Volume 4, Issue 1, January 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Comparative Study on Biometric Technology

Yesha Pruthi*, Harsha Singh, Aditi Verma

PDMCEW,MDU,Rohtak

India

Abstract— Biometrics is defined as an automated measurement of behavioral and psychological characteristics to determine or authenticate a person's identity living or dead. In a layman's language it is a fundamental pattern recognition system that not only recognizes a person but also authenticates by using different psychological characteristics as finger print, facial recognition, iris scan, hand geometry, vascular patterns, retinal scan and DNA and also various behavioral characteristics such as voice/speaker recognition, signature/handwriting and keystroke/patterning. Forensics, prison security and secured access widely use this growing technology for authentication. Authentication may be defined as the process of identifying a person by making use of security systems. Biometric technology not only attracts the interest of the computer science researchers but neuroscientists and psychologists are also attracted towards it. This paper highlights different biometric techniques such as iris scan, hand geometry, retina scan and face recognition techniques in concern with human interface.

Keywords— Biometrics, facial recognition, Biometric Identification, Biometric testing, Biometric applications.

I. INTRODUCTION

A biometric technology verification system verifies a person's identity by comparing either behavioral or psychological trait of a person to a previously stored sample of the trait. The cost effectiveness, reliability and high accuracy in certain applications has increased the number of possible application areas for biometric identity verification. Today, you can get silicon fingerprint scanner measuring only 2*15*15mm by only spending few dollars.

Previously biometrics included the identification of people by distinctive body features such as scars or grouping of others psychological criteria like height, complexion and eye colour. Several advantages are offered by biometric technology over traditional methods which included personal identification numbers (PIN) or id cards for several reasons.

a) The person to be identified/verified need to be physically present at the point of identification.
b) Identification based on biometric techniques obviates the need to remember a password or carry a token.

Most fingerprint verification systems use minutiae point matching. Minutiae points are the points in fingerprint images where the fingerprint ridges either end or splits up into two new ridges. There are two main approaches to minutiae detection in fingerprint images, direct grayscale detection and binary detection. This thesis prevents a binary approach to minutiae detection.

With the growth of computers and internet in our day today lives it is important to protect our personal data. By replacing PIN's biometric techniques can turn aside unauthorized access to:

a) ATM's
b) Laptops
c) Desktop pc's
d) Cellular phones
e) Workstations
f) Computer networks
g) Smartcards

The problem with the PIN's and passwords is they may be forgotten and token based identification methods like driver license's, PAN cards, passports etc may be stolen or lost.

II. IDENTIFICATION VS VERIFICATION

Sometimes identification and verification are interpreted as similar terms but they have two different meanings. A biometric system can either be a 'verification' system or an 'identification' system which may be defined as:

a) *Identification* (1:n): One to many. A person's identity can easily be determined by using biometrics even without his awareness or approval. This may include scanning a crowd with the help of a camera and by using facial recognition technology one can easily verify matches that are already present in the database.
b) *Verification* (1:1): One to one. It can also be used to verify a person's identity such as one can grant access to a bank account to any ATM by using retina scan.

III. BOMETRIC CHARACTERISTICS

Biometric is generally coupled with the set of unique physiological characteristics to identify a person, some of the major characteristics of biometrics are:

a) *Uniqueness*: Every person must possess a characteristic, an identical trait wont appear in two people.
b) *Measurability*: Must be easy to gather the attribute data passively and measured/captured with simple technical instruments.
c) *Privacy*: This process should not break the privacy of the individual.
d) *User friendly*: Are easy and comfortable to measure.
e) *Acceptance*: The capturing should be possible in a manner acceptable to a large fraction of the residents.

