Impact Factor (SJIF): 3.632

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

(Special Issue for ITECE 2016)

AN EMERGING DEVELOPMENT OF BIOMETRIC SYSTEM: A NOVEL APPROACH OF SECURITY

N.C.Kaneriya[1], B.M.Mori[2], S.Rangarajan[3]

[1]Lecturer, A.V.Parekh Technical Institute, Rajkot
[2] Lecturer, A.V.Parekh Technical Institute, Rajkot
Lecturer, A.V.Parekh Technical Institute, Rajkot

Abstract — Biometrics is a growing technology, which has been widely used in forensics, secured access and prison security. A biometric system is fundamentally a pattern recognition system that recognizes a person by determining the authentication by using his different biological features i.e. Fingerprint, retina-scan, iris scan, hand geometry, and face recognition are leading physiological biometrics and behavioral characteristic are Voice recognition, keystroke-scan, and signature-scan. In this paper different biometrics techniques such as Iris scan, retina scan and face recognition techniques are discussed.

***Keywords-component;* Biometric, Iris scan, Palm scan,**

I. INTRODUCTION

One of the first important steps towards preventing unauthorized access is user authentication. The authentication of user means whether the user is the actual user who he claims to be is there or not conventionally, user authentication is grouped into three classes:

- Knowledge - based,
- Object (or Token) - based,
- Biometric - based.

The knowledge-based authentication is based on something one knows and is characterized by secrecy. The examples of knowledge-based authenticators are commonly known passwords and PIN codes. The object-based authentication relies on something one has and is characterized by possession. Traditional keys to the doors can be assigned to the object-based category. However, usually the token-based approach is combined with the knowledge-based approach. An example of this combination is a bank-card with PIN code. Biometric authentication is based on something one is. [1][2][7][12]

In knowledge-based and object-based approaches, passwords and tokens can be forgotten, lost or stolen. There is also usability limitations associated with them. For instance, managing multiple passwords/PINs, and memorizing and recalling strong passwords are not an easy task. According to a survey, the heavy IT user has to remember on average 21 passwords (some up to 70), 49% of the users write down or store their passwords in a file and 67% never change passwords .[1][2][7][12]

Biometric-based person recognition lacks above mentioned difficulties of knowledge-based and object based approaches. However, one of the most important aspects of biometrics is that they establish more direct and explicit link with humans than passwords or tokens do, since biometrics use measurable physiological and behavioral features of human being. Thanks to this, nowadays the demand for biometrics-based systems is increasing. There are various types of human traits that can be used as biometric, e.g. fingerprint, face, iris, hand geometry, gait and so on.

A biometric system can be either an 'identification' system or a 'verification' (authentication) system, which are defined below.

Identification (1: n) – One-to-Many: Biometrics can be used to determine a person's identity even without his awareness or approval. Such as scanning a crowd with the help of a camera and using face recognition technology, one can verify matches that are already store in database.

Verification (1:1) One-to-One: Biometrics can also be used to verify a person's identity. Such as one can allow physical access to a secure area in a building by using finger scans or can grant access to a bank account at an ATM by using retina scan.

Paper is bifurcated into many sections. Section-2 describes the working of biometrics; section 3 gives detail about biometrics characteristics.Section-4 gives the details on biometrics technology.Section-5 gives the challenges of the technology.Section-6 gives the conclusion of the paper.

II. WORKING OF BIOMETRICS

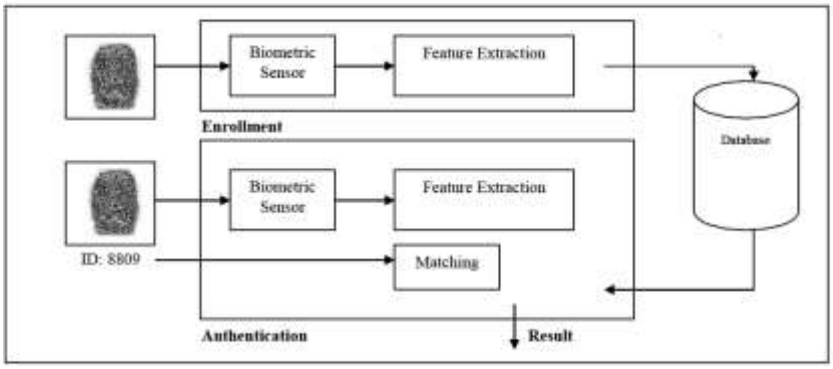


Fig.1: Biometric System [1]

All Biometric Systems work in a four-stage process that consists of the following steps.

Capture: A biometric system captures the sample of biometric characteristics like fingerprint, voice etc of the person who wants to login to the system.

Extraction: Unique data are extracted from the sample and a template is created. Unique features are then extracted by the system and converted into a digital biometric code. This sample is then stored as the biometric template for that individual.

