ISSN (Online): 2230-7893
www.IJCEM.org

Biometric Recognition: Personal Identification Technique

Zatin Singhal[1], Preeti Gupta[2], Kavita Garg[3]

[1]Assistant Professor, Department of Computer Science, MVN Education City, Palwal, Haryana
zatin.gupta2000@gmail.com

[2]Assistant Professor, Department of Computer Science, MVN Education City, Palwal, Haryana
preetigupta.gupta75@gmail.com

[3]Assistant Professor, Department of Computer Science, MVN Education City, Palwal, Haryana
kavitagoyalmca@gmail.com

Abstract

The recent advances of information technology and the increasing requirement for security have led to a rapid development of intelligent personal identification systems based on biometrics. As humans, we all use our natural abilities to recognize people through their voices, faces and other characteristics. Technology advances, particularly in biometrics, are helping to close the gap between human perception and machine recognition. A priority goal of the use of biometrics is to provide identity assurance or the capability to accurately recognize individuals with greater reliability. Biometric recognition or, simply, biometrics refers to an automatic recognition of individuals based on their physiological and/or behavioral characteristics. This paper gives a brief overview of biometric, biometric recognition system, and various biometric recognition methods and their advantages, and disadvantages.

Keywords: *Biometrics, Working of Biometrics, Types of Biometrics*

1. Introduction

In the past years, an extensive research and development has been taken place in the areas of unique identification.

There are two main techniques which are in use from last few years and that are Barcode identification & Radio Frequency Identification (RFID).

Barcode is a set of bars and spaces representing alphabet or numeric data for identification of a particular product, service or a process. Barcode technology is the best-known and most widely used method of Automatic Identification. Automatic identification or "Auto ID" encompasses the automatic recognition and recording of data, most commonly through the printing and reading of information encoded in barcodes thereby eliminating risk of human error.
Early applications of bar code scanning, which included retail point-of-sale, item tracking and inventory control, have been expanded to include more advanced applications such as time and attendance, work-in process, quality control, sorting, order entry, document tracking, shipping and receiving, and controlling access to secure areas.

The packet of Wrigley's chewing gum was the firs-ever product to be bar-coded and scanned at Marsh's supermarket in Troy, Ohio in the year 1974.

RFID means Radio Frequency Identification is a wireless identification technique which becomes very popular these days and is used for the identification of physical objects like products, humans etc by the use of radio frequency.

This technique is much more advantageous, safe, secure and easy with lower overhead in contrast with the other conventional technique used. It is much faster.

There are many similarities and differences between RFID and barcode. The most common similarity is that both are being used for identifying an item. They differ in the area of line of sight, distance, effectiveness and many more like environmental conditions, capacity, efficiency etc.

The RFID doesn't require line of sight (LOS) between reader and chip while barcode requires LOS.

RFID reader can read more than 100 chips or tags simultaneously while barcode only 1 chip at a time. So, RFID takes less time than barcode and hence it is more efficient than barcode.

In RFID radio frequency Technology is used whereas in barcode LASER Technology is used.

RFID is reprogrammable i.e. its programming can be modified after some time but barcode is not reprogrammable i.e. once it's programmed, after that its contents can't be changed.

It is very much difficult to copy RFID tag but barcode chip can easily copy.

The Solution of the problems occurs in RFID & Barcode is well known as Biometric Identification System, is essentially a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database.

2. Biometric History

The term "biometrics" is derived from the Greek words bio (life) and metric (to measure). The word refers to automated methods of authentication based on physical or behavioral characteristics of an individual.

The first known example of biometrics was a form of finger printing being used in China to distinguish the young children from one another by stamping children's palm prints and footprints on paper with ink. This is one of the earliest known cases of biometrics in use and is still being used today.

Although biometrics emerged from its extensive use in law enforcement to identify criminals, it is being increasingly used today in to establish person recognition in a large number of civilian applications.

To make a personal recognition, biometrics relies on who the person is or what he does, as opposed to what he knows (such as a password) or what he possesses (such as an ID card).

2.1 Measurement Requirements

Any human physical and/or behavioral characteristic can be used as a biometric characteristic if it satisfies the following requirements:

- Universality
- Distinctiveness
- Permanence
- Collectability
- Performance
- Acceptability
- Circumvention

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.

