An Overview on Technologies Used in Biometric System

Sharmila Sharad More[1,] B.T.Jadhav[2]

Assistant Professor, Dept. of Animation Science, Y.C.I.S.Satara, Maharashtra, India[1]

Associate Professor, Dept. of Electronics, Y.C.I.S.Satara, Maharashtra, India[2]

ABSTRACT: Biometrics is the term used in computer science and network security for identification, verification and access control of human by using their behavioural and physiological characteristics. Attendance in educational institutions, industries will require more paper work and time. To reduce this, biometric system is used. Biometric Studies commonly used Fingerprints, Face, Iris , Voice, Signature, Vascular, Retinal, DNA and Hand geometry recognition and verification. Different types of technologies used in biometric system to increase the system performance and then system become secure; simple easy and time saving comparisons are happened. This paper gives information about technologies used in Biometric system.

KEYWORDS: Biometric, Crisp Logic, Fuzzy Logic, Microcontroller, Microprocessor, Embedded System

I.   INTRODUCTION

Biometrics authentication is the term used in computer science for identifying human by their characteristics. It is used in computer science and Network security for identifying individuals in group. Biometric system used to identified, verified and gives authenticated access control to human by comparing their behavioural and physiological characteristics with the enrolled data. And then it gives access controlled to authorized people. Biometrics is the emerging technology used for identification. Biometric refers to automatic identification of a person based on biological characters such as finger print, iris, facial recognition, etc. Attendance in educational institutions, industries will require more paper work and time. To reduce this, biometric system is used.
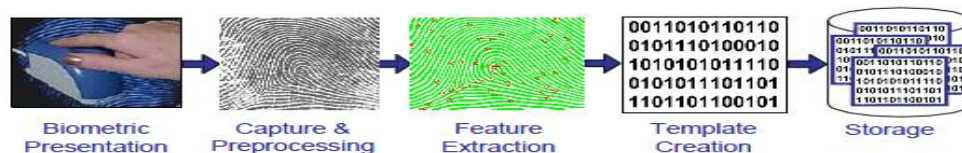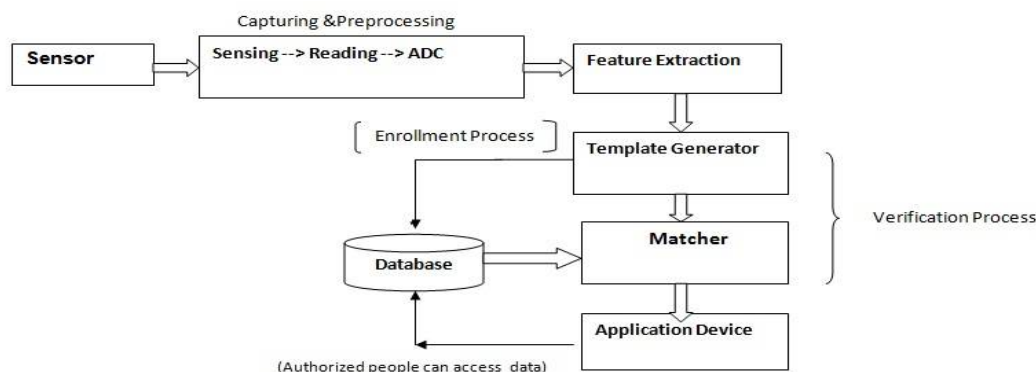

Fig. 1-Block diagram of biometric system

The biometric system use the three steps i.e. capturing , processing and enrolment, but all these steps always passing through verification and identification mode. Biometric techniques are classified into two classes.
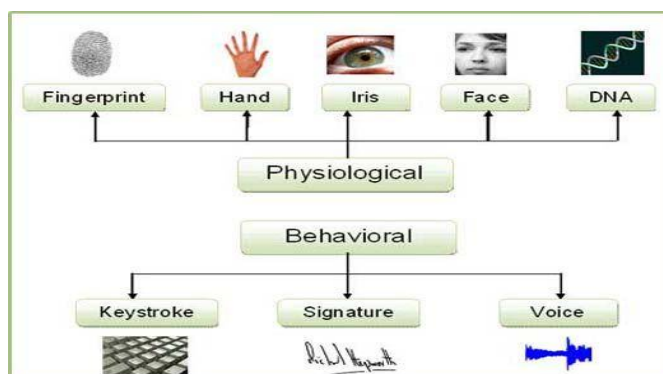
Fig 2. – Types of biometric system