Comparison: New samples now come to the picture and given template will be compared with respect to it. The biometric data are then stored as the biometric template or reference template for that person.

Match/non-match: The system then decides whether the features extracted from the new sample are a match or a non-match with the template. When identity needs checking the person interacts with the biometric system, a new biometric sample is taken and compared with the template. If the template and the new sample match, the person's identity is confirmed else a non-match is confirmed.

III. BIOMETRIC CHARACHTERISTICS

Biometric characteristics will be classified into two classes.

Physiological Class: This is related to the shape of the body.

Behavioral Class: This is related to the behavior of a person. Example includes, but is not limited to typing rhythm, gait and voice. Some researchers have coined the term "behavioral metric" for this class of biometrics.

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

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.

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

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.

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.

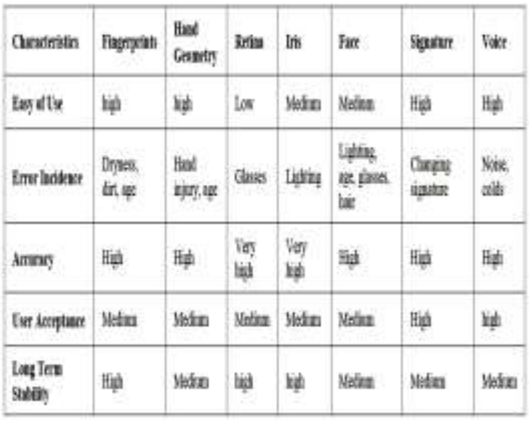
Reducibility: one has to develop such a file in which captured data should be reduced, stored and handled efficiently.

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

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

Comparable: 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.

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



Characteristics	Fingerprints	Hand Geometry	Retina	Iris	Face	Signature	Voice
Easy of Use	high	high	Low	Medium	Medium	High	High
Error Incidence	Dryness, dirt, age	Hand injury, age	Glasses	Lighting	Lighting, age, glasses, hair	Changing signature	Noise, colds
Accuracy	High	High	Very high	Very high	High	High	High
User Acceptance	Medium	Medium	Medium	Medium	Medium	High	high
Long Term Stability	High	Medium	high	high	Medium	Medium	Medium

Table 1: Comparison of Various Techniques vs. Characteristics [1]

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.[1][2][7][12]

IV. BIOMETRIC TECHNOLOGY

- Fingerprint Recognition
- Voice Recognition
- Signature Recognition
- Face Recognition
- Palm scan
- Iris-scan
- Retina-scan
- Hand geometry
- Signature-scan
- Keystroke-scan

Face Recognition

The biometric system can automatically recognize a person by the face. This technology works by analyzing specific features in the face like - the distance between the eyes, width of the nose, position of cheekbones, jaw line, chin ,unique shape, pattern etc. These systems involve measurement of the eyes, nose, mouth, and other facial features for identification. To increase accuracy these systems also may measure mouth and lip movement. Face recognition captures characteristics of a face either from video or still image and translates unique characteristics of a face into a set of numbers. These data collected from the face are combined in a single unit that uniquely identifies each person. Sometime the features of the face are analyzed like the ongoing changes in the face while smiling or crying or reacting to different situation etc. The entire face of the person is taken into consideration or the different part of the face is taken into consideration for the identity of a person. It is highly complex technology. The data capture by using video or thermal imaging. The user identity is confirmed by looking at the screen. The primary benefit to using facial recognition as a biometric authenticator is that people are accustomed to presenting their faces for identification and instead of ID card or photo identity card this technique will be beneficial in identifying a person. As the person faces changes by the age or person goes for plastic surgery, in this case the facial recognition algorithm should measure the relative position of ears, noses, eyes and other facial features.[1][2][5][8][11][12][13]\

Hand Geometry

This technique works on user’s hand and fingers. It analyses finger image ridge endings, bifurcations or branches made by ridges. Hand geometry measures and records the length and width, thickness, and surface area of the person to be tested. It is used in applications like access control and time and attendance etc. A camera captures a 3 dimensional image of the hand. A verification template is created and stored in the database and is compared to the template at the time of verification of a person. Fingerprint identification. Currently fingerprint readers are being built into computer memory cards for use with laptops or PCs and also in cellular telephones, and personal digital assistants. It is successfully implemented in the area of physical access control.[1][2][3][7][12]

Eye Recognition

This technique involves scanning of retina and iris in eye. Retina scan technology maps the capillary pattern of the retina, a thin nerve on the back of the eye. A retina scan measures patterns at over 400 points. It analyses the iris of the eye, which is the colored ring of tissue that surrounds the pupil of the eye. This is a highly mature technology with a proven track record in a number of application areas. Retina scanning captures unique pattern of blood vessels where the iris scanning captures the iris. The user must focus on a point and when it is in that position the system uses a beam of light to capture the unique retina characteristics. It is extremely secure and accurate and used heavily in controlled environment. However, it is expensive, secure and requires perfect alignment and usually the user must look in to the device with proper concentration. It is used in airports for travelers. Retina scan is used in military and government organization. Organizations use retina scans primarily for authentication in high-end security applications to control access, for example, in government buildings, military operations or other restricted quarters, to authorized personnel only. The unique pattern and characteristics in the human iris remain unchanged throughout one's lifetime and no two persons in the world can have the same iris pattern.[1][2][6][7][12]

