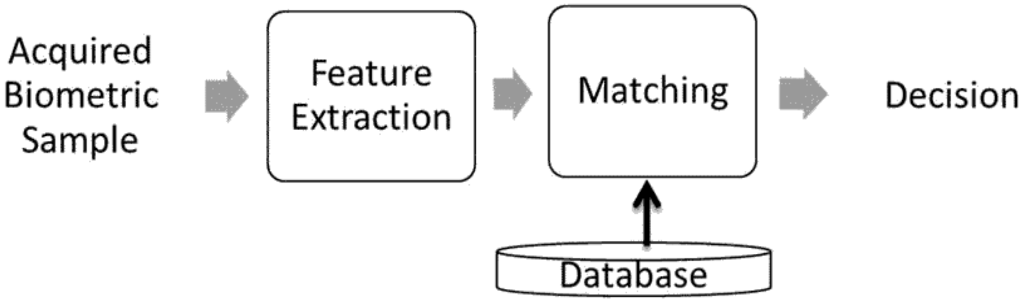
CHAPTER - 3

BIOMETRIC PERFORMANCE ANALYSIS

3.1 INTROCUCTION

Biometrics is measurements of the characters of a person for authentication. The various characters include iris, face, fingerprint, palm print etc., which are physical and also signature, voice etc., which are behavioral. Measurements related to each character will differ. Biometric system is analyzed based on cost, accuracy, complexity, inter-operability and system security. Accuracy of the biometric system defines the efficiency with which it works. Improving the efficiency of an existing system is an effective method. This can be achieved by using different approaches for feature extraction, using multiple classifiers, multiple samples of the trait etc. Various standards like NISIT/ANSI were set for the measurements and analysis of a biometric system. Performance measurement tools like FRVT 2002, VTB, and ATB were set to standardize the software, sensors, interface, which helps in future upgrading by the integration of products and inter- operability.

Performance of a biometric system is analyzed with error estimation like false match, false mismatch, impostor acceptance rate, ROC, DET, plots etc. Reliable person identification is a critical issue in many applications. Any biometric system is not a fool proof secured. By analyzing the performance, one can identify the factors that contribute in improving the efficiency of a biometric system.



Flowchart of a Typical Biometric System

Fig: 3.1 Biometric processing

3.2 BIOMETRIC PARAMETERS

Various factors, functionalities and notations that contribute in analyzing the performance of biometric systems are given in this section [18].

Biometric system can make two types of errors

False match (FM): Biometric system which declares incorrectly as a successful match between input pattern and the stored template pattern.

False non match (FNM): Biometric system which declares incorrectly as a failure between input pattern and stored template pattern.

Biometric image is first captured by a sensor. Errors encountered at the sensor level can be

Failure to capture (FTC) and Failure to enroll (FTE): Number of times the user not able to enroll in to the system. It gives the degree of accuracy of the system designed.

Biometric system performance evaluation is based on FM, FNM, FTC and FTE. False match and false non match are also called as False accept rate (FAR) and false reject rate (FRR) respectively, which can be evaluated as

FAR = Number of false acceptance/Number of impostor attempts

FRR = Number of False rejection/Number of genuine user attempt

A False acceptance allows an impostor to get an access, and a false reject denies an access to the enrolled user. A threshold is set by the system to decide either to accept or to reject the enroller.

Equal Error Rate (EER): EER is a threshold set to evaluate the performance of the recognition, which is a midpoint region between False accept and false reject ROC plot. It is also a measurement to say how accurate the system is in rejecting an impostor. EER is also called as cross over error rate between FAR and FRR.

Receiver Operating Characteristics (ROC): A graphical representation giving a relationship between FAR and FRR. It is used as a measure of summarizing the performance of a biometric system. Performance of different biometric system can also be compared by representing on ROC plots with their thresholds made independent.

Detection Error Rate (DET): A logarithmic plot which distinguishes between false match rates vs false non-match rate for a range of thresholds is represented as DET plots.

