2023 Birla Institute of Technology and Science Pilani (BITS PILANI))

A Survey of Privacy-Preserving Biometric Authentication: Techniques and Challenges

Chaitanya Krishna Chauhan   
*Department of Computer Science and Information Systems*

*Bits Pilani, Pilani Campus*Pilani, Rajasthan, India  
f20201869@pilani.bits-pilani.ac.in

*Abstract*— Biometrics is physical or behavioral characteristics which are unique for every individual that are time invariant and can be easily used for verification. Reliability in biometrics is increasing manifold in today’s digital world where old and conventional password management processes are vulnerable to several attacks like brute force, man in the middle attacks etc. The idea is to replace them with biometrics or should be used in conjunction with biometrics to ensure a high level of security. The concept of remembering one’s password is also eliminated with this step and is gaining popularity for industrial usage. This paper tries to give an insight on the field of biometrics and highlight various biometric authentication techniques including its strengths, potential risks and challenges and how to overcome them.

Keywords—Biometric, Applications of biometric, Biometric traits, Feature extraction, Classification, Palm prints, Security system, authentication, password management, privacy protection.

# Introduction

Biometric Authentication is a means to provide security by using any physiological and/or behavioral characteristics or features to verify an individual’s identity. It is a pattern recognition system and could be a fingerprint, an eye scan, a retina scan, palm of hand or some physical attribute depending upon the infrastructure and level of security. The technique of identification based on biometric characteristics is preferred over any traditional way of storing PIN or passwords for many reasons like: Physical presence is necessary at the time of identification and it also removes the need to remember a password. The physical quality being examined is mapped to a username with biometric authentication. The username is then used to make decisions after a person is authenticated.

Since, today, a lot of applications need reliable verification algorithms to confirm someone’s identity, recognizing humans based on their body features has become more and more fascinating in emerging technology usage. Biometric authentication is a fairly concrete way of authentication and is widely used by many firms today. The selection of a particular biometric for deployment in a specific department is based on a weighting process of several factors. Seven factors that are used to weigh any trait for use in biometric authentication are: Universality, Uniqueness, Permanence, Measurability Performance, Acceptability and Circumvention [1]. Universality, as the name suggests, means that the biometric being considered should be valid for all to maintain a uniformity. Uniqueness refers to the fact that it should not be a common way of identification which could be compromised easily. Permanence implies the manner in which any trait varies with time. Measurability or collectability is related to the ease of acquisition or measurement of the trait [2]. Moreover, the acquisition should be such that the relevant feature sets could be extracted and subsequently processed. Performance takes into account the accuracy, speed and robustness of the technology being used. Acceptability is the acceptance of the new system by the relevant people and if they are willing to have their biometric trait captured and examined. Lastly, Circumvention relates to the ease with which a particular feature could be duplicated or imitated using a substitute or artifact.

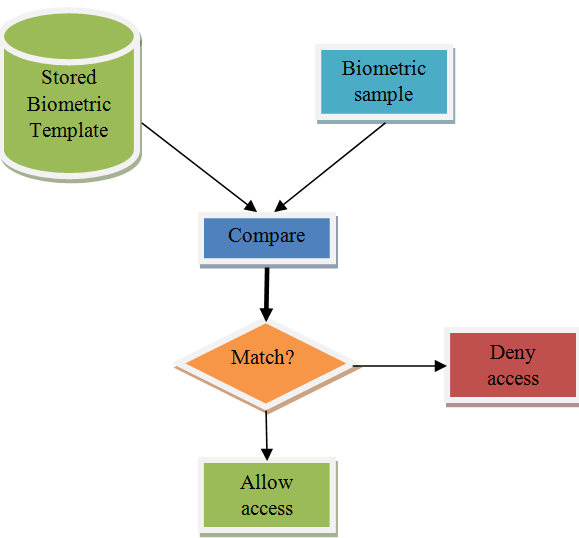


Fig 1.

The Fig. 1 depicts the pictorial representation of how a biometric authentication works. We have a stored biometric template of registered users. If a user comes for authentication, his sample is compared with the stored collection of records. If there is match, then the access is allowed else denied. There are a wide variety of physiological and behavioral characteristics being used today for biometric authentication which includes: fingerprints, voice, iris, retina, hand, face, geometry, voice, handwriting, keystroke, and finger shape [3]. This is only a partial list and advanced technologies keep on coming but with some limitations. Some of the current technologies in use are gait, ear shape, head resonance, ECG and body odour. There are a few latest companies who have pushed the usage of biometrics in their organization like PayPal, Behaviosec, SayPay, Alibaba, iProov, Biyo, Bionym, Sign2Pay, Matrix, SecurAX, Pentagon and many more.

