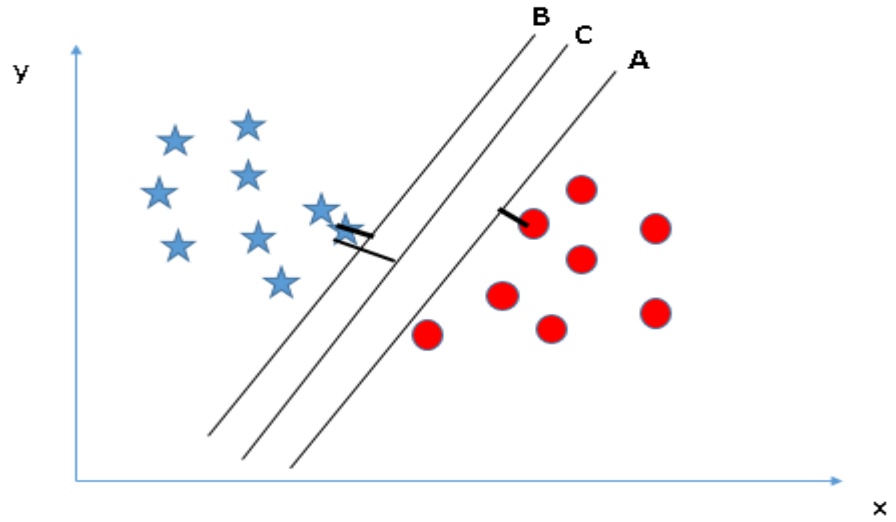
- **Identify the right hyper-plane (Scenario-1):** Here, we have three hyper-planes (A, B and C). Now, identify the right hyper-plane to classify star and circle.



- **Identify the right hyper-plane (Scenario-2):** Here, we have three hyper-planes (A, B and C) and all are segregating the classes well. Now, how can we identify the right hyper-plane?

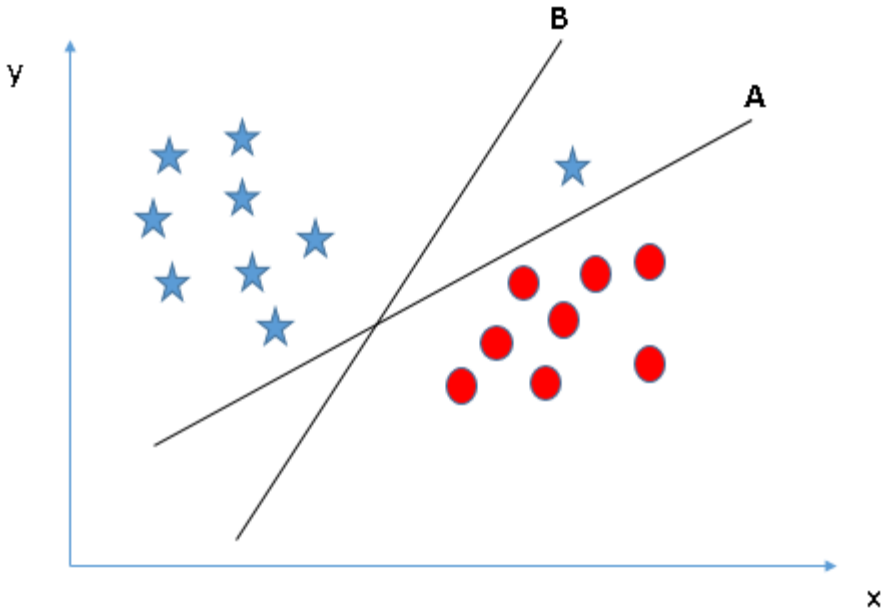


Here, maximizing the distances between nearest data point (either class) and hyper-plane will help us to decide the right hyper-plane. This distance is called as **Margin**. Let's look at the below snapshot



