International Journal of Advances in Computer Science & Its Applications– IJCSIA
Volume 5 : Issue 2 [ISSN : 2250-3765]
Publication Date: 30 October, 2015

BiometricAuthentication An Introduction

[Dr.K.R.Badhiti]

***Abstract*—Providing security has become a challenging factor in today's advanced computerized engineering and Technological environment. Traditional methods like memorizing passwords, carrying ID cards have their own draw backs. Biometric Authentication has become more and more reliable, secured and most convenient tool. Simply Biometrics refers to establishing identity based on the physical and behavioral characteristics of an individual such as face, fingerprint, hand geometry, iris, keystroke, signature, voice, etc. Biometric systems offer several advantages over traditional authentication schemes. They are inherently more reliable than password-based authentication as Biometric traits cannot be lost or forgotten.This paper explains various Biometric Traits which helps in authentication process and explain how iris is more reliable,when compared with other Biometrictraits.**

Keywords—BiometricAuthentication,Traditional Authentication,Biometric Traits

Introduction

The term Biometrics is derived from the Greek word Bios means "life" and metric means "measure". Biometric can be defined as the study of measuring those biological characteristics which include both physiological as well as behavioral characteristics that make human beings unique for recognition purposes. Traditionally, machines perform recognition using knowledge based techniques (ex: passwords) and / or token based techniques (ex: ID cards). In cases where high levels of security are required, identification is carried out by combining these two techniques with the intervention of authorized persons who verify the information provided. These levels have various problems i.e. they can be lost or forgotten. The security field uses three different types of authentication:

Something you know — a password, PIN, or piece of personal information.

Something you have — a card key, smart card, or token.

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.Personal Identification system should be reliable, fast, automated human requirement system.

Biometric definition

The definition of Biometrics given by National institute of Standards and Technology divides Biological measurements into two categories:

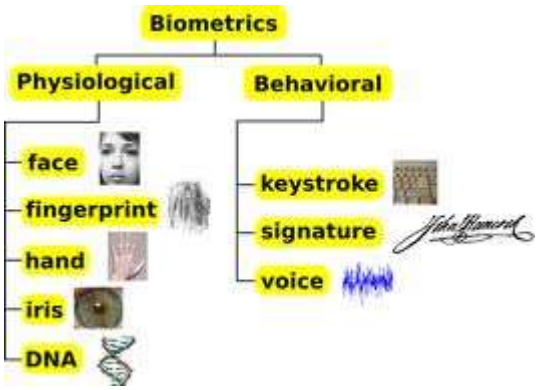

Fig-1

History of Biometrics

The first recorded evidence of using biometric authentication was in ancient Egypt, trusted traders were identified based on certain characteristics such as height, eye color and complexion. Using human features for Identification is not a modern technique. First reports on Biometrics are dated as far back as the 14th century when Chinese merchants used ink to register children's finger prints for Identification purposes. With the significant progress both in fingerprint and signature identification, at the end of 20th century; Biometrics became feasible and better known. Several Biometric systems have been installed at airports to facilitate the identification of travelers for security purposes and for border registration control. The Application of Biometrics has increased considerably it is now frequently found in health care environment at school facilities and used for physical access to several company premises. Biometric systems have been applied to a broad range of applications on several fields of our society such as forensic science, financial and trade security, physical access control check points, information systems security, customs and immigration, national identification cards, and driver licenses, among other examples.

Biometric Modalities

Several human characteristics have been proposed and evaluated for Biometric applications in the past few decades. The term modality in Biometrics refers to the **Trait** to be recognized by the system. Ex finger print or face. Not all human traits can be used for Biometrics. Among all the

Author Dr .Kezia Rani Badhiti

University Collegeof Engineering and technology Adikavi Nannaya university Andhra Pradesh,India

different traits a human being has, several requirements on the traits have been compiled and studied.

Requirements: In order to qualify as a Biometric identifier, the following general requirements must be met:

Uniqueness, Universality, Permanence, Collectability, Per*formance, Acceptability, Circumvention.*

How A Biometric System Works

Biometric relies on pattern recognition science, which bases its performance on statistics. Pattern recognitions attempts to find new mathematical spaces where different samples from the same object tend to be in the same space area, at a distance from other object areas.

In mathematical terms, we can say that we are trying to establish a new space where the Intra class distance (distance between samples from the same object) is significantly lower that the Inter class distance (distance between samples from different objects).Several samples should be distinguishable, but in the initial space all seem to be mixed. An algorithm is applied to transform all these sets into a new space where the differentiation between each sample is clear.