HIT Rate: The FRR curve is based on threshold set and the area under the curve defines the maximum threshold. If false reject rate is zero it implies that all the users are accepted for the set threshold. HIT rate is a plot with zero FRR.

The biometric system is defined by using various terms.

Enrolment: The user biometric character is acquired and registered into the system.

Verification: The user's biometric character is verified with his own template stored in the database. (One to one matching)

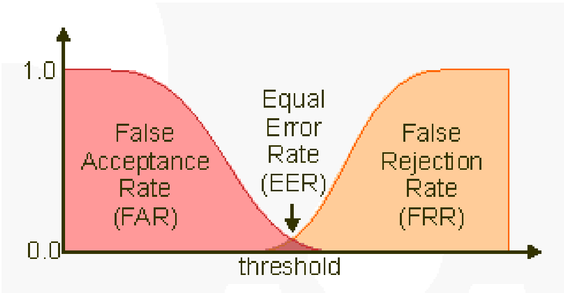
Identification: The user biometric character is compared with all the templates stored in the database (one-to-many).

Authentication: The process of confirming the user identity after verification and identification.

Templates / feature sets: The features extracted from the biometric characters are stored in the database as templates.

Query input/modality/trait/character: The biometric used for person identification i.e., face, iris, finger prints, palm and prints.

Threshold: A user setting for biometric systems operation can be in verification or identification mode. The acceptance or rejection of biometric data is dependent on the match score falling above or below the threshold. The threshold is adjustable depending on the requirements of a given biometric application. Performance of a biometric system can be enhanced by computing user specific threshold. These thresholds are computed using individual biometric trait or may be computed after consolidating scores provided by the multiple traits. This reduces the false rejection rate and enhances the performance of a biometric system.



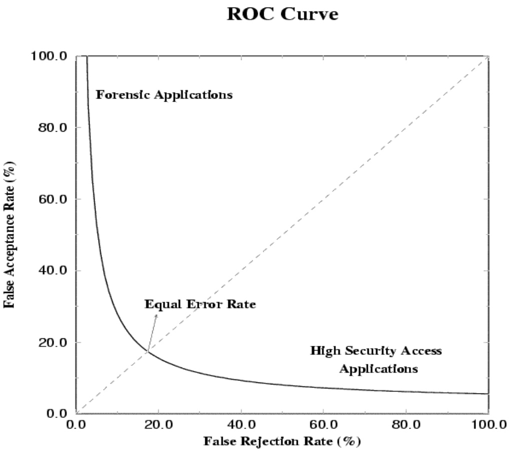
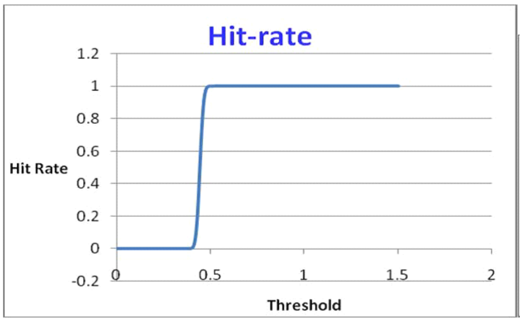


