International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-3, Issue-4)

Research Article | **April 2014**

Biometrics – Introduction, Characteristics, Basic technique, its Types and Various Performance Measures

Pankaj Sareen
Department of Computer Applications,
Baddi University of Emerging Sciences & Technology, India

Abstract:

Biometrics is the science of measuring physical and/or behavioral characteristics that are unique to each individual and they verify that an individual is who he or she claims to be. I have discussed about various biometric characteristics. Then I discussed the basic technique and operation that every biometric system follows. This paper explains the various biometric methodologies with their comparison with each other. Then various decision factors for selecting a particular biometric technology for a specific application are discussed. This paper also discusses various biometric performance measures, areas of concerns, how biometric systems are being used and advantages and disadvantages of the biometric system.

Keywords: Characteristics, Enrollment, Verification, Biometric techniques, Selection Criteria, False Acceptance Rate

I. INTRODUCTION:

Biometrics can be defined as the science and technology of measuring and statistically analyzing biological data. They are measurable physiological and / or behavioral characteristics that can be utilized to verify the identity of an individual. For a layman, it could be said that biometrics are the science of measuring physical and/or behavioral characteristics that are unique to each individual and they verify that an individual is who he or she claims to be. "Biometrics" means "life measurement" but the term is usually associated with the use of unique physiological characteristics to identify an individual. The application which most people associate with biometrics is security. However, Biometrics [1] identification has eventually a much broader relevance as computer interface becomes more natural. Knowing the person with whom you are conversing is an important part of human interaction and one expects computers of the future to have the same capabilities.

A number of biometric traits have been developed and are used to authenticate the person's identity. The idea is to use the special characteristics of a person to identify him. By using special characteristics we mean the using the features such as face, iris, fingerprint, signature etc.

II. **BIOMETRIC CHARACTERISTICS**

A number of biometric characteristics may be captured in the first phase of processing. However, automated capturing and automated comparison with previously stored data requires that the biometric characteristics satisfy the following characteristics [2]:

A. Universal

Every person must possess the characteristic/attribute. The attribute must be one that is universal and seldom lost to accident or disease.

B. 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 either episodic or chronic disease.

C. Measurability

The properties should be suitable for capture without waiting time and must be easy to gather the attribute data passively.

D. 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 all attributes that are unique assuming a particularly precise measure, but do not offer enough points of differentiation to be useful for more than categorizing.

E. Acceptance

The capturing should be possible in a way acceptable to a large percentage of the population. Excluded are particularly invasive technologies, i.e. technologies which require a part of the human body to be taken or which (apparently) impair the human body.

F. Reducibility
The captured data should be capable of being reduced to a file which is easy to handle.

G. Reliability and tamper-resistance:
The attribute should be impractical to mask or manipulate. The process should ensure high reliability and reproducibility.

H. Privacy
The process should not violate the privacy of the person.

I. Comparable
It should be able to reduce the attribute to a state that makes it digitally comparable to others. The less probabilistic the matching involved, the more authoritative the identification.

J. Inimitable
The attribute must be irreproducible by other means. The less reproducible the attribute, the more likely it will be authoritative.

Among the various biometric technologies being considered, the attributes which satisfy the above requirements are fingerprint, facial features, hand geometry, voice, iris, retina, vein patterns, palm print, DNA, keystroke dynamics, ear shape, odor, signature etc.

III. BASIC TECHNIQUE AND OPERATION:

A biometric system is a real-time identification system which identifies a person by measuring a particular physical or behavioral characteristic and later comparing it to a library of characteristics belonging to many people. Fingerprint and other biometric devices consist of a reader or scanning device, software that converts the scanned information into digital form, and wherever the data is to be analyzed, a database that stores the biometric data for comparison with previous records. When converting the biometric input, the software identifies specific points of data as match points. The match points are processed using an algorithm into a value that can be compared with biometric data scanned when a user tries to gain access.

Thus biometric devices can be explained with a 3-step procedure [1]. They are -

- A sensor takes an observation. The type of sensor and its observation depend on the type of biometrics device used. This observation gives us a Biometric *Signature* of the individual.
- A computer algorithm normalizes the biometric signature so that it is in the same format (size, resolution, etc.) as the signatures on the system's database. The normalization of the biometric signature gives us a normalized Signature of the individual.
- A matcher compares the normalized signature with the set (or sub-set) of normalized signatures on the system's database and provides a similarity score that compares the individual's normalized signature with each signature in the database set (or sub-set). What is then done with the similarity scores depends on the biometric system's application.