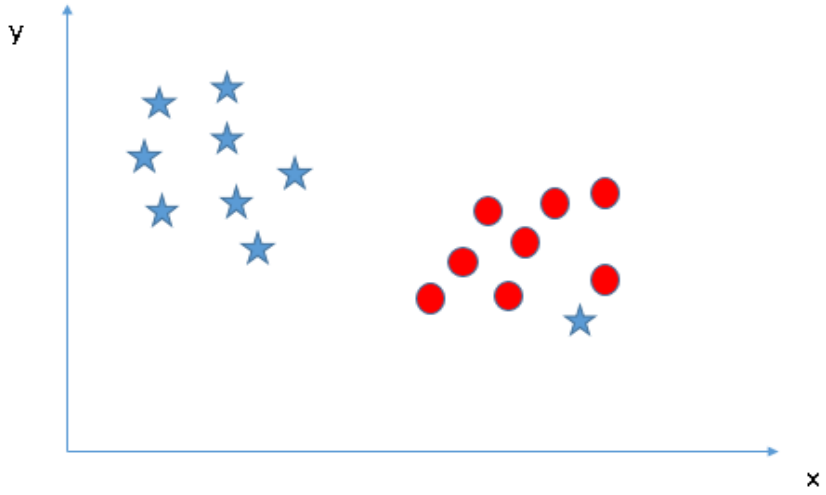
Above, you can see that the margin for hyper-plane C is high as compared to both A and B. Hence, we name the right hyper-plane as C. Another lightning reason for selecting the hyper-plane with higher margin is robustness. If we select a hyper-plane having low margin then there is high chance of miss-classification.

- **Identify the right hyper-plane (Scenario-3):** Hint: Use the rules as discussed in previous section to identify the right hyper-plane.



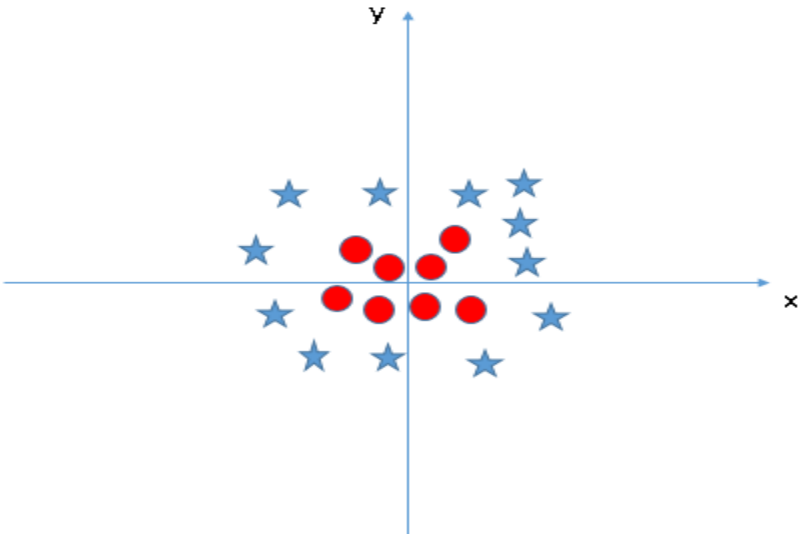
Some of you may have selected the hyper-plane **B** as it has higher margin compared to **A.** But, here is the catch; SVM selects the hyper-plane which classifies the classes accurately prior to maximizing margin. Here, hyper-plane B has a classification error and A has classified all correctly. Therefore, the right hyper-plane is **A**

- **Can we classify two classes (Scenario-4)?:** Below, I am unable to segregate the two classes using a straight line, as one of star lies in the territory of other(circle) class as an outlier.

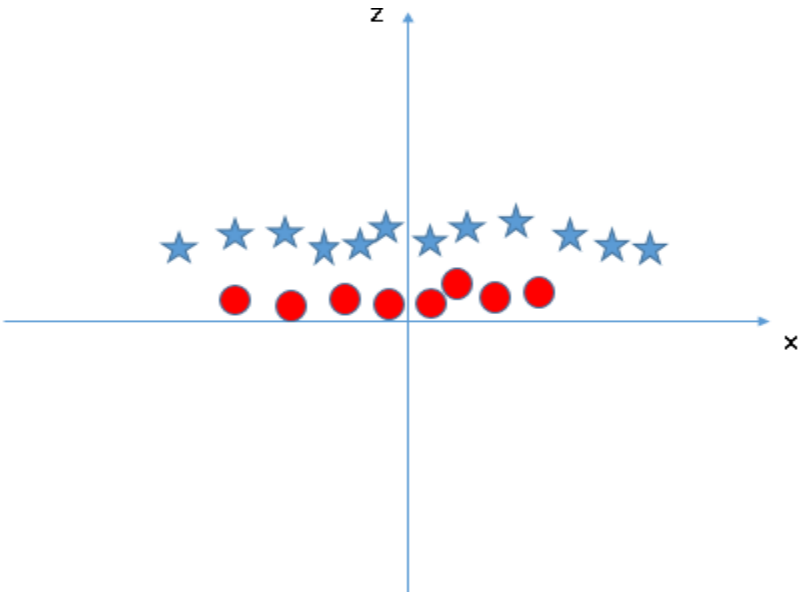


As I have already mentioned, one star at other end is like an outlier for star class. SVM has a feature to ignore outliers and find the hyper-plane that has maximum margin. Hence, we can say, SVM is robust to outliers.

