ISSN No. 0976-5697

Volume 7, No. 6(Special Issue), November 2016

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

A Comparative Study of Different Biometric Features

Sandhya Vats
Assistant Professor
Guru Nanak College, Budhlada
profsandhyavats@gmail.com

Harkeerat Kaur
Assistant Professor
Guru Nanak College, Budhlada
harkeeratkaur007@gmail.com

Geetu
Assistant Professor
Guru Nanak College, Budhlada
single.geetu@gmail.com

Abstract: *In human identification biometrics is one of the biggest tendencies. Nowadays, in many real applications like forensic, security and other identification and recognition purposes biometrics is widely used. Here we have discussed and comparisons of different biometric features along with their uses. In biometrics fingerprint is the most widely used. Even further multimodal biometrics can improve the reliability and performance of biometric authentication.*

Keywords: Biometric System, Identification, Recognition

INTRODUCTION

Biometric terms comes from the Greek words bios (life) and metric (measure).Biometric systems are automated methods of recognizing or verifying the living person identity on the basis of some physiological characteristics, like face pattern, fingerprint and hand, or some aspects of behavior, like keystroke patterns, signature and voice. No system can be secure completely. So, it is very difficult to compromise the system. The security becomes more intrusive, if the system is more secure. Bertillon age is the first type of biometrics came into form in 1890, created by an anthropologist named Alphonse Bertillon. He based his system on the claim that measurement of adult bones does not change after the age of 20.[1]Biometric method consisting of various body measurements of a person like height, arm length, breadth and circumference of the head, the length of forearms, the length of different finger, length of feet etc.

1. Biometric Systems

A biometric system operates in two modes i.e. identification and verification.

1.1 Verification Mode:

In verification mode, the system identifies a person's identity whose biometric template(s) stored in database. The captured her own biometric data compared with prestored biometric template that is already stored in database. In such system ,any person who wants to be recognized can claims an identity by a PIN(Personal Identification Number),a smart card, a user name, etc, and the claim is true or not true the system conducts one to one comparison.(e.g., "Does this biometric data belong to particular person who entered in system?").In verification mode only the authorized people can access the system which has the unique ID. Aim of positive recognition is to protect the multiple people who have the same identity.

1.2 Identification Mode:

In the identification mode, the system recognizes an individual by searching the entire templates in the database matching for all the users Therefore, to establish an individual's identity the system conducts a one-to-many comparison (if the subject is not enrolled in the system database that fail)) having to claim an identity without the subject (e.g., "Whose biometric data is this?"). In negative recognition applications identification of any person is very critical component whether the person is who she (explicitly or implicitly).The negative recognition is protect a single person who have multiple identities. For positive recognition traditional methods of personal recognition such as PINs, passwords, tokens and keys may work. Only the negative recognition can be established through biometrics.

3. Types of Biometrics

978-93-85670-72-5 © 2016 (RTCSIT)

CONFERENCE PAPER
International Conference on
Recent Trends in Computer Science & Information Technology (RTCSIT-2016)
21st August 2016
Guru Nanak College Budhlada, Punjab India

3.1 DNA

DNA or Deoxyribonucleic acid is the part of a cell that contains genetic information (chemical structure) unique for each person that used in form of identification. With some degree of probability DNA to distinguish people. For an origination DNA biometrics can improve the security scheme of network.DNA never be changed during human death and life. The analysis of DNA took days, week and months to process. The sample of DNA collect from the various different sources like plastic cup sand paper, sweat T-shirt, socks ear wax, chewed gum, urine, hair, nails ,blood.DNA consist of four bases which all together make DNA code.

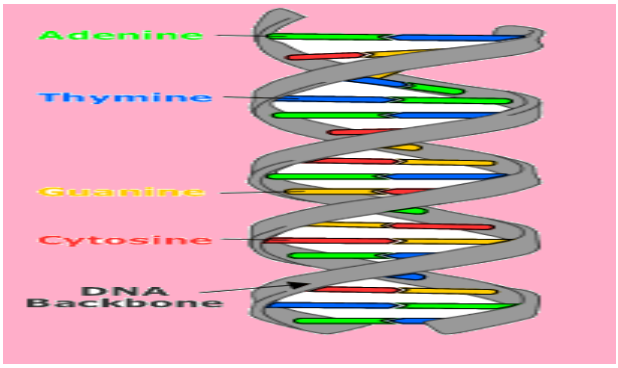

Figure 1: Structure of DNA

- Adenine (A)
- Cytosine (C)
- Guanine (G)
- Thymine (T)

Identification process of DNA take a lengthy time its chemical structure identify in laboratory.(Identical Twins) can have the same DNA.