# Biometric Authentication System

A biometric authentication system is a security mechanism that uses a person's physical characteristics to verify their identity. Here is the general process of how a biometric authentication system works:

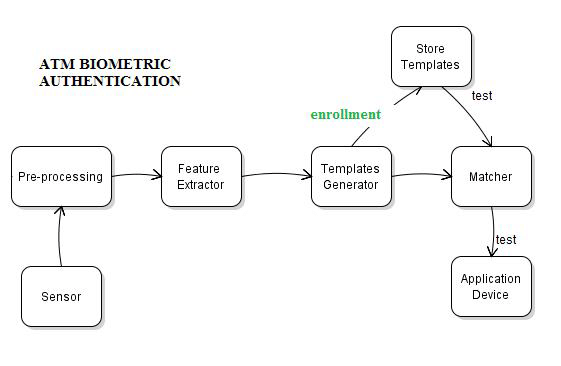


Fig 2.

## Enrollment

Firstly, each new user is registered into a database by capturing the information about a certain characteristic of the person.

## Authentication Request

When the user wants to authenticate themselves, they must submit a request to the system. It could be in any form like scanning the fingerprints or recording voice using a microphone.

## Feature Extraction

As shown in Fig 2, the information of enrolment is usually passed through an algorithm once an authentication request is made that turns the information into a template that the database stores [4]. Note that it is the template that is maintained in the system and not the original biometric measurement as many people may suspect.

## Comparison

When a person needs to be recognised, the system will take required measurements, translate this information into a template using the same algorithm and then checks if it matches with the stored record of templates previously enrolled.

## Decision

If a match is found in the enrolled users, then the access will be granted otherwise an appropriate message will be displayed and access will be denied.

## Logging

Finally, all the logs of authentication, successful and unsuccessful are recorded in a file for audit purposes.

It is important to note here that even after following these steps, biometric authentications are susceptible to errors and hacks which need to be dealt accordingly. Therefore, it is prescribed to use them with an additional security to ensure maximum protection.

# Biometric Authentication Techniques

There are several ways to enable a biometric authentication process available today each with its own set of strengths and weaknesses and the choice depends on the application. It isn’t guaranteed that a single biometric attribute could effectively serve its purpose and sometimes can be clubbed with another. A brief description of the biometric characteristics that are currently used or are under development is given below [5].

1. **Fingerprints**

Finger based authentication is one of the most popular and effective authentication systems and has been there for the longest period of time. It makes use of the unique pattern of ridges and valleys on our finger’s surface for verification. Fingerprint scanners take a digital rendering of the fingerprint and converts it into a template data using a digital algorithm for storage. It is a secure way of storing individual unique data for authentication as even the identical twins have different fingerprints.

There can be different kinds of scanners used for scanning: optical scanner, Capacitive scanner, ultrasound scanner, thermal scanner. The unique data of fingerprint is filtered and saved as a mathematical representation (algorithm) or as an encrypted biometric key. The fingerprint image itself is not saved, only the binary code (or series of numbers) is retained and used for verification purposes [6]. This algorithm cannot be reverse engineered to recapture the image of the fingerprint and thus cannot be duplicated. Due to its distinctiveness, compactness, and compatibility with features used by human fingerprint experts, minutiae-based representation has become the most widely adopted fingerprint representation scheme [7].

1. **Iris Scan**

The iris is the circular pigmented part of our eyes behind the cornea and surrounds the pupil. It is responsible for pupil dilation and contraction. Each iris is distinct and just like fingerprints, even identical twins have different iris and retina. Additionally, it is very easy to detect artificial irises. An iris recognition uses the inner and outer boundaries (pupil and limbus) for localization in an image of eye. Further, the accessories like eyelids and eyelashes are excluded [8].

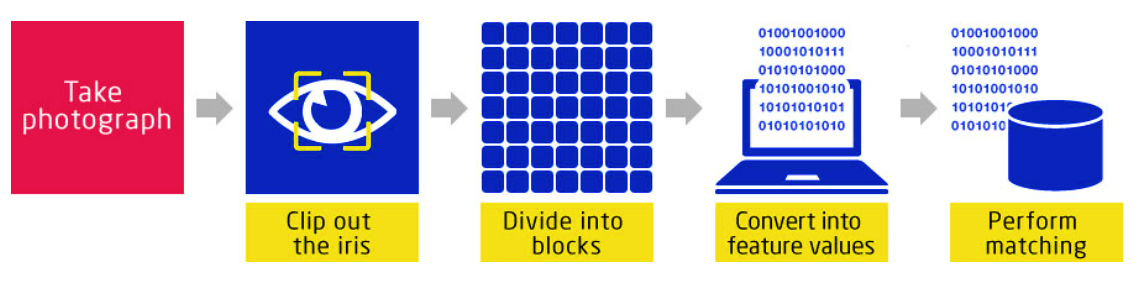


Fig 3.

