INTERNATIONAL JOURNAL OF RESEARCH – GRANTHAALAYAH
A knowledge Repository

RACSIT - 17

# BIOMETRICS-A PRELIMINARY APPROACH

**Rohini B.R. [*1], Dr.Thippeswamy G. [2]**

[*1] Department of Information Science and Engineering, Don Bosco Institute of Technology, India

[2] Department of Computer Science and Engineering, BMS Institute of Technology, India

**DOI:** https://doi.org/10.29121/granthaalayah.v5.i4RACSIT.2017.3350

## Abstract

Authentication plays a vital role in Information security. The need for identification of legitimate user has increased in the waking concerns for global security. Biometric recognition Systems is a major tool for Authentication mechanism. Biometrics is the ability to identify and authenticate an individual using one or more of their behavioral or physical characteristics. The Study of Different Biometric Modalities gives a better understanding of Biometric Techniques. We focus our Study on Face Biometrics. This paper emphasizes on better understanding of introduction to Biometrics, Biometric Modalities and Face recognition Techniques.

***Keywords:*** Biometrics; Modalities; Face recognition.

***Cite This Article:*** Rohini B.R., and Dr.Thippeswamy G.. (2017). "BIOMETRICS-A PRELIMINARY APPROACH." *International Journal of Research - Granthaalayah*, 5(4) RACSIT, 47-52. https://doi.org/10.29121/granthaalayah.v5.i4RACSIT.2017.3350.

## 1. Introduction

In the advent of Information Security person authentication has evolved to play a critical role in personal, national, and global security. Identity management using biometrics has nowadays become a reality where User Authentication mechanism is a major challenge. The issues in information security entail the protection of identity elements of the users thereby ensuring that only authorized users are able to access the legitimate data. There is a need to robust human recognition techniques in critical applications such as secure access control, international border crossing and law enforcement where Identity management plays an important role.

A Biometric Recognition System is one such Identity management tool. Biometrics is the science of recognizing the identity of a person based on the physical or behavioural attributes of the individual such as face, fingerprints, voice and iris [1]. The protection of personal data is the basic requirement of security. Traditional Authentication mechanisms used are Knowledge-based methods (What you know) and Token-based methods (What you have).

Knowledge based methods is based on a user's knowledge characterized by its secrecy. Examples include passwords, PINs, etc. In Token based methods the user possesses a physical and portable device which contains the user’s identity. Examples of such devices include smart cards, token codes, bankcards, driver's licenses, passports, etc. These methods do not verify who is requesting the access. Since the information can easily be lost, shared or manipulated. Biometrics overcomes the disadvantage of the traditional authentication mechanism. i.e, Biometrics (What you are) verifies who is the person requesting the access. The user submits to the system his physical and/or behavioral characteristics. As a result, the individual is either accepted as a valid user or is rejected.  Biometrics is also an authentication mechanism, which is more reliable and natural.

Biometric Recognition System includes both Verification and Identification (also Authentication) [10].

**Identification (1: n) –** One-to-Many: Biometrics can be used to identify a person based on biometric trait. This biometric trait has to be compared with all the registered persons. It is used to o determine a person's identity even without his awareness or approval. Such as scanning a crowd with the help of a camera and using face recognition technology, one can verify matches that are already store in database.

**Verification (1:1)** One-to-One: Biometrics can also be used to verify a person's identity either accepting or rejecting the identity claim. Such as one can allow physical access to a secure area in a building by using finger scans or can grant access to a bank account at an ATM by using retina scan.

Basically, there are two types of approaches in Identification and Verification process: Intrusive and Non-intrusive In the intrusive approach, system asks the user to perform some actions such as smiling, chewing, rotating head in a particular direction etc. On the other hand, there is no involvement of user in the non-intrusive approach. No user response is required.

## 1.1.History of Biometrics

For thousands of years, humans have used body characteristics such as face, voice, gait, and so on to recognize each other. In the mid-19th century, Alphonse Bertillon, chief of the criminal identification division of the police department in Paris, developed and then practiced the idea of using various body measurements (for example, height, length of arms, feet, and fingers) to identify criminals. In the late 19th century, just as his idea was gaining popularity, it was eclipsed by a far more significant and practical discovery: the distinctiveness of human fingerprints. Soon after this discovery, many major law-enforcement departments embraced the idea of “booking” criminals’ fingerprints and storing them in databases (initially, card files). Later, police gained the ability to “lift” leftover, typically fragmentary, fingerprints from crime scenes (commonly called *latents*) and match them with fingerprints in the database to determine criminals’ identities. Biometrics first came into extensive use for law-enforcement and legal purposes—identification of criminals and illegal aliens, security clearances for employees in sensitive jobs, paternity determinations, forensics, positive identifications of convicts and prisoners, and so on. Today, however, many civilian and private-sector applications are increasingly using biometrics to establish personal recognition [2].

