A Study of Biometrics Technology Methods and Their Applications- A review

Manasi G. Vaidya
Assistant Professor
R.C.Patel, Institute of Management
Research & Development, Shirpur
Dist. Dhule

Abstract - This paper discusses the methods of biometrics recognition technology and applications that used as personal identifying factors. Biometric recognition refers to an automatic recognition of individuals based on a feature vector(s) derived from their physiological and/or behavioral characteristic. Technologies are being developed to verify or identify individuals on the basis of measurement of face, hand geometry, iris, retina, finger, ear, voice, signature, DNA and even body order. Biometric recognition systems should provide a reliable personal recognition schemes to either confirm or determine the identity of an individual. The importance of biometrics in current fields like computer systems security, secure electronic banking, mobile phones, credit cards, secure access to buildings, E-voting, health and social services. This technology can be utilized alone or integrated with other technologies such as smart cards, encryption keys and digital signatures, biometrics is anticipated to pervade nearly all aspects of the economy and our daily lives. There are many tools and techniques that can support the management of information security. But system based on biometric has evolved to support some aspects of information security. Biometric authentication supports the facet of identification, authentication and non-repudiation in information security. Biometric systems for today's high security applications must meet stringent performance requirements. The main reason for the acceptance of the biometrics as a tool for security is its universality, distinctiveness, permanence and collectability. Thus the biometrics methods are used as authentication technologies which offer high level accuracy for identification.

Keywords: Biometrics, Recognition, Verification, Identification, Security, Uses.

I. INTRODUCTION

The term *biometric* comes from the Greek words *bios* (life) and *metrikos* (measure). It is well known that humans intuitively use some body characteristics such as face, gait or voice to recognize each other. By using biometrics a person could be identified based on "who she/he is" rather then "what she/he has" (card, token, key) or "what she/he knows" (password, PIN). Biometric technologies of today have been possible by the advances in computing technology and the need arises owing to universal presence and connectivity with all over the world. Information security is concerned with the assurance of confidentiality, integrity and availability of information in all forms. Biometric based authentication applications include workstation and network access, single sign-on, application logon, data protection, remote access to resources, transaction security, and Web security. The promises of e-commerce and e-government can be achieved through the utilization of strong personal authentication procedures. Secure electronic banking, investing and other financial transactions, retail sales, law enforcement, and health and social services are already benefiting from these technologies. Biometric technologies are expected to play a key role in personal authentication for large scale enterprise network authentication environments, Point-of-Sale and for the protection of all types of digital content such as in Digital Rights Management and Health Care applications

A simple biometric system consists of four basic components:

1) *Sensor module* which acquires the biometric data;
2) *Feature extraction module* where the acquired data is processed to extract feature vectors;
3) *Matching module* where feature vectors are compared against those in the template;
4) *Decision-making module* in which the user's identity is established or a claimed identity is accepted or rejected.

Any human physiological or behavioral trait can serve as a biometric characteristic as long as it satisfies the following requirements:

1) *Universality*. Everyone should have it;
2) *Distinctiveness*. No two should be the same;
3) *Permanence*. It should be invariant over a given period of time;
4) *Collectability*..

Enrollment and Recognition process of biometric technology:
A generic biometric system goes through six basic steps as indicated in figure

1. **Sample acquisition**: In this first step, the biometrics data must be controlled using an appropriate sensor, for example, an image capture in the case of iris recognition or saliva sample in the case of DNA.
2. **Feature Extraction**: This step performs the transformation from the sample into the template. In general, the template is numerical data
3. **Quality Verification**: This step establish a reference image or template by repeating first two operations as many times as needed so as to ensure that system has to captured and recognized data correctly.
4. **Storage of reference template**: This step registers the reference template. Several storage media are possible and choice depend on the requirement of application.
5. **Matching**: This step compares the real time input data from an individual with the reference template(s) or image(s).
6. **Decision**: This step uses the result of the matching steps to declare a result in accordance with application- dependent criteria, for example, for verification task , the result would say whether the user claiming an ID should be authenticated.