The set of pixels containing the iris explicitly is used for analysing. The image is extracted and encoded into a bit pattern which could be stored and matched for authentication of a user. A careful balance of light, focus, resolution, brightness and contract is required to give the desired output and there may be errors in it if the eye isn’t positioned in the appropriate manner. Iris scan can sometimes deny the right user depending upon the image captured as it is a highly precise recognition system. There is research going on in this field to improve this system.

1. **Palm print**

Like fingerprints, palms of the human hands contain unique pattern of ridges and valleys. The area of the palm is much larger than the area of a finger and, as a result, palm prints are expected to be even more distinctive than the fingerprints.

The combination of data displayed in a friction ridge imprint serves as the foundation for palm identification, exactly as fingerprint identification. The flow of the friction ridges (Level 1 Detail), the presence or absence of characteristics along the individual friction ridge courses and their sequences (Level 2 Detail), and the detailed detail of a single ridge (Level 3 Detail) [9] are some examples of this information. Fig. 4 shows these details.

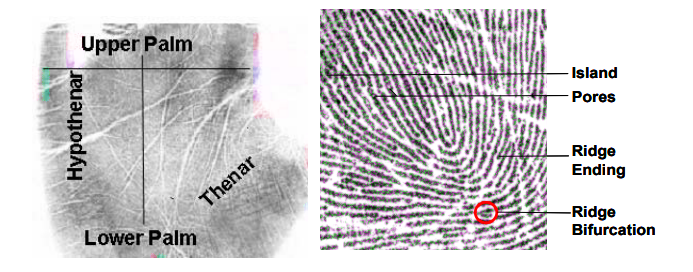


Fig 4.

1. **Hand Geometry**

Hand geometry biometrics identifies user from their hand shapes and characteristics. The features can be measured using a computer-based imaging process and measurement techniques to identify an individual with his/her hand. This can be used for smaller populations such as a firm for authentication of employees by the shape of their hands. The hands are examined and allotted a particular Unicode character based on the algorithm developed by researchers [10]. It can be called one of the oldest method of biometrics and has been used even before fingerprints biometric.

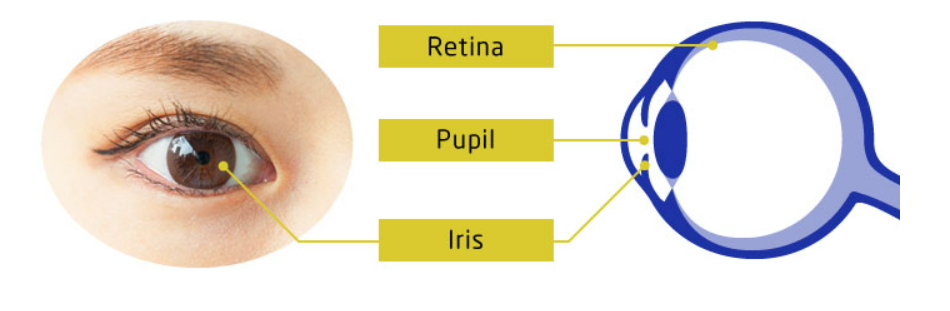
In Hand geometry devices, we can capture the hand features and process it to produce a digital biometric template that can be used to establish identity for verification. They are efficient way of biometrics. The person has to enter his PIN first which fetches the record based on that PIN. To have their hand scanned, a user must place their hand on the platen. Modern hand recognition systems include rapid scanning and verification processes that last less than a second. In Fig 5, a hand geometry biometrics is displayed.



Fig 5.