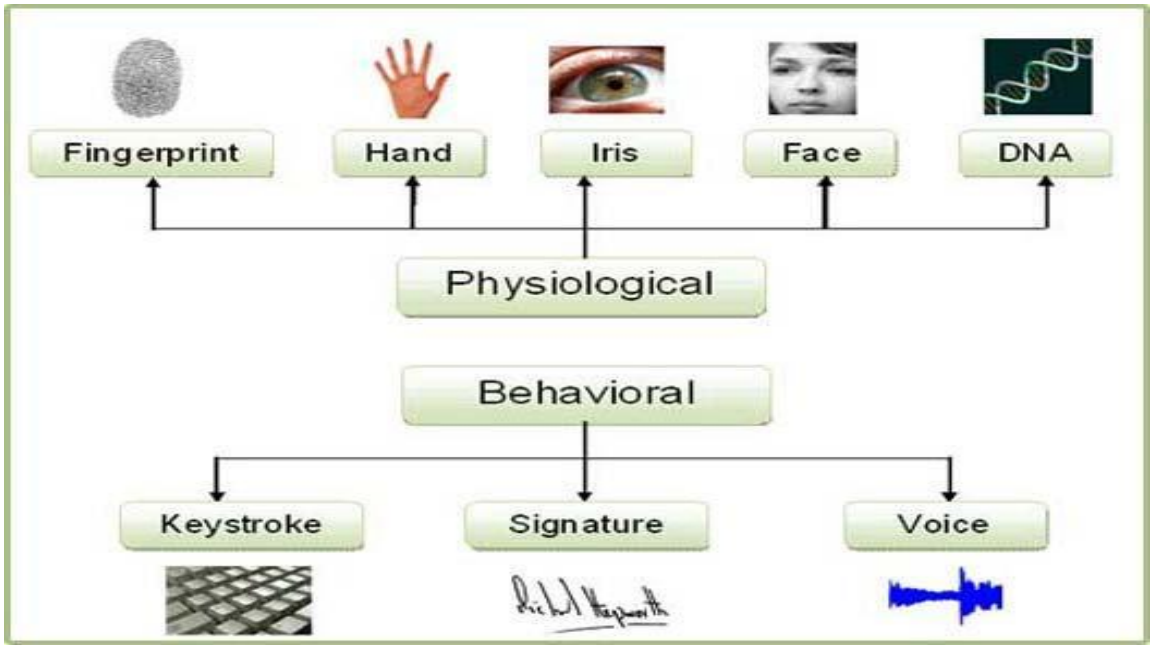
IV. ADVANTAGES OF BIOMETRICS

a) At the time of authentication we require the person to be authenticated at that point.
b) Passwords can easily be lost/forgotten while biometric traits cannot be.
c) Biometric traits are difficult to copy, distribute and share.

V. PSYCHOLOGICAL VS BEHAVIORAL

It is important to distinguish between psychological and behavioral human characteristics while referring to biometric technology. A stable human physical characteristic such as fingerprint, iris pattern or blood vessel pattern on the back of eye is generally referred to as psychological characteristic. Without significant duress this type of measurement is unchanging and unalterable.

Behavioral characteristic is a reflection of an individual's psychological makeup although some physical traits have a major influence such as size and gender. Some examples of the behavioral traits include: keystroke dynamics and speech verification/identification. The person's identity can be resolved in two ways: Identification and verification. Verification means "I am who I claim to be?" on the other hand identification means "who am I?".



Physical biometrics includes:

a) Fingerprint
b) Facial recognition
c) Iris scan
d) Hand geometry
e) Retina scan
f) DNA: for analyzing genetic makeup
g) Vascular patterns

Behavioral biometrics includes:

a) Speaker/voice recognition
b) Keystroke patterning
c) Handwriting/signature

VI. BIOMETRIC TECHNIQUES

a) *Fingerprint recognition*: This technology is most widely used biometric technology. By analyzing the trivia of a human being we can define the uniqueness of a fingerprint (optical, silicon, ultrasound). Trivia includes sweat

pores, distance stuck between ridges and bifurcation. The arrangement of ridge patterns of any two persons cannot be same even identical twins. With changeable degrees of accuracy and correctness there are several sub-methods in fingerprinting. A low level framework is provided by fingerprint SDK with fingerprint reader, capture an image, extract the minutiae data from the image and compare the two sets of extracted minutiae data. The major advantage of this technique is its very high accuracy and most economic biometric PC user authentication technique. Today it is one of the most developed biometrics. It is standardized.

b) *Face recognition*: One commonly looks at faces to recognize a person which differentiate one person another. In this technique unique shape, positioning of facial features and pattern are analyzed. Our face is a key component in a way we humans remember and recognize each other that's why face is a natural biometric. Face recognition is largely software based and highly complex technology. To simulate human interpretation of faces artificial intelligence is used. The major drawback of this technology is that people do change over time such as wrinkles, glasses, beard and positioning of the head can change the performance. Some kind of machine learning has to be implemented to increase the accuracy and to adapt these changes. The two methods to capture are: using video or thermal imaging. As standard video cameras can be used video is more common. In this the spatial geometry of unique features of face is recorded. This technology is cheap and non intrusive. This technology is very useful for personal verification and recognition and on the other hand it is difficult to implement as different situation that a human face can be found. Face recognition is a five step process which include:
   a) Acquiring the image of an individual's face
   b) Locate image of face
   c) Analysis of facial image
   d) The face by the software is compared to all the created face prints the system has in its database.
   e) Match or don't match

c) *Voice recognition*: The visual features of human body are not measured in voice recognition. Sound sensations of a person are compared and measured to an existing dataset. A secret code is usually required to be spoken by the person to be identified. Voice identification has been derived from the basic principles of speech recognition. The major advantages of voice recognition is it high social capability, the verification time is also less approximately about five seconds and it is cheap too. Its disadvantages includes low accuracy, the voice of a person van change if one is suffering from an illness such as cold which may make identification difficult.

d) *Signature recognition*: To recognize an individual's handwritten or signature the process of signature recognition is used. To confirm the identity of a computer client dynamic signature verification technology uses the behavioral biometrics of handwritten signature. Analyzing the shape, speed, stroke and pen pressure during the act of signing natural does this. For asserting ones identity signature is one of the most accepted method. To ensure the uniqueness of its author the static geometry of signature is not enough. Within dynamic signature verification number of characteristics can be extracted from the physical signing of process. It takes less time for verification that is about 4-5 seconds. It is inexpensive technology.