3. Biometric Systems

A biometric system is essentially a pattern-recognition system that recognizes a person based on a feature vector derived from a specific physiological or behavioral characteristic that the person possesses. That feature vector is usually stored in a database or recorded on a smart card after being extracted. Biometric system operates in one of two modes: verification or identification.

Data Acquisition: Digital cauterization of the biometric is done here and the results are transferred to the signal processing functions.

Transmission Channel: This is the communication path between the primary functional components. For self-contained systems, transmission channels are internal but for distributed systems (remote data acquisition) transmission channel might be LAN, private intranet, or even the internet.

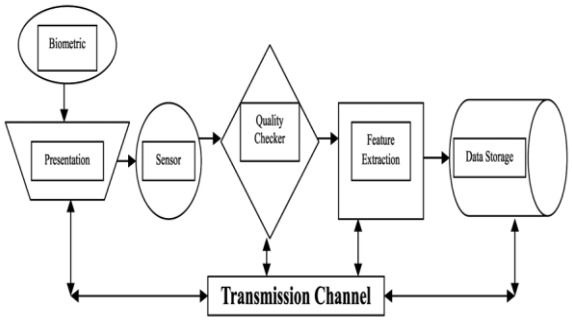

Figure 1: Data Acquisition/ Collection

Signal Processing: This is where the raw biometric data is processed for matching. Processing consists of segmentation of the sample, then isolate and extracting relevant features from the data, and creating a biometric template i.e. mathematical representation of the original biometric. Segmentation is the process of separating relevant features from the background information.

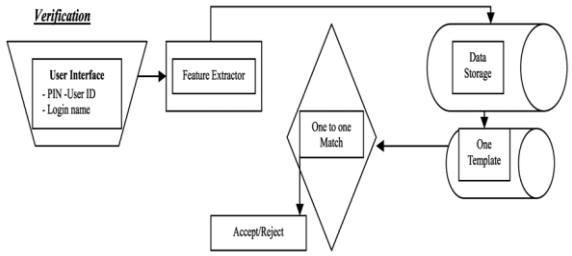

Figure 2: Signal Processing- Verification

The result of extraction segmentation is a quality score, reflecting the quality of the input by how successful the feature extraction was. Then the newly created template is then compared to one or more reference templates by the matching algorithm. The result of matching algorithm is a match score, indicating how similar the templates are.

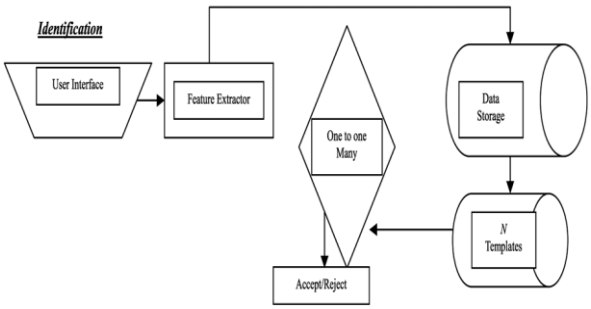

Figure 3: Signal Processing- Identification

Decision Policy: It makes a final determination whether there is a match or not. Normally, empirically determined thresholds are used for the quality score and match score. If both scores are met then a match is produced (yes). If only the quality threshold is met, negative match (no). If the quality threshold is not met, the application might refuse the match because of the poor quality data and request a new sample.

4. Biometric Methods

The physical and/or behavioral characteristics of a person like finger prints, face, voice, iris etc. are known as biometric. Each biometric has its strengths and weaknesses, and the choice depends upon its application & biometric properties. No single biometric is sufficient to meet the requirements of all the applications. So, no biometric is "optimal".

An overview of commonly used biometrics is given below:

A. DNA

Deoxyribonucleic acid (DNA) is the one-dimensional (1–D) ultimate unique code for one's individuality - except for the fact that identical twins have identical DNA patterns.. DNA requires an actual tangible physical sample for comparison as opposed to an impression, image, or recording.

Benefits:
Accurate: the chance of 2 individuals sharing the same DNA profile is less than one in a hundred billion with 26 different bands studied.

DNA is intrinsically digital and unchangeable during a human's life and even after death.

Applications: Used in forensic applications for person recognition, used for paternity testing, identification of missing or dead people.

