BIOMETRICS : A FURTHER ECHELON OF SECURITY

Siddhesh Angle, Reema Bhagtani, Hemali Chheda

Department of Biomedical Engineering, Thadomal Shahani Engineering College, T.P.S III, Bandra, Mumbai-50
E-mail: sidangle@ieee.org, reema@ieee.org, hemali185@yahoo.co.in

ABSTRACT

The term "biometrics" is derived from the Greek words bio (life) and metric (to measure). Biometrics refers to the automatic identification of a person based on his/her physiological or behavioral 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, one has to establish a person's 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. Every medium of authentication has its own advantages and shortcomings. With the increased use of computers as vehicles of information technology, it is necessary to restrict unauthorized access to or fraudulent use of sensitive/personal data. Biometric techniques being potentially able to augment this restriction are enjoying a renewed interest.

1. INTRODUCTION

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.[3]
- **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.[3]

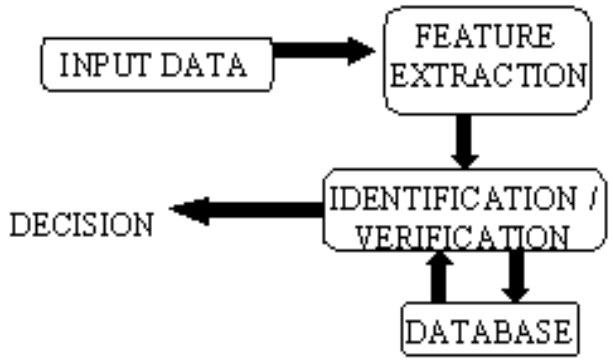

Fig. 1: Basic Biometric Authentication System.

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. [3]

2. TYPES OF BIOMETRICS

➢ *Bertillonage*, 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. The method consisted of identifying people by taking various body measurements like a person's height, arm length, length and breadth of the head, the length of different fingers, the length of forearms, etc. using calipers. However, the methodology was unreliable as non-unique measurements allowed multiple people to have same results, decreasing the accuracy and hence is no longer used.[6]

➢ *Fingerprint Recognition* 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 [2]:

- *Minutae based* matching stores minutiae as a set of points in a plane and the points are matched in the template and the input minutiae.
- *Correlation based* matching superimposes two fingerprint images and correlation between corresponding pixels is computed.
- *Ridge feature based* matching is an advanced method that captures ridges, as minutiae capturing are difficult in low quality fingerprint images.

To capture the fingerprints, current techniques employ *optical sensors* that use a CCD or CMOS image sensor; *solid state sensors* that work on the transducer technology using capacitive, thermal, electric field or piezoelectric sensors; or *ultrasound sensors* that work on echography in which the sensor sends acoustic signals through the transmitter toward the finger and captures the echo signals with the receiver. [2]

Fingerprint scanning is very stable and reliable. It secures entry devices for building door locks and computer network access are becoming more common. Recently a small number of banks have begun using fingerprint readers for authorization at ATMs.

➢ *Face recognition* technique records face images through a digital video camera and analyses facial characteristics like the distance between eyes, nose, mouth, and jaw edges. These measurements are broken into facial planes and retained in a database, further used for comparison. Face recognition can be done in two ways:

- *Face appearance* 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. [3] The distinctiveness of the face is captured without being oversensitive to noise such as lighting variations.
- *Face geometry* models a human face created in terms of particular facial features like eyes, mouth, etc. and layout of geometry of these features is computed. Face recognition is then a matter of matching constellations.[3]

Another face identification technology, *Facial thermograms*, uses infrared heat scans to identify facial characteristics. This non-intrusive technique is light-independent and not vulnerable to disguises. Even plastic surgery, cannot hinder the technique. This technique delivers enhanced accuracy, speed and reliability with minimal storage requirements.[4] 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.[6] This technique is gaining support as a potential tool for averting terrorism, law enforcement areas and also in networks and automated bank tellers.

➢ *Voice Recognition* combines physiological and behavioral factors to produce speech patterns that can be captured by speech processing technology. Inherent properties of the speaker like fundamental frequency, nasal tone, cadence, inflection, etc. are used for speech authentication.[4]

Voice recognition techniques can be divided into categories depending on the type of authentication domain. [3,5]

- *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 are claimed to be below 10^{-12}.

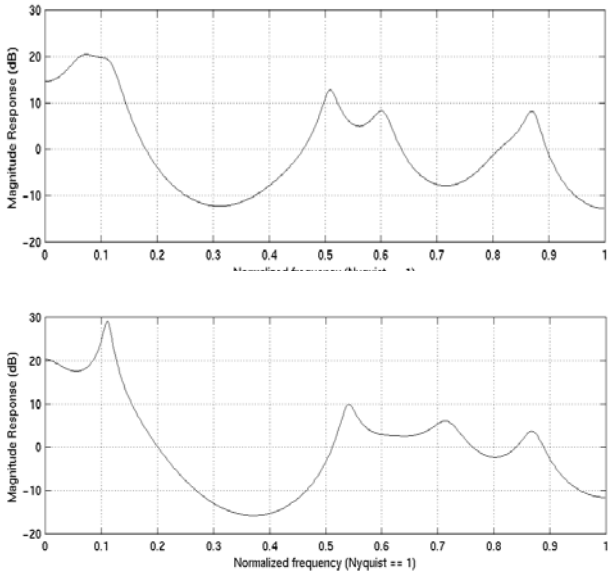

Fig. 2. Illustrates the differences in the models for two speakers saying the same vowel.