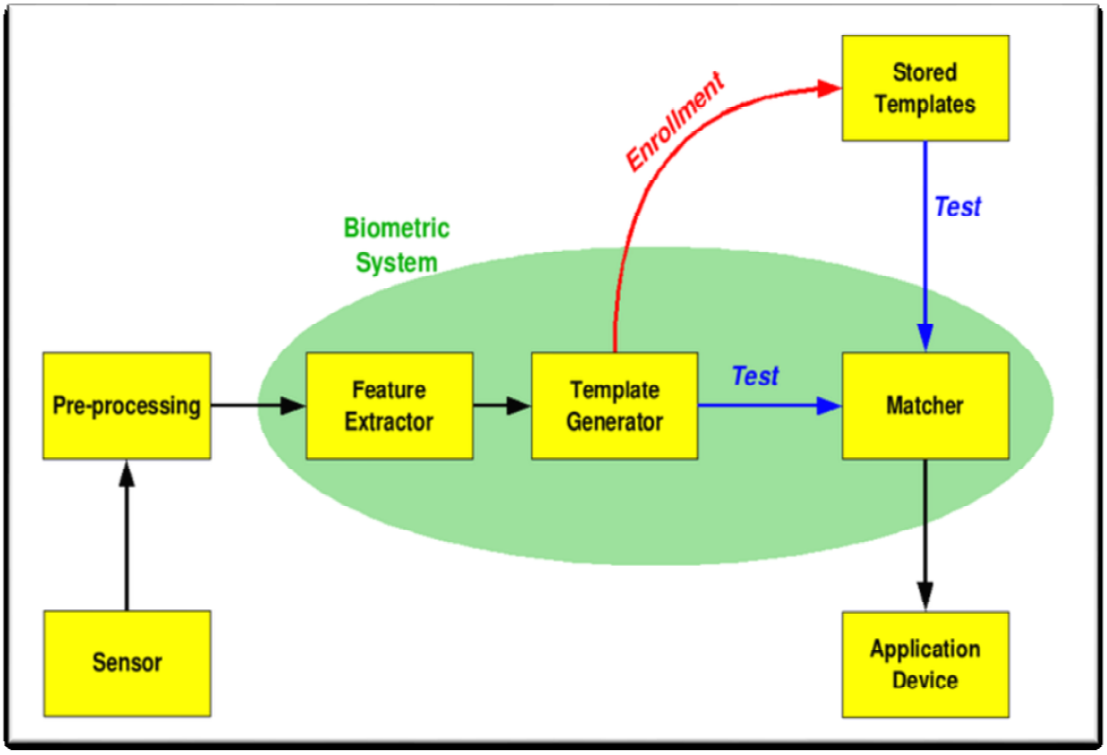

Figure 1: Biometrics enrollment and matching process.

II. DIFFERENT TYPES OF BIOMETRIC

1] Face Recognition :

Facial recognition technology is widely used various systems, including physical access control and computer user accounts security. The biometric system can automatically recognize a person by the face. Face verification involves extracting a feature set from a 2D image of user's face and matching it with the templates stored in a database. This technology is based on either (1) by analyzing specific features in the face like - the distance between the eyes, width of the nose, position of cheekbones, jaw line, chin, lips and their spatial relationships or (2) the overall analysis of face image that represents a face as weighted combination of number of canonical faces. 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. 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.

2] Hand Geometry:

Hand geometry is techniques that capture the physical characteristics of a user's hand and fingers. It is based on the fact that nearly every person's hand is shaped differently and that the shape of a person's hand does not change after certain age. Various method are used to measure the hands- Mechanical or optical principle. There are two sub-categories of optical scanners. Devices from first category create a black and white bitmap image of the hand's shape. It analyses finger image ridge endings, bifurcations or branches made by ridges. These systems measure and record the length, width, thickness, and surface area of an individual's hand. 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.

Fig. Hand Geometry Recognition Scanner.

It is used in applications like access control and time and attendance etc. It is easy to use, relatively inexpensive and widely accepted. 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.

3] 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. Iris recognition is one of the most reliable biometric identification and verification methods. 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.