Find the hyper-plane to segregate to classes (Scenario-5): In the scenario below, we can't have linear hyper-plane between the two classes, so how does SVM classify these two classes? Till now, we have only looked at the linear hyper-plane.



SVM can solve this problem. Easily! It solves this problem by introducing additional feature. Here, we will add a new feature z=x^2+y^2. Now, let's plot the data points on axis x and z:



In above plot, points to consider are:

- All values for z would be positive always because z is the squared sum of both x and y

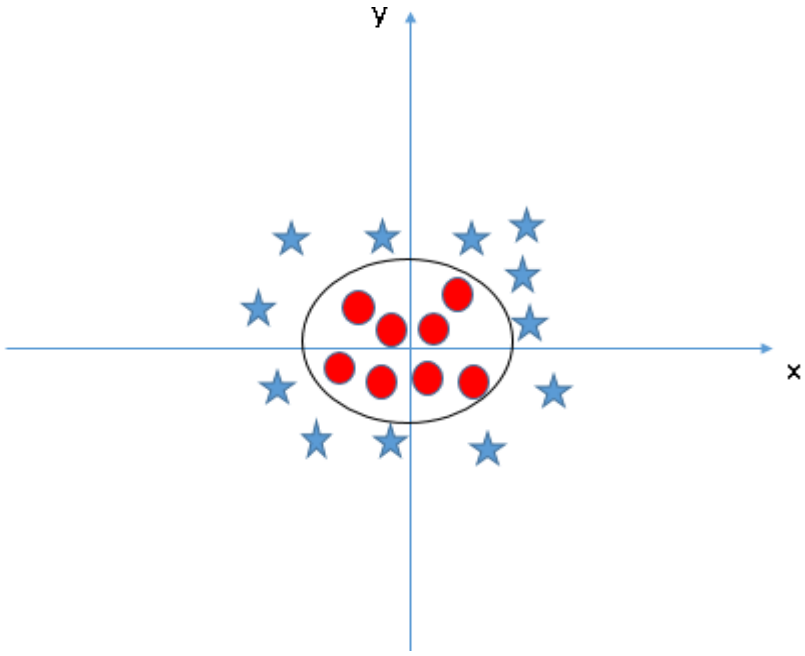
- In the original plot, red circles appear close to the origin of x and y axes, leading to lower value of z and star relatively away from the origin result to higher value of z.

In SVM, it is easy to have a linear hyper-plane between these two classes. But, another burning question which arises is, should we need to add this feature manually to have a hyper-plane. No, SVM has a technique called the **kernel trick.**

These are functions which takes low dimensional input space and transform it to a higher dimensional space i.e. it converts not separable problem to separable problem, these functions are called kernels.

t is mostly useful in non-linear separation problem. Simply put, it does some extremely complex data transformations, then find out the process to separate the data based on the labels or outputs you've defined.

When we look at the hyper-plane in original input space it looks like a circle:



Topic 6: Biometric Authentication by Hand Geometry

Description:

- Hand or finger geometry is an automated measurement of many dimensions of the hand and fingers.
- Neither of these methods take prints of the palm or fingers. Rather, only the spatial geometry is examined as the user lays his hand on the sensor's surface and uses guiding poles between the fingers to place the hand properly and initiate the reading. Finger geometry typically uses two or three fingers.
- During the 1996 Summer Olympics, hand geometry secured access to the athletes' dorms at Georgia Tech.
- Hand geometry is a well-developed technology that has been thoroughly field-tested and is easily accepted by users.
- Hand geometry recognition relies on measuring the structure of the hand.
- The acquisition stage takes measurements of almost 100 points on the top of the hand (size of knuckles, length of fingers, etc.) and computes a mathematical formula based on those measurements to create the template.
- The cooperation of the individual is required at this stage. Users tend to find hand recognition systems simpler to use because the readers are more intuitive
- In addition, such systems do not hold negative connotations; thus facilitating user acceptance.
- The hand's lower level of distinctiveness compared to other biometrics makes it suitable for verification and medium-scale identification applications.
- Compared to other biometrics, the accuracy of hand geometry is somewhat lower but it produces a very low false reject rate.
- The relatively simple and cost effective setup are also major strengths of hand recognition systems as is the fact that it performs well in both internal and external environments and generates less privacy concerns.
- The hand is a popular biometric for certain applications; its most widespread use is for physical access control and for time and attendance applications (e.g. S.Francisco Airport employees' access - 30000 enrolees).