Fig: 3.2 FAR, EER, FRR

Fig: 3.3 ROC plot of FRR VS FAR



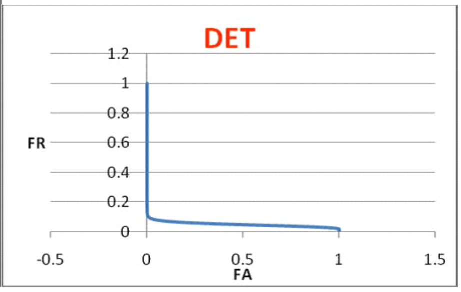
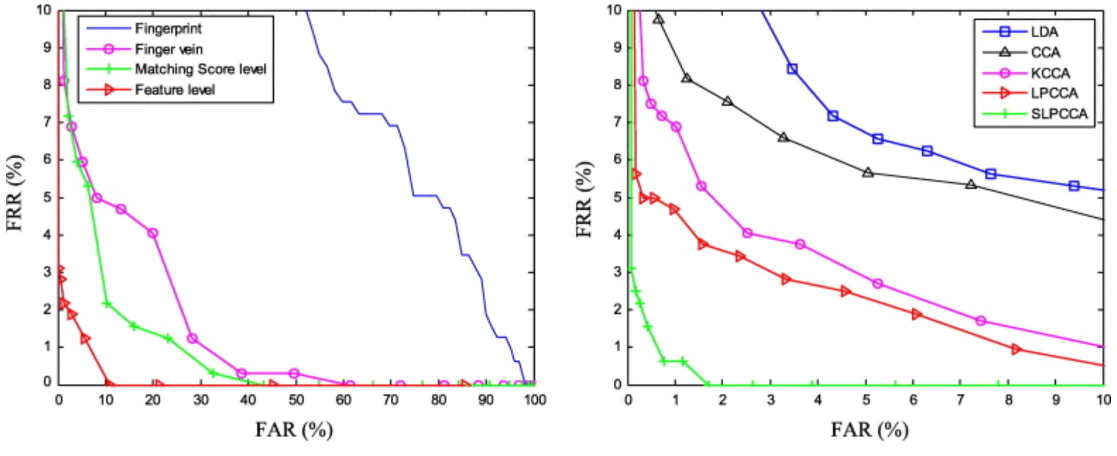


Fig: 3.4 HIT rate

Fig: 3.5 DET plot



(a) (b)

Fig: 3.6 a) ROC plots for biometric character b) ROC plots for approaches used [16]

Modality	**Test**	**Test parameter**	**FRR**	**FAR**
Face	FRVT 2000	Variable lighting	10%	1%
Finger print	FVC 2004	20 years average	2%	2%
Voice	NIST 2000	Text independent	10-20%	2-5%

Table 3.1 Error rates of biometric character as per standard testing

3.3 BIOMETRIC SYSTEM SCENARIO

Biometric system can be operated in various scenarios.

Verification mode: A one to one matching is performed by the system between the claimed identity and the template stored in database. Biometric system uses verification mode of operation in applications like passport, immigration, election id, driving license, airport security, crime detection, forensic etc.

Identification mode: One-to-many matching is performed by the system between the claimed identity and all the templates stored database. The commercial applications like banking, networking, and access control etc., uses biometric system in identification mode. System with a large database operates in identification mode.

Attended vs. non-attended: It is supervised vs. non-supervised biometric authentication. Login access at the office entrance, attendance proof in an organization etc., are considered as non-supervised type of authentication where it is not supervised for each individual entering the premises. This type of biometric is in addition to the main security employed by many organizations. Applications like airport security, pass port offices, government organizations, etc. needs supervised authentication.

Habituated: Users presenting biometric as a daily routine in an organization.

Non-Habituated: Is the one where user has not given a biometric for verification over a long period of time e.g., users authentication at the time of passport renewal, immigration renewal, driver license verification etc.