## 2. Biometric Modalities

A biometric recognition system relies on who we are or what we do. Physical characteristics are genetically implied and possibly influenced by the environment. Physical biometric characteristics include face, fingerprint, hand, iris, DNA. Behavioural or psychological characteristics are characteristics that are gathered or learned over a period of time. Behavioural biometrics includes signature, keystroke dynamics, voice recognition, gait recognition, etc. A biometric system is a pattern-recognition system. The biometric system aims to recognize a person based on a feature vector deduced from physiological or behavioural characteristic that the person possesses.

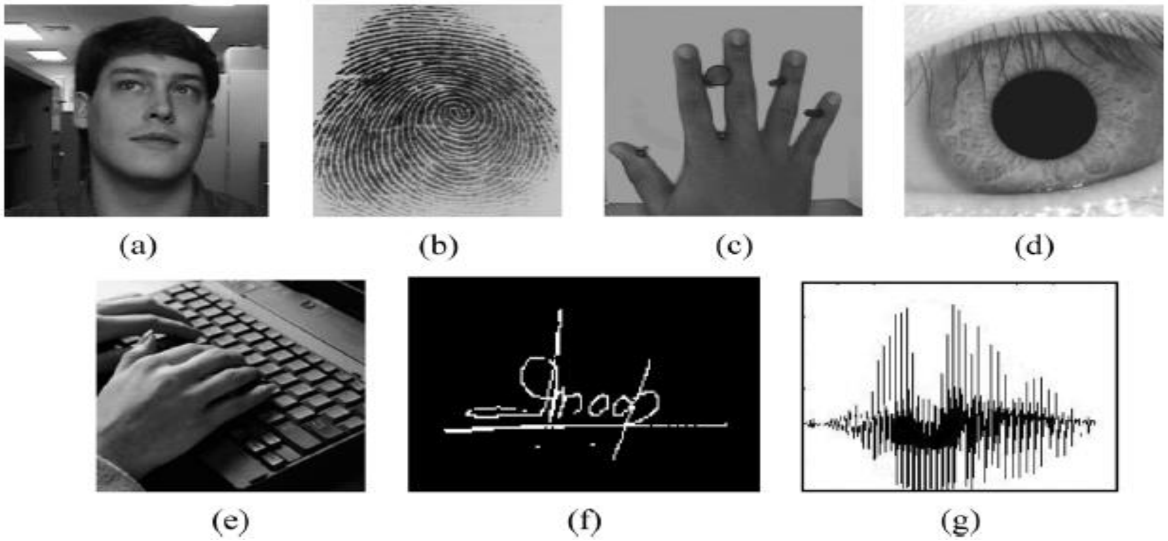

Figure 1: Biometric characteristics (a) face (b) fingerprint (c) hand geometry (d) iris (e) keystroke (f) signature (g) voice

### 2.1.Fingerprint Biometrics

Most widely used biometric is Fingerprint. Its popularity is due to the unique characteristic of Fingerprint made up of ridges, furrows and minutiae [3]. Fingerprint authentication refers to the automated method of verifying a match between two human fingerprints. An array of fingerprint sensors are in use today that are capable of capturing the fingerprint biometric and authenticating a person based on analysis of the ridges and furrows which make the fingerprint distinct. These devices are used for enrolment and template matching. Fingerprint has a long tradition of its use as an immutable identification in law enforcement and its samples can be collected with ease.

### 2.2.Iris Recognition

The low cost of eye-scanning technology makes iris recognition play an important role in security applications. The iris is the colored part of the eye that lies behind the cornea, in front of the lens, and is protected by the eyelid. The iris contains complex patterns of ligaments, furrows, ridges, crypts, rings and corona that allow algorithms to be produce a pattern can be used to identify an individual. The patterns are then encoded using 2D Gabor wavelet demodulation to create a phase code that is Iris code. In order to enrol a person for future identification, the IrisCode is stored in a database or on a smart token [4]. Due to efficient mechanism for Identification and verification Iris recognition is considered as a major biometric trait for recognition.

