



Performance Analysis of Biometric Systems: A Security Perspective

Dr. Deepak Kumar Verma¹, Savita Ojha²

Department of Computer Science, Babasaheb Bhimrao Ambedkar University (A Central University), Lucknow, India^{1,2}

Abstract: In the modern era of digitization Security has become a critical and challenging issue not only for the defence or government departments but also for a common man because today we are very much dependent on machines that authenticate the person by some identity to allow for use of them. Biometric Systems are automated methods of verifying or recognizing the identity of a living person on the basis of some physiological characteristics, like a fingerprint or face pattern, or some aspects of behaviour, like handwriting or keystroke patterns. In this paper we have studied the physiological and behavioural characteristics of biometric systems by means of performance analysis in context with security perspective.

Keywords: Biometric, Security, Authentication, Digitization

I. INTRODUCTION

The term "biometrics" is derived from the Greek words bio (life) and metric (to measure). For our use, biometrics refers to technologies for Measuring and analysing a person's physiological or behavioural characteristics. These characteristics are unique to individuals hence can be used to verify or identify a person [1]. Biometrics, described as the science of recognizing an individual based on his or her legitimate method for determining an individual's identity [3]. Biometrics is the automated use of physiological or behavioural characteristics to determine or verify identity. All biometric identifier can be divided into two big groups:

1. Physiological
2. Behavioural



The figure1 shows various Physiological and Behavioural biometrics examples to distinguish the difference among them. Biometrics is based on the measurement of distinctive physiological and behavioural characteristics. Finger-scan, facial-scan, iris-scan, hand-scan, and retina-scan are considered physiological biometrics, based on direct measurements of are considered behavioural biometrics; they are based on measurements and data derived from an action and



therefore indirectly measure characteristics of the human body. The element of time is essential to behavioural biometrics-the characteristic being measured is tied to an action, such as a spoken or signed series of words, with a beginning and an end. The physiological/behavioural classification is a useful way to view the types of biometric technologies, because certain performance and privacy related factors often differ between the two types of distinction is slightly artificial. Behavioural biometrics is based in part on physiology, such as the shape of the vocal cords in voice-scan or the dexterity of hands and fingers in signature-scan. Physiological biometric technologies are similarly informed by user behaviour, such as the manner in which a user presents a finger or looks at a camera [2].

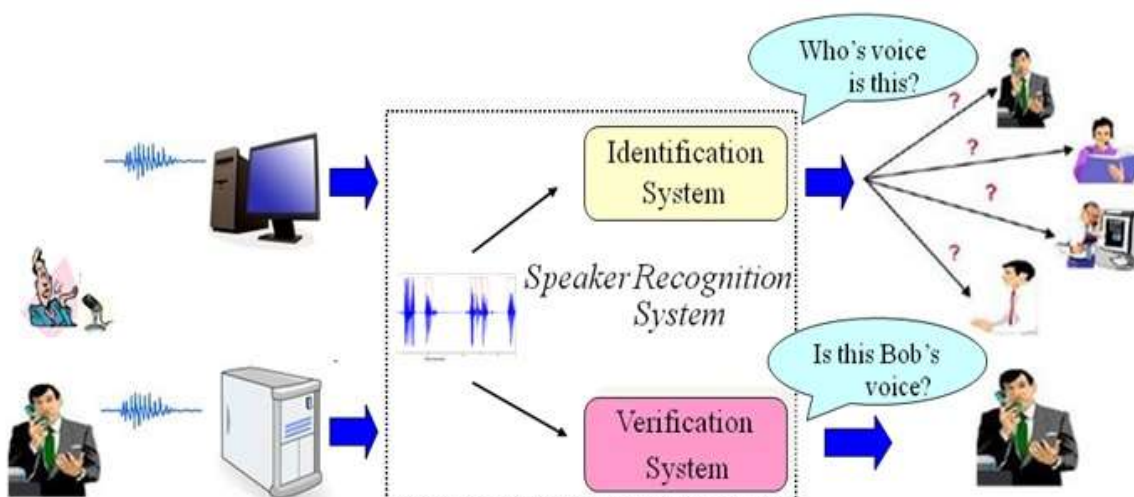
Fingerprint scanning-A fingerprint is a combination of the friction ridges. A friction ridge is a raised portion of digits (fingers and toes) or plantar (sole) skin, including of one or more connected ridge units. In current time, live finger print readers are used because these readers are based on optical, thermal, silicon or ultrasonic principles. A Fingerprint is made of ridges and valleys on the surface of fingertips. Upper skin layer segments are called ridges and lower skin layer segments are called Valleys.