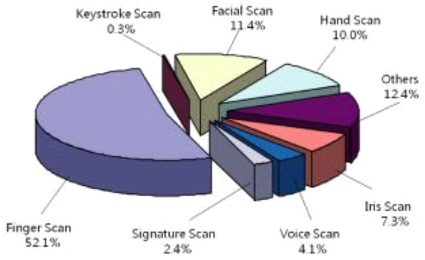


Fig: 3.7. Biometric characters used

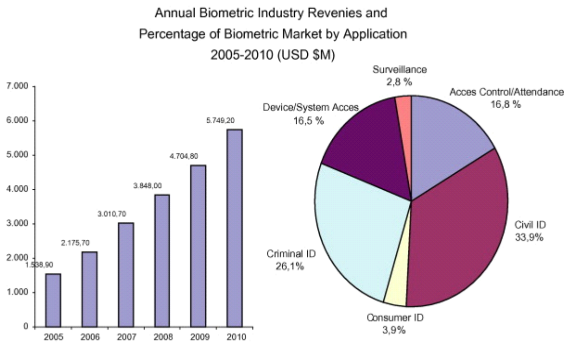


Fig: 3.8 Biometric applications

BIOMETRIC SCENARIO

Fig: 3.9 Biometric application scenarios

3.4 Biometric system requirement

Any biometric system designed should satisfy the following conditions for the biometric character chosen [24].

Universality: The biometric character chosen must be present in all human beings and should perform satisfactorily for a larger group. The finger print biometric character may not be suitable for a manual labour with cuts and bruises.

Uniqueness: The biometric character features used for identification should be unique. For example facial features are unique for a person (even for identical twins the palm print, finger print differs in their features and textures).

Permanence: The biometric character used should be stable over a period of time. It should not be subjected to significant variations. (Face variations due to aging, variations in the finger prints due to manual work, variations in biometric character due to illness, disease etc. are major limitations to fulfill the permanence requirement)

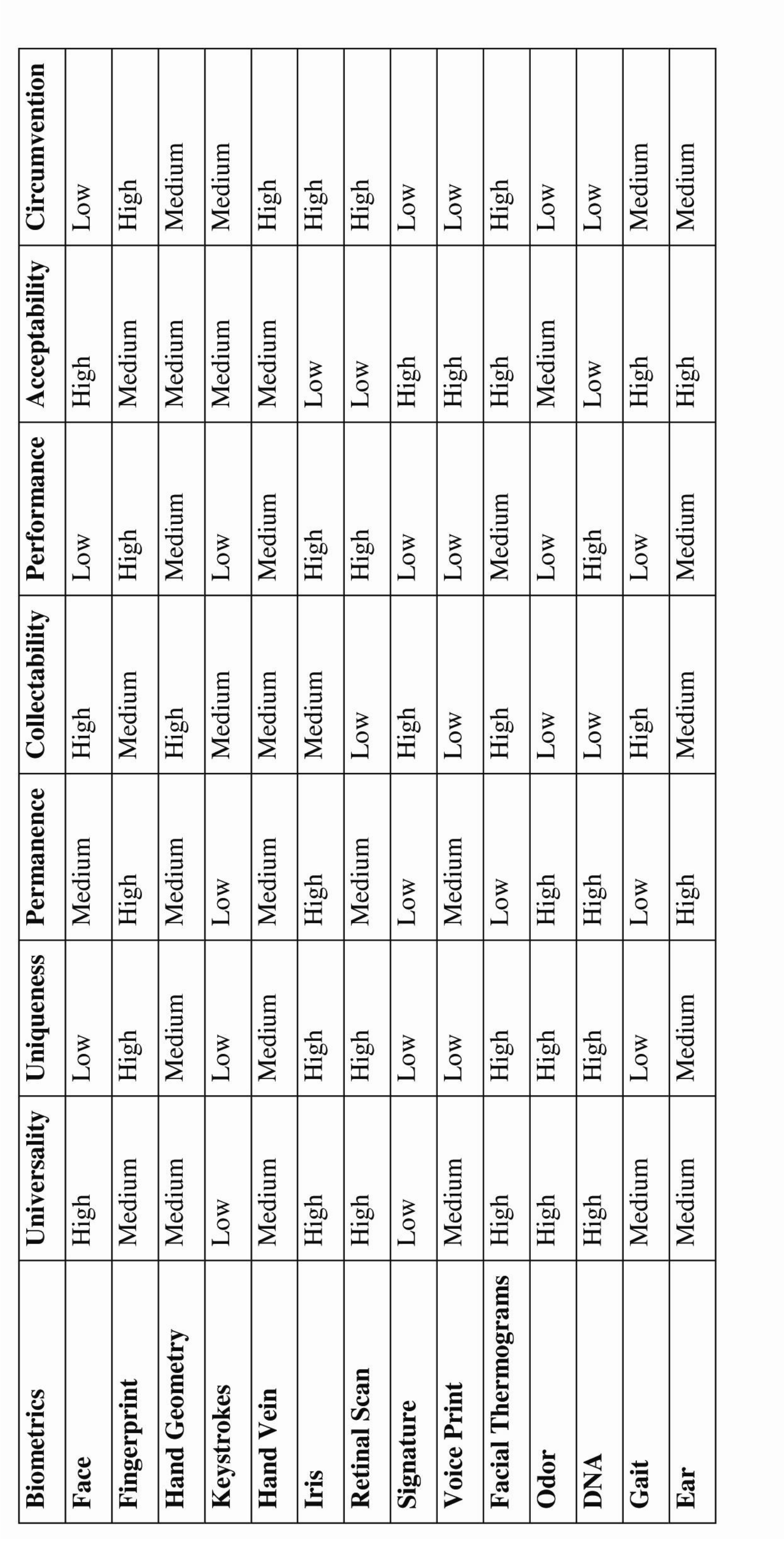
Collectability: The process of acquisition of characters must me user friendly and easily collected and should have a high acceptability. Face recognition is user friendly for a larger database system of commercial application when compared to finger print. For secured applications such as passport and immigration data acquisition, multiple biometric information is collected and acceptability may not be the criteria as it becomes mandatory.