- It is also utilised for border control, e.g. frequent traveller programme at Tel Aviv's Ben Gurion airport and the US Immigration and Naturalization Service Passenger Accelerated Service System (INSPASS) programme used at nine airports.
- Because hand and finger geometry have a low degree of distinctiveness, the technology is not well-suited for identification applications.
- Recent research has developed new recognition methods aimed at increasing performance.
- Finally, some projects are studying hand recognition as a promising candidate for web-access.

Advantages

- Easy to capture
- Believed to be a highly stable pattern over the adult lifespan

Disadvantages

- Use requires some training
- Not sufficiently distinctive for identification over large databases; usually used for verification of a claimed enrollment identity
- System requires a large amount of physical space.

Topic 7: Securing and trusting a biometric transaction

Description:

- The use of biometrics in banking is increasing because more consumers understand its potential as a predominant method of identifying themselves to access banking services such as branch banking, online banking, ATM networks, and mobile banking.
- Biometric identification methods are automated and provide fast and accurate customer authentication.
- Due to the fact that biometric systems can provide optimal identification accuracy and security, the technology is already in use within different industries such as law of

enforcement, government identity and authority border control agencies as a reliable security tool.

- As a reliable security tool, biometrics in banking can eliminate loopholes of a banking system that criminals can exploit and has the versatility to secure all financial transactions such as branch banking, internet banking, mobile banking, and ATM networks.
- Adopting biometrics for customer identification in a banking system secures transactions and brings numerous benefits and a positive impact in this industry.

Biometrics in Branch Banking

- Adopting a biometric banking system in branches can provide a convenient way for banks to quickly and accurately authorize customer identities.
- When customers visit branches they can be authenticated conveniently at the counter through fingerprint and finger vein biometric scanners that match the customer's existing biometric template within the bank database.
- After successful authentication, the customer will be allowed to move forward with their banking transactions. This will help to maintain a concrete audit trail of every transaction and can prevent fraudulent activity.
- For example, the Arig bank of Mongolia introduced biometrics in their banking system with anti-spoofing capabilities to provide optimal accuracy and stronger security in banking transactions.

Biometric Banking System for ATMs

- Due to the fact that ATMs are automated and require customer self-authentication, biometric technology in banking ATM networks is the most suitable technology to ensure identification accuracy.
- Biometrics for customer ATM transactions are already a popular security tool in developed countries and the adoption rate is growing significantly.
- Biometric identification is automated and provides faster and more accurate identification, therefore implementing biometrics in banking ATMs can improve the user

experience and eliminate the security loopholes of using traditional passwords and PINs to perform a transaction.

- Unibank of Haiti integrated biometrics with their core banking system to introduce fast, simple and secure branchless banking facilities throughout the country.

Biometrics for Online Banking

- Online banking is now very popular among consumers because it provides a convenient way to perform transactions from anywhere using smart devices like a laptop, computer, and even smartphones.
- However, these emerging online banking transactions are highly vulnerable because identity thieves are using high-tech methods to gain access to user information such as passwords, PINs and security questions.
- Even tokens are not safe to perform online transactions! Implementing a biometric authentication system in the online banking system will help this industry to protect customer's identity and financial information by providing stronger authentication methods like fingerprint scanning, facial recognition, and voice recognition.
- Due to the fact that biometrics are unique for every individual and cannot be easily forged, it will protect customer information from being compromised by fraudsters.
- Many computers, laptops, and even smartphones already have webcams, microphones, and fingerprint scanners, offering flexibility for banks to easily adopt biometric authentication for online banking services.

