Biometrics Authentication System

Ms.MadhuriGhongane,Ms.AmrutaShinde
University Of Mumbai (MCA)
ASM's Institute of Management & Computer Studies
C-4, Wagle Industrial Estate, Check Naka, Thane (W)-400604.

***Abstract*-In computer security biometrics refers to authentication techniques that rely on measurable physical characteristics that can be automatically checked. The technology is mainly used for identification and access control for identifying individuals. The basic principle of biometric authentication is that every individual is unique and can be identifying identified by his or her physical traits. Biometrics authentication technology centers on the capture of measurement and comparing to previously derived string of numbers called template.**

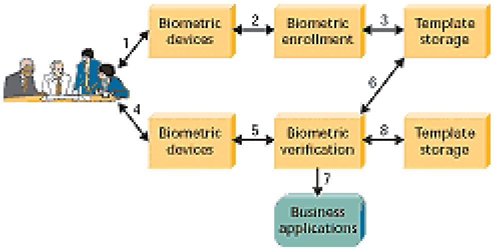
***Keywords*-Working, characteristics, Technology, Application.**

I. INTRODUCTION

Biometrics refers to metrics related to human characteristics. Biometrics is automated method of recognizingperson based on physiological or behavioral characteristics .Biometrics authentication is used in computer science as form of identification it is also used to identify individuals in groups that are under the surveillance. The past features of biometrics for identification includes distinctive body feature, scars or grouping of other physiological criteria such like height, eye color and complexion. The present features are fingerprints,handwriting,hand geometry,vein,voice ,retinal scan and face recognition The selection of particular biometric for use in specific application involves weighting of several factors. Proper biometric use is very application dependent. Certain biometrics will be better than others based on require level of convenience and security. No single biometric will meet all the requirements of every possible application. As the level of security breach and transaction scam increases, the need for well secure identification and personal verification technologies become apparent.

The biometric technologies arefingerprints, retinal scanning, hand-geometry, signatureverification, and voicerecognition, iris scanning and facial recognition. Biometricsauthentication system can be either anidentificationauthentication system or verification authentication system. In identification system biometrics can be used to determine a person's identity even without his awareness. Such as scanning crowd with the help of camera, one can verify matches that already stored in database. Inverificationsystem Biometrics can also be used to verify a person's identity .Such as one can grant access to bank account at an ATM by using retina scan.

Fig1.process image



II.BIOMETRICS CHARACTERISTICS

A. *Universality*

Universality means the every person using asystem should possess the trait.

B. *Uniqueness*

Uniqueness means that trait should be sufficiently different for individuals in the relevant population. *Singularity* Each expression of the element must be distinctive to the person. The characteristics should have adequate distinctive properties to distinguish one person from another.

C. *Acceptability*

Acceptability related to the how well individuals accept the technology.

D. *Reducibility*

The capture data should be able of being reduced to a file which is easy to handle.

E. *Reliability*

The attribute should be impractical to modify.

F. *Privacy*

The process should maintain the privacy of individuals.

G. *Comparable*

It has less probabilistic for similarity and more dependable on the identification.

II.BIOMETRICS TECHNOLOGY

Fingerprint Recognition

Using fingerprints for identification is the oldest use of biometrics. Today fingerprint devices are by far the most popular form of biometric security used .A fingerprint made of pattern of ridges and furrows as well as characteristics that occurs at minute point. Standard systems are comprised of sensor for scanning the fingerprint and a processor which stores thefingerprint database andsoftware which compares and matches him fingerprint to the predefined database. Within the database, a fingerprint is matched to a reference number or PIN number which is then matched to person's name or account. Nowadays, even laptopand sub

Pen drives can be found with fingerprint readers. The fingerprint is the most common form of biometric security because fingerprint remains reliable even as you age, Also you will not need to change anything about the appearance of your fingerprints.

