IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 5, June 2022
Impact Factor: 6.252

Biometric System

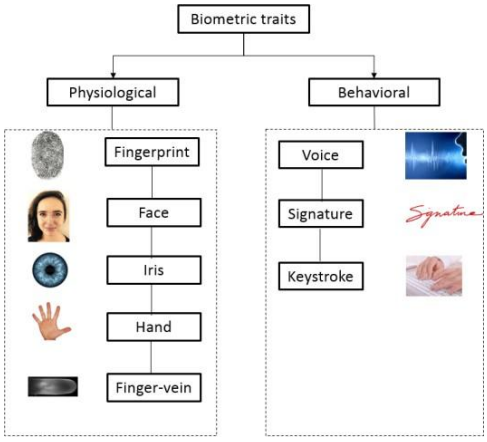
Kirti Sindhwani
Department of Computer Science & Information Technology
Dronacharya College of Engineering, Gurugram, India

Abstract: *Nowadays, for lot of people biometric system is kind a remote, extremely scientific or completely unheard of. But the truth is that we are seeing it more and more in our daily lives and they say it will soon end up replacing our passwords or door keys. Biometric becomes the most popular technique of its efficiency and liability. Because of need of high security we are using the biometric broadly. It is used in controlling workplace access and identifying criminals by forensics.*

Keywords: Biometric System

I. INTRODUCTION

The need for reliable user authentication techniques has increased in the wake of heightened concerns about security and rapid advancements in networking, communications and mobility. Biometrics, described as the science of recognizing an individual based on his or her legitimate method for determining an individual's identity. Biometric authentication or simply biometrics refers to establishing identity based on the physiological and behavioural characteristics shown in Figure 1.1 (also known as traits or identifiers) of an individual such as face, fingerprints, hand geometry, iris, keystroke, signature, voice, etc. Biometrics systems offer several advantages over traditional authentications schemes. They are inherently more reliable than password – based authentication as biometric traits cannot be lost or forgotten; biometric traits are difficult to copy, share and distribute; and they require the person being authenticated to be present at the time and point of authentication. Thus, biometrics – based authentication scheme is a powerful alternative to traditional authentication schemes. A number of biometric characteristics have been in use for different applications [1, 2]



II. BIOMETRIC SYSTEM

A biometric system is a technology which takes an individual's physiological, behavioural, or both traits as input, analyses it, and identifies the individual as a genuine or malicious user. The biometrics is largely statistical. The more data available from sample the more the system is likely to be unique and reliable. It can work on various modalities pertaining to measurement of individual's body and features and behavioural patterns. The modalities are classified based on the persons biological traits. There are various traits present in humans, which can be used as biometric modalities. The biometric modalities fall under three types:

1. Physiological
2. Behavioral
3. Combination of Physiological and behavioural modality

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 5, June 2022
Impact Factor: 6.252

2.1 Physiological Modality

The physiological modalities are measured from the sensors that are attached to the body like iris fingerprint, shape, and position of fingers, etc. These help in recognizing the emotions of the human being. Some of the physical traits in the human body remain unchanged throughout a person's life. They can be treated as useful resource which helps in identifying an individual. Below are the some examples of Physiological Modality.

2.2 Fingerprint Recognition System

Fingerprint recognition systems work by examining a finger pressed against a smooth surface. The finger's ridges and valleys are scanned, and a series of distinct points, where ridges and valleys end or meet, are called minutiae. These minutiae are the points the fingerprint recognition system uses for comparison. In order to identify an individual, the valleys (minutiae) and ridges are used which are found on the surface tips of a human finger.

Due to the rapid advancement in sensor technology, a new biometric authentication system has been developed for handheld electronic devices which is robust. It has been implemented by fusing the movements of finger in 3D with cerebral activities in an intelligent manner to verify the signatures using the next-generation sensor consumer electronic (CE) devices and the classifiers such as Random Forest (RF) and Hidden Markov Model (HMM) [17]. A novel authentication system using biometric based on FPGA has been proposed by utilizing TRSG (True Random and Timestamp Generator) for implementing fast and secure fingerprint authentication with more accuracy [1]. Fingerprint is oldest type and most familiar recognition technique. Fingerprint matching techniques are of three types

A. Minutiae Based Techniques

These techniques help in finding out the minutiae points that are mapped in search of respective position on the finger. These techniques are helpful, but it is difficult to find out the minutiae points correctly if the image obtained is of poor quality. It mainly concentrates on local position of ridges and furrows; not global.

B. Correlation Based Method

It gives richer grey scale information. It helps to rectify the problems that faced in minutiae-based method which gives at times poor quality data. But, this method too has some of its own problems like localization of points.

C. Pattern Based Image Based Matching (Image − Pattern based matching algorithms helps in comparing the basic fingerprint patterns such as (arch, whorl, and loop) between a stored template and a live person's fingerprint.