Voice Biometrics

Voice biometrics, uses the person's voice to verify or identify the person. It verifies as well as identifies the speaker. A microphone attached with PC is required to identify the person’s characteristics. Mostly used in telephone-based applications. Voice verification is easy to use and does not require a great deal of user education. For enroll, Particular pass phrase will be spoken by users into microphone or telephone handset. The system then creates a template based on numerous characteristics, including pitch, tone, and shape of larynx. Typically, the enrollment process takes less than a minute for the user to complete. Voice verification is one of the least intrusive of all biometric methods. Furthermore, voice verification is easy to use and does not require a great deal of user education.[1][2][7][12]

Signature Verification

Signature verification technology is the analysis of an individual's written signature, including the speed, acceleration rate, stroke length and pressure applied during the signature. There are different ways to capture data for analysis i.e. a special pen can be used to recognize and analyze different movements when writing a signature, the data will then be captured within the pen. Information can also be captured within a special tablet that measures time, pressure, acceleration and the duration the pen touches it .As the user writes on the tablet, the movement of the pen generates sound against paper an is used for verification. An individual's signature can change over time, however, which can result in the system not recognizing authorized users. Signature systems rely on the device like special tablet, a special pen etc. When the user signs his name on an electronic pad, rather than merely comparing signatures, the device instead compares the direction, speed and pressure of the writing instrument as it moves across the pad.[1][2][7][12]

V. CHALLENGES

Following are the various challenges that biometric system has to suffer so one should develop such system in which one can overcome the problems

- spoofing
- usability
- accessibility
- hygiene
- safety
- secondary use public perception

VI. CONCLUSION

Biometric System works to identify a person based on their anatomical or behavioral characteristics. It gives several advantages over traditional approach. Various Approaches have been developed like face recognition, signature verification, Iris Scan, Palm Scan and so on. Each technique has its own pro’s and con’s. This paper compares all the existing biometric techniques with each other. Apart from all this pro’s and con’s all the biometric Techniques have been proved highly confidential and secure mechanism.

REFERENCES

.
[1] Rahul Bhatiya, “Biometric and Face recognition Techniques”,International Journal of Advanced Research in Computer Science and Software Engineeering,vol.3,issue 5,May-2013

[2] Jitendra Choudhary, “Survey of Different Biometric Techniques”,International Journal of Modern Engineering Research(IJMER),Vol.2,Issue. 5,Sep-Oct-2012

[3] Faundez Zanuy,”Biometric Verification by means of Hand Geometry”, International carnahan Conference on Security Technology,2005

[4] M.Arif, F.A.Afsar, M.Hussain, ” Fingerprint Identification and Verification System using Minutiae Matching”, National Conference on Emerging Technologies,2014.

[5] Steve Lawrence, C. Lee Giles, Ah Chung Tsoi, Andrew D. Back, “Face Recognition: A Convolutional Neural Network Approach”, IEEE Transactions on Neural Networks

[6] John Daugman, “ How Iris Recognition Works”,IEEE Transaction on Circuits and Systems for Video Technology,Jan-2004

[7] A.K.Jain, A. Ross, S. Prabhakar, ” An Introduction to Biometric Recognition”,IEEE Transaction on Circuits and Systems for Video Technology,Jan-2004

[8] C.Benabdelkader, R.Cutler,L.Davis, ”Stride and Cadence as a biometric in automatic person identification and verification”,5th IEEE International Conference on Automatic Face and Gesture Recognition,May-2002

[9] Yanmei Chai,Jinchang Ren,Rongchun Zhao, Jingping Jia, “Automatic Gait Recognition using dynamic variance features”,International Conference on Automatic Face and Gesture Recognition,2006

[10] Davrondzhon Gafurov,”A Survey of Biometric Gait Recognition : Approaches,Security and Challenges”

[11] Dilip Dandotiya,Ravikant Gupta,Satyendra Dhakad,Yogesh Tayal,”A Survey paper on Biometric Based Face Detection Techniques”,International Journal of Software and Web Sciences

[12] Sulochana Sonkamble,Dr. Ravindra Thool, Balwant Sonkamble, ”Survey of Biometric Recognition Systems and Their Applications”, Journal of Theorerical and Applied Information Technology,2005-2010

[13] S.P.Khandait,R.C.Thool,”Hybrid Skin Detection Algorithm for Face Localization in Facial Expression Recognition”,IEEE International Advanced Computing Conference(IACC),Patiala,March-2009