3.2 Iris Recognition

Iris is also a unique characteristic of every person. Iris is stable and it cannot be changed throughout the whole life of a human. Iris recognition uses camera technology, with subtle infrared illumination reducing specular reflection from the convex cornea, to create images of the detail-rich, intricate structures of the iris [2]

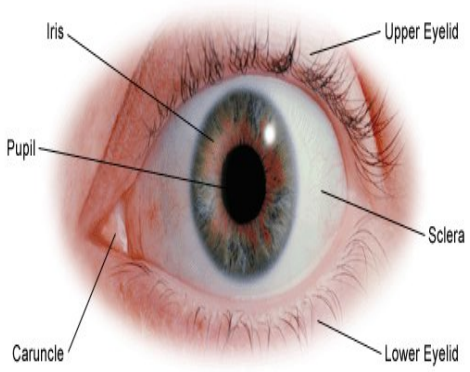

Figure 2: Structure of Iris

Surrounding the pupil features like furrows, sclera, caruncle and upper and lower Eyelid existing in the colored tissue. Iris scans by regular video camera that works through contact lenses and glasses.

3.3 Face Recognition

Face recognition means measurement of facial features. It is computer system application for automatically verifying or determining an individual from a digital image or a video framework from a video source. One of the techniques to do this is simply by evaluating selected facial features from the image as well as from facial database.[1]Through a digital video camera this technique records face images and examine various characteristics. Face recognition effected by camera brightness, light, angle etc.There are two types of technologies used in Facial recognition.

Figure 3: Structure of Face

2-D: 2-D method does not need any expensive equipment, but reliability is very low. Method strongly depends on the light. Problem may be occurring if the person has beard, glasses etc.

3-D: 3-D face recognition also has various methods. Each method uses different types of scanners and database. it does not

978-93-85670-72-5 © 2016 (RTCSIT)

create any problem if the person has beard, glasses etc.This method is more expensive.

3.4 Fingerprint Recognition

Fingerprint is one of the oldest method for recognize person identity. Fingerprints are made of a series of ridges and furrows on the surface of the finger and have a core around which patterns like swirls, loops, or arches are curved to ensure that each print is unique [3].

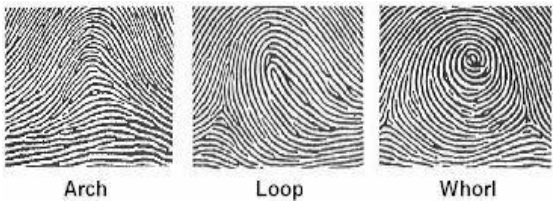

Figure 4: Finger prints

Finger print is classified into three parts:
Whorls: In this pattern the ridge are usually circular
Arch: In this pattern from one side the ridges entered make a rise in the center and opposite side generally exit.

Loops: In a loop pattern from the other side ridges enter, re-curve and pass out the same side.
A fingerprint scanner system has two basic jobs, it needs an image of your finger and to determine whether the pattern of ridges and valleys in image matches the pattern in pre-scanned images.

3.6 Voice Recognition

It combines the behavioral and logical factors that produce speech patterns. For speech authentication inherent properties of the speaker like cadence, nasal tone, inflection, and fundamental frequency are used. The words spoken by any person transferred into electronic signals and matched with pre-recorded voice database.

3.7 Signature Recognition

Signature are behavioral biometric that can change with person age. The role of a signature is not solely to provide evidence of the identity of the contracting party, but rather to additionally provide evidence of deliberation and informed consent [2].Signature verification approach based on feature like number of vertical slope components and number of interior contours.

3.5 Pulse Study

It has been in the practice in system of Ayurvedic treatment that Dieses and identification of a person having mother and father of different countries can be identified by Pulse beating calculation. Even the lie detection is also possible by the saying pulse beating too. Even the people believe in this therapy and results are along awaited having permanent remedy.Altough such people are few one.

Conclusion

Biometric Authentication refers to identify a person by different methods. Authentication refers to identification and verification of person whose information is pre stored in biometric system. In various organizations to increase security level protect data from unauthorized person using the biometric techniques. It is clear that each trait has different parameters in the field of efficiency, speed, cost, accuracy and security. Moreover it has played a vital role in criminology section many culprits are identified as the real criminals one's

Refrences

[1] Dr.Rajinder Singh, ShaktiKumar,"Comparison of Various Biometric Methods",(IJETCAS)

[2] Kalyani Mali, Samayita Bhattacharya,"Comparartive Study of Different Biometric Features",International Journal of Advanced in Computer and Cmmunication Engineering Vol.2, Issue 7, July 2013.

[3] 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.

[4] U. Park and A. Jain, "Face Matching and ret rival Using Soft Biometrics", *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 3, pp.406-415, Sep-2010.

[5]K.Arthi,N.M.Nandhitha,S.EmaldaRoslyn, "A Study and Evaluation of Different Authentication Methods and Protocols, "IJCSMR, Volume 2,Issue 1 January 2013.

[6] Bolle R, Connell J, et al," Guide to Biometrics", Springer, 2003.

[7]https://www.comp.nus.edu.sg/~tsim/documents/wonder-ears.pdf

978-93-85670-72-5 © 2016 (RTCSIT)

CONFERENCE PAPER
International Conference on
Recent Trends in Computer Science & Information Technology (RTCSIT-2016)
21st August 2016
Guru Nanak College Budhlada, Punjab India