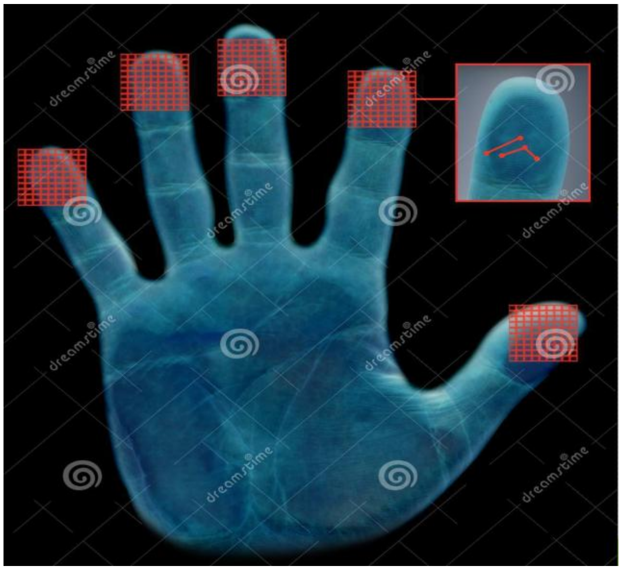


Fig2.Fingerprint recognition image

Face Recognition

Humans have always had the innate ability to recognize and distinguish between faces, however computers solely recently have shown same ability. Within the mid-1960s, scientists began work on using the computer to recognize human faces... Since, then facial recognition software has come a long way. In face recognition first physical or behavioral sample is captured by the system throughout the enrollment then distinctive data is extracted from the sample and template is made. The template is then compared with new sample. Finally the system then decides if he features extracted from the new sample are matchingor not. Oneof the strongest positive aspects of facial recognition is that it's non-intrusive. Verification can be accomplished from two or additional, and without requiring user to wait for long period's time or anything more than look at the camera... This technology used at Airports, companies, Stadiums, Government offices and public transportation.

Fig3.Face Recognition image

Voice Recognition

Everyone has unique voice because of the shape of your vocal cavities and the way we move our mouth when we speak. Voice is consisting of a physiological component represented by voice tract and behavioral component called accent. The combination of the two is difficult to replicate. However voice based system can be fooled by using recorded voice therefore securitysystem insist upon randomly chosen password and general voiceprints. Software requires the user to read a random phase or sequences of numbers, using recording devices to capture the utterance for later use. Voice Recognition software is more user friendly compared to others biometrics devices like iris scanners, fingerprint scanners, facial scanners and so on. According to DR.JudithA.Markowitz, aspeech and biometric consultant based in Chicago, voice recognition technology can be text dependent or text independent text dependent technology is dependentupon phrases or sequences of numbers using it as password. And text independent technology does not dependent on fixed pattern.it requires the individual to utter a free speech which is then analyzed for unique vocal characteristics.

Voice Recognition system is cheaper system. It used to activate or reset passwords, accessing financial data, conducting telephonic inquires and so on.

Fig 4.Face Recognition image

Palm Scan

The palm Secure sensor, made by Fujitsu, is easier to use and less intrusive than fingerprinting identification. We simply have to hold our palm several inches above the two-inches-square sensor for several seconds .Like fingerprints the blood veins in our palm stay the same position as we age and through sickness or injury, making it unique to us. Palm vein pattern readers use digital encryption specific to user's system, providing an extra layer of privacy and assurance that the patterns cannot be used for identification by anyone else.

Fig5.Palm Scan image

Iris Scan

In 1936 US ophthalmologist Frank Burch suggest the idea of recognizing the people from their iris patterns long before technology for doing so isfeasible. The unique pattern of your eye has to be Recognized so you can be positively identified. The iris is visible butProtectedstructure and it does not usually change over time, making it ideal for biometric identification. Most of the time people's eye remains unchanged after eye surgery, and blind people can use iris scanners as long as their eyes have irises. Basically two stages involved in Iris scanning the first is enrollment-the first time you use the system, when it learns to recognize you. The second is verification-where you are checked on subsequent occasions

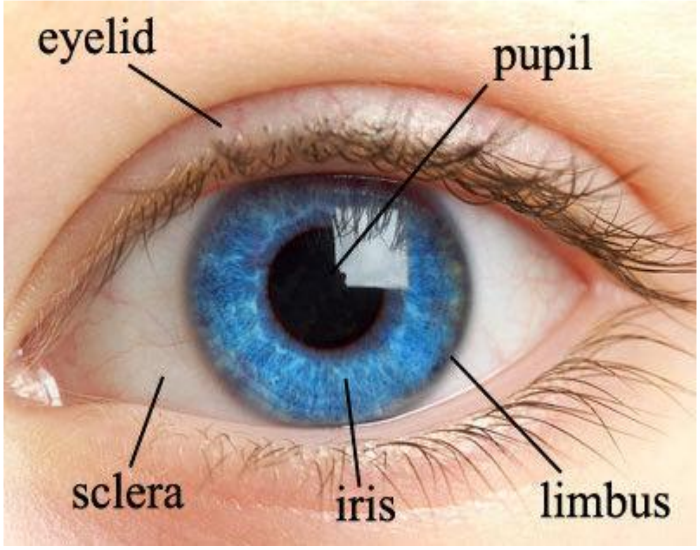


Fig6.***Iris Scan Image***

Signature Recognition

This technology comes under the behavioral biometric authentication system. Biometric signature recognition system will measure and analyze the physical activity of signing, such as the stroke order, the pressure applied and the speed. This technology consists of primarily of a pen and specialized writing tablet, which are then connected to local or central computer for template processing and verification. The procedure is start with data acquisition phase in which individual sign their name multiple times on the writing tablet. But data acquisition stage includes so many constraints such as signature should not be too long or too short, individual must complete the process in same type of condition. After the data acquit ion phase the signature recognition systemthen extracts unique feature from behavioral characteristics, which includes the time utilized by the individual to sign their name; the pressure applied from the pen to the writing tablet; the rate of speed in signing signature; overall size of signature; and the quality and the various direction of the strokes in the signature. Benefits of signature recognition system is that it is to copy the image if a signature but extremely difficult to mimic the behavior of signing. People are used to signdocument, so signature recognition system are not perceived to be invasive.