Biometrics in Mobile Banking

- Mobile banking is growing rapidly worldwide, and according to Juniper Search, 400 million people performed a mobile banking transaction in 2013.
- Despite this large number, many bank customers still have a lack of trust over the security of mobile banking platforms and concerns over security.
- Bank transactions or customer services could be performed through a voice or speech recognition system where customers need to verify their identity using the microphone in their phones.

Topic8: Matching Location

Description:

Matching can be done in one of four locations. The location where the templating occurs can be independent of where the matching takes place. The next sections will discuss where templating could take place for use with each of the following matching locations:

1. Trusted device
2. Local host
3. Authentication server
4. MOC (smart card)

Local Host

- The local host is the interaction point of the biometric system with the software requesting biometric authentication.
- If a trusted device is used, then there is a secure link between the device and the local host.
- Also, as described earlier, it is ideal if both the local host and the trusted device have authenticated each other through the use of certificates. This assures the software running on the local system that the match/no match response from the trusted device is valid.
- If the local host is not interacting with a trusted device, then the local host will need to exhibit one of two behaviors.
- If the local host is not doing the matching, then it must act as a secure conduit for the biometric information to reach an authentication server.
- If this is the case, then the local host may do the templating of the raw biometric data. This may involve the local host decrypting the raw data from the reader, templating the data, and re-encrypting the data for transmission and eventually comparison at the authentication server.
- This would mean that while templating is taking place, the raw biometric data and the template itself are exposed to possible interception and attack. To reduce the risk of the

raw data or template being compromised, the templating could take place at the authentication server.

- ❖ If the templating does take place at the authentication server, this adds another level of activity for the server. If the server is intended to do high-volume matching, the templating of individual user data will only slow it down. Thus, templating often takes place on the local host.

If templating must occur on the local host, then the following precautions should be taken:

- The templating and encrypt/decrypt operation should take place in a secure area of memory.
- All temporary buffers and variables should be cleared after use.
- The data should never be written to disk.
- The local workstation should be up-to-date with the latest operating system service packs and security patches.
- Anti-virus software should be run to prevent malicious code from being introduced on the system.
- The matching software should validate that its components have not been switched, or that its underlying resources have not been tampered with.
- If possible and supported by the host operating system, the matching should be done through statically linked applications. This prevents dependencies on underlying system components that could be compromised.

Authentication Server

- ❖ The authentication server is generally a single-purpose server. It is used to verify the reference template to the stored template.
- ❖ In doing so, it provides services with biometrics similar to those network login servers provide for passwords.
- ❖ Thus, the authentication server needs to be protected in the same manner as a network login server.
- ❖ These servers are generally used in a secure room or facility with controlled access to the console.

- Secure access to the machine and the console is necessary in order to safeguard the integrity of the server.
- It is well-known that if an attacker can reach the server physically, it can in general be compromised.
- In addition to keeping the server physically secure, the same precautions that were taken for local host authentication are also applicable.
- If the authentication server will also template the raw data, then the authentication device and the server should authenticate to each other with certificates.
- This way, the device knows that its raw data will arrive at the trusted authentication server, and the authentication server knows that it is talking directly to a device and not to a replay of a previous transaction.
- In addition, the local host now acts as a conduit for data. As such, the local host should not touch the transmitted data other than to assist in its forwarding to the authentication server.
- If the local host will template the data, then the authentication server must secure the transactional link and support encryption of the data.
- The same methodologies that were outlined in the electronic hardening of a trusted device are also useful in securing the communications between the server and local host, or the device itself.
- The authentication server needs to authenticate itself with the local host so that it can transmit the outcome of biometric data matching in a secure manner.
- Matching on the server is preferred over local host matching. It is still more preferable to have a trusted device. If a trusted device is cost-prohibitive, then having a properly secured server is a powerful second option.

Match on Card (MOC)

As the name implies, biometric matching can take place on a smart card. While this appears to be an ideal solution, the implementation of the solution is very important. When considering MOC, the following questions need to be answered:

- Where does the template get created?

- What communication methods are used between the biometric device and smart card?
- How is the algorithm implemented on the card?

Where is the template created?

- When the templating is done on the local host, this opens the transaction up to attack. If by using a MOC solution the actual templating takes place on the local host, then this is no better a solution than matching on the local host.
- Once the template is exposed to the PC bus, even with the precautions discussed in local host templating, an element of uncertainty has now been introduced into the transaction.
- MOC solutions may template on the local machine due to a lack of speed or system resources on the smart card. For an ideal solution, the card itself would do the biometric templating.