Face Recognition- Facial recognition is a biometric software application capable of uniquely identifying or verifying a person by comparing and analysing patterns based on the person's facial contours. Facial recognition is mostly used for security purposes, though there is increasing interest in other areas of use. In fact, facial recognition technology has received significant attention as it has potential for a wide range of application related to law enforcement as well as other enterprises.

Iris scanning- Iris scanning is an automated method of biometric identification that uses mathematical pattern-recognition techniques on video images of one or both of the irises of an individual's eyes, whose complex patterns are unique, stable, and can be seen from some distance. They are even unique for the identical twins. Iris is used for various authentication and security applications that include identity cards and passports, prison security, database access and computer login, border control and Government programmes [4]. This will cause a difference between intra and inter class comparisons. Therefore we decided to isolate the effects of the eye-lid and the effects of the eye-lashes by using only the left and right part of the iris area for the iris recognition. Most of the method extracts the complete iris image, but we extract part of the iris image for the recognition [5]

Hand Geometry- Hand geometry is a biometric that identifies users by the shape of their hands. Hand geometry readers measure a user's hand along many dimensions and compare those measurements to measurements stored in a file. Viable hand geometry devices have been manufactured since the early 1980s, making hand geometry the first biometric to find widespread computerized use. It remains popular; common applications include access control and time-and-attendance operations. Since hand geometry is not thought to be as unique as fingerprints, palm veins or irises, fingerprinting, palm veins and iris recognition remain the preferred technology for high-security applications. Hand geometry is very reliable when combined with other forms of identification, such as identification cards or personal identification numbers. In large populations, hand geometry is not suitable for so-called one-to-many applications, in which a user is identified from his biometric without any other identification.

Speaking style- Speech recognition, on the other hand, is a user interface technology. In today's increasingly mobile and connected world, having hands free interface options is critical. Speech recognition technology, also called voice command, allows users to interact with and control technologies by speaking to them.





II. RELATED WORK

Er. Upasana Dutta, Er. Shikha Tuteja, 2015, in this paper author discussed contain survey of papers which present a range of approach for the recognition of speech and fingerprint. The impasse is found more compounds when dispensation on randomly varying analog signals such as speech signals or physical traits like fingerprints.

Lokesh Sharma, Manish Mathuria, In this paper is to discuss the details of fingerprint biometrics and its comparisons with multifactor authentication techniques. And the last but not least is the loss of privacy and security. It is also aimed to discuss the solutions related to privacy and security.

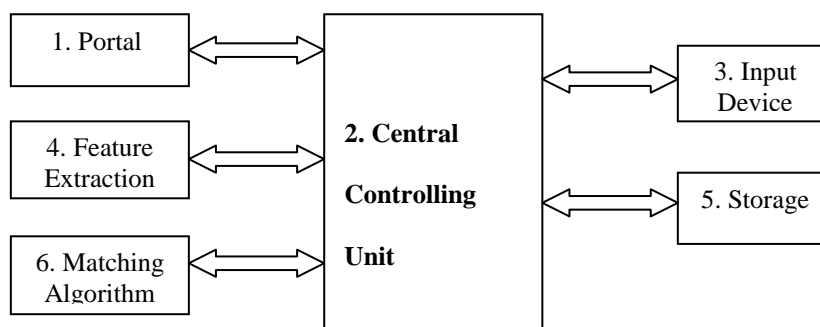
Abhilash Kumar Sharma, 2015, In this paper the review of Biometric System is provided. The main steps involve in biometrics is: Image Formation, Image Processing and Image Matching. Because of need of high security systems we are also using the biometrics broadly. Another feature of biometric is its efficiency. It is very easy to use and handle.