Physiological based techniques :
- **Face Biometrics** :
    The facial recognition techniques measures facial characteristics. It measure the position, shape and size of facial features such as eyebrows, eye's , nose , lips and chin.
- **Fingerprint Biometrics**:
    The fingerprint recognition technique is oldest but quickly identified and consistently used .It match arch, loop and whorl of finger i.e. it analyzing fingerprint patterns.
- **Hand Biometrics**:
    The hand recognition techniques measures shape of the hand
- **Iris Biometrics** :
    The iris recognition technique analyzing feature of colored ring of the eye.
- **Retinal Scan** :
    It analyzing blood vessels in the eye .
- **Vascular patterns :**
    It analyzing vein patterns .
- **DNA recognition** :
    Deoxyribo Nucleic Acid – analyzing genetic makeup.

Behavioural based techniques:
- **Speaker (Voice) recognition** :
    It analyzing vocal behaviour.
- **Signature recognition :**
- It analyzing signature dynamics.
     Keystroke recognition :
    It measures the time spacing of typed words.
- **Smart card**- It combining biometrics with identification cards.

Technologies used in Biometric System:
1. **Modern Biometric system uses Microprocessor:**
    Biometric implementation consists of a platform based on a microprocessor, which makes reasonable and optimal use of the peripherals and instructions for the functions that are to be developed. In order to develop a biometric system for person identification, this platform is composed of the Serial Interface, RAM, ROM & EPROM memory peripherals. In the Microprocessor based biometric consist of optimization of all resources, no extra memory and overhead computations due to the presence of operating systems. A standalone execution is carried out, and only required functions are implemented, which is not the case with general purpose computers.
But there are some limitations in the microprocessor based biometric system circuit.

- Problem related to the development and maintenance of the application.
- It does not use floating-point arithmetic.

2. **Modern Biometric system uses Microcontroller**:

Microcontroller based biometric system is easy to use ,it does not contain any manual error, requires no special training or equipment, high accuracy in terms of security and unwanted data is not coming in results. But there are some limitations in the microcontroller based biometric system circuit.

- There is a chance of misusing the technology by placing a fake finger print.
- Modules are sensitive and they need to be handled carefully.

3. **Modern Biometric system uses Embedded system:**

An embedded system is a computer system with a dedicated function within a larger mechanical or electrical system, often with real-time computing constraints. It is embedded as part of a complete device often including hardware and mechanical parts. Embedded systems control many devices in common use today. In many applications user authentication has to be carried out by portable devices. Usually these devices are personal tokens carried by users, which have many constraints regarding their computational performance, occupied area, and power consumption. These kinds of devices must deal with such constraints, while also maintaining high performance rates in the authentication process.

II.   ORIGIN OF THE MODEL

Generation of Biometric machines
a)**First Generation (14 th century -18th century)** :

i) Biometric theme was first time used in China in 14 th century by Joao de Barros. He said
that, the Chinese merchants were stamping children's palm prints and footprints on paper with ink to distinguish the young children from one another.

ii) **1858 – First systematic capture of hand images for identification purposes is recorded:**
Sir William Herschel, working for the Civil Service of India, recorded a handprint on the back of a contract for each worker to distinguish employees from others who might claim to be employees when payday arrived. This was the first recorded systematic capture of hand and finger images that were uniformly taken for identification purposes.

ii) **1870 – Bertillon develops anthropometries to identify individuals:**
The Bertillon system of measuring various body dimensions, which originated in France. These measurements were written on cards that could be sorted by height, arm length or any other parameter. This field was called anthropometries.

iii)   **1892 – Galton develops a classification system for fingerprints:**
Sir Francis Galton wrote a detailed study of fingerprints in which he presented a new classification system using prints from all ten fingers. The characteristics that Galton used to identify individuals are still used today. These details are often referred to as Galton's details.