- What communication methods are used between the biometric device and the smart card?
- Regardless of where the template is created from the raw data, either the raw data or an externally created template needs to reach the smart card.
- This communication path needs to be as secure as possible. If this path involves exposure to the PC bus, then once again, an element of uncertainty is introduced into the transaction.
- If, on the other hand, the biometric data moves internally in the device, never leaves the device, and travels across secure buses, then this is a strong matching solution from a security standpoint.

How is the algorithm implemented on the card?

- Many vendors , when trying to implement a MOC solution, take shortcuts with their algorithm to get acceptable performance from the matching.
- Any change to the algorithm invalidates the current biometric statistics. Therefore, it is important to have a vendor clearly state what its biometric statistics are for MOC.
- Getting the performance increases that MOC providers are looking for can involve templating taking place elsewhere.

- When templating takes place off the card, the template can be compromised. Thus, a certain degree of uncertainty is introduced into the transaction.
- Another method of increasing performance is to have some binning and pre-comparison work for the match take place on a faster processor.
- This normally involves using the local host. As seen before, the same issues with using a matching location can affect this plan.
- A vendor may also adjust its measurements of any algorithm's strength. When matching takes place in application software, algorithm strength may be greater.
- For example, the vendor may have biometric security levels of high, medium, and low for matching in application software.
- The vendor could say that the MOC has a high, medium, and low level of biometric security. Since the same vendor is claiming the same security levels regardless of where the matching takes place, the user might assume that the security settings are equivalent.
- As we have seen, this may not be the case, depending on whether the same algorithm is implemented in both locations in the same way.

Final thoughts on matching location

- As in every other business decision that needs to be made, risk is a large deciding factor.
- If the risk of a compromised transaction is sufficiently strong, then the use of a trusted device is warranted.
- For most transactions and applications, the use of an authentication server will meet the users' needs appropriately.
- For much lower risk transactions, or if using biometrics purely for convenience, local host matching may be sufficient.

Topic 9: Multibiometrics and Two Factor Authentication

Description:

- Two-factor authentication (2FA), often referred to as two-step verification, is a security process in which the user provides two authentication factors to verify they are who they say they are. 2FA can be contrasted with single-factor authentication (SFA), a security process in which the user provides only one factor -- typically a password.

- Two-factor authentication provides an additional layer of security and makes it harder for attackers to gain access to a person's devices and online accounts, because knowing the victim's password alone is not enough to pass the authentication check.
- Two-factor authentication has long been used to control access to sensitive systems and data, and online services are increasingly introducing 2FA to prevent their users' data from being accessed by hackers who have stolen a password database or used phishing campaigns to obtain users' passwords.

Types of two-factor authentication products

- There are many different devices and services for implementing 2FA -- from tokens, to RFID cards, to smartphone apps.
- Two-factor authentication products can be divided into two parts: tokens that are given to users to use when logging in, and infrastructure or software that recognizes and authenticates access for users who are using their tokens correctly.
- The authentication tokens may be physical devices, such as key fobs or smart cards, or they may exist in software as mobile or desktop apps that generate PIN codes for authentication.
- On the other side, organizations need to have some system in place to accept, process and allow -- or deny -- access to users authenticating with their tokens. This may be server software, a dedicated hardware server or provided as a service by a third-party vendor.

Two-factor authentication for mobile authentication

- Smartphones offer a variety of possibilities for 2FA, allowing companies to use what works best for them.
- Some devices have screens capable of recognizing fingerprints; a built-in camera can be used for facial recognition or iris scanning and the microphone can be used for voice recognition. Smartphones equipped with GPS can verify location as an additional factor.
- Voice or Short Message Service (SMS) may also be used as a channel for out-of-band authentication.

- Apple iOS, Google Android, Windows 10 and BlackBerry OS 10 all have apps which support 2FA, allowing the phone itself to serve as the physical device to satisfy the possession factor.
- Authenticator apps replace the need to obtain a verification code via text, voice call or email.
- For example, to access a website or web-based service that supports Google Authenticator, the user types in their username and password a knowledge factor.
- The user is then prompted to enter a six-digit number. Instead of having to wait a few seconds to receive a text message, Authenticator generates the number for them.
- These numbers change every 30 seconds and are different for every login. By entering the correct number, the user completes the user-verification process and proves possession of the correct device -- an ownership factor.