

Literature Survey of Biometric Recognition Systems

Shrutika Deokar¹, Sudeep Talele²

MITAOE, Pune University, Department of Electronics, Pune, India

Email: shrutika.deokar@gmail.com¹, sudeeptalele@gmail.com²

Abstract — Biometrics is gaining immense importance in today’s technical world. This paper presents an overview to various biometric systems. Biometrics has scope in various fields of science. This paper introduces us to different types of biometrics that are used for authentication and identification purpose.

Index Terms — Biometric Systems, iris, fingerprint, retina, DNA, face, signature, gait, speaker recognition and hand geometry.

I. INTRODUCTION

The science and technology of measuring and analyzing biological data for authentication or identification purpose is called as Biometrics. The system that successfully identifies and measures the biological data from the human body is called as a biometric system. Biometric Systems are computerized methods of verifying or recognizing the identity of an individual on the basis of some physical features or appearances, like a fingerprint or face pattern or some traits of behavior, like handwriting or keystroke patterns.

II. PROBLEM DEFINITION

In the present hi-tech world, there is an ever growing need to authenticate and identify people for security purposes. A wide variety of modern systems requires consistent personal recognition schemes to either confirm or determine the identity of an individual requesting their services. The objective is to ensure that the rendered services are accessed only by a legitimate user and no one else, to discourage fraud and enhance security and to specifically identify individuals in corporate areas.

Person identification methods are generally classified into three categories namely,

a) Knowledge-based approach: Person who knows something to make his/her personal identity such as password or personal identification number (PIN).

b) Token based approach: It uses particular ID, such as a passport, keys, ID card.

c) Biometric based approach: This approach uses physiological or behavioral features of an individual which cannot be stolen or lost.

The biometric identification method consists of three operations, they firstly capture biometric sample of the person and make a digital representation of the sample, then extract unique features from the digital representation using feature extractor, and then compare the extracted feature set against the template set in the database via matcher. The results determine if the person is identified or not. Figure 1 shows the block diagram of biometric system.

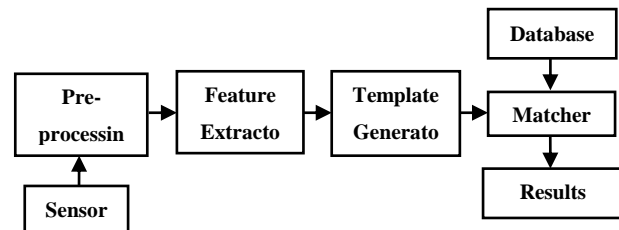


Figure 1. Basic block diagram of biometric system

III. HISTORICAL BACKGROUND

Biometrics can measure both physiological and behavioral characteristics. The measurements and data derived from direct measurement of a part of the human body contribute to physiological biometrics. And the measurements and data derived from an action contribute to behavioral biometrics. The most commonly used biometric features are briefed in figure 2:

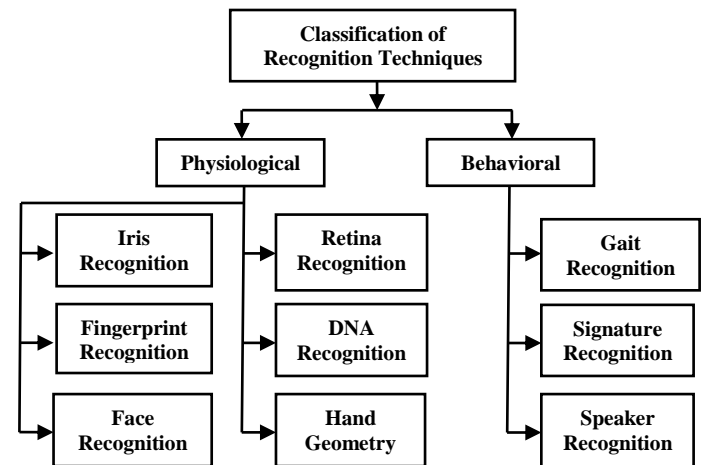


Figure 2. Classification of Biometric Features

I. BIOMETRIC SYSTEM

A. Iris Recognition

A person in iris recognition system is identified based on the uniqueness of the iris pattern of the eye. Basically, iris is defined as a circular region between pupil and sclera of human eye which exhibits bizarre texture that is unique for each individual [1], responsible for controlling the diameter and size of the pupil. This technique uses a high-quality camera to capture high resolution

images of iris. A high-quality image of the iris is captured to acquire every detailed feature while remaining noninvasive to the human operator. Figure 3 shows image of an iris.