b)   **Second Generation** (1903-1960)
  i) **1903 – Bertillon System collapses:**
The Bertillon measurements were not enough to differentiate between these two individuals.
  ii) **1936 – Concept of using the iris pattern for identification is proposed :**
Ophthalmologist Frank Burch proposed the concept of using iris patterns as a method to recognize an individual.
  iii) **1960s – Face recognition becomes semi-automated :**
The first semi-automatic face recognition system was developed by Woodrow W. Bledsoe under contract to the US Government. This system required the administrator to locate features such as eyes, ears, nose and mouth on the photographs. This system had the ability to extract useable feature points. It calculated distances and ratios to a common reference point that was compared to the reference data.

iv)   1960 – First model of acoustic speech production is created

A Swedish Professor, Gunnar Fant, published a model describing the physiological components of acoustic speech production. His findings were based on the analysis of x-rays of individuals making specified phonic sounds. These findings were used to better understand the biological components of speech, a concept crucial to speaker recognition.

c)   Third Generation (1963-1970)

i) 1963 – Hughes research paper on fingerprint automation is published
ii)   1965 -Automated signature recognition research begins :

North American Aviation developed the first signature recognition system in 1965.

iii)   1969 – FBI pushes to make fingerprint recognition an automated process:

The Federal Bureau of Investigation (FBI) began its push to develop a system to automate its fingerprint identification process, which was quickly becoming awesome and required many man-hours. The FBI contracted the National Institute of Standards and Technology (NIST) to study the process of automating fingerprint identification. NIST identified two key challenges: (1) scanning fingerprint cards and identifying minutiae and (2) comparing and matching lists of details.

iv)   1970s – Face Recognition takes another step towards automation:

Goldstein, Harmon, and Lesk used 21 specific subjective markers such as hair color and lip thickness to automate face recognition. The problem with both of these early solutions was that the measurements and locations were manually computed.

v)   1970 – Behavioural components of speech are first modelled :

The original model of acoustic speech production, developed in 1960, was expanded upon by Dr. Joseph Perkell, who used motion x-rays and included the tongue and jaw. The model provided a more detailed understanding of the complex behavioural and biological components of speech.

d)   Fourth Generation(1974-1985)
i)   1974- First commercial hand geometry systems become available:

The first commercial hand geometry recognition systems became available in the early 1970s, arguably the first commercially available biometric device after the early deployments of fingerprinting in the late 1960s. These systems were implemented for three main purposes: physical access control; time and attendance; and personal identification.

ii)   1976 – First prototype system for speaker recognition is developed

Texas Instruments developed a prototype speaker recognition system that was tested by the US Air Force and The MITRE Corporation.

iii)   1977 – Patent is awarded for acquisition of dynamic signature information:

Veripen, Inc. Was awarded a patent for a "Personal identification apparatus" that was able to acquire dynamic pressure information. This device allowed the digital capture of the dynamic characteristics of an individual's signature characteristics. The development of this technology led to the testing of automatic handwriting verification (performed by The MITRE Corporation) for the Electronic Systems Division of the United States Air Force.

iv)   1985 – Concept that no two irises are alike is proposed:

Drs. Leonard Flom and Aran Safir, ophthalmologists, proposed the concept that no two irises are similar.

e)   Fifth Generation(1988- 1994)
i)   1988 – First semi-automated facial recognition system is deployed

In 1988, the Lakewood Division of the Los Angeles County Sheriff's Department began using composite drawings (or video images) of a suspect to conduct a database search of digitized mug shots.

ii)   1988 – Eigen face technique is developed for face recognition

Kirby and Sirovich applied principle component analysis, a standard linear algebra technique, to the face recognition problem. This was a highlighted because it showed that less than one hundred values were required to approximate a correctly associated and normalized the face image.

iii)   1994 – Integrated Automated Fingerprint Identification System (IAFIS) competition is held

The next stage in fingerprint automation occurred at the end of the Integrated Automated Fingerprint Identification System (IAFIS) competition. The competition identified and investigated three major challenges: (1) digital fingerprint acquisition, (2) local ridge characteristic extraction, and (3) ridge characteristic pattern matching. The demonstrated model systems were evaluated based on specific performance requirements. Lockheed Martin was selected to build the FBI's IAFIS.

f)   Sixth Generation(2000- 2013)

i)   2000 – First research paper describing the use of vascular patterns for recognition is published:

This paper describes the technology that was to become the first commercially available vascular pattern recognition system in 2000. The technology uses the subcutaneous blood vessel pattern in the back of the hands to achieve recognition.