III. HAND GEOMETRY RECOGNITION BIOMETRICS

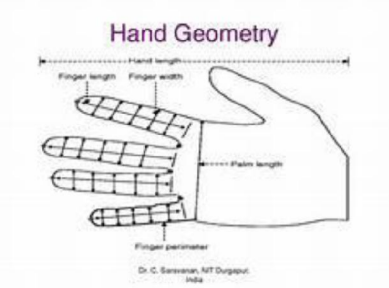
Now applications of hand geometry recognition biometric are not as apparent as other biometric modalities like fingerprint or face recognition. Despite that it is still relevant in many physical access and time/attendance applications. Hand geometry recognition biometrics leverages the idea that hand geometry of each individual is unique. There is no documentary evidence of hand geometry of a person being unique, but given the possibility of variation of anatomical structure of a group of people, hand geometry can be considered a human physiological characteristic that can be used to uniquely identify an individual.

The concept of hand geometry recognition was introduced by David Sidlauskas in 1985 following a commercial launch of world's first hand geometry recognition system next year. One of the notable deployments of hand recognition systems

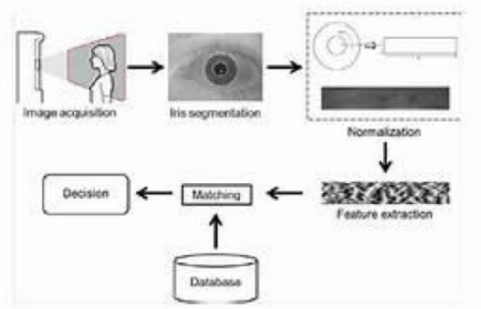
IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 5, June 2022
Impact Factor: 6.252

took place in the 1996 Olympic Games, in which physical access to the Olympic Village was controlled and protected using hand geometry recognition systems. Though fingerprint time clocks are now taking over employee time tracking and attendance applications, many organizations still rely on hand geometry recognition systems along with time clocks for employee attendance applications. It helps in measuring length and width of palm, surface area, length and position of fingers, and overall bone structure of the hand. A person's hand remains unique and helps in identifying a person from others. There are two types of Hand Geometry systems-

1. **Contact Based-**A hand is kept on scanner's surface. The hand is positioned in between five pins which help to place the candidate hand in position correctly for the camera.
2. **Contact Less-**In this approach neither pins nor platform are required for hand image acquisition.



Iris Recognition-It is a biometric identification method that works with mathematical pattern-recognition techniques on video images. The complex metrics of this identification system are unique, fast and stable compare to other modalities. The iris is a pigmented elastic tissue that has circular opening which is adjusted in the center. It helps to control the diameter of pupil. In adult humans, the iris texture remains stable throughout their lives. The iris patterns of left and right eyes are different. Each person has different iris pattern and colour.



3.1 Facial Recognition System

Facial recognition system is based on mainly finding out shape and size of jaw, chin, shape and location of the eyes, eyebrows, nose, lips, and cheekbones. There are facial scanners such as 2D a facial scanner which helps to read face geometry and records it on the grid. This facial geometry is then transferred to the database in terms of points. The face matching is performed by comparison algorithms and finally comes up with the results. Facial recognition is performed in the following ways −

- Facial Metrics − In this type, the distance between pupils or from nose to lip or chin are measured.
- Eigen faces − It is the process of identifying the full image of a face as a weighted combination of a number of faces.
- Skin Texture Analysis − The unique lines, patterns, and spots apparent in a person's skin are located.

3.2 Examples of Facial Recognition Technology

1. **Amazon** previously promoted its cloud-based face recognition service named **Rekognition** to law enforcement agencies. However, in a June 2020 blog post, the company announced it was planning a one-year
2. moratorium on the use of its technology by police. The rationale for this was to allow time for US federal laws

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 5, June 2022
Impact Factor: 6.252

to be initiated, to protect human rights and civil liberties.

3. **Apple** uses facial recognition to help users quickly unlock their phones, log in to apps, and make purchases.
4. **British Airways** enables facial recognition for passengers boarding flights from the US. Travellers' faces can be scanned by a camera to have their identity verified to board their plane without showing their passport or boarding pass. The airline has been using the technology on UK domestic flights from Heathrow and is working towards biometric boarding on international flights from the airport.
5. **Cigna**, a US-based healthcare insurer, allows customers in China to file health insurance claims which are signed using a photo, rather than a written signature, in a bid to cut down on instances of fraud.
6. **Coca-Cola** has used facial recognition in several ways across the world. Examples include rewarding customers for recycling at some of its vending machines in China, delivering personalized ads on its vending machines in Australia, and for event marketing in Israel.