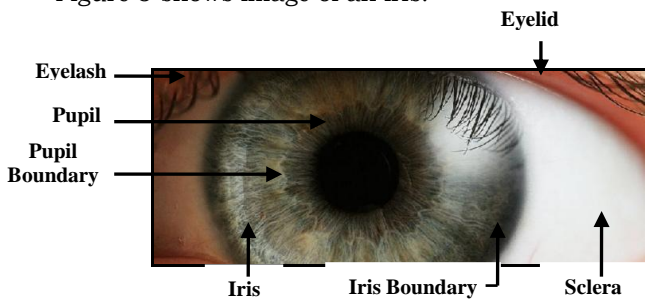


Figure 3 Iris

Advantages of iris scan:

- a. The iris has a fine texture because of which the extraction of features becomes easy.
- b. Every distinct individual has completely independent and unique iris textures.
- c. Iris is highly stable over lifetime.

Disadvantages of iris scan:

- a. Difficult to capture for some individuals.
- b. To acquire the iris pattern, requires a great deal of user cooperation or to use expensive and complex input devices.
- c. The presentation of iris authentication may be weakened by glasses, sunglasses and contact lenses.
- d. It is not useful for forensic applications as evidence of iris biometric on crime scene is not left.

B. Fingerprint Recognition

The pattern of ridges and grooves on surface of a fingertip is fingerprint. Fingerprints are highly unique and stable for an individual. The uniqueness of fingerprint is determined by three features:

1. Coarse features: Coarse features have strong genotypic influences and are suitable for presorting during identification with a very large data base. Coarse features consist of loops, arch and whorls.
2. Fine features: Fine features, also called as minutiae are the endings and the bifurcating of the finger lines because these follow a strong random pattern. They are the carriers of "uniqueness".
3. Pore structure: Pore structure is rarely used, as it shows large fluctuations in the quality of the scanning procedure. Figure 4 shows the pattern of fingerprint.



Figure 4 Pattern of finger print

Merits of finger print recognition:

- a. Subjects have multiple fingers so we get many features for accurate authentication and identification.
- b. Easy to use.
- c. Low technology devices can be used to collect samples.

Demerits of finger print recognition:

- a. Fingerprints can be easily impersonated by using various conspiracies.
- b. With the age, the fingerprints undergo certain changes which can pose uncertainty in identification.

C. Face Recognition

A facial recognition technique uses an individual's face for identification purpose. This is done by automatically identifying a person from a digital image or a video frame from a video source. The algorithms can be geometric feature-based and appearance-based. 3-Dimensional face recognition systems are most widely used as they provide accurate results because they capture the actual shape of faces. 3D models of faces are made by the system and the 3D faces are compared for recognition. The features used to identify an individual are position of eyes, nose and mouth, cheekbones, distance between eyes, eyebrow thickness and position, face outline, jaw shape. These features are then compared with the database images for identification.

Advantages of Face Recognition:

- a. The biometric works with legacy photograph databases, video tape and other image sources.
- b. It is a good biometric identifier for small-scale verification application.
- c. Face recognition systems are the least intrusive because they neither require contact nor the awareness of the subject.

Disadvantages of Face Recognition:

- a. Face can be blocked by hair, glasses, hats, etc. sensitive to changes in illumination, gesture and expression.
- b. Faces change with time.
- c. A face needs to be well-lit by controlled light sources in automated face authentication systems.

D. Voice Recognition

Speaker recognition is a generic term which refers to any task that discriminates between people based upon their voice characteristics. There are two specific tasks that have been studied extensively. These are speaker identification and speaker verification. The difference between identification and verification is simple. The speaker identification task is to classify an unlabeled voice gesture as belonging to one of a set of N reference speakers, whereas the speaker verification task is to decide whether or not an unlabeled voice gesture belongs to a specific reference speaker [2]. Speaker verification focuses on the vocal characteristics like the dimensions of the vocal tract, nasal cavities, mouth and the other speech processing mechanism of the human body that produce speech. Speaker verification does not focus on the sound or the pronunciation of speech itself [3]. In voice recognition “sound spectrogram” devices are used. Sound spectrogram makes a graph visible and shows sound amplitude on the vertical axis and shows the time on the horizontal axis as shown in Figure. 5.