Thus a biometric system is essentially a pattern recognition system, which makes a personal identification by determining the authenticity of a specific physiological or behavioral characteristic possessed by the user. An important issue in designing a practical system is to determine how an individual is identified. Depending on the context, a biometric system can be either a verification (authentication) system or an identification system.

A. Operation of a Biometric System Biometric System [3]

Biometric system is a pattern recognition system that:

- acquires biometric data from an individual
- extracts a salient feature set from the data
- compares the feature set against feature set(s) stored in the database
- executes an action based on the result of the comparison

Simple biometric systems usually consist of the following four components:

1) Sensor modules: This module acquires biometric user data. Examples of sensor modules would be a retina-scanner or a fingerprint sensor.

2) Feature extraction modules: This module is responsible for extracting feature values of a biometric trait. If hand geometry would be used as a biometric trait then feature values would include width of fingers at various locations, width of the palm, thickness of the palm, length of fingers etc.

3) Matching modules: The matching modules compare the acquired biometric features against those stored in a database.

4) Decision-making modules: The user's identity is either established or a claimed identity is accepted or rejected. This is done based on the results of the matching modules.

B. Enrollment, Verification and Identification

Enrollment (see Fig. 1) mode refers to the stage in which the system stores some biometric reference information about the person in a database. This reference information may be in the form of a template (features extracted from the biometric sample or parameters of a mathematical model that best characterizes the extracted features) or the biometric sample itself (e.g., faces or fingerprint image). In many applications, some identity attributes about the person (name, ID number, etc.) is also stored along with the biometric reference

In Verification (see Fig. 2) mode the system performs a one-to-one comparison of a captured biometric with a specific template stored in a biometric database in order to verify the individual is the person they claim to be.

In Identification (see Fig. 3) mode the system performs a one-to-many comparison against a biometric database in attempt to establish the identity of an unknown individual. The system will succeed in identifying the individual if the comparison of the biometric sample to a template in the database falls within a previously set threshold. Identification mode can be used either for 'positive recognition' (so that the user does not have to provide any information about the template to be used) or for 'negative recognition' of the person "where the system establishes whether the person is who she (implicitly or explicitly) denies to be.