ii) 2004 – First state-wide automated palm print databases are deployed in the US:

In 2004, Connecticut, Rhode Island and California established state-wide palm print databases that allow law enforcement agencies in each state to submit unidentified latent palm prints to be searched against each other's database of known offenders.

iii) 2013 – Apple includes fingerprint scanners into consumer-Target smart phones

Touch ID is a fingerprint recognition feature, designed and released by Apple Inc., that was made available on the iPhone 5S, the iPhone 6 and iPhone 6 Plus, the iPad Air 2, and the iPad Mini 3. Touch ID is heavily integrated into iOS devices, allowing users to unlock their device, as well as make purchases in the various Apple digital media stores, and to authenticate Apple Pay online or in apps. On announcing the feature, Apple made it clear that the fingerprint information is stored locally in a secure location on the Apple A7 , A8 , or A8X chip, rather than being stored remotely on Apple servers or in cloud, making it very difficult for external access.

III. SIGNIFICANCE OF THE MODEL

- Proposed model requires less memory space to store information.
- It requires minimum time for comparisons of template.
- The complexity is occurring in identifying the extracted data, this can be minimized by using fuzzy logic and data mining approach.
- In this model we use image processing which is helpful for biometric data security.
- Simplifies the design complexity.

IV. OBJECTIVES OF THE MODEL

- To study the overview of existing system.
- To develop a algorithm for biometric system using .Net.
- To develop fuzzy algorithm for biometric system.

V.   RESEARCH METHODOLOGY

Primary data: Observation, Discussion and Survey.
Secondary data: Internet, Books and journals.
Methodology:
- Survey Methods
- Comparative methods
- Technological based comparison methods
- Software based classification
- Development of system
- Performance measurement methods
- Producing high number of matching results.

- The hand vein biometric recognition techniques is fairly new and the effect of heart attack or other medical problems are not clear.

VI. ANALYSIS OF THE MODEL

Crisp logic concepts used with data mining, which overcome the problem of ambiguity, complexity and non- linearity in identification. It contains the statement that are True or False i.e. 1 or 0, but it is not always possible to store accurate information by using only 1or 0.Crisp logic has some difficulties in solving the problem of complexity, Non-linearity, accuracy and ambiguity , so this is overcome by fuzzy logic.

Fuzzy logic is problem solving control system methodology . It is an approach to computing based on " Partial Truth" or "Degrees of Truth". The idea of fuzzy logic was first introduced by Dr. Lofty Zadeh of the University of California at Berkeley in 1960's.Fuzzy sets are appropriate for pattern recognition and its classification. Fuzzy logic not only consider 1or 0 value but also the truth values ranges in degree between 0 to 1. Fuzzy logic is used to simplify the job of the system designer and compute more accurate results. Fuzzy association rules used to find abstract co-relation among the different security features. The fuzzy association rules easy to write and understand. It is to fuzzy designer to describe the fuzzy system adequately. There is complexity in identifying the extracted data, this can be minimized by using fuzzy logic . A fuzzy method requires less memory to store information and minimum time for comparisons of template as compared to crisp logic. Fuzzy system requires Fuzzy Extractor, which is used to convert biometric data into random strings. Cryptographic techniques are easy to apply on random strings , which is helpful for biometric data security. They are used to Encrypt and Authenticate user records with biometric inputs as key. Fuzzy system requires auxiliary memory to store binary sets .Fuzzy logic is a form of multivalved logic instead of fixed and extract logic. Following figure shows flow chart of fuzzy logic approach for extracting biometric data.
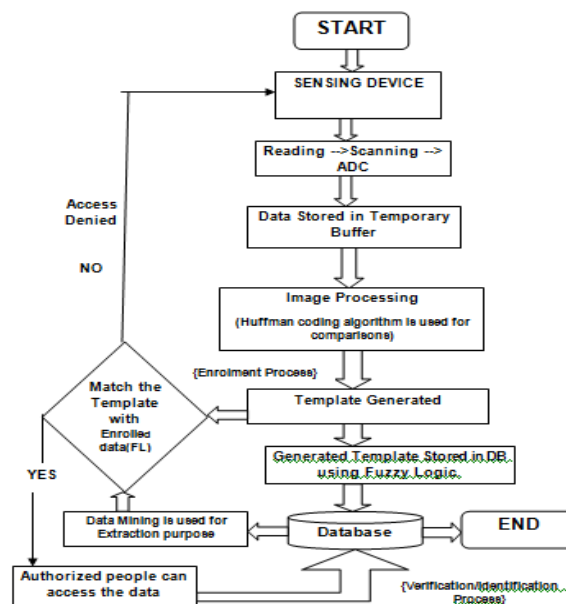

Fig 3: Flow chart of working of Biometric system using Fuzzy logic and Data Mining.