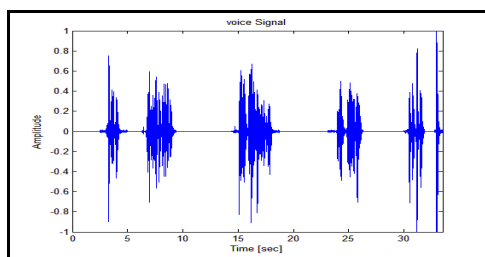


Figure 5. Voice signal

Advantages of Speaker recognition:

- a. Voice is a natural biometric (one that people use instinctively to identify each other).
- b. The voice biometric requires only inexpensive hardware and is easily deployable over existing, ubiquitous communications infrastructure (the telephone system). Voice is therefore very suitable for persistent security management.

Disadvantages of Speaker recognition:

- a. Voice recognition requires a high quality audio signal with no noise and unwanted signal interference.
- b. Not sufficiently distinctive for identification over large databases.

E. Retina Recognition

A colored region between the pupil and sclera is known as iris whereas retina is located at back region of eye. The foundation of retinal recognition is the blood vessel pattern. Retinal recognition is the most reliable and stable due to its rich and unique vascular pattern. It is almost impossible to forge a human retina as it is located at back of eye and is not exposed to external environment.

Retina is scanned using a camera which is normally used by ophthalmologists for treatment of retinal diseases. In order to scan retina, the person must position his eye very close to the lens of camera. During scanning process, he must remain still and also must remove glasses to avoid signal interference. Once the scanner is activated, then green light moves to complete circle and vascular pattern of retinal is captured. Due to a complicated acquisition process, retinal recognition systems are not used widely but due to their stability and reliability, retina biometrics systems are suited for maximum security areas such as Government and military [4]. A skilled operator is required and the person being scanned has to follow his or her direction. However, retina scanning systems are said to be accurate, and find its application in high security concerns. Figure 6 shows retina of the left eye.

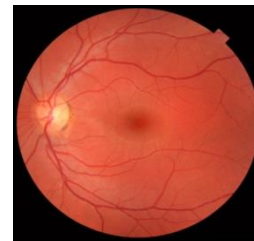


Figure 6. Retina of the left eye.

Advantages of Retina Recognition:

- a. Very high accuracy.
- b. There is no known way to replicate a retina.

Disadvantages of Retina Recognition:

- a. Very intrusive.
- b. Very expensive.
- c. It has the dishonor of consumer's thinking it is potentially harmful to the eye.

F. Signature Recognition

It is the process used to recognize an individual's signature. It can be operated in two different ways: static and dynamic or offline and online. Static: In this mode, users write their signature on paper, which is digitized through an optical scanner or a camera, and then the biometric system is used to recognize the signature by analyzing its shape. This group is also known as “off-line mode”. Whereas the in dynamic, users write their

signature in a digitizing tablet. This mode is used as a real time system hence known as “on-line mode”.

The application of identification of the writer using his signature is in wide areas, such as, to solve the expert problems in criminology by forensic expert decision-making systems, where a narrowed-down list of identified writers is provided by the writer identification system [5]. Figure 7 shows the signature recognition system.



Figure 7. Signature recognition

Advantages of Signature Recognition:

- a. Possible detection of inconsistent user during enrollment stage.
- b. Fast and simple training.
- c. Cheap hardware.
- d. Little storage requirements.

Disadvantages of Signature Recognition:

- a. Consistent manner of signature is required for enrolling and verification of the individual.

G. Hand Geometry

Hand geometry recognition systems use a number of measurements taken from the human hand, including its shape, size of palm, lengths and widths of the fingers, finger baselines [6]. Nearly, shape of every person’s hand different and that the shape of a person’s hand does not change after certain age. Image acquisition for hand biometrics may be contact type and guided one, which needs a flat platform to put the hand and pegs to guide the placement of the user’s hand, or platform-free, non-contact techniques. Its recognition devices are bulky but identification is done in a seconds. Figure 8 shows hand geometry recognition system.



Figure 8. Hand geometry recognition system

Advantages of Hand geometry:

- a. Acquisition convenience and good verification performance of system.
- b. Suitable for medium and low security application.
- c. Works in harsh environments.

Disadvantages of hand geometry:

- a. Large size of hand geometry device is needed.
- b. Single hand use only in one time.
- c. Not highly unique.