Chetan Jamdar, Amol Boke, 2017, In this paper use multimodal biometric method to overcome this problem. multimodel biometric system is one of the major area of study identified with large application in recognition system. We perform on face identification and recognition method Face recognition method are used for security purpose but in this paper we use for identification of person face from crowed area is challenge.

Hitesh Walia, Neelu Jain, 2016,[10] In This paper incorporates the problems of attendance systems presently in use, working of a typical fingerprint based attendance system, study of different systems, their advantages, disadvantages and comparison based upon important parameters. There is a need to replace these traditional methods of attendance recording with biometric attendance system. The unique nature of fingerprint makes it ideal for use in attendance management systems.

III. MODULES OF A BIOMETRIC SYSTEM

Any biometric system is basically made of six components as shown in the figure:



- 1. Portal-** Its purpose is to protect some assets. An example of a portal is the gate at an entrance of a building. If the user has been successfully authenticated and is authorised to access an object then access is granted.
- 2. Central controlling unit-** It receives the authentication request, controls the biometric authentication process and returns the result of user authentication.
- 3. Input device-** The aim of the input device is biometric data acquisition. During the acquisition process user's liveness and quality of the sample may be verified.
- 4. Feature extraction-** This module processes the biometric data. The output of the module is a set of extracted features suitable for the matching algorithm. During the feature extraction process the module may also evaluate quality of the input biometric data.
- 5. Storage-** It is the storage of biometric templates. This will typically be some kind of a database. Biometric templates can also be stored on a user-held medium (e.g., smartcard). In that case a link between the user and her biometric template must exist (e.g., in the form of an attribute certificate).
- 6. The biometric matching algorithm-** It compares the current biometric features with the stored template. The desired security threshold level may be a parameter of the matching process. In this case the result of the matching will be a yes/no answer. Otherwise a score representing the similarity between the template and the current biometric sample is returned. The central unit then makes the yes/no decision.



➤ Working of Biometric system

Biometrics systems work by recording and comparing biometric characteristics. In many cases, characteristics are recorded as images, but for speaker recognition a waveform is recorded, and for signature recognition, time series data. For efficiency reasons, rather than using recorded characteristics directly, it is usual to extract identifying features from the samples and encode these features in a form that facilitates storage and comparison.

When an individual first uses a biometric system, their identifying features are enrolled as a reference for future comparison. Depending on the needs of the application, this reference may be stored in a central database or on a personal device such as a phone or a card. When biometric recognition is required, the individual's biometric characteristics are recorded again. This time however, the identifying features are compared by the system with the stored reference to determine if there is a close match.

There are two modes for biometric recognition: verification and identification. In verification, an identity is claimed and the comparison process is limited to checking the reference corresponding to this identity. In identification, no claim of identity is necessary and the system searches its reference database to find if a stored reference matches the biometric characteristics recorded.