Performance: The biometric system should achieve the desired accuracy for which it was designed. Performance of biometric system is prone to numerous errors; failure to control (FTE), false accept rate (FAR), and false reject rate (FRR). The accuracy of a biometric system is not static, but it data dependant and influenced by several factors; biometric quality of image, size of database, robustness of employed algorithm etc.

Acceptability: The biometric character chosen for a specific application should have a high acceptability by the user. It should be user friendly especially for commercial and civilian applications. Face and finger print are universally accepted biometric when compared to iris.

Circumvention: The biometric system should be fool proof and spoof attack is to be taken care. (Signatures can be forged, voice can be imitated, similarity in faces, fingerprints etc.).

Biometric performance of various modalities



Biometrics	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	High	Low	Medium	High	Low	High	Low
Fingerprint	Medium	High	High	Medium	High	Medium	High
Hand Geometry	Medium	Medium	Medium	High	Medium	Medium	Medium
Keystrokes	Low	Low	Low	Medium	Low	Medium	Medium
Hand Vein	Medium	Medium	Medium	Medium	Medium	Medium	High
Iris	High	High	High	Medium	High	Low	High
Retinal Scan	High	High	Medium	Low	High	Low	High
Signature	Low	Low	Low	High	Low	High	Low
Voice Print	Medium	Low	Medium	Low	Low	High	Low
Facial Thermograms	High	High	Low	High	Medium	High	High
Odor	High	High	High	Low	Low	Medium	Low
DNA	High	High	High	Low	High	Low	Low
Gait	Medium	Low	Low	High	Low	High	Medium
Ear	Medium	Medium	High	Medium	Medium	High	Medium

Table 3.2 Biometric character performance [18]