A Biometric system, regardless of the trait being studied follows the block diagram:

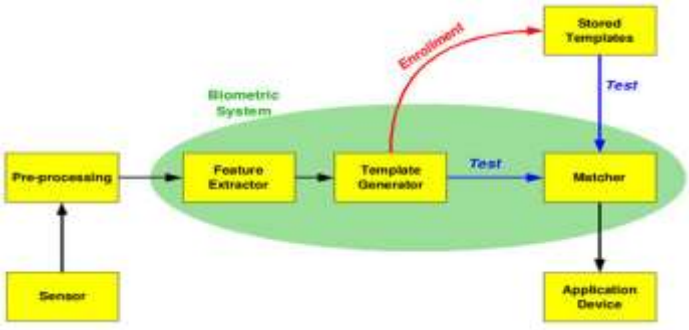

Fig-2

The first module in the scheme is the sensor module, Biometric reader or scanner. This module is in charge of acquiring the raw biometric trait of the user. The next module is required for pre-processing of the sample; this block is responsible for two main tasks...

1. To detect whether the quality of the raw sample obtained is sufficient enough to perform further processing.
2. The preprocessing itself, within the extraction block, may require previous processing to prepare data from which our representation is to be extracted. Among the possible functions performed by this block, is the segmentation of data to be checked i.e., detect where a face is in an image, isolate the iris from the rest of an image, detect the core point of a finger print. The function of features extraction consists of obtaining data which represents univocally the initial data and that can be used for later comparison. The data resulting from this block is generally called a feature vector. This enhancement facilitates the comparison between the current vector and those that are previously stored in the following block allowing a decision to be made. The result from the comparison is a similarity score. Thus a threshold can be set to detect if this value is sufficient to ascertain the data as belonging to one user or another. The choice of thresholds depends on system requirements.

Identification & Verification

Identification and Verification are two possible recognition processes which are performed at each time when a potential user attempts to access a system. Identification is understood as the process of finding the identity of a user where no identifications are provided or no indications are provided i.e., it should answer the question "who am I?".A biometric sample is acquired without any associated identity claim. The task is to identify the unknown sample as matching one of a set of previously enrolled known samples. The set of enrolled samples is often called a Gallery and the unknown sample is called a probe. The probe is matched against all of the entries in the gallery, and the closest match, assuming it is close enough, is used to identify the unknown sample.

In a verification scenario, a person claims a particular identity and the biometric system is used to verify or reject the claim. Verification is done by matching a biometric sample acquired at the time of the claim against the sample previously enrolled for the claimed identity. If two samples match well enough, the identity claim is verified, and if the two samples do not match well enough, the claim is rejected.

Biometric Error Analysis

All Biometric systems suffer from two forms of errors:
Form-1 is a false acceptance and Form-2 is a false rejection.
Form-1 happens when the Biometric system authenticates an imposter. Form-2 means that the system has rejected a valid user.Biometric systems accuracy is determined by combining the rate of false acceptance and rejection.

Accuracy and System Performance

In Biometric processes the sample acquired is always different from that previously stored. These samples lead to feature vectors, which in spite of being from a single user, are slightly different however if the differences between other users templates are noticeable, the sample being verified or can be misidentified with another identity, provoking an error in the system performance. Measuring the errors in Biometrics is important, because these systems are not just subject to errors from pattern recognition problem, but also from the capture process.

Biometric System Error Rates

The most commonly used error rates are.:

False Match Rate (FMR): This is the probability that the system incorrectly declares a successful match between the input sample and an incorrect template.

False Non-Match Rate (FNMR): This is the probability that the system incorrectly declares match failure between the input pattern and the matching template from the database. It measures the percentage of valid inputs being rejected.

Equal Error Rate: Is the rate when both the accept and reject errors are equal. The equal error rate is commonly used when

a rapid comparison of two systems is required. The lower the EER value the more accurate the system is considered to be.

Template Capacity: The maximum number of data sets which can be included in the system.

The traits studied can be divided into two major groups:

Physical or behavioral. Physical modalities are those referred to as the name indicates physical characteristics of the user such as face finger print or hand geometry. Whereas behavioral modalities are those related to the way a user does something. Samples of behavioral modalities are speech recognition, signature and key dynamics. Behavioral modalities are non invasive and therefore are more accepted by users.