IV. BENEFITS OF BIOMETRICS SYSTEM

1. **Easy and Safe to Use:** The biometric employee attendance is less time consuming, dependable, user-friendly, anyone can be used by accessing their identification. Biometric will make the world more secure and more convenient. If you follow common guidelines for security, you should have almost nothing to worry about.
2. **Time-Saving:** This is one of the most important advantages. Biometric identification is extremely quick. A person can be immediately identified or rejected within a second. Therefore, it is considered very quick and time-saving compared to process paper sheets and time cards. It saves time that is wasted in the calculation of the employee attendance. By using the attendance machine one can focus more on business.
3. **Increased Productivity:** Biometrics saves employee time, decreases staffing overhead, and provides accurate labor data to the employees' system to effectively manage business operations. The time and effort saved combined with data accuracy help in optimizing the use of resources which lead to increased productivity and improves profits.
4. **Easy Integration:** Biometric facial systems are also easy to integrate into your company. Usually they will work with existing software that you have in place [7].
5. **Improved Job Satisfaction:** If you have employees working from an office, from home, or at distant locations. An attendance management system allows organizations to track employee time using a variety of clocking options, such as smartphones, internet networks, swiping technologies, biometric terminals or desktop readers easily. Sometimes employees have to work overtime to address an unusual situation. When used correctly, an accurate time clock system will alert you to excessive overtime situation which helps to more fairly balance the workload. As a result, employees do not feel as overworked. When they do work overtime, they can feel confident it has been noticed.
6. **Guarantee the Attendance:** You can easily configure a biometric system to administer office rules. Many companies are still using badges or cards to log employee time. If cards are lost, badges are misplaced, it does not only do the business lose money and time but also security may be at risk. With a help of biometric attendance system, there's no need to worry about the loss. Employers won't need to reset door codes or inactivate cards. A biometric attendance system is a great way for employers to ensure attendance, reduce time theft, and spend less time and money maintaining their timekeeping system.
7. **Security:** Most attendance management systems are built around highly secure systems and planning. Specifically, biometric systems are highly reliable and secure and can help to avoid time theft, buddy punching. Biometric attendance system can help an organization in doing away with time-consuming, unreliable, inaccurate, and very poorly secured manual security system where everybody has to enter them in time, time out. These systems are of particular utility to organizations where security is a primary concern.







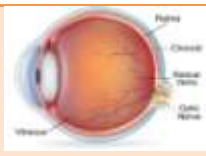
V. PERFORMANCE ANALYSIS OF BIOMETRIC SYSTEMS

To confirm the personal identity are used by different physiological characteristics and behavioural features. In practice constantly discovering new ways to measure the attributes and the uniqueness. Some of these systems are constantly under development and are not available in a form that could be used in identification systems. There are many characteristics which make it possible to compare the biometric systems. We have selected three most used performance metrics for analysis of biometrics systems:






- **False Rejection Rate (FRR)**-The probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percentage of valid inputs which are incorrectly rejected.
- **False Acceptance Rate (FAR)**-The probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percentage of invalid inputs which are incorrectly accepted.
- **Verification Time**-The amount of time consumed in comparison of a captured biometric with a specific template store in a biometric database in order to verify the individual is the person.

The table1 shows the performance analysis of various Identification and verification method.

Table 1: Identification and verification methods

Identification & verification methods	Images	Methodology/ Characteristics	False Rejection Rate (FRR)	False Acceptance Rate(FAR)	Verification time
Hand		Measuring the physical characteristics of hand and fingure from a three dimensional perspective	0.1%	0.1%	1 or 2 sec
Fingerprint		Optical, capacitive or thermal fingerprinting(“minut azne”body alebo tvar papilar)	Less than 1%	from 0.0001% to 0.00001% depending on type	0.2- 1 Sec.
Face		Face recognition	Less than 1%	0.1%	3 Sec
Eye		Iris scanning	0.00066%	0.00078%	2 Seconds
		Retina	The analysis of the capillary vessels located at the back of the eye.		



Other Methods		DNA	DNA is an increasingly useful biometric, and is encountered most often in forensics and healthcare. DNA of the user in the form of blood, tissue, hair, nails is collected for confirming. DNA also is unique characteristic but a hair or nail can be stolen.
		Digital Signature	Dynamic analysis of the shape, size of signature, writing speed, time taken for signing, pressure applied by user's hand on the screen while signing etc.
		Voice	The analysis of the tone, pitch, cadence and frequency of a person's voice. Voice or speaker recognition is the ability of a machine or program to receive and interpret dictation or to understand and carry out spoken commands.
		Vein	The analysis of pattern of veins.
		Ear	The analysis of ear shell shape.