3.3 Behavioural Modality

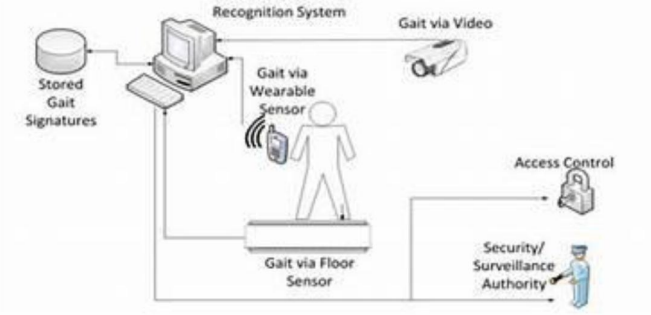
A person's character depends upon his behaviour. No two persons have the same behaviour. We can analyse the person's character whether he/she is good or bad through their behaviour. So, behavioural modalities in biometrics related to the behaviour indicated by the people or the way in which people perform specific tasks such as walking, signing, and typing on the keyboard.

Behavioural biometrics modalities targets higher variations due to the dependence on the external factors such as fatigue, mood swings, etc. This causes higher FAR and FRR as compared to solutions based on a physiological biometrics.

Below given are the some example of behavioural modality

Gait Recognition

Gait recognition is a behavioural biometric modality that identifies people based on their unique walking pattern. In comparison with other first-generation biometric modalities that include fingerprint and iris recognition, gait has the advantage of being unobtrusive, in that it requires no subject contact. Gait recognition is based on the notion that each person has a distinctive and idiosyncratic way of walking, which can easily be discerned from a biomechanics viewpoint. Human movement does consist of synchronized movements of hundreds of muscles and joints, though basic movement patterns are similar, gait does vary from one person to another in terms of timing and magnitude.



Keystroke Recognition

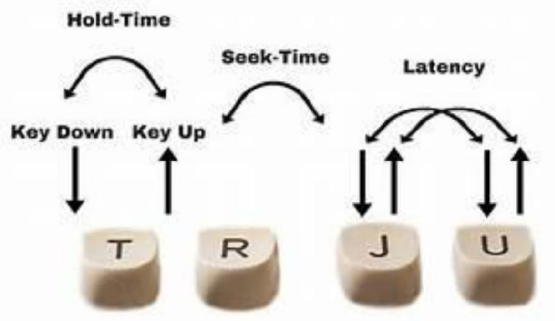
Keystroke recognition is a behavioural biometric which utilizes the unique manner in which a person types to verify the identity of an individual. Typing patterns are predominantly extracted from computer keyboards, but the information can potentially be gathered from any input device having traditional keys with tactile response (i.e., cellular phones, PDA's, etc). Although other measurements are conceivable, patterns used in keystroke dynamics are derived mainly from the two events that make up a keystroke: the Key-Down and Key-Up. The Key-Down event takes place at the initial depression of a key and the Key-Up occurs at the subsequent release of that key. Various unique features are then calculated based on the intra-key and inter-key timing variations between these events.

This biometric identifies candidate's typing pattern, the rhythm, and the speed of typing on a keyboard. The dwell time and flight time measurements are used in keystroke recognition.

- Dwell time − It is the duration of time when a key is pressed.
- Flight time − It is the elapsed time between releasing a key and pressing the following key.

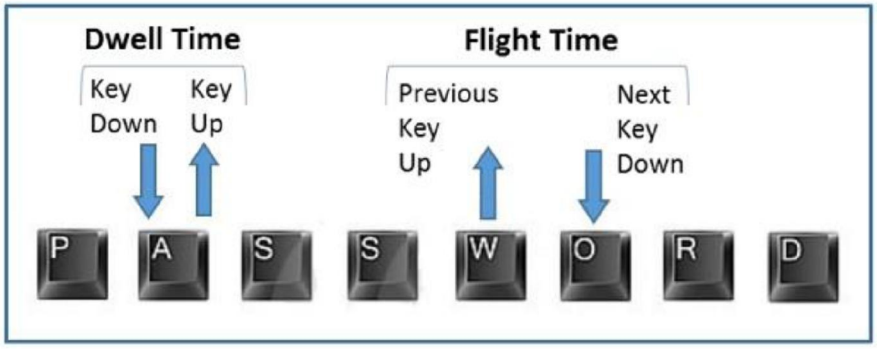
IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 5, June 2022
Impact Factor: 6.252

There will be variation in candidates typing behaviour on the keyboard as the time they take to find the right key, the flight time, and the dwelling time. Their speed and rhythm of typing also changes according to their comfort level with the keyboard. Keystroke recognition system monitors the keyboard inputs thousands times per second in a single attempt to identify the candidates typing skills based on their habits.



