IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-3, Issue-2 E-ISSN: 2347-2693

A Characteristic study on Multimodal Recognition applications in Biometrics

J. Mohana Sundaram[1*], K. Vembandasamy[2] R. Karthik Raj[3]

[1.2, 3]*Department of Computer Science*
[1, 2, 3] *PSG College of Arts and Science, Coimbatore, Tamil Nadu, India,*
[1] mohanpsgphd@gmail.com, [3] rkarthykraj@gmail.com

www.ijcaonline.org

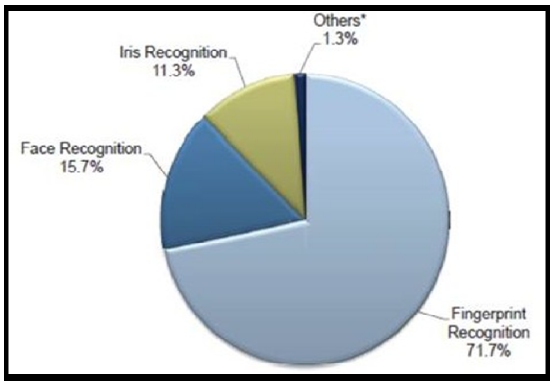
Received: Feb /6/2015 Revised: Feb/14/2015 Accepted: Feb/23/2015 Published: Feb/28/ 2015

Abstract - Nowadays advances in technology made our life easier by giving higher levels of knowledge thru the inventions devices. There are many technical innovation harbors the hidden threats to the users. Users try to secure their data with encrypted passwords and ID cards. The abuse and stealing of these security measures are enlarged. In ID cards technologies the cards being duplicated and misused. This increasing misuse behaviour made the cyber security lead the birth to invention of biometric securities. Biometrics is used to uniquely recognize humans on one or more essential physical or behavioural characteristics. Biometrics technology is used for its uniqueness and measurable physical, biological characteristics of individual which is then processed and then identify a person with biometric traits such as face, iris, hand geometry, etc. but the physiological traits include face, finger print, hand, iris, DNA and the behavioural traits include key stroke, signature, voice.

Keyword - Biometric, Biometric Security, Recognition Methods, Facial Recognition, Fingerprint Reader, Voice Recognition, Iris/Retinal Recognition, Vein Recognition, DNA Recognition, Privacy, Safety, Advantages And Disadvantages.

I. INTRODUCTION

BIOMETRICS is defined as measurable characteristics which is been employed for verification to identify a person's identity. It is well-known that humans use some body characteristics such as face, body language or voice to recognize each other. Since, today a wide variety of applications require reliable verification outlines are avail to confirm the identity of an individual, recognizing humans based on their body characteristics became more and more interesting in emerging technology applications. Traditionally, passwords and ID cards have been used to restrict access to secure systems but these methods can easily be breached and are unreliable. Biometric cannot be borrowed, stolen, or forgotten, and forging one is practically impossible. Biometrics means a study of methods for recognize humans uniquely based upon one or more essential physical or biological traits. A practical biometric system should meet the specified recognition accuracy, speed, and resource. Requirements, be harmless to the users, be accepted by the intended population, and be sufficiently robust to various fraudulent methods and attacks to the system.



II. LEADING AREAS OF BIOMETRICS TECHNOLOGY

- Fingerprint
- Facial recognition

- Voice recognition
- Iris recognition
- Hand geometry
- Signature-scan
- Keystroke-scan
- DNA
- Ear shape
- Nail bed identification
- Vein-scan
- Odor

Based on the characteristics of human, biometrics classified into a Physiological Behavioral. Let us see about some of the Advanced Trends in BIOMETRICS

III. 3D FACIAL RECOGNITION

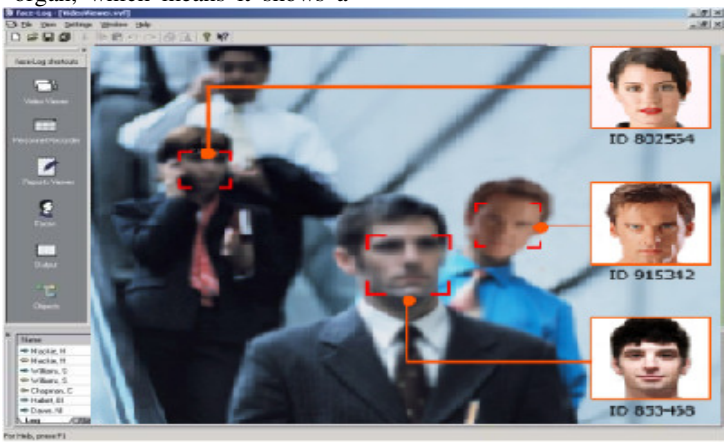
Facial recognition system should detect face automatically to an image, extract the features and then identify its general viewpoint (i.e., from any pose) which is a rather difficult task. Another problem is the truth that is the face is a changeable organ, which means it shows a variety of expressions. New technology in facial recognition application uses 3D model, which titles to give additional accuracy. Capturing 3D image of a face, 3D facial recognition has unique features of the face in which the face rigid tissue and bone is most seeming, such as curves in eye socket, nose and chin will identify subjects. These areas in our face are unique all time and it will never change over time. 3D facial recognition can used in darkness also and it has ability to recognize the human face at different angles with potential which recognize up to 90 degrees

Detection

Getting an image can be proficient by scanning in digital technique, existing 2D photograph or by recording video and acquire image to a live picture for a subject (3D).

Alignment

If it detects a face once, the system defines the position of head its size, Pose. As mentioned previously, the human face is being recognized up to 90 degrees, But with the help of 2D, the head must be rotated at least 35 degrees toward camera.