Fig7.Signature Recognition image

III. APPLICATIONS

A. Identification of criminals

Collecting he evidence in the scene of crime (e.g. Fingerprints) it is possible to compare with data of suspects or make search in the database.

B. Voter ID and Elections

Many countries are use the biometry for the control of voting and voter registration for the national or regional elections.

C. Employee Authentication

The government use of biometric for pc,network, and data access is also important for security of building and protection of information.

Military Programs

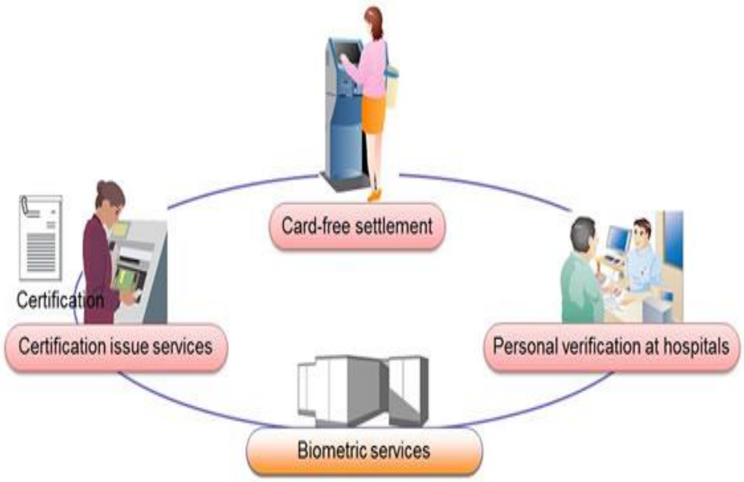
The military has long been interested in biometrics and the technology has enjoyed extensive support from the national security community.

E. Physical Access

Biometric is widely used for controlling the access to

Buildings or specially for restricted area

Fig8.Application Image


Card-free settlement
Certification
Certification issue services
Personal verification at hospitals
Biometric services

F. E-commerce

Biometric e-commerce is the use of biometrics to verify of identity of the individual conduction remote transaction for goods or services

G. ATMs

The use of biometrics in the ATM allows more security

Patient Identification

In case of emergency, when patient does not have identification document and is unable to communicate, biometric identification may be good alternative to identify.

I. . .Border Crossing

The use of biometrics to control the travelers crossing the national or state border is increasing, especially in regions with high volume of travelers or illegal immigrants.

J. Account Access

The use of biometry for the access to the account in the bank allows to keep the definitive and auditable records of account access by employees and customer. Using biometry the customer can access account and employees can log into their workstation.

Above fig that shows application of biometric technology

IV.DRAWBACKS

Biometric identification machines are more expensive to buy than traditional ones. In addition some users may rejects biometrics as whole, seeing it as aninvasion ofprivacy. Also biometric machines are not always entirely accurate,

For example. An individual with cold may not be able to identify himself using voice identification device, and people who gain or loss weight may suddenly lose access to place protected by system analyzing facial features. In case of voice Recognition a person's voice can be easily recorded and used for unauthorized PC or network. Similarly for signaturerecognition individuals who do not sign their names nine consistent manner may have difficulty enrolling and verifying in signature verification.

V.CONCLUSION

Biometrics points are helpful for creating identification with camera system, however they rely upon the existence of a previously generated database so distances can be compared. Biometrics technology is new technology for many people because it has only been implemented in public for short period of time. There are several application of biometrics technology uses in security system. Although the biometrics security system still has several considerations like information privacy, physical privacy, users cannot deny the very fact that this technology can change our lives for the better. Biometric systems aren't a general replacement for different authentication technology, although combining biometrics approaches with different strategies can argument security in those application where the user cooperation can be inferred. It's impracticable to positively state if a biometric techniques successful run, it is essential to find factors that helps to reduce affect system performance. The international biometric group Strike System Strikes are: in Fingerprint Dry/oily finger, in Voice recognition Cold or illness that effects voice, in Facial recognition Lighting conditions ,in Iris-scan too much movement if head or eye and in signature scan completely different signing position.

ACKNOWLEDGEMENT

We than our college IMCOST who provided insight and expertise

That greatly assisted he research, although they may not agree with

All of the conclusions of this paper.

We thank Mrs.Trupti for assistance with methodology of this research.

REFERENCES

[1] http://www.google.com

[2]EyeDenify,http://www.eyedentify.com

[3] IridianTechnologies,http://www.iriscan.com

[4] ZdeneK R IHA Vaclav Matyas "Biometrics Authentication System", FI MU Report Series, November 2000.

[5] Ratha N.K, J.H.Connell ,and RM Bolle(2001)."Enhancing security and privacy in Bimetrics based authentication systems".IBM Systems Journal40(3):614-613.