VII.CONCLUSION

In this paper we have given the generations of the biometric system, their period of development and modern techniques used in the system. Paper gives information regarding the development in the biometric system. This information is useful for the further improvement used in the biometric system. We also explain the Microprocessor, Microcontroller based biometric system. Separately build biometric system known as embedded system are also

informed. In this paper we also focus on limitations of crisp logic and complexity in authentication and identification with the advantages of Fuzzy logic. Data mining techniques are used to dig and extract the data from large database for analysis and executive decision making by using crisp logic. But fuzzy logic is very useful for removing ambiguity, non-linearity and also easy for identification and verification of biometric data.

VIII.   SUGGESTION

It is beneficial to safeguarding our citizens' privacy then it will enhance our economic efficiencies. It is also helpful to the education system. Manually difficult to check record of their employees check in /out then we will suggested to use biometric model, in which fuzzy algorithms are used for extracting biometric data. Then employee become punctual, helps in checking the attendance, absenteeism can be controlled and helps in achieving targets on time.

REFERENCES

 [1] A. Jain, R. Bolle, and S. Pankanti, , S. P. A. Jain and R. Bolle, Eds.,Biometrics: Personal Identification in a Networked Society. Norwell, MA: Kluwer, 1999.
[2] M. Faundez-Zanuy, "Biometric security technology," IEEE A&E Syst.Mag., vol. 21, no. 6, pp. 15–26, Jun. 2006.
[3] Sharmila J.Shinde ,"Biometrics: Overview and potential use for E- Governance Services", Volume 4, Issue 6, June 2014 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering,
[4] C. Militello, V. Conti, F. Sorbello,S. Vitabile,"A Novel Embedded Fingerprints Authentication System Based on Singularity Points",International Conference on Complex, Intelligent and Software Intensive Systems,0-7695-3109-1/08 $25.00 © 2008 IEEE.
[5] "Development of Microcontroller-Based Biometric Locker System with Short Message Service Crystalynne" D. Cortez, Jaswinder S. Badwal, Jocelyn R. Hipolito, Ditche Jane C. Astillero, Melvie S. Dela Cruz, and Jaira C. Inalao
[6] IOSR Journal of Engineering (IOSRJEN) ISSN (p): 2278-8719 Vol. 04, Issue 05 (May. 2014), " Advanced Microcontroller Based Bio-Metric Authentication Voting Machine "B.FarhathAnjum1 M.Deepa2 rs.C.N.Kalaivani.
[7] Mary Lourde R and Dushyant Khosla, "Fingerprint Identification in Biometric Security Systems" ,
International Journal of Computer and Electrical Engineering, Vol. 2, No. 5, October, 2010.
[8] D. Vinod kumar, Prof.M R K Murthy, " Fingerprint Based ATM Security by using ARM7", IOSR Journal of Electronics and Communication Engineering IOSRJECE) ISSN : 2278-2834 Volume 2, Issue 5 (Sep-Oct 2012).
[9] International Journal of Innovative Computing, Information and Control ICIC International c 2012 ISSN 1349-4198 Volume 8, Number 11, November 2012 "TECHNICAL ISSUES AND CHALLENGES OF BIOMETRIC APPLICATIONS AS ACCESS CONTROL TOOLS OF INFORMATION SECURITY" Sharifah Mumtazah Syed Ahmad, Borhanuddin Mohd Ali and Wan Azizun Wan Adnan
[10] "Biometrics of Next Generation: An Overview" AnilK. Jain1, Ajay Kumar2
[11] Sharmila S. More, B.T.Jadhav," Fuzzy Logic Algorithmsfor Extracting Biometric Data"   ISBN : 978-81-928732-2-0 in   the National Conference on Modern Approach for Green Electronics and Computing 2014.