Due to different positioning on the acquiring sensor, imperfect imaging conditions, environmental changes deformation, noise and bad user's interaction with the sensor, it is impossible that two samples of the same biometric characters, acquired in different sessions, exactly coincide. For this reason a biometric matching systems response is typically a matching score 's'(normally a single number) that quantifies the similarity between the input and the database template representations, the higher the score, the more certain the system is that the two samples coincide. A similarity score 's' is compared with an acceptance threshold 't' and if 's' is greater than or equal to t compare samples belong to a same person. Pairs of biometric samples generating scores lower than 't' belong to a different person. The distribution of scores generated from pairs of samples from different persons is called an imposter distribution, and the score distribution generated from pairs of samples of the same person is called a genuine distribution.

Physiological Modalities: Face

Facial recognition is the most intuitive Biometric modality as it is the instinctive manner in which humans identify each other. Face techniques are based on two main ideas. Consider the face as a unique organ, and therefore taking each face as a unique pattern. Measure important points on the face such as eyes, nose, mouth etc and the distance between them.

Drawbacks

It is important to remark that a face is not a univocal trait e.g. twins or people with similar faces can be miss identified. Furthermore artificial techniques can be used to change the structure of the face to make them similar to others, such as makeup or plastic surgery. These problems as well as changes due to aging, lead to errors and decrease the performance of these systems. However the high user acceptance has made these modalities as one of the most demanded.

Finger Print

A fingerprint is defined by a pattern of ridges and valleys on the surface of the finger tip. This pattern is developed in the early stage of the fetal development and follows a stochastic process.Fingerprint systems can be divided into two different types. Those based on macroscopic features and those based on microscopic details. The macroscopic system base their search on the comparison on region of interest of the finger print, meanwhile microscopic solution looks for the distance between ridges or bifurcations.

Drawbacks

Finally fingerprints are a universal feature. However a small fraction of the population may have fingerprints unsuitable for recognition because of genetic factors like aging, environmental or for occupational reasons. This problem is usually related to the sensor technology used, as some sensors present problems when acquiring samples from the above mentioned populations.

Iris

The Iris begins to form in the 3rd month of gestation and the structures creating its pattern are largely completed by the eight month. Its complex pattern can contain many distinctive features such as arching ligaments, furrows, ridges, crypts, rings, corona, freckles and a zigzag collarets. Iris scanning is less intrusive than retinal because the iris is easily visible from several meters away.

Responses of the Iris to changes in light can provide an important secondary verification that the iris presented belongs to a live subject. Irises of identical twins are different, which is another advantage. Newer systems have become more users friendly and cost effective. A careful balance of light, focus, resolution and contrast is necessary to extract a feature vector from localized image. While the iris seems to be consistent throughout adulthood, it varies somewhat up to adolescence.

Capturing the image:

The image can be captured by a standard camera using both visible and infrared light.

The procedure can be manual or automated. In the manual procedure the iris should be in focus and the length between the camera and iris should be within six and twelve inches , while in automated procedure the length is between three and a half inches and one meter.

Define the location of the iris and optimizing the image:

When the iris is in focus, the iris recognition system just identifies the image with the best focus and clarity. The image is analyzed. The purpose of the analysis is to identify the outer boundary of the iris where it meets with white sclera of the eye, the pupillary boundary and the centre of pupil. The result of the analysis is the precise location of the circular iris, Iris recognition system tries to identify the areas suitable for feature extraction and analysis: removing areas covered by the eyelids, deep shadows, reflective areas. This attempt is known as optimization of the image.

Store and compare the image: the process of division, filtering and mapping segments of the iris into hundreds of vectors takes place. Vectors can be easily understand as "what" and "where" of the image. Iris image is saved as so-called Iris Code, 512-byte record. The record is stored in a database. When there is a need in comparison the same process takes place but instead of storing, the system compares the given sample with the record stored in the database.

Among the advantages of iris recognition method the first place is taken by fact that iris remains stable during the whole life. There is no direct contact between the user and camera.

The laser does not be used, just video technology. The high level of accuracy put the method in one row with fingerprinting. The method is remarkable for its high speed, scalability.

Drawbacks

The iris is a small organ and it is impossible to take the process of scanning from a distance. For people with such eye problems as blindness and cataracts, it will be very difficult to take part in the process of recognition as it is very difficult to read the iris. Without correct amount of illumination it is difficult to capture image.