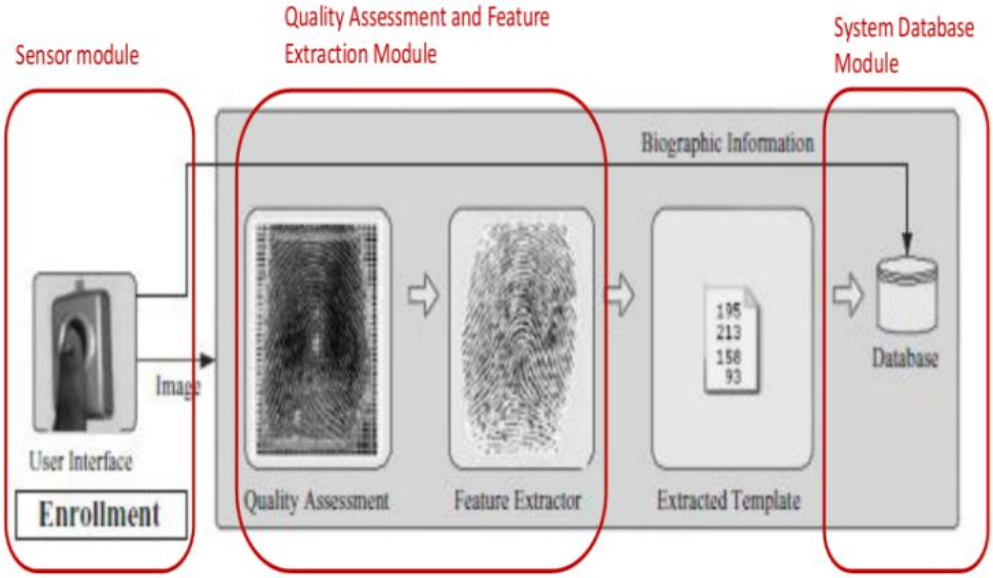

Fig. 1: Enrollment

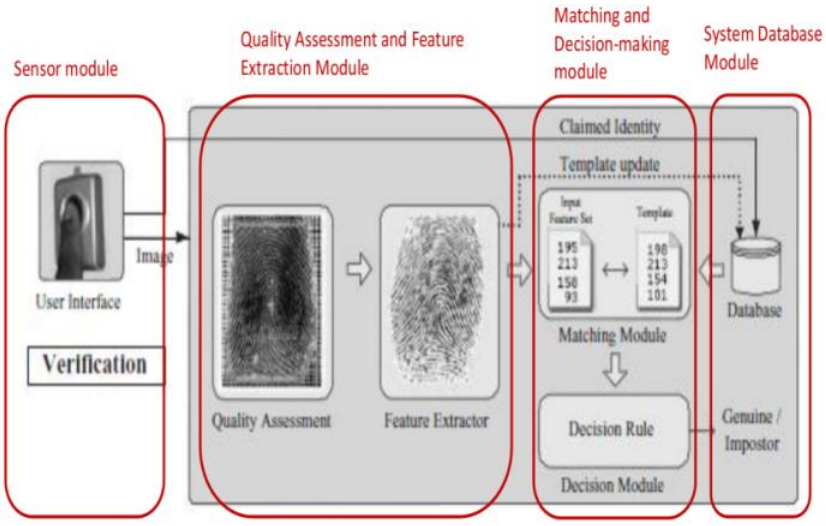

Fig.2: Verification

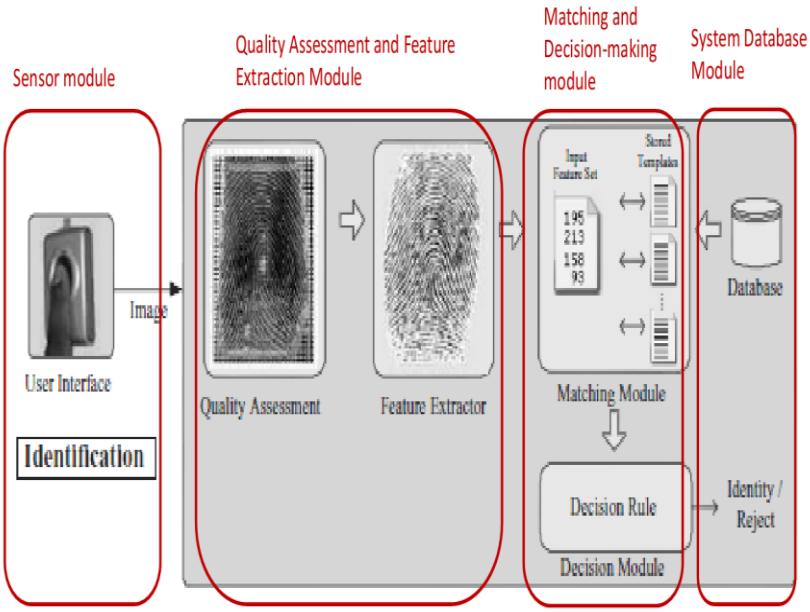

Fig.3: Identification

IV. VARIOUS METHODOLOGIES

Presently, biometrics gravitate around the following methodologies -

A. Fingerprint Verification:

Fig.4: fingerprint

There are a variety of approaches to fingerprint verification (see fig. 4). Some of them try to emulate the traditional police method of matching minutiae, others are straight pattern matching devices, and some adopt a unique approach all of their own, including ultrasonic. There are a greater variety of fingerprint devices available than other biometric systems at present. Potentially capable of good accuracy (low instances of false acceptance) fingerprint devices (see fig.5) can also suffer from usage errors among insufficiently disciplined users (higher instances of false rejection) such as might be the case with large user bases. Fingerprint verification may be a good choice for in house systems where adequate explanation and training can be provided to users and where the system is operated within a controlled environment. It is not surprising that the workstation access application area seems to be based almost exclusively around fingerprints, due to the relatively low cost, small size (easily integrated into keyboards) and ease of integration.

fig 5. This laptop features a fingerprint scanner, Bringing biometric security to the home

Fingerprint biometrics [4] is probably the most common form of biometrics available today. This form of data encryption has evolved out of the use of fingerprints for identification purposes over the last several decades. By having an individual scan their fingerprint electronically to decode information, the transmitter of the data can be certain that the intended recipient is the receiver of the data. When scanned electronically, fingerprints provide a higher level of detail and accuracy can be achieved over manual systems.