B. Face

The dimensions, proportions and physical attributes of a person's face are unique [13]. Facial recognition systems will measure and analyze the overall structure, shape and proportions of the face:

Measurements (facial expressions, user's smile, blink, nod their head) help in recognizing a person wearing a mask.
The main facial recognition methods are: feature analysis, neural network and automatic face processing.

Benefits: Not intrusive, can be done even without the user awareness.

Weakness: More suited for authentication than for identification

Applications: Access to restricted areas and buildings, banks, embassies, military sites, airports, law enforcement.

C. Fingerprint

Finger print comprises of ridges and valleys. The ridges are the dark area of the fingerprint. The ridges form so-called minutia points: ridge endings (where a ridge end) and ridge bifurcations (where a ridge splits in two). In this, the overall characteristics of the fingerprints (minutia points, ridge thickness, curvature, or density) are compared with the registered template. The fingerprints of individuals are unique, even for twins. The main technologies used to capture the fingerprint image with sufficient detail are optical, silicon, and ultrasound.

Benefits: Easy to use, Cheap, Small size, Low power, Non-intrusive, Large database already available.

Weakness:

Acquiring high-quality images is complicated because of affected ridge patterns by cuts, dirt or wear and tear.

People with no or few minutia points cannot enroll or use the system.

Applications:

Fingerprint sensors are best for devices such as cell phones, USB flash drives, notebook computers.

Used for law enforcement, background searches to screen job applicants, healthcare and welfare.

D. Retina Scan

Retinal scan captures the pattern of eye's blood vessels. Retina is very difficult to spoof. Retinal patterns are different for right and left eye, for identical twins, do not change with age. Moreover, the image will not fall on the retina for dead person

In it, low-intensity coherent light source is projected onto the retina to illuminate the blood vessels which are then photographed and analyzed. A coupler is used to read the blood vessel patterns.

A retinal scan has an error rate of 1 in 10,000,000, compared to fingerprint identification error being sometimes as high as 1 in 500.

Applications: Suited for environments requiring maximum security, such as Government, military and banking.

E. Iris

The iris is the elastic, pigmented, connective tissue that controls the pupil & remains stable throughout life. It has a unique pattern, from eye to eye and person to person and even does not affect by glasses, contact lenses, and eye surgery.

An iris scan will analyze over 200 points of the iris, such as rings, furrows, freckles, and the corona.
Iris scanning systems vary the light and check that the pupil dilates or contracts to prevent image or photo from being used.

Benefits: Low False Acceptance Rates

Weakness: User must hold still while the scan is taking place.

Applications: Border control, prison security, database access and computer login, schools, aviation security, controlling access to restricted areas

F. Voice Recognition

Voice recognition systems can discriminate between two very similar voices, including twins. Voice recognition utilizes various audio capture devices (microphones, telephones and PC microphones). Its performance depends on the quality of the audio signal. Unauthorized access via tape recording can be prevented by asking the user to repeat random phrases

Benefits: Use existing telephones & can be automated, and coupled with speech recognition systems

Weakness: High false non-matching rates.

Applications: Mostly used for telephony-based applications: government, healthcare, call centers, electronic commerce, financial services, and customer authentication for service calls.

The applicability of a specific biometric technique depends on application domain. Each biometric technique is admissible. Some techniques are better for one application and other techniques for other application.

5. Conclusion

Biometrics refers to automatic recognition of an individual based on her behavioral and/or physiological characteristics. Reliable personal recognition is critical to many business processes. This paper presents biometric recognition system and methods for personal identification. From this, we have concluded that it helps security system up to some extent but one can't fully rely on this system. There are lot of techniques for recognition i.e. Retina, Iris, DNA, Face, Finger Recognition. In short, this method of recognition is far better in contrast with Barcode or RFID Identification.

References

[1] Zatin Singhal, Rajneesh Gujral, Anytime Anywhere-Remote Monitoring of Attendance System based on RFID using GSM Network, International Journal of Computer Applications (0975 – 8887) Volume 39– No.3, February 2012

[2] Salil Prabhakar, Sharath Pankanti, and Anil K. Jain, "Biometric Recognition: Security and Privacy Concerns", IEEE Security Privacy Mag., Vol. 1, No. 2, pp. 33-42, 2003.

