BIOMETRICS: AN INTRODUCTION TO NEW MODE OF SECURITY

Manoj Parmar[1], Ritesh Patankar[2]

[1]*IT Department, G.P.Himatnagar*
[2]*EC Department, G.P.Gandhinagar*

Abstract— The term "biometrics" is derived from the Greek words bio means life and metric means to measure. That means Biometrics is referred to the identification of a person based on his/her behavioral or physiological characteristics. This method of identification is preferred over traditional methods involving passwords and PIN numbers for its accuracy and case sensitiveness. A biometric system is essentially a pattern recognition system which makes a personal identification by determining the authenticity of a specific physiological or behavioral characteristic possessed by the user. An important issue in designing a practical system is to determine how an individual is identified. Depending on the context, a biometric system can be either a verification (authentication) system or an identification system. Verification involves confirming or denying a person's claimed identity while in identification, person must establish his/her identity. Biometric systems are divided on the basis of the authentication medium used. They are broadly divided as identifications of Hand Geometry, Vein Pattern, Voice Pattern, DNA, Signature Dynamics, Finger Prints, Iris Pattern and Face Detection. These methods are used on the basis of the scope of the testing medium, the accuracy required and speed required.

Keywords— Biometrics, Identification, Physiological, Behavioral, Recognitions, verification

I.   INTRODUCTION

Biometrics is the measurement and statistical analysis of people's physical and behavioral characteristics. The technology is mainly used for identification and access control, or for identifying individuals that are under surveillance. Reliable authorization and authentication has become an integral part of every man's life for a number of routine applications. Biometrics is automated method of recognizing a person based on a physiological or behavioral characteristic. Biometrics though in its nascent form has a number of tractable aspects like security, data integrity, fault tolerance and system recovery. It is considered a reliable solution for protecting the identity and the rights of individuals as it recognizes unique and immutable features. Biometrics is used for two authentication methods (Illustrated in Fig. 1):

• **Identification**:

This involves establishing a person's identity based only on biometric measurements. The comparator matches the obtained biometric with the ones stored in the database bank using a 1: N matching algorithm for identification. [1]

• **Verification**:
It involves confirming or denying a person's claimed identity. A basic identity (e.g. ID number) is accepted and a biometric template of the subject taken is matched using a 1:1 matching algorithm to confirm the person's identity.
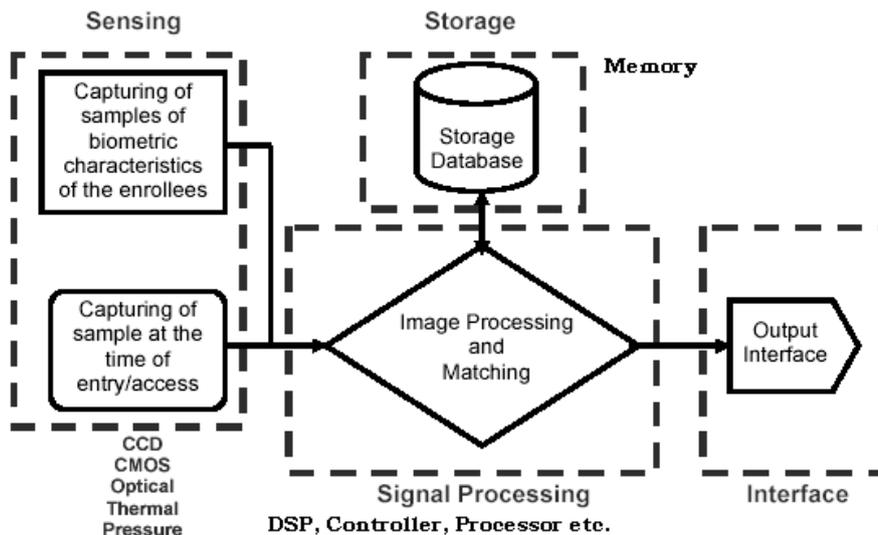
"Figure 1: Basic Biometric Authentication System."