Some other strength associated with fingerprint biometrics are that giving fingerprints is more widely accepted, convenient and reliable than other forms of physical identification, especially when using technology. In fact, studies have shown that fingerprint identification is currently thought to be the least intrusive of all biometric techniques. One concern of fingerprint biometrics is that latent prints left on the glass will register the prior user; however there already exist units that will not scan unless a "live" finger is on the glass and will only register the later imprint. Furthermore, the error rate experienced with this form of encryption is approximately one in one hundred thousand scans.

Lastly, one of the most important features of fingerprint biometrics is its cost. Scanners are already available fairly cheap and as the technology becomes more common this cost should only decrease. In fact, in anticipation of widespread use of this technology in the future, some "mouse" manufacturers are developing their products with fingerprint scanner technology built right into the "mouse" itself.

B. Handwriting:

At first glance, using handwriting to identify people might not seem like a good idea. After all, many people can learn to copy other people's handwriting with a little time and practice. It seems like it would be easy to get a copy of someone's signature or the required password and learn to forge it.

But biometric systems don't just look at how you shape each letter; they analyze the act of writing. They examine the pressure you use and the speed and rhythm with which you write (see fig.6). They also record the sequence in which you form letters like whether you add dots and crosses as you go or after you finish the word.

Fig. 6 This Tablet PC has a signature verification system.

Unlike the simple shapes of the letters, these traits are very difficult to forge. Even if someone else got a copy of your signature and traced it, the system probably wouldn't accept their forgery.

A handwriting recognition system's sensors can include a touch-sensitive writing surface or a pen that contains sensors that detect angle, pressure and direction. The software translates the handwriting into a graph and recognizes the small changes in a person's handwriting from day to day and over time.

Signing documents is something that most every adult is familiar with. In our personal lives we sign everything from personal checks to birthday cards. In the business world we sign things such as expense accounts and other official documents. This lends itself well for signature recognition to be used as a means of biometric verification in electronic commerce. This type of signature identification [5] is different however from the normal two-dimensional signature that one would find on a form or document. Biometric signature recognition operates in a three-dimensional environment where, not only is the height and width of pen strokes measured, but also the amount of pressure applied in the pen stroke to measure the depth that would occur as if the stroke was made in the air. This helps to reduce the risk of forgery that can occur in two-dimensional signatures.

One drawback to this form of encryption is that people do not always sign documents in exactly the same manner. The angle at which they sign may be different due to seating position or due to hand placement on the writing surface. Therefore, even though it is three dimensional which adds to its ability to discern impostors, it is not as accurate as other forms of biometric verification.

These types of systems are not as expensive as some of the higher end systems such as iris scanners, and they are priced more in the range of voice and fingerprint scanners which makes them quite affordable for network us

C. Hand and Finger Geometry

Fig. 7: Hand Geometry

Hand geometry (see fig. 7) is concerned with measuring the physical characteristics of the users hand and fingers, from a three-dimensional perspective. One of the most established methodologies; it offers a good balance of performance characteristics and is relatively easy to use. This methodology may be suitable where we have larger user bases or users who may access the system infrequently and may therefore be less disciplined in their approach to the system. Accuracy can be very high if desired. Hand geometry readers (see fig. 8) are deployed in a wide range of scenarios, including time and attendance recording where they have proved extremely popular. Ease of integration into other systems and processes, coupled to ease of use makes hand geometry an obvious first step for many biometric projects.

Fig. 8 A hand geometry scanner

People's hands and fingers are unique -- but not as unique as other traits, like fingerprints or irises. That's why businesses and schools, rather than high-security facilities, typically use hand and finger geometry readers to authenticate users, not to identify them. Disney theme parks, for example, use finger geometry readers to grant ticket holders admittance to different parts of the park. Some businesses use hand geometry readers in place of timecards.