VI. CONCLUSIONS

In this paper we have analyzed the performance of various biometric system based on physiological and behavioral characteristics as shown in table 1. On the basis of the analysis we can say that physiological characteristics are more reliable than one which adopts behavioral features, even if the latter may be easier to integrate within certain specific applications. Fingerprint biometrics is the cheapest, fastest, most convenient and most reliable way to identify someone. Fingerprint authentication has many usability advantages over traditional systems such as passwords. We discussed some solutions regarding privacy and security of fingerprint biometrics on the basis of the performance analysis. Future research work can be carried out on Fingerprint biometrics to improve the quality of the images by improving the imaging enhancement techniques and to develop a better matching technique for partial and rotated fingerprint images.

REFERENCES

- [1]. Prof. Marios Savvides, "Biometric technologies and application", Caregie Mellon CYLAB, PP.01-73.
- [2]. Abhilash kumar Sharma, Ashish Raghuvanshi, Vijay kumar Sharma, "Biometric system," International Journal of computer science and information technologies, vol.6(5), pp.4616-4619, 2015.
- [3]. Anil k.Jain, Arun Ross and Sharath Pankanti, "Biometrics : A Tool for Information Security", IEEE Transactions on Information Forensics and Security, vol.2, pp.21-38, june 2005.
- [4]. Geetika Manavjeet Kaur, "fuzzy vault with Iris and Retina:A Review" International Journal of advanced Research in computer science and Software Engineering, vol.3, april 2013.
- [5]. Savita Wavelet Feature for IRIS, "Extraction of deal tree complex Wavelet Feature for IRIS Recognition" International Journal of Advanced Research in Communication Engineering, vol.2, July 2013.
- [6]. Lokesh Sharma, Manish Mathuria, "Fingerprint Biometric and Security", Journal of Information, knowledge and Research in computer Engineering, vol.04, pp.903, 16Oct to oct 17.
- [7]. Sakshi Goell, Akhil Kaushik, Kirtika Goel, "Facial Recognition", International Journal of Scientific Research Engineering and Technology (IJSRET), VOL.1, PP.012-017, Aug12.
- [8]. Chetan Jamdar, Amol Boke, "person Identification system using multi-model Biometric Based on Face", International Journal of science, Engineering and Technology Research(IJSETR), vol.6, pp.628, april2017.
- [9]. Er. Upasana Dutta, Er. Shikha Tuteja, "Fingerprint and Speech Recognition", International journal of Engineering Research and Technology(IJERT) vol.4, pp.188, April2015.



- [10]. Hitesh Walia, Neelu Jain, "Fingerprint Basad Attendance Systems", International Research Journal of Engineering and Technology (IRJET), VOL.03, PP.1168, May2016.
- [11]. Matyas, V., fu'ha, Z. (2000). Biometric Authentication Systems. Technical report. <http://www.ecom-monitor.com/papers/biometricsTR2000.pdf>.
- [12]. Jain, A., Bolle, R. and Pankanti S. (1999). BIOMETRICS: Personal Identification in Networked Society. Kluwer Academic Publishers.

BIOGRAPHY



Dr. Deepak Kumar Verma, MCA, UGC-NET, Ph.D.(CS), pursued Bachelor of Science and Master of Computer Application from University of Lucknow, India in year 2011. Dr Verma completed his doctrate in Computer Science in the year 2016 and currently working with Department of Computer Science, Babasaheb Bhimrao Ambedkar University(A Central University), Lucknow, India. His research interests are Artificial intellegence, data security and Software Engineering. He has published number of research papers in reputed national/international journals and conferences.



Ms. Savita Ojha, pursued Bachelor of Computer Application (BCA) from Uttarakhand Technical University, Dehradun. She is currently pursuing Master of Computer Application (MCA) from Department of Computer Science, Babasaheb Bhimrao Ambedkar University (A Central University), Lucknow, India. Her Research Interests are data Security, Data Analysis.