1. **Retina Scan**

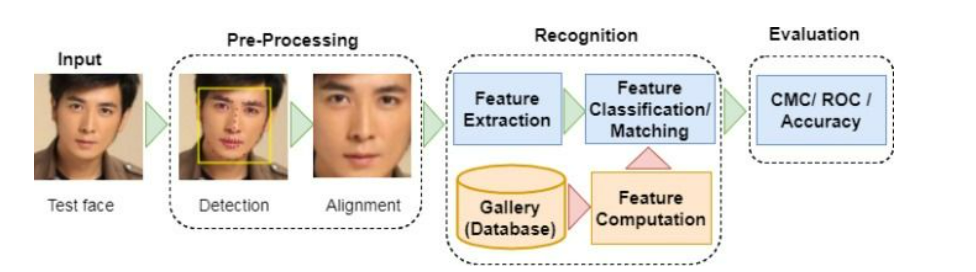
The human retina is a thin tissue composed of neural cells that is located in the posterior portion of the eye. Every person’s retina is unique due to the complex nature of capillaries supplying blood to retina. Retina scan biometrics is a form of biometric authentication technology that maps the unique patterns of an individual’s retina using a low intensity light source. One study on biometric authentication discovered that the false rejection rate of retinal scanning technology stands at 1.8% [11].

Fig 6.

Retina scan biometric systems use specialized cameras to capture a high-resolution image of the retina, which is then analysed to create a template or "map" of the blood vessels. The first company to implement retinal recognition was EyeDentify Inc. which used “fundus cameras” to capture the images. The steps involved in retinal biometric identification are: 1. Image acquisition 2. Retinal matching 3. Representation. The main step is the first step where the user looks into a green light in a white background where the scanner is activated and it goes in a complete circle (360 degrees) to completely record the blood vessel pattern [12].

1. **Face**

Face recognition biometrics is a form of biometric authentication technology that uses the unique facial features of an individual to identify and verify their identity. It is a method of BAS where we measure and record a person’s facial measurements to identify it later using any audio-visual element of his face. Unlike other privacy preserving measures, face recognition uses eccentric mathematical and dynamic pattern modules to store its data [13]. Moreover, it doesn’t require any physical contact with the device and hence, is hygienic and non-intrusive. The objective of face recognition during matching is to look for same data set values in a person’s facial with the trained set of faces from database. It captures and analyses various features of the face, such as the distance between the eyes, the shape of the nose, the width of the mouth, and the contours of the face. The aforementioned steps are depicted in Fig 7.

Fig 7.

Face recognition biometrics technology is widely used in a variety of applications, such as security and access control, mobile devices, and social media platforms. It is considered to be convenient but can be affected by factors such as changes in lighting conditions, facial expressions, and aging, which can reduce its accuracy.

There are also concerns about the potential misuse of face recognition biometrics technology, particularly in the areas of surveillance and privacy. As a result, there is ongoing debate about the appropriate use and regulation of this technology to ensure that it is used ethically and responsibly.

1. **Voice**

Voice-based biometrics, also known as speaker recognition, is a form of biometric authentication technology that uses the unique characteristics of an individual's voice to identify and verify their identity. It is also known by the names voice printing and voice authentication. Each of us have different styles and ways of speaking based on our anatomy and behavioral speech patterns. The shape and size of mouth, pitch and speaking patterns along with pace of speech is recorded. It seems easy but is really hard to mimic all sets of voices of an individual by even a mimic artist. Hence, it can be termed as secure way of BAS. Fig 8. Shows the steps in audio recognition. A user provides one or more audio samples, which the system analyses to create a unique voiceprint for the speaker. Whenever the user calls in, the software compares the speaker’s voiceprint to the voiceprint on file [14]. We can consider as the imprint of each person’s voice that is as unique as their fingerprints.

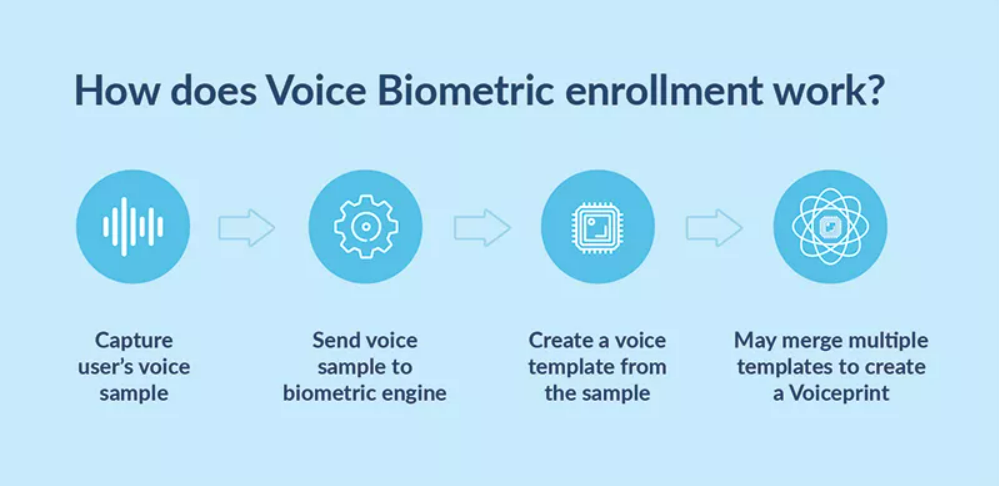
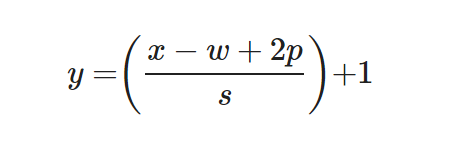


Fig 8.