Systems that measure hand and finger geometry use a digital camera and light. To use one, you simply place your hand on a flat surface, aligning your fingers against several pegs to ensure an accurate reading. Then, a camera takes one or more pictures of your hand and the shadow it casts. It uses this information to determine the length, width, thickness and curvature of your hand or fingers. It translates that information into a numerical template.

Hand and finger geometry systems [6] have a few strengths and weaknesses. Since hands and fingers are less distinctive than fingerprints or irises, some people are less likely to feel that the system invades their privacy. However, many people's hands change over time due to injury, changes in weight or arthritis. Some systems update the data to reflect minor changes from day to day.

D. Iris scanning

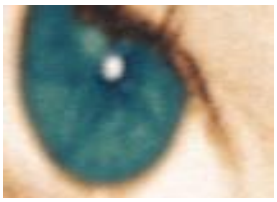

Fig. 9: Iris scanning

Iris scanning (see fig. 9) is the less intrusive of the eye related biometrics. It utilizes a conventional camera element and requires no intimate contact between user and reader. In also has the potential for higher than average template matching performance. It has been demonstrated to work with spectacles in place and with a variety of ethnic groups and

is one of the few devices that can work well in identification mode. However, ease of use and system integration has not traditionally been strong points with the iris scanning devices.

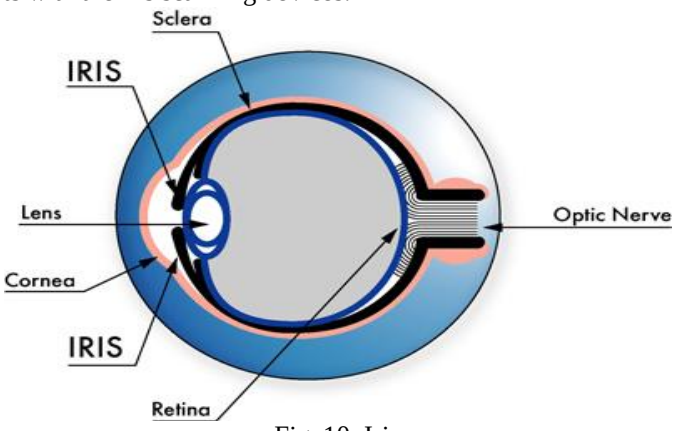

Fig. 10: Iris

Iris scanning can seem very futuristic, but at the heart of the system is a simple CCD digital camera. It uses both visible and near-infrared light to take a clear, high-contrast picture of a person's iris. With near-infrared light, a person's pupil is very black, making it easy for the computer to isolate the pupil and iris.

When you look into an iris scanner (see fig.11), either the camera focuses automatically or you use a mirror or audible feedback from the system to make sure that you are positioned correctly. Usually, your eye is 3 to 10 inches from the camera. When the camera takes a picture, the computer locates:

- The center of the pupil
- The edge of the pupil
- The edge of the iris
- The eyelids and eyelashes

It then analyzes the patterns in the iris and translates them into a code.

Fig. 11 An iris scanner

Iris scanners are becoming more common in high-security applications because people's eyes are so unique (the chance of mistaking one iris code for another is 1 in 10 to the 78th power. They also allow more than 200 points of reference for comparison, as opposed to 60 or 70 points in fingerprints.

The iris is a visible but protected structure, and it does not usually change over time, making it ideal for biometric identification. Most of the time, people's eyes also remain unchanged after eye surgery, and blind people can use iris scanners as long as their eyes have irises. Eyeglasses and contact lenses typically do not interfere or cause inaccurate readings.

E. Facial Recognition

This type of technology has been popularized in many action movies as a means of identifying villains as they enter a building. Facial biometrics can function from either short distances or over greater distances. This form of biometric however is often less reliable then more common forms such as fingerprints and iris scans. The interpretative functions the computer must perform to find a match is much more subjective using this technology. An image is examined for overall facial structure which works well over short distances but progressively loses accuracy the greater the distance between the individual and the scanner. Changes in lighting can also increase the error rate in these devices.