### 2.3.Hand Geometry

Hand geometry recognition systems are based on a number of measurements taken from the human hand, including its shape, size of palm, and lengths and widths of the fingers [8]. Hand features are extracted from a color photograph taken when the user has placed his hand on a platform designed for such a task. Pattern recognition techniques have been tested to be used in classification and/or verification [9]. Environmental factors, such as dry weather or individual anomalies such as dry skin, do not have negative effects on the authentication accuracy of hand geometry- based systems. Hand geometry information is not invariant during the growth period of children. An individual’s jewelry (e.g., rings) or limitations in dexterity (e.g., from arthritis), pose further challenges in extracting the correct hand geometry information. The physical size of a hand geometry-based system is large which requires larger devices for implementation than those used for other biometrics (e.g., fingerprint, face, and voice).

### 2.4.Voice Recognition

Voice is a mixture of physical and behavioural characteristics. The individual features of voice are based on the shape and size of the appendages (e.g., vocal tracts, mouth, nasal cavities, and lips) that are used in the synthesis of the sound [5]. The physical characteristics of human speech are invariant for an individual, but the behavioral part of the speech of a person changes over time due to age, medical conditions (such as common cold), emotional state, etc. Voice discrimination may not be appropriate for large-scale identification. These Speaker recognition systems are both text independent and text dependent. Speaker recognition is most widely used in phone-based applications.

### 2.5.Keystroke Dynamics

The keystroke dynamics is a behavioral biometric. It aims to obtain biometric data as a user types on the computer keyboard. In the authentication process of keystroke dynamics the following features of users keystroke are considered: typing speed, keystroke seek time, flight time, characteristic errors, and characteristic sequences [6]. The time between keystrokes is known as a diagraph and is a vital part of the keystroke biometric data. In matching the keystroke data obtained with templates in a database, correlation is used. Though keystroke dynamics is not unique in nature it offers sufficient invariance that performs identity verification. Keystrokes characteristics of a person can be unobtrusively monitored .This biometric trait involves in “continuous verification” of an individual over a period of time.

### 2.6.Signature

Signatures are a behavioral biometric where the way each person signs his or her name is characteristic. Even though signature require contact with the writing instrument and requires user involvement, they have been accepted as method of authentication in government, legal, and commercial transactions [7]. The Signatories physical and emotional conditions are variant in nature. Signature verification systems have different Offline and Online Verification systems. Professional forgers may be able to reproduce signatures that fool the system.

## 3. Face Recognition

Face recognition applications gain their importance in study and development due to its non-intrusive nature and Biometric data of the faces (photos, videos) can be easily taken with available devices like cameras. Therefore, face recognition has been widely used in Identification and Recognition.

### 3.1.Face Authentication

The following figure describes an Authentication mechanism for face recognition. In this model, each user has an account and a corresponding ID in the Face Database. On a user logging in the system, Face Authentication will use face recognition technologies to analyze and determine his ID as well as his permissions on the system.

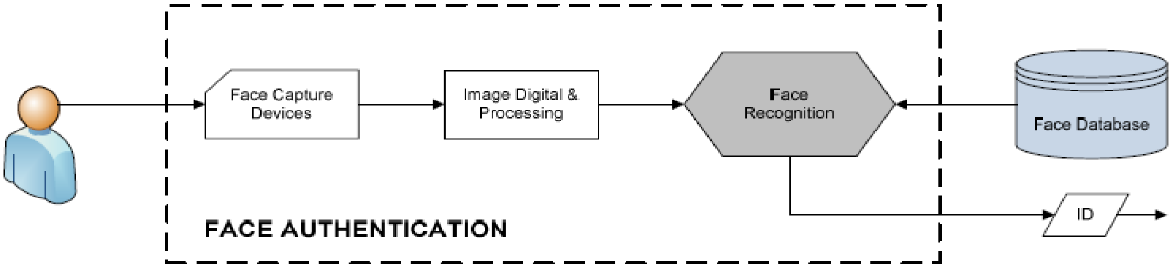

Figure 2: Face Authentication Mechanism

This model can be applied to Authentication systems in members of an office or a family and user accounts in an operating system. For Face Authentication to satisfy all the security issues of an Authentication system face recognition algorithms plays a vital role.