[3] Anil K. Jain, Arun Ross, and Salil Prabhakar, "An Introduction to Biometric Recognition", IEEE Transactions on circuits and Systems for Video Technology, Vol. 14, No. 1, pp. 4-20, January 2004.

[4] Zatin Singhal, Ashish Gupta, "RFID: Unique Identification Technique for Attendance System", IJREAS Volume 2, Issue 2 (February 2012) ISSN: 2249-3905

[5] Vijaykumar Bhagavatula and Marios Savvides, "Correlation Pattern Recognition for Biometrics", SPIE the International Society for Optical Engineering Mag., 2006.

[6] K. Delac and M. Grgic, "A Survey of Biometric Recognition Methods", 46th International Symposium Electronics in Marine, ELMAR-2004, Zardar, Croatia, pp. 184-193, June 2004.

[7] Jasobanta Laha, "Biometric Techniques - Enhancing Security Standards In High Performance Enterprise", Computer and Technology Article, June 2008.

[8] S. Sonkamble, R. Thool, and B. Sonkamble, "Survey of Biometric Recognition Systems and their Applications", Journal of Theoretical and Applied Information Technology, pp. 45-51, 2005.

[9] Sandra Maestre and Sean Nichols, "DNA Biometrics", ISM 4320-001, http://danishbiometrics.files.wordpress.com/ 2009/08/nst.pdf, 2009.

[10] Md. Mahbubur Rahman, Md. Rashedul Islam, Nazmul Islam Bhuiyan, Bulbul Ahmed, and Md. Aminul Islam, "Person Identification Using Ear Biometrics", International Journal of The Computer, the Internet and Management, Vol. 15, No. 2, pp. 1-8, May - August, 2007.

[11] Ming-Hsuan Yang, David J. Kriegman, and Narendra Ahuja, "Detecting Faces in Images: A Survey," IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 24, No. 1, pp. 34- 58, January 2002.

[12] W. Zhao, R. Chellappa, P. J. Phillips, and A. Rosenfeld, "Face Recognition: A Literature Survey," ACM Computing Surveys, Vol. 35, No. 4, pp. 399–458, December 2003.

[13] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, "FVC2002: Fingerprint verification competition," IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 24, No. 3, pp. 402- 412, March 2002.

D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, "FVC2002: Fingerprint verification competition," IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 24, No. 3, pp. 402- 412, March 2002.

Jeffrey E. Boyd and James J. Little, "Biometric Gait Recognition," M.Tistarelli, J.Bigun, and E.Grosso (Eds.): Biometrics School 2003, Springer-Verlag Berlin Heidelberg, LNCS 3161, pp. 19–42, 2005.

Davrondzhon Gafurov, "A Survey of Biometric Gait Recognition: Approaches, Security and Challenges", Norsk Informatikkonferanse NIK-2007, November 2007.

Li Ma, Tieniu Tan, Yunhong Wang, and Dexin Zhang, "Personal Identification Based on Iris Texture Analysis", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 25, No. 12, pp. 1519- 1533, December 2003.

Edmond Lau, Xia Liu, Chen Xiao, and Xiao Yu, "Enhanced User Authentication through Keystroke Biometrics", Computer and Network Security Final Project Report, Massachusetts Institute of Technology, December 2004.

Chatchawal Wongchoosuk, Mario Lutz, and Teerakiat Kerdcharoen, "Automated Human Body Odor Recognition System", National Instruments article, http://digital.ni.com/ worldwide/singapore.nsf/web/all/CDB1F6BC59B4973C8625763 A0039AEE9.

N. Paveši, S. Ribari, and D. Ribari, "Personal authentication using hand-geometry and palmprint features – the state of the art", http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.93.877 1, 2004.

K. Saraswathi, B. Jayaram, and R. Balasubramanian, "Retinal Biometrics based Authentication and Key Exchange System", International Journal of Computer Applications (0975 – 8887), Vol. 19, No. 1, pp. 1- 6, April 2011.

Hong Ye, Youzheng Zhang, and Jianwei Shen, "Study on Speech Recognition of Greeting Based on Biomimetic Pattern Recognition", IEEE, 2nd International Workshop on Intelligent Systems and Applications (ISA), Wuhan, May 2010.