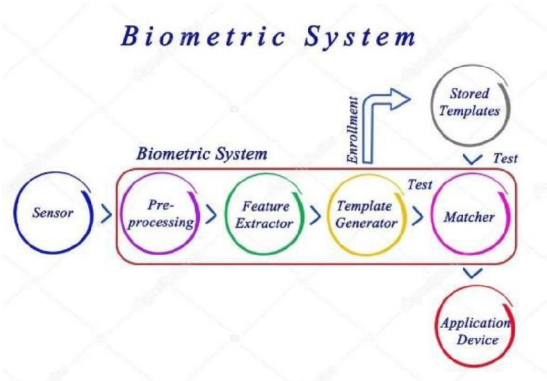
There are two types of keystroke recognition −

- **Static**− It is one time recognition at the start of interaction.
- **Continuous** − It is throughout the course of interaction.



3.4 How Biometrics Works

Biometrics seems to use who you are to authenticate you rather than something you have (like a key) or whatever you know (like a password). Biometrics can involve physical attributes like your face, fingerprints, irises, or veins, as well as behavioural features such as your voice, calligraphy, or typing rhythm. Personal qualities, unlike keys and passwords, are exceedingly difficult to lose or remember.



They can also be tough to imitate. As a result, many individuals believe they are safer and better than locks or passwords. There is no disputing that biometrics appears sophisticated, however all biometrics increased portion the same three steps:

- **Enrolment:** When you're using a biometric system from scratch, it captures basic information concerning you, such as your name or an identification number. It then records or takes a picture of your unique attribute.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 5, June 2022
Impact Factor: 6.252

- **Storage:** Unlike what you would see in movies, most systems do not save the entire image or video. Instead, they study your characteristic and convert them into to a code language graph. Some systems additionally save this information on a smart card that you take around with you.
- **Comparison:** The program compares the characteristics you offer to the information on record the next moment you utilise it. Then it either accepts or rejects you claiming to be who you say you are.

3.5 Components of Simple Biometric System

1. Sensor module which acquires the biometric data; Web cam, Digitizing Table, Scanner.
2. Feature extraction module where the acquired data is processed to extract feature vectors; Projection [offline], DCT on Coordinates [online, offline]
3. Matching module where feature vectors are compared against those in the template ;(Neural Networks, Algorithm)
4. Decision-making module in which the user's identity is established or a claimed identity is accepted or rejected. (Final results) [18]

Biometrics As noted earlier refers to technologies that measure and analyse human body characteristics, such as DNA, fingerprints and eye retina and irises and hand measurements, for authentication purposes.

REFERENCES

[1]. Anil K. Jain, Arun Ross, and Sharath Pankanti, "Biometrics: A Tool for Information Security", IEEE Transactions on Information Forensics and Security, vol. 1, no. 2, pp 21-38, June 2005.
[2]. Anil. K.Jain, Arun Ross, Salil Prabhakar, "An introduction to biometric recognition", IEEE Transactions on circuits and systems for video technology, vol. 14, no. 1,pp 67-80, Jan 2004.
[3]. http://www.weexcel.in/NewsDesc1.aspx?cod=86.
[4]. http://www.theseus.fi/bitstream/handle/10024/44684/Babich_Ale ksandra.pdf?sequence=1.
[5]. Essam-Eldean F. Elfakhrany, Ben Bella S. Tawfik, "IRIS Recognition using Conventional Approach" IEEE 9th International Colloquium on Signal Processing and its Applications, 8 - 10 Mac,2013.
[6]. Geetika, Manavjeet Kaur " Fuzzy Vault with Iris and Retina: A Review" International Journal of Advanced Research in Computer Science and Software Engineering , Volume 3, Issue 4, April 2013.
[7]. Asima Akber Abbasi, M.N.A. Khan and Sajid Ali Khan "A Critical Survey of Iris Based Recognition Systems" Middle-East Journal of Scientific Research 15 (5): 663-668, 2013.
[8]. http://www.griaulebiometrics.com/en-us/book/understanding biometrics/introduction/history
[9]. http://www.nationalbiometric.org/about_history.php
[10]. Sukhwinder Singh, Ajay Jatav "A closure looks to Iris Recognition system" IOSR Journal of Engineering (IOSRJEN) e- ISSN: 2250-3021, p-ISSN: 2278-8719 Vol. 3, Issue 3 (Mar. 2013).
[11]. Senbhaga S " A Survey on Iris Segmentation using Distantly Acquired Face Images" International Journal of Scientific & Engineering Research, Volume 4, Issue 5, May-2013 118 ISSN 2229-5518.
[12]. Mojtaba Najafi and Sedigheh Ghofrani "A New Iris Identification Method Based on Ridge let Transform" International Journal of Computer Theory and Engineering, Vol. 5, No. 4, August 2013.
[13]. D R Prithvi, R Madhu "Recognition Using Secret Key in I