This type of technology is in place in several airport terminals and at many border crossings to help determine the identities of individuals at a distance who may be involved in criminal activities without alerting the individual that they are being monitored. One of the more attractive features of these types of products is their cost. Units can typically be

purchased for as little as $150. At this price, this type of technology might lend itself to electronic commerce, but the units can be cumbersome to use and still are not as reliable as other forms of biometrics to be used for encryption purposes.

Facial recognition devices have been difficult to substantiate in practice and extravagant claims have sometimes been made them. Facial recognition is very attractive from the user perspective and they may eventually become a primary biometric methodology

F. Voice verification

This is a potentially interesting technique if the amount of voice communication that takes place with regard to everyday business transactions is considered. Some designs have concentrated on wall-mounted readers whilst others have sought to integrate voice verification into conventional telephone handsets. Whilst there have been a number of voice verification products introduced to the market, many of them have suffered in practice due to the variability of both transducers and local acoustics. In addition, the enrolment procedure has often been more complicated than with other biometrics leading to the perception of voice verification as unfriendly in some quarters. However, much work has been and continues to be undertaken in this context and it will be interesting to monitor progress accordingly.

There are several distinct advantages that voice recognition [7] has for use in encryption technology. Not only are voice biometrics perfect for telecommunication applications, most of the modern personal computers already possess the necessary hardware to utilize the applications. Even if they don't, sound cards can be purchased for as little as $50 and condenser microphones can be purchased for as little as $10. Therefore, for less than $100 individuals can possess the technology needed to have fairly reliable biometric encryption technology for use over the Internet.

The error rate for this type of biometric is not as accurate, however, as some other forms. The error rate for this type of technology ranges between two and five percent, however it lends itself well for voice verification over the public telephone system and is more secure than PINs.

Some drawbacks to this technology are that voiceprints can vary over the course of the day, and ones health, such as a cold or laryngitis, can affect verification of the user by the system.

V. SELECTION OF BIOMETRIC TECHNIQUES

There are a lot of decision factors for selecting a particular biometric technology [8] for a specific application.

A. Economic Feasibility or Cost:

The cost of biometric system implementation has decreased recently; it is still a major barrier for many companies. Traditional authentication systems, such as passwords and PIN, require relatively little training, but this is not the case with the most commonly used biometric systems. Smooth operation of those systems requires training for both systems administrators and users.

B. Risk Analysis

Error rates and the types of errors vary with the biometrics deployed and the circumstances of deployment. Certain types of errors, such as false matches, may pose fundamental risks to business security, while other types of errors may reduce productivity and increase costs. Businesses planning biometrics implementation will need to consider the acceptable error threshold.

C. Perception of Users

Users generally view behavior-based biometrics such as voice recognition and signature verification as less intrusive and less privacy-threatening than physiology-based biometrics.

D. TechnoSocio Feasibility

Organizations should focus on the user-technology interface and the conditions in the organizational environment that may influence the technology's performance. The organization should create awareness among the users how to use the techniques and should overcome the psychological factors as user fears about the technology. Organization has to also consider the privacy rights of users while implementing the biometric techniques.

E. Security

Biometric techniques should have high security standards if they will be implemented in high secure environment. The biometric techniques should be evaluated on the basis of their features, potential risk and area of application, and subjected to a comprehensive risk analysis.

F. User friendly and social acceptability

Biometric techniques should be robust and user friendly to use and they should function reliably for a long period of time. The techniques should not divide the society into two group i.e. digital and non digital society.

G. Legal Feasibility

Government has to form a regulatory statutory framework for the use of biometric techniques in various commercial applications. It should form a standard regulatory framework for use of these techniques in commercial applications or transactions. If required the framework has to be regulated and changed time to time.

H. Privacy

As biometric techniques rely on personal physical characteristics, an act has to be made to protect the individual's privacy data not to be used by other. A data protection law has to be created in order to protect the person's privacy data.

VI . BIOMETRIC PERFORMANCE MEASURES [8]

A. False acceptance rate (FAR) or false match rate (FMR):

The probability that the system incorrectly declares a successful match between the input pattern and a non-matching pattern in the database. It measures the percent of invalid matches. These systems are critical since they are commonly used to forbid certain actions by disallowed people.

B. False reject rate (FRR) or False non-match rate (FNMR):

The probability that the system incorrectly declares failure of match between the input pattern and the matching template in the database. It measures the percent of valid inputs being rejected.