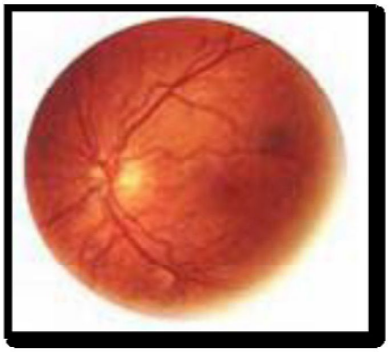

Fig. Image of Retina.

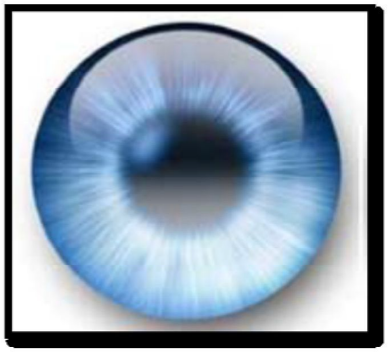

Fig. Image of Iris

4] 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 on a standard PC with software is required to analyze the unique characteristics of the person. Mostly used in telephone-based applications. Voice verification is easy to use and does not require a great deal of user education. To enroll, the user speaks a given pass phrase into a 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.

5] 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.

6] Keystroke:

This method relies on the fact that every person has her/his own keyboard-melody, which is analyzed when the user types. It measures the time taken by a user in pressing a particular key or searching for a particular key.

SOME OTHER BIOMETRICS TECHNIQUES ARE:

- **Vein/vascular patterns**: Analyses the veins in, for example, the hand and the face.
- **Nail identification**: Analyses the tracks in the nails.
- **DNA patterns**: it is a very expensive technique and it takes a long time for verification/identification of a person
- **Sweat pore analysis**: Analyses the way pores on a finger are located.
- **Ear recognition**: Shape and size of an ear are unique for every person.
- **Odors detection**: Person is verified or identified by their smell.
- **Walking recognition**: It analyses the way the person walks.

Table I Comparison of various biometric technologies [2]

Biometric Characteristic	Universit-y	Distinctiv-eness	Perman-ence	Collecta-billity	Perfor-mance	Universa-lity	Distinctiv-eness
Facial thermo gram	H	H	L	H	M	H	L
Hand vain	M	M	M	M	M	M	L
Gait	M	L	L	H	L	H	M
Keystroke	L	L	L	M	L	M	M
Odor	H	H	H	L	L	M	L
Ear	M	M	H	M	M	H	M
Hand geometry	M	M	M	H	M	M	M
Fingerprint	M	H	H	M	H	M	M
Face	H	L	M	H	L	H	H
Retina	H	H	M	L	H	L	L
Iris	H	H	H	M	H	L	L
Palm print	M	H	H	M	H	M	M
Voice	M	L	L	M	L	H	H
DNA	H	H	H	L	H	L	L

III. PRACTICAL IMPLEMENTATION OF BIOMETRIC TECHNOLOGIES IN INDUSTRIES:

1. Punjab National Bank (PNB) installed its first biometric ATM at a village in Gautam Budh Nagar (UP) to spread financial inclusion. "The move would help illiterate and semi-literate customers to do banking transaction any time.
2. Union Bank of India biometric smart cards launched. Hawkers and small traders could avail loan from the bank using the card.
3. In Coca-Cola Co., hand-scanning machines are used to replace the time card monitoring for the workers. In New Jersey and six other states, fingerprint scanners are now used to crack down on people claiming welfare benefits under two different names.
4. In Cook County, Illinois, a sophisticated camera that analyzes the iris patterns of an individual's eyeball is helping ensure that the right people are released from jail. At Purdue University in Indiana, the campus credit union is installing automated teller machines with a finger scanner that will eliminate the need for plastic bankcards and personal identification numbers.
5. MasterCard International Inc. and Visa USA Inc., the world's two largest credit card companies, have begun to study the feasibility of using finger-scanning devices at the point of sale to verify that the card user is really the card holder. The scanners would compare fingerprints with biometric information stored on a microchip embedded in the credit card.
6. Walt Disney World in Orlando has started taking hand scans of people who purchase yearly passes. These visitors now must pass through a scanner when entering the park preventing them from lending their passes to other people.