Measurement

The system will measure; a curve presents in the face on a millimeter scale and creates a model.

Representation

The application will transfer the model into code which uniquely defined. This code is given to each and every model. That is, set of numbers to identify the features on a person's face.

Verification or Identification

In verification, the recognized image is matched with the image present in database (1:1, image is matched with only one image in database). For example, an image taken from a person's face is matched to an image in Motor Vehicles Department database to verify a particular person who he is. Here identification is the only goal, so the image is compared to each and every image in the database which will results in a value for each likely match (1: N). In this case, you take an image and compare to database.

Matching:

If the image is in 3D and the database also contains 3D image, then matching takes place without any changes made to image. But there is a challenge facing in databases which is still in 2D images also. 3D image provides a live and moving subject is compared to flat, and stable image. New technology emerged to face this challenges. That is, if a 3D image is taken, several points are identified. For instance, outside of eye, inside the eye and tip of nose will be measured. Once the measurements are taken by application, an algorithm is applied to the image. The algorithm is used to convert a 3D dynamic image to 2D static image. After conversion are made, the application compares with 2D images available in database to find a perfect match.

IV. FINGERPRINT RECOGNITION

Fingerprint recognition technology is probably the widely used familiar biometric systems. Fingerprint recognition based on the features found in the impressions made by unique ridges on fingertips. Two types of fingerprints: they are flat and rolled.

Flat prints are an impression only in central area of the finger pad.

Rolled prints capture impression on the sides of the finger and also central portion of the finger that is between the tip and first knuckle.

Fingerprint are scanned, enhanced, and converted to models. These models are saved in database for future comparisons using scanners. Scanner are several types they are Ultrasound, optical. Ultrasound is the most accurate, but rarely used. Optical scanners are used often. According to report given by the U.S. General Accounting Office, the fingerprint readers will approximately cost $1,000 to $3,000.

There are also additional software applications in which the licensing expenses is about $4/user. Smaller fingerprint readers will also maintain the costs around 15% to 18% of purchase price. The larger 3D scan is about $25,000 and also costs is about 14% of reader's cost.

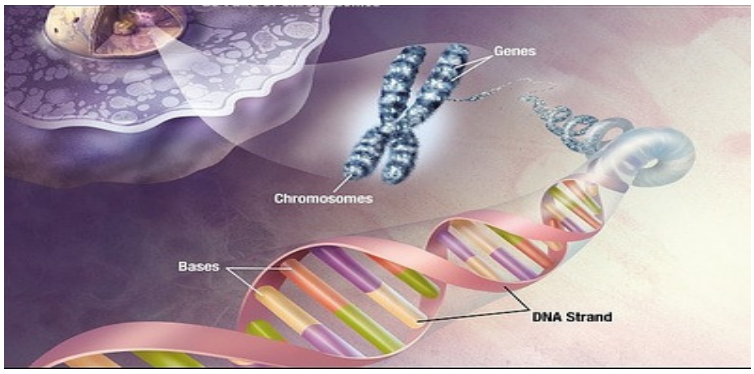
urity problems for the
the implementation of
ure for instance a

A small % of people cannot be enrolled. Because the ridges in fingers have been dry, damaged with age, or damaged from corrosive chemicals usage. In addition to this, some people are uncomfortable with this technology because the relationship to forensic fingerprinting certain cultures. The fingerprints collected for one purpose can also use to track individual's activities. People rarely complain about touching a scanner that other people have touched, thinking that it is unhygienic. Fingerprint biometric do not work everywhere; they may also inappropriate sometimes. For instance, in gloved environments like operation theaters in hospitals.

Advantages

- Fast to compute.
- Less cost, easy to implement.
- Easy maintenance.
- Reasonable uniqueness.

V. DNA RECOGNIZATION



Advance of DNA in Biometrics:

High level of confidentiality and the security of DNA database (access rights, length of information retention). Currently, the National Science and Technology Council (NTSC), Committee on Technology, Committee on Homeland and National Security and Subcommittee on Biometrics are part of the internal deliberative process of NTSC. These agencies develop and implement multi-agency policies that aid in moving the biometric sciences to meet public and private needs.

Health Issues

Most of the biometric systems in place today use sensors to obtain the individual's biometric information. The majority of health concerns are those we encounter in our daily lives such as: touching a handprint sensor. This type of concern is in direct relation to touching a doorknob in a public place. However, there are other concerns specifically related to scanning devices. There are fears that the devices can create health issues when the iris is scanned or when the face is scanned.

Analysis of DNA will take weeks and even a months to process. But research, developers had been

reduced the whole process to less than 30 minutes. NEC have developed the world's first human DNA recognizer. This analyzer integrates each and every steps of DNA process, which is able to do within a time span of 25 minutes (approx.). But this is completely incompatible to access a secure facility and also insupportable to use in Security Network Environment.

Advantages:

- Very high accuracy (i.e. it is impossible to the system to make mistakes).
- It is consistent.

VI. CONCLUSION

As technology grows and time goes on, more private and public service units use biometrics for accurate credentials. There will be no legal restrictions on biometrically recognizing information. But there also severe restrictions based on the collection of records, creating a records, maintaining database of recognizable personal data. The immediate conclusion we should draw is, the biometrics authentication should be traceless.

REFERENCE

[1] Jain, A. K.; Ross, A. & Pankanti, S., "Biometrics: A Tool for Information Security", IEEE Transactions On Information Forensics And Security, June 2006.
[2] "Progress and Directions", IEEE Transactions on Pattern Analysis and Machine Intelligence Special Issue, July 2007.
[3] Wikipedia– Advanced biometrics article.
[4] www.biometrics.tibs.org.
[5] National Conference on Computer Applications In Service Sector (NCCASS 2012), 7th September, 2012