e) *Palm recognition*: A process is carried out which includes collecting a 3 dimensional image of the hand and then extracting the feature vector and then comparing it with the database feature vector. Though these devices are bulky but on the other hand identification is done in short time. As with finger images ridges, valleys and other miniature data are found on the palm. Some vendors are also looking at the access control market and follow the footsteps of finger scanning.

f) *Hand Geometry*: a process is carried out which includes collecting the 3-D image of top and sides of hands and fingers and then extracting and comparing the feature vectors with the dataset feature vectors. In hand geometry the image of the hand is taken and the shape and length of fingers and knuckles are measured. Though it is convenient and fast this technology does not achieve the highest levels accuracy. Cameras positions on or above and on the side of hand capture images from which measurements are taken at selected points.

g) *Iris Scan*: for iris scan technology a specialized camera is required very close to the subject not above their feet, uses an infrared images to illuminate the eye and capture very high resolution photograph. This process takes only few seconds for its completion and give details about the iris knowingly procedure, it then records and store in the database for future identification and verification. Due to the presence of eye glass and contact lens the quality of iris image does not get affected.

h) *Retina Scan*: It is done by taking the pattern of blood vessels in the retina of the eye. It also uses a part of the eye and this technology is much older than the iris scan technology. In 1953 EyeDentify launched the first retinal scanning system. A coherent infrared light source is necessary to illuminate the retina as retina is not directly visible. In blood yatch the infrared energy is immersed more rapidly than by surrounding tissue. For characteristics points within the pattern the image of the retina blood vessel pattern is then analyzed.

VII. PERFORMANCE

The performance metrics for biometric systems the following are used:

a) *False Match Rate or False accept rate (FMR or FAR*): It may be defines as the probability that the system incorrectly matches the input pattern to a non matching trait in the dataset. The percent of invalid input which are incorrectly accepted are measured.
b) *False Non Match Rate or False Reject Rate (FNMR or FRR*): It may defined as the probability the system fails to detect a match between an input pattern and a matching trait in the dataset. The percent of valid inputs that are incorrectly rejected are measured.
c) *Receiver Operating Characteristic or Relative Operating characteristic (ROC*): The visual characterization of the trade of between FRR and FAR is known as Roc plot on a threshold which determines how close to a template the input need to be for it to be considered a match the matching algorithm performs a decision based. These will be less false non matches but more false accepts if the threshold is reduced. Correspondingly a highest threshold will reduce the FAR but increase the FRR. A common variation which is obtained using normal deviate scales on both ones is DETECTION ERROR TRADE (DET). For higher performances this liner graph illuminates the differences.
d) *Cross Over Error rate or Equal Error Rate (CER or EER*): it is the rate at which both accept and reject errors are equal. From the ROC curve the value of EER can easily be obtained. To compare the accuracy of devices with different ROC curves we make use of EER. The device with lowest EER is most accurate. The accuracy of the system increases as the EER decreases.
e) *Failure To Enroll Rate (FER)*: The rate at which attempts to create a template from an input is unsuccessful. Low quality inputs are the major cause of failure to enroll rate.
f) *Failure To Capture Rate (FTC*): The probability that the system fails to detect a biometric input when presented correctly.
g) *Template Capacity*: It refers to the maximum number of sets of data which can be stored in the system.

VIII. CONCLUSION

Biometrics is based on the development of pattern recognition systems. Electronic or optical sensors like cameras and scanning devices are used to record images and videos or measurement of a person's unique characteristics. Biometric is a process that is accepted globally in establishing forensic evidence in a law courts. There are numerous forms of biometrics now being built into technology platforms. This rapidly evolving technology is used widely in security forensics prevent unauthorized access in Banks and ATMs, smart cards, cellular phones and computer networks. The International Biometric group strike system includes: fingerprint dry/oily finger, in facial recognition lighting conditions, in voice recognition cold or illness that affects voice, in hand geometry bandages, in iris scan to much movement of head or eye and in signature scan. In biometric technology lots of applications and solutions are used in security systems which can improve our lives such as: improved security, it is reduced and password administrator costs, easy to use and make life more secure and comfortable.

REFRENCES

[1]. Renu Bhatia, Department of Computer Science and Application, *Biometrices and Face Recognition Techniques* International Journal of Advanced Research in Computer Science and Software Engineering Vol 3, Issue 5, May 2013.
[2]. K P Tripathi, *International Journal of Computer Applications (0975-8887) volume 14-No.5, january2011.*
[3]. EyeDentify, http://eyedentify.com/
[4]. A. K. Jain, R. Bolle, and S. Pankanti, eds., *Biometrics: Personal Identification in Networked society.* Kluwer Academic Publishers, 1990
[5].Paul Reid, Biometrics for Network Security, Prentice Hall of India.
[6].Roger Clarke, "Biometrics And Privacy".
[7].Wikipedia, http://www.wikipedia.org/, http://en.wikipedia.org