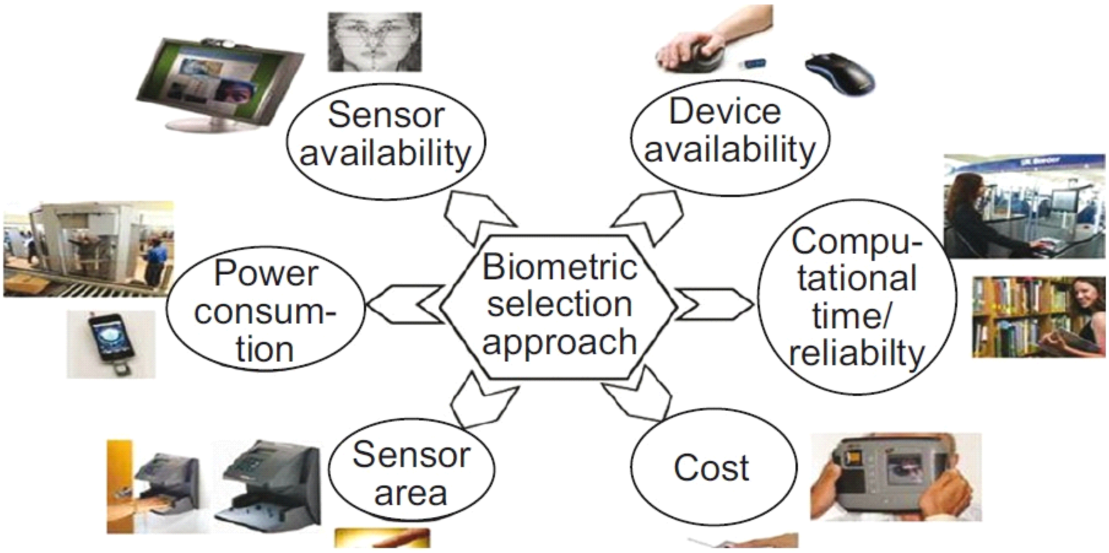


Fig: 3.10 Biometric selection approaches

3.5 BIOMETRIC SYSTEM SECURITY AND ATTACKS

Biometric system is subjected to system attacks by various forms of threats. Threat on a biometric system is a security concern and degrades its performances. Many of these attacks are applicable to any form of biometric system which is to be analyzed and counter measures are to be taken in designing the biometric system. [5] [6].

Fake Biometric: A fake biometric sample may be given to a sensor to get an access to the system. Finger print made from silicon, fake face mask, lens on an iris etc. are few such attacks on sensor.

Replay Attack: It is an attack in a biometric system where data stream is injected between sensor and the processing system. A replay attack can be two or three stage process first intercepting or copying the sensor transmission, then possibly modifying the data and finally replaying the data.

Spoofing the Feature set: Replacing the feature set with a fake or altered feature set.

Template Attack: The templates stored in the database can be stolen or replaced or can be modified.

Trojan Horse attack: The feature extractor itself is replaced to generate the desired features and to add to the existing database.

Spoof detection technology has become an essential part of a biometric system .With a growing concern for security, biometric attacks are to be identified, controlled and minimized. Researchers developed various approaches for a secure biometric system.

Hill climbing based attack system against finger print matchers, Steganographic and Water marking techniques to increase the security of biometric template, Liveness detection mechanism to thwart attacks, soft biometrics, multimodal biometric etc. are various approaches used to ensure a reliable biometric system.[13 [14].

Fig: 3.11 Biometric System attacks

3.6 DISCUSSION

Biometric system refers to automatic recognition of a person using his behavioral or physical characteristics like voice, signature, face, fingerprints, palm etc. Biometric system processing stage involves image capture, pre-processing, feature extraction and template storage in the system database. During verification the input query image features are compared with stored features for final authentication. Biometric system has various limitations like noisy sensor data, spoof attacks, inter class similarity and intra class variations etc. To increase the performance accuracy and to design a biometric system or to propose a new approach to the existing system one has to understand the basic biometric system, its parameters used, limitations, biometric scenario, biometric characters used for an application, types of errors and existing approaches. Any biometric system is not optimal. Always there is a need for improving the accuracy and performance of the biometric system.

3.7 CONCLUSION

In this chapter biometric system performance is analyzed by addressing various issues such as biometric limitations, biometric scenario, biometric system requirement and biometric security. With the help of the analysis, palm print and face are chosen as biometric character for their rich feature information and are to be used in the implementation of multi modal biometric recognition system and enhancement of feature extraction methods.