H. DNA Recognition

The biological activity of every living organism is controlled by billions of individual cells. The control center of each cell is the De-oxyribo Nucleic acid (DNA) that contains a complete set of instructions needed to direct the functioning of each and every one of the cells [7]. Each person’s DNA is unique except for identical twins. It can thus be considered a perfect modality for identity verification. This method of capture still has to be refined. So far the DNA analysis has not been sufficiently automatic to rank the DNA analysis as a biometric technology, where analysis of human DNA can be completed within 10 minutes. As soon as the technology advances so that DNA can be matched automatically in real time it may prove more significant. But at present DNA System is very deep-rooted in crime detection and so will remain in the law enforcement area [8, 9].

Advantages of DNA recognition:

- a. Very accurate method.

Disadvantages of DNA:

- a. It is expensive method.

I. Gait Recognition

The contribution of gait as a biometric for people identification in surveillance application has attracted researchers from computer vision as Gait can be perceived from a distance. Although gait recognition is still a new biometric, it overcomes most of limitation that other biometric suffer from such as face, speaker, fingerprint recognition. Gait can be defined as the coordinated and cyclic combination of movements that result in human locomotion. Gait is a complex locomotion pattern which involves synchronized movement of body parts, joints [10]. The gait feature used to identify person are stride length, cadence, height, distance between head and pelvis, maximum distance between pelvis and feet, the distance between feet [11]. Figure 9 shows the silhouette of gait cycle.

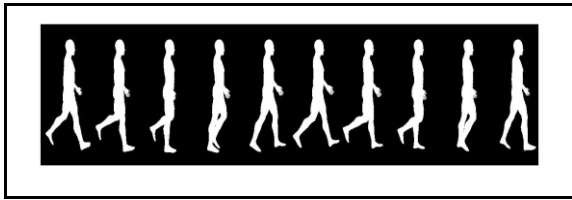


Figure 9. Complete gait cycle

The choice of a particular human characteristic, to be used as a biometric feature depends on the following criteria:

- a. Uniqueness is how well the biometric separates individually from another.
- b. Permanence measures how well a biometric resists aging.
- c. Collectability eases of acquisition for measurement.
- d. Performance accuracy, speed, and robustness of technology used.
- e. Acceptability degree of approval of a technology.
- f. Universality the quality of being universal; existing everywhere.

REFERENCES

- [1] U. Jaruwareet and N. Covavisaruch, "An Improvement of Iris-Blob map Approach for Iris Identification," Proceedings of ECTI-CON, 846 – 850, E-ISBN 978-1-4244-5607-9, Print ISBN 978-1-4244-5606-2, INSPEC Accession Number 114102752010, 2010.
- [2] George R. Doddington, "Speaker Recognition-Identifying People by their Voices", Proceedings of The IEEE, Vol 73, No. 11, November 1935.
- [3] Prof. G. Ramaswamy, Vudasreenivasarao, Dr. P. Ramesh, D. Ravikiran, "A Novel Approach for Human Identification through Fingerprints", International Journal of Computer Applications (0975 – 8887) Volume 4 – No.3, July 2010.
- [4] M. Usman Akram, Anam Tariqy and Shoab A. Khanz, "Retinal Recognition: Personal Identification using Blood Vessels", 6th International Conference on Internet Technology and Secured Transactions, 11-14 December 2011, Abu Dhabi, United Arab Emirates.
- [5] W. Zhao, R. Chellappa, P. J. Phillips, A. Rosenfeld, "Face Recognition: A Literature Survey", ACM Computing Surveys, Vol. 35, No. 4, December 2003, Pp. 399-458.
- [6] Nonglukcovavisaruch, Pipatprateepamornkul, Puripantruchikachorn, and Piyanaattaksaphan, "Personal Verification and Identification Using Hand Geometry", ECTI Transactions on Computer and Information Technology Vol.1, No.2 November 2005.
- [7] S. Panneer Arokiaraj, L. Robert, "Pattern Recognition based DNA Sequence Compressor", 978-1-4673-1344-

5/12 2012 IEEE International Conference on Computational Intelligence and Computing Research.

- [8] Anil K. Jain, Fellow, IEEE, Arun Ross, Member, IEEE, and Sharathpankanti, Senior Member, IEEE, "Biometrics: A Tool for Information Security", IEEE Transactions on Information Forensics and Security, Vol. 1, No. 2, June 2006.
- [9] Joseph P. Campbell, Jr., Senior Member, "Speaker Recognition: A Tutorial", Proceedings of the IEEE, Vol. 85, No. 9, September 1997.
- [10] Sreeraj.M, Sumam Mary Idicula, "A Survey on Writer Identification Schemes", International Journal of Computer Applications (0975 – 8887) Volume 26– No.2, July 2011.