DNA

DNA is probably the most reliable biometrics. It is in fact a one dimensional code unique for each person exception is identical twins. This method however has some drawbacks
Contamination and sensitivity since it is easy to steal a piece of DNA from an individual and use it for an ulterior purpose.
No real time application is possible because DNA matching requires complex chemical methods involving expert's skills.
Privacy issues since DNA sample taken from an individual is likely to show susceptibility of a person to some diseases. All these limits the use of DNA matching to forensic application.

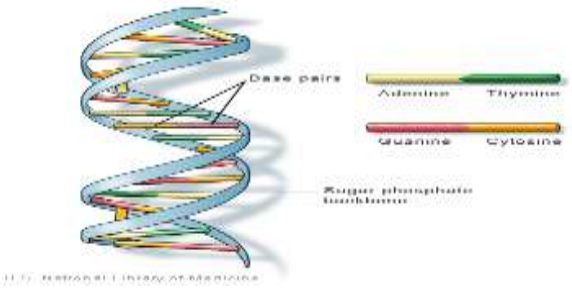

Fig-3

Behavioural Biometrics:Gait

Gait is the peculiar way one walks and it is a complex spatial – temporal Biometrics. It is not supposed to be very distinctive but can be used in some low security applications. Gait is a behavioral Biometric and may not remain the same over a long period of time, due to change in body weight or serious brain damage. Acquisition of gait is similar to acquiring a facial picture and may be an acceptable biometric since video sequence is used to measure several different movements this method is computationally expensive.

Signature

Signature is a simple, concrete expression of the unique variations in human hand geometry. The way a person signature his or her name is known to be characteristic of that individual. Collecting samples for this biometric includes subject cooperation and requires the writing instrument. Signatures are behavioral Biometric that change over a period of time and are influenced by physical and emotional conditions of a subject. In addition to the general shape of the signed name, a signature recognition system can also measure pressure and velocity of the point of the stylus across the sensor pad.

Voice

The features of an individual's voice based on physical characteristics such as vocal tracts, mouth, nasal cavities and lips that are used in creating a sound. These characteristics of human speech are invariant for an individual, but the behavioral part changes over time due to age, medical conditions and emotional state. Voice recognition techniques are generally categorized according to two approaches
Automatic speaker verification (ASV) and Automatic Speaker Identification (ASI). Speaker verification uses voice as the authenticating attribute in a two-factor scenario. Speaker identification attempts to use voice to identify who an individual actually is. Voice recognition distinguishes an individual by matching particular voice traits against templates stored in a database.

Keystroke

It is believed that each person types on a key board in a characteristic way. It is a behavioral biometric for some individuals, one could expect to observe large variations in typical typing patterns. Advantages of this method are that keystrokes of a person using a system could be monitored unobtrusively as that person is keying information. Modern keystroke dynamics utilizes behavioral biometrics in an effort to identify individuals by the manner and rhythm that he or she types characters on a keyboard or keypad. The keystroke rhythms of the user are measured to develop a unique biometric template of the user's typing pattern for future authentication. Raw measurements available from most every keyboard can be recorded to determine dwell time (the time a key is pressed) and flight time (the time between key down and the next key down and the time between key up and the next key up).After the recording is made, it is processed through a specialized algorithm, which determines a primary pattern for future comparison.

Fig-4

Unimodel Biometric systems

There is a variety of problems with biometric systems installed in real word applications which prove that biometric is not fully solved problems. There is still plenty of scope for improvement.

Limitations of Biometric systems using any single biometric characteristic:

Noise in sensed data: Example is a fingerprint with a scar. Noisy data can also result from accumulation of dirt on a sensor or from ambient conditions.

Intra class variations: Biometric data acquired from an individual during authentication may be very different from the data that was used to generate the template during enrollment. This variation is typically caused by user who is incorrectly interacting with the sensor.

Distinctiveness:

While a biometric trait is expected to vary significantly across individuals, there may be large inter class similarities in the feature sets used to represent these traits. This limitation restricts the discriminalities provided by the biometric trait.

Non-universality: While every user is expected to posses the biometric trait being acquired in realty it is possible that a group of users do not posses that particular biometric characteristic.

Spoof attacks: An individual may attempt to forge the Biometric trait. This is particularly easy when signature and voice are used as an identifier.

Multi model Biometric system:

Using one single modality presents several disadvantages:

The trait studied in some cases is not universal and therefore, becomes impossible to be measured in some individuals.