### 3.2.Face Recognition Model

Face recognition systems are based on "*learning*" mechanism to collect data on facial characteristics of users. Hence, the most important technique in a face recognition model is the *Face Database* storing this information. When the system finishes scanning a video or photo of a user's face, the digitalized information will go through the following phases:

- ***Face Detection*:** locating the face in the photo or video and removing unnecessary details on the background.
- ***Feature Extraction*:** Extracting facial characteristics needed for recognition.
- ***Feature Match*:** Comparing scanned information with database to decide if it matches some user's face. If the face matched, the ID of the corresponding is returned.

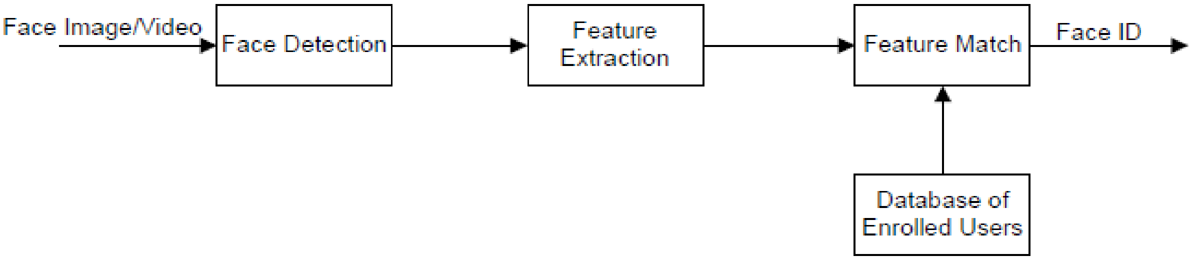

Figure 3: Face Recognition Process

## 4. Conclusions

Biometrics is a rapidly evolving technology that is being widely used in law enforcement and surveillance systems. To prevent unauthorized access and to develop a strong Authentication mechanism is hence an important issue. Example in bank or ATMs, in cellular phones, smart cards, PCs, in workplaces, and computer networks. Hence the basic understanding of biometric modalities is most important. Face Recognition being the widely acknowledged Biometric trait due to its non-intrusive nature. The challenging factor in Face Recognition model is how to get best biometric information on the faces. Therefore, Feature Extraction is the most important module of the system hence, a Research Issue.

## References

[1] Anil K. Jain, Patrick Flynn, Arun A Ross, “Handbook of Biometrics”,2008.
[2] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: security and privacy concerns," Security & Privacy, IEEE, vol. 1, pp.33-42, 2003.
[3] R. Saini and N. Rana, "Comparison of Various Biometric Methods" International Journal of Advances in Science and Technology (IJAST), vol. 2, 2014.
[4] Mary Dunker, “Dont Blink: Iris Recognition for Biometric Identification”, SANS Security Essentials, July 2003.
[5] J. P. Campbell, “Speaker recognition: a tutorial,” Proc. IEEE, vol. 85,no. 9, pp. 1437-1462, Sep. 1997.
[6] Y. W. Sabbah, I. A. Saroit, and A. M. Kotb, "A Smart Approach for Bimodal Biometric Authentication in Home-Exams (SABBAH Model)" Biometrics and Bioinformatics, vol. 4, pp. 32-45, 2012.
[7] Khamael Abbas, A Dulaimi “Handwritten Signature Verification Technique Based on Extract Features”, International Journal of Computer Applications (0975 –8887), Volume 30–No.2, September 2011.
[8] R. Sanchez-Reillo, C. Sanchez-Avila, and A. Gonzales-Marcos, “Biometric identification through hand geometry measurements” IEEE Trans. Pattern Anal. Mach. Intell., vol. 22, no. 10, pp. 1168–1171, Oct. 2000.
[9] Raul Sanchez-Reillo, Carmen Sanchez-Avila, and Ana Gonzalez-Marcos, “Biometric Identification through Hand Geometry Measurements”, IEEE Transactions On Pattern Analysis And Machine Intelligence, Vol. 22, No. 10, October 2000.
[10] Renu Bhatia, “Biometrics and Face Recognition Techniques”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5,May 2013.

*Corresponding author.
*E-mail address:* rohini.br@gmail.com