The validity of a biometric system cannot be measured accurately, and can only be enumerated on the occurrence of errors like the chance of accepting an intruder i.e. the False Accept Rate (FAR) and conversely the probability of rejecting a genuine individual i.e. False Reject Rate (FRR) which could Turn out to be detrimental to any system. [2]

II.   TYPES OF BIOMETRICS

Biometrics is classified in to two broad categories.

a. Physiological
   a. Fingerprint recognition
   b. Face recognition
   c. Iris recognition
   d. Hand geometry
   e. DNA recognition

b. Behavioral
   a. Keystroke recognition
   b. Signature recognition
   c. Voice recognition

A. Fingerprint Recognition

This technique involves taking an image of a person's fingertips and records its characteristics like whorls, arches, and loops   along with the patterns of ridges, furrows, and minutiae. Fingerprint matching can be achieved in three ways.[1]

• **Minutiae** based matching stores minutiae as a set of Points in a plane and the points are matched in the template and the input minutiae. [4]

"Fig.2 Fingerprint Basic Details"

• **Correlation** based matching technique superimposes two fingerprint images and correlation between corresponding pixels is computed.
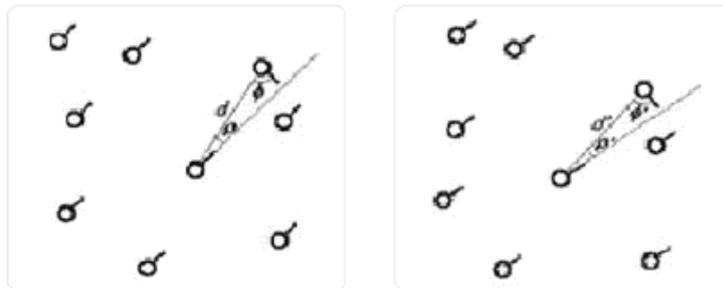
Matching
"Fig.3 Fingerprint Matching technique"

• **Ridge** feature based matching is an advanced method that takes ridge capturing, because minutiae capturing is difficult in the case of low quality fingerprint images.[4] To capture the fingerprints, different techniques uses solid state sensors that work on the transducer technology like capacitive, thermal or piezoelectric sensors etc; optical sensors that use a CCD or CMOS image sensor. Fingerprint scanning is very stable and reliable. It secures entry devices for building door locks and computer network access is becoming more common. Currently in India Dena bank started to use fingerprint readers for authorization at ATMs for persons who are not literate enough to access using Pin number and so on.

B. Face recognition

This technique records face images through a digital video camera and analyses characteristics of human face like the distance between eyes, nose, mouth etc. These measurements are broken into facial planes and retained in a database, then it is used for comparison. [1][4] Face recognition can be done in two ways:

• Face appearance
It employs Fourier transformation of the face image into its fundamental frequencies and formation of eigenfaces, consisting of Eigen vectors of the covariance matrix of a set of training images. The distinctiveness of the face is captured without being oversensitive to noise such as lighting variations.

• Face geometry
In this recognition method, the models a human face created in terms of particular facial features like eyes, mouth, etc. and
layout of geometry of these features is computed. To prevent a fake face or mold from faking out the system, many systems now require the user to smile, blink, or otherwise move in a way that is human

before verifying. This technique is gaining support as a potential tool for averting terrorism, law enforcement areas and also in networks and automated bank tellers.

C. Voice Recognition

Voice recognition uses combination of physiological and behavioral factors to produce speech patterns that can be captured by speech processing technology. Basic properties of the speaker like fundamental frequency, nasal tone, cadence, inflection, etc. are used for speech authentication. Voice recognition techniques can be divided into categories depending on the type of authentication domain. [3]