The algorithm used does not provide sufficient performance results for identification purposes. Indexing in large databases can take a long time according to the modality considered. Some biometric modalities are easily forgeable, such as voice or fingerprint recognition.Data acquired by the system can be noisy or even corrupt, increasing the failure-to-capture rate. Additionally, sensor malfunction can increase this rate.

Levels of consolidation

Information presented by multiple traits may be consolidated at various levels. At the feature extraction level, the data obtained from each sensor is used to compute a feature vector. Since data from various traits are independent of each other they can be concatenated to a new vector with higher dimensionality that represents a person's identity in a new hyperspace.This new vector is then used in the matching and decision making modules of the biometric system. At the matching score level, each individual system provides a matching score and those scores are combined to affirm the authenticity of the claimed identity. At the decision level, each individual system provides multiple biometric data and the resulting vectors are individually classified into two classes accept or reject. Final decisions are consolidated by employing techniques such as majority voting.

Integration at feature extraction level is expected to perform better fusion at two other levels. However this is not always the best solution. The feature shapes of multiple Biometrics may not be compatible and even if they are compatible there is still a problem of combining the feature set. Concatenation could result in a feature vector with a large dimensionality. Fusion at the decision level is considered to be rigid due to the availability of limited information.

Fusion at the matching score level seems to be the logical choice as it is relatively easy to access and combine scores presented by the different modalities. It is generally believed that a combination scheme applied as early as possible in the recognition system is more effective.

Multi model Biometric systems can be designed to operate in five integration scenarios.

1. Multiple sensors
2. Multiple Biometrics
3. Multiple units of same Biometrics
4. Multiple snapshots of same Biometrics
5. Multiple representations and matching algorithms of same Biometric.

Conclusion

Even though Biometric system playing an important role in security issues, there are still drawbacks. Elaborate Research work should be done on Liveness Detection in order to eradicate Spoofing, which is a threat to Biometric systems.

References

[1] A. K. Jain, A. Ross, S. Prabhakar, "An Introduction to Biometric Recognition", IEEE Trans. on Circuitsand Systems for Video Technology, Vol. 14, No. 1, pp 4-19, January 2004.

[2] Matthew A. Turk, Alex P. Pentland, "Face recognition using Eigen faces" Proc. IEEE Conference on Computer Vision and Pattern Recognition: 586–591. 1991.

[3] A. Jain, A. Ross, S. Prabhakar, "Fingerprint matching using minutiae and texture features", International Conference on Image Processing (ICIP), Thessaloniki, Greece, 2001, pp. 282–285.

[4] X. Tan and B. Bhanu, "Fingerprint matching by genetic algorithms," Pattern Recognition, vol. 39, no. 3,pp. 465– 477, 2006.

[5] John Daugman, "How Iris Recognition Works", IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 14, NO. 1, JANUARY 2004,pp 21-30

[6] R. Wildes, "Iris Recognition: An Emerging Biometric Technology" Proceedings of the IEEE, vol.85, no.9, September 1997 http://ieeexplore.ieee.org/iel3/5/13673/00628669.pdf

[7] M. Negin et al., "An iris biometric system for public and personal use", IEEE Computer Volume 33, Issue 2, pp 70 – 75, Feb. 2000

[8] Individual Biometrics – Iris Scan http://ctl.ncsc.dni.us/biomet%20web/BMIris.html

[9] John Daugman, Iris recognition border-crossing system in the UAE, 2004 http://www.cl.cam.ac.uk/~jgd1000/UAEdeployment.pdf

[10] Max Chasse, La Biometrie au Quebec, Les enjeux, july 2002http://www.cai.gouv.qc.ca/06_documentation/01_pdf/biom_enj.pdf

[11]Iris –An emergent Biometric Technology for Personal Authentication Kezia rani badhiti,Dr.T.Sudha ,International Journal of Engineering and Information Technology ResearchVol 3 issue 4 Oct 2014,pg 37-48.

[12]Spoofing-A Threat to Biometric Systems,Kezia Rani Badhiti,Dr T Sudha,Journal of Computer Science and Engineering Vol 7,issue 2.

[13] Personal Identification based on Human Iris,Kezia rani Badhiti,Dr.T.Sudha,International Journal of application or Innovation in Engineering and Management vol 2,issue 6 june 2013.

[Dr.Kezia Rani Badhiti having 10 years of teaching experience,Many Research papers are published in International journals,Automated Personal Identification based on Human iris is the research topic,Interested in Image processing,Artificial Intelligence,Web technologies,network systems.