C. Receiver (or relative) operating characteristic (ROC):

In general, the matching algorithm performs a decision using some parameters (e.g. a threshold). In biometric systems the FAR and FRR can typically be traded off against each other by changing those parameters. The ROC plot is obtained by graphing the values of FAR and FRR, changing the variables implicitly. A common variation is the Detection error trade-off (DET), which is obtained using normal deviate scales on both axes.

D. Equal error rate (EER):

The rates at which both accept and reject errors are equal. ROC or DET plotting is used because how FAR and FRR can be changed, is shown clearly. When quick comparison of two systems is required, the ERR is commonly used. Obtained from the ROC plot by taking the point where FAR and FRR have the same value. The lower the EER, the more accurate the system is considered to be.

E. Failure to enroll rate (FTE or FER):

The percentage of data input is considered invalid and fails to input into the system. Failure to enroll happens when the data obtained by the sensor are considered invalid or of poor quality.

F. Failure to capture rate (FTC):

Within automatic systems, the probability that the system fails to detect a biometric characteristic when presented correctly.

G. Template capacity:

The maximum number of sets of data which can be input in to the system.

For example, performance parameters associated with the fingerprint reader may be:

- A false acceptance rate of less than or equal to 0.01 percent
- A false rejection rate of less than 1.4 percent
- The image capture area is 26×14 mm.

Obviously, these two measures should be as low as possible to avoid authorized user rejection but keep out unauthorized users. In applications with medium security level a 10% False Rejection Error will be unacceptable, where false acceptance rate error of 5% is acceptable.

False Acceptance When a biometric system incorrectly identifies an individual or incorrectly verifies an impostor against a claimed identity. It is also known as a Type II error.

FAR is the probability that a biometric system will incorrectly identify an individual or will fail to reject an impostor. It is also known as the Type II error rate.

It is stated as follows:

FAR = NFA / NIIA or FAR = NFA / NIVA

Where FAR is the false acceptance rate

NFA is the number of false acceptances

NIIA is the number of impostor identification attempts

NIVA is the number of impostor verification attempts

FRR is the probability that a biometric system will fail to identify an enrollee, or verify the legitimate claimed identity of an enrollee. It is also known as a Type I error rate.

It is stated as follows:

FRR = NFR / NEIA or FRR = NFR / NEVA

Where FRR is the false rejection rate

NFR is the number of false rejections

NEIA is the number of enrollee identification attempts

NEVA is the number of enrollee verification attempts

Crossover Error Rate (CER) Represents the point at which the false reject rate = the false acceptance rate.

It is good for comparing different biometrics systems

A system with a CER of 3 will be more accurate than a system with a CER of 4

VII. AREAS OF CONCERNS:

There are significant privacy and civil liberties concerns regarding the use of devices using biometrics that must be addressed before any widespread deployment. Briefly there are six major areas of concern [9]:

- Storage. How is the data stored, centrally or dispersed? How should scanned data be retained?
- Vulnerability. How vulnerable is the data to theft or abuse?
- Confidence. How much of an error factor in the technology's authentication process is acceptable? What are the implications of false positives and false negatives created by a machine?
- Authenticity. What constitutes authentic information? Can that information be tampered with?
- Linking. Will the data gained from scanning be linked with other information about spending habits, etc.? What limits should be placed on the private use (as contrasted to government use) of such technology?
- Ubiquity. What are the implications of having an electronic trail of our every movement if cameras and other devices become commonplace, used on every street corner and every means of transportation?
-

VIII. APPLICATIONS

Most of the biometric applications [9] are related to security and are used extensively for military purposes and other government purposes. The applications in the public domain that are available to common people include:

- Prison visitor systems, where visitors to inmates are subject to verification procedures in order that identities may not be swapped during the visit - a familiar occurrence among prisons worldwide.
- Driver's licenses, whereby drivers are expected to have multiple licenses or swapped licenses among themselves when crossing state lines or national borders.
- Canteen administration, particularly on campus where subsidized meals are available to bona fide students, a system that was being heavily abused in some areas.
- Benefit payment systems - In America, several states have saved significant amounts of money by implementing biometric verification procedures. The numbers of individuals claiming benefit has also dropped dramatically in the process, validating the systems as an effective deterrent against multiple claims.
- Border control - A notable example for this is the INSPASS trial in America where travelers were issued with a card enabling them to use the strategically based biometric terminals and bypass long immigration queues. There are other pilot systems operating elsewhere in this respect.
- Voting systems, where eligible politicians are required to verify their identity during a voting process. This is intended to stop ‘proxy’ voting where the vote may not go as expected.
- Junior school areas where problems are experienced with children being either molested or kidnapped.
- In addition there are numerous applications in gold and diamond mines, bullion warehouses and bank vaults as well as the more commonplace physical access control applications in industry.