• Fixed text method is a technique where the speaker is required to say a predetermined word that is recorded during registration on the system. In the text dependent method the system prompts the user to say a specific word or phrase, which is then computed on the basis of the user's fundamental voice pattern. The text independent method is an advanced technique where the user need not articulate any specific word or phrase. The matching is done by the system on the basis of the fundamental voice patterns irrespective of the language and the text used.
• Conversational technique verifies identity of the speaker by inquiring about the knowledge that is secret or unlikely to be known or guessed by a sham. This interactive authentication protocol is more accurate as the FAR is kept very low.
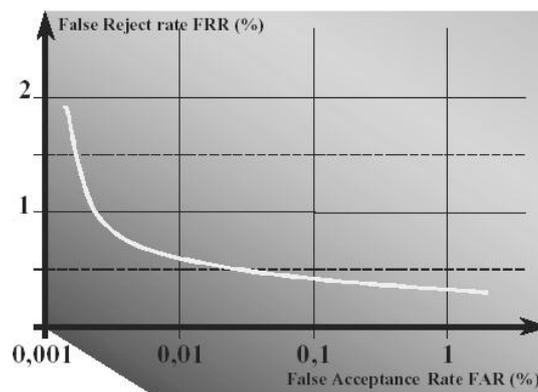
"Fig.4 FRR vs FAR characteristic"

The vocal-tract is represented in a parametric form as the transfer function H(z). Ideally, the transfer function should contain poles as well as zeros. However, if only the voiced regions of speech are used then an all-pole model for H(z) is sufficient. Furthermore, linear prediction analysis can be used to efficiently estimate the parameters of an all-pole model. Finally, it can also be noted that the all-pole model is the minimum-phase part of the true model and has an identical magnitude spectra, which contains the bulk of the speaker-dependent information (Illustrated in Fig. 2). [5]
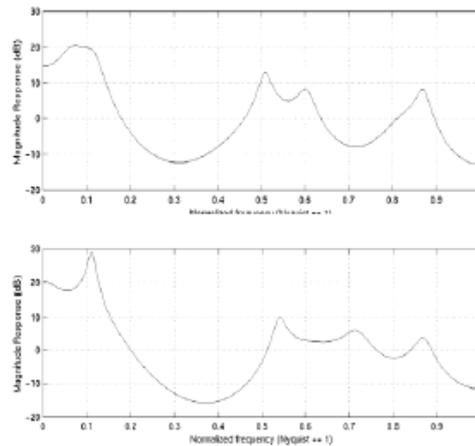
"Fig.5 illustrates the differences in the models for two speakers saying the same vowel."

This technique is inexpensive but is sensitive to background noise and it can be duplicated. Also, it is not always reliable as voice is subject to change during bouts of illness, hoarseness, or other common throat problems. Applications of this technique include voice-controlled computer system, telephone banking, m-commerce and audio and video indexing.

D. Iris recognition:

This method analyzes features like rings, furrows, and freckles existing in the colored tissue surrounding the pupil. The scans
use a regular video camera and works through glasses and contact lenses. The image of the iris can be directly taken by making the user position his eye within the field of a single narrow-angle camera. This is done by observing a visual feedback via a mirror. The isolated iris pattern obtained is then demodulated to extract its phase information. [1][6] Iris image acquisition can be done in two ways:

• **Daugman System** that uses an LED based point light source in conjunction with a standard video camera. The system zaptures images with the iris diameter typically between 100-200 pixels from a distance of 15-46 cm using 330mm lens.

• **Wildes System** in comparison results in an illumination rig that is more complex. The system images the iris with approximately 256 pixels across the diameter from 20cm using an 80mm lens. Iris recognition was piloted in Saudi Arabia as a method of keeping track of the millions making Haj. Also it is used a Berkshire County jail for prisoner identification and   Frankfurt airport for passenger registration.

E. Hand geometry:

This technique suggests the involvement of the measurement and analysis of the human hand. Features like length and width of the fingers, aspect like length and width of the fingers, aspect ratio of the palm or fingers, width of the palm, thickness of the   palm, etc are computed. The user places the palm on a metal surface, which has guidance pegs on it to properly align the palm, so that the device can read the hand attributes. [1][6] The basic procedure involves capturing top and side views of the hand   using a single camera by judicious placement of a single 45° mirror. To enroll a person in a database, two snapshots of the hand are taken and the average of resulting feature vectors is computed and stored. Four different distance matrices (Absolute,   weighted absolute, Euclidean and weighted Euclidean) are calculated. Hand Geometry is employed at locations like the Colombian

legislatures, San Francisco International Airport, day care centers, a sperm bank, welfare agencies, hospitals, and immigration facilities.