7. The technology also received widespread attention at summer's Olympic Games Atlanta, where 65,000 athletes, coaches and officials used a hand-scanning system to enter the Olympic Village.
8. Japan's Bank of Tokyo-Mitsubishi made Palm Vein identification technology available to customer on 5000 ATM's from October 2004.

IV. DISCUSSION

Biometric authentication is highly promising, because physical human characteristics are much more difficult to forge then security codes, passwords and hardware keys. Tokens such as smart card, magnetic stripe cards, ID cards, physical keys, can be lost, stolen, duplicated or left at home. Password can be forgotten, shared or observed. Moreover, today's fast-paced electronic world means people are asked to remember a multitude of passwords and Personal Identification Number (PINs) for computer accounts, banks, ATMs, E-Mail, wireless, phones ,websites and so forth. Biometrics holds the promise of fast, easy, accurate, reliable and less expensive authentication for a variety of application. Nowadays, particularly after the increase in human terrorism, biometrics is used to describe methods for non-invasive identification of individuals. From all the we can also used the biometric system for the animal identification such as Traditional methods for marking animals can potentially affect their behavior and cause harm, leading to erroneous research results and poor animal welfare. Any method used to apply a marker to an animal entails some degree of stress related to capture, handling and restraint. In addition, many common marking procedures also involve tissue damage and therefore cause pain, such as branding (heat, cold or chemicals), tattooing, toe clipping, ear notching and tagging. Furthermore, wearing a mark may alter the animal's appearance, social interaction, other behaviors and ultimately its survival. An ideal method should identify individuals reliably and permanently with no adverse effects on the animals. Biometric methods have therefore been developed to recognize animals based on physical characteristics or behavioral signs. Also we can use biometrics authentication system for the handicap people for applications like handling the automated teller machine. In this paper we trying to promote the application or used of biometric authentication is very powerful tool in security aspects.

V. CONCLUSION

We have so far able to understand the meaning of biometrics, its different types in brief. Also Biometrics refers to an automatic recognition of a person based on her behavioral and/or physiological characteristics. In future it is necessary to rely upon biometrics since using biometrics is the only way to guarantee the presence of the owner when a transaction is made. Biometrics is used for authentication in a variety of situations; as the industry is still evolving and emerging in today's century. At present, the amount of applications employing biometric systems is quite limited. In spite of all this it is certain that biometric-based recognition will have a great influence on the way we conduct our daily business in near future.

REFERENCES

[1] IJCITAE Volume 4, No. 2, Jully-December 2010
[2] International Journal of u- and e- Service, Science and Technology Vol. 2, No. 3, September, 2009 Debnath Bhattacharyya1, Rahul Ranjan1, Farkhod Alisherov A.2, and Minkyu Choi3
[3] 46th International Symposium Electronics in Marine, ELMAR-2004, 16-18 June 2004, Zadar, Croatia 184
[4] A SURVEY OF BIOMETRIC RECOGNITION METHODS Kresimir Delac 1, Mislav Grgic 2, International Journal of Scientific Research Engineering & Technology (IJSRET) Volume 1 Issue 5 pp 012-017 August 2012
[5] A Review Paper on Biometrics: Facial Recognition, Sakshi Goel1, Akhil Kaushik2, Kirtika Goel3, IETE Technical Review Volume 27, No. 4, Jul-Aug 2010
[6] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric Recognition: Security and Privacy Concerns", *IEEE Security and Privacy Magazine*, Vol. 1, No. 2, pp. 33-42, 2003.
[7] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, "FVC2002: Fingerprint Verification Competition", *Proc. International Conference on Pattern Recognition (ICPR)*, pp. 744-747, Quebec City, Canada, August 2002.
[8] Book of Information system security by Nina Godbole
[9] http://www.biometrics.gov
[10] http://ezinearticles.com
[11] www.bimetricnewsportal.com
[12] www.questbiometrics.com