IX. ADVANTAGES OF BIOMETRICS [10]

- Increase security - Provide a convenient and low-cost additional tier of security.
- Reduce fraud by employing hard-to-forge technologies and materials. E.g. minimize the opportunity for ID fraud, buddy punching.
- Eliminate problems caused by lost IDs or forgotten passwords by using physiological attributes. For e.g. prevent unauthorized use of lost, stolen or "borrowed" ID cards.
- Reduce password administration costs.
- Replace hard-to-remember passwords which may be shared or observed.

- Integrate a wide range of biometric solutions and technologies, customer applications and databases into a robust and scalable control solution for facility and network access.
- Make it possible, automatically, to know WHO did WHAT, WHERE and WHEN!
- Offer significant cost savings or increasing ROI in areas such as Loss Prevention or Time &Attendance.

X. DISADVANTAGES OF A BIOMETRIC SYSTEM [10]

- The finger print of those people working in Chemical industries is often affected. Therefore these companies should not use the finger print mode of authentication. It is found that with age, the voice of a person differs. Also when the person has flu or throat infection the voice changes or if there is too much noise in the environment this method may not authenticate correctly. Therefore this method of verification is not workable all the time
- For people affected with diabetes, the eyes get affected resulting in differences.
- Biometrics is an expensive security solution.

XI. Conclusion

In this study I have studied about various biometric characteristics. I have discussed the Enrollment, Verification and Identification procedure for the Biometric System. I have studied various biometric techniques with their advantages and disadvantages and explained what the need was for new biometric technique. Decision factors for selecting a particular biometric technology and various performance measures were also discussed. Biometric systems still have many areas of concerns.

The next five years promise to be a time of continued change, as complex and expensive research programs delivers refinements to current biometric systems and the development of completely new technologies and applications. Perhaps the future is actually staring us in the face, looking right into our eyes and sitting in the palm of our hand all at the same time.

References

[1] Biometric Technique retrieved on 29 Jan 2014 from <http://ewh.ieee.org/r10/bombay/news5/Biometrics.htm>
[2] Introduction to Biometrics and its Characteristics retrieved on 5 Feb 2014 from <http://www.cse.iitk.ac.in/users/biometrics/pages/what_is_biom_more.htm>
[3] Operation of Biometric System retrieved on 12 Feb 2014 from <http://www.cvip.uofl.edu/wwwcvip/education/ECE523/Spring%202011/Lec1.pdf>
[4] Finger Print Verification retrieved on 18 Feb 2014 from <http://www.emory.edu/BUSINESS/et/biometric/Fingerprint.htm>
[5] Handwriting Verification or Signature Verification retrieved on 22 Feb 2014 from <http://www.emory.edu/BUSINESS/et/biometric/Signature.htm>
[6] Hand and Finger Geometry System retrieved on 1 March 2014 from <http://science.howstuffworks.com/biometrics.htm>
[7] Voice Verification System retrieved on 25 Feb 2014 from <http://www.emory.edu/BUSINESS/et/biometric/Voice.htm>
[8] Decision Factors for Selecting a Particular Biometric System retrieved on 7 March 2014 from <http://ezinearticles.com/?Biometric-Techniques-Enhancing-Security-Standards-In-High-Performance-Enterprise&id=1224599>
[9] Areas of Concerns of Biometric System retrieved on 14 March 2014 from <http://ewh.ieee.org/r10/bombay/news5/Biometrics.htm>
[10] Advantages and Disadvantages of Biometric System retrieved on 2 March 2014 from <http://wiki.answers.com/Q/What_are_the_disadvantages_and_advantages_of_biometrics>