F. Hand Vascular Pattern:

This method of recognition uses a no harmful near infrared light to produce an image of person's vein pattern in their face, wrist, or hand, as veins are relatively stable through the person's life. It is a non-invasive, computerized comparison of shape and size of subcutaneous blood vessel structures in the back of a hand. The vein "tree" pattern, picked up by a video camera, is sufficiently idiosyncratic to function as a personal code that is extremely difficult to duplicate or discover. The sensor requires no physical contact, providing excellent convenience and no performance degradation even with scars or hand contamination. Verification speed of the system is fast (0.4 sec/person) and the False Acceptance Rate is FAR) and False Rejection Rate (FRR) are extremely low at 0.0001 % and 0.1% respectively. Though minimally used at the moment, vascular pattern scanners can be found in testing at major military installations and is being considered by some established companies in the security industry and multi-outlet retailers.[5]

G. Retina Recognition:

Retina technology uses infrared scanning and compares images of the blood vessels in the back of the eye, the choroidal vasculature. The eye's inherent isolation and protection from the external environment as an internal organ of the body is a benefit. Retina scan is used in high-end security applications like military installations and power plants.

H. Signature recognition:

This is an instance of writer recognition, which has been accepted as an evidence in courts of laws. The way a person signs his name is known to be a characteristic of that individual. Approach to signature verification is based on features like number of interior contours and number of vertical slope components. Signatures are behavioral biometric that can change with time, influenced by physical and emotional conditions of the signatories. Furthermore, professional forgers can reproduce signatures to fool an unskilled eye and hence is not the preferred choice.

I. DNA Recognition:

Deoxyribo Nucleic Acid (DNA), which is the ultimate unique code for ones individuality. However, it is currently used mostly used in the context of forensic applications. The basis of DNA identification is the comparison of alleles of DNA sequences found at loci in nuclear genetic material. A set of loci is examined to determine which alleles have been identified. However, issues like contamination, sensitivity, and automatic real-time recognition limits the utility of this biometric.

III. CONCLUSION

Applications of Biometric Systems The applications of biometrics can be divided into the following three main groups: • Commercial applications such as computer network login, electronic data security, ecommerce, Internet access, ATM, credit card, physical access control, cellular phone, PDA, medical records management, distance learning, etc. • Government applications such as national ID card, correctional facility, driver's license, social security, welfare-disbursement, border control, passport control, etc. • Forensic applications such as corpse identification, criminal investigation, terrorist identification, parenthood determination, missing children, etc. Traditionally, commercial applications have used knowledge-based systems (e.g., PINs and passwords), government applications have used token-based systems (e.g., ID cards and badges), and forensic

applications have relied on human experts to match biometric features. The merit of biometrics is proven by endeavors of the G8 countries to apply it to prevent forgery of passports and other travel documents as part of their fight against terrorism. Without doubt the age of biometrics is here and the technology will directly affect everyone over the next few years.

IV. ACKNOWLEDGEMENT

REFERENCES

[1] Anil K. Jain, Salil Prabhakar, Handbook of Fingerprint Recognition, 2002
[2] Anil K. Jain, Arun Ross and Salil Prabhakar, An Introduction to Biometric Recognition, IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics, Vol. 14, No. 1, January 2004.
[3] 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.
[4] A. Kumar, D. C. Wong, H. C. Shen, and A. K. Jain, "Personal verification using palmprint and hand geometry biometric," presented at the 4th Int. Conf. Audio- and Video-based Biometric Person Authentication, Guildford, U.K., June 9–11, 2003
[5] http://www.accesscontrolsystem.in
[6] http://www.biometricsinfo.org
[7] http://biometrics.cse.msu.edu