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]

This technique is inexpensive but is sensitive to background noise and it can be duplicated. [8] 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.

➢ *Iris recognition* 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. [6] 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.[3] The isolated iris pattern obtained is then demodulated to extract its phase information.[1]

Iris image acquisition can be done in two ways:

- *Daugman System* that uses an LED based point light source in conjuction with a standard video camera. The system captures 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. [8]Also it is used a Berkshire County jail for prisoner identification and Frankfurt airport for passenger registration.[6]

➢ *Hand geometry*, as the name suggests, involves the measurement and analysis of the human hand. Features 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.[3]
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.[3] Four different distance matrices (Absolute(i), weighted absolute(ii), Euclidean(iii) and weighted Euclidean(iv))

$$\sum_{j=1}^{d} | qj - rj | < \varepsilon a \quad \text{(i)} \qquad \sum_{j=1}^{d} \frac{| qj - rj |}{\sigma j} < \varepsilon wa \quad \text{(ii)}$$

$$\sqrt{\sum_{j=1}^{d} (qj - rj)2} < \varepsilon e \quad \text{(iii)} \qquad \sqrt{\sum_{j=1}^{d} \frac{(qj - rj)^2}{\sigma j^2}} < \varepsilon we \quad \text{(iv)}$$

corresponding to following equations 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.

➢ *Hand Vascular Pattern Identification* uses a non-harmful near infrared light to produce an image of one's vein pattern in their face, wrist, or hand, as veins are relatively stable through one's life. [4,7] 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. [4] The sensor requires no physical contact, providing excellent convenience and no performance degradation even with scars or hand contamination.[7] 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. [7] 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.[6]

➢ *Retina Recognition* technology uses infrared scanning and compares images of the blood vessels in the back of the eye, the choroidal vasculature.[3] The eye's inherent isolation and protection from the external environment as an internal organ of the body is a benefit.[4] Retina scan is used in high-end security applications like military installations and power plants.

➢ *Signature recognition* is an instance of writer recognition, which has been accepted as irrefutable evidence in courts of laws. [3] 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 contour*s and *number of vertical slope components*. [3] 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. [2]

Table 1: Illustration comparing biometric types. [6]

BIOMETRIC TYPE	Fingerprint	Facial Recognition	Hand Geometry	Speaker Recognition	Iris Scan	Retinal Scan
Verification	✓	✓	✓	✓	✓	✓
Identification	✓	×	×	×	✓	✓
Accuracy (4)	4	3	3	2	4	4
Reliability(4)	3	2	2	1	3	3
Security Level (4)	3	2	2	2	3	3
Longterm Stability (4)	3	2	2	2	3	3
Acceptance (4)	2	2	2	3	2	2
Ease of Use (4)	3	2	3	3	2	1

➢ *DNA Recognition* employs Deoxyribo Nucleic Acid, which is the one-dimensional ultimate unique code for ones individuality, except for the fact that identical twins have identical DNA patterns. [2] 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. [3] A set of loci is examined to determine which alleles have been identified. However, issues like contamination, sensitivity, and automatic real-time recognition limit the utility of this biometric. [3,2]

3. CONCLUSION

Current electronic security systems, which rely primarily on personal identification to ensure that a client is an authorized user of a system, have a common vulnerability: the verification can be duplicated which can be nearly eliminated using biometrics. [4] Biometrics can be used by various organizations to increase security levels and protect their data and patents. Biometrics although interdisciplinary, it is not the eventual choice of the masses due to its high cost and legal considerations like privacy issues. [4] 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.[8] Without doubt the age of biometrics is here and the technology will directly affect everyone over the next few years. [8]

4. ACKNOWLEDGEMENTS

We take this opportunity to express our gratitude to our guides Ms. Mita Bhowmick, Incharge, Department of Biomedical Engineering, Thadomal Shahani Engineering College and Mr. Veetrag Bafana, Managing Director, ZEOS Infotech Pvt. Ltd.

5. REFERENCES:

[1]J.G.Daugman. High confidence visual recognition of persons by a test of statistical impedance. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 15(11): 1148-1161, November 1993

[2] Davide Maltoni, Durio Maio, Anil K. Jain, Salil Prabhakar, *Handbook of Fingerprint Recognition*, 2002

[3] Ruud M. Bolle, Jonathan H. Connell, Sharath Pankanti, Nalini K. Ratha, Andrew W. Senior, *Guide To Biometrics, 2003*

Websites (accessed latest on January 13, 2005.)

[4]. http://csc.noctrl.edu

[5]. http://www.biometricsinfo.org

[6]. http://ctl.ncsc.dni.us/

[7] http://www.gizmo.com.au

[8] http://www.iirme.com