Voice-based biometric systems typically use specialized microphones or sensors to capture a sample of the individual's voice, which is then processed using advanced algorithms to create a voiceprint.

1. **Ear**

Ear biometrics is a type of biometric authentication system that recognises and authenticates people by using the distinctive characteristics of their ears. The shape structure of the human ear is robust and trustworthy, and it does not alter much with ageing. To develop a special template or "ear print" for each person, it photographs and evaluates the ear's different properties, including its size, shape, and curves.



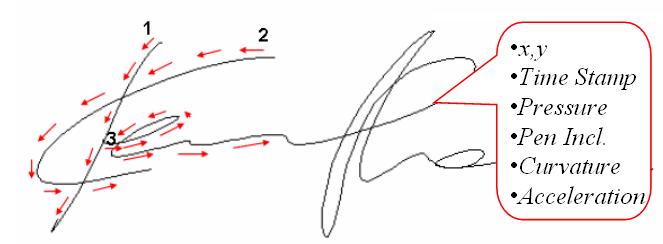
The majority of ear biometric systems take pictures of the ear using specialised cameras or sensors, which are then analysed using sophisticated algorithms to build a template. The identification of the person is then confirmed by comparing this template to a previously registered template.

The usage of ear biometrics is currently somewhat limited compared to other biometric technologies like fingerprint or face recognition. Currently, it is being investigated for use in a variety of settings, including security, access control, and healthcare.

1. **Signature**

Signature biometrics is an example of behavioral BAS that identifies a person based on their handwriting and signatures. It can be operated in two steps: static and dynamic. In static signature recognition, the users write their signature on paper which is digitalized through an optical scanner and then converted to bits using image processing. The biometrics can even analyse the signature based on its shape [15]. The static step is known as ‘off-line’. In dynamic mode, we acquire the signature in real time and makes use of a several set of coordinates to authenticate the user such as (Fig 9.):

* spatial coordinate x(t)
* spatial coordinate y(t)
* pressure p(t)
* azimuth az(t)
* inclination in(t)
* pen up/down

Fig 9.

1. **Gait**

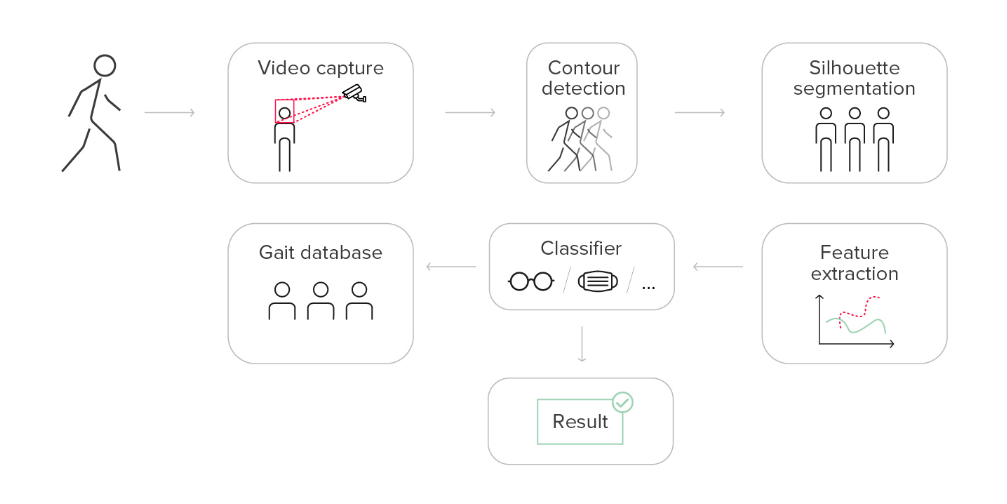
Gait biometrics is a modern way of biometrics which makes use of manner or style of walking of an individual to authenticate. Studies in psychophysics suggest that people can identify familiar individuals using just their gait. This has given rise to several algorithms to identify users based on their gaits [16]. Such a system consists of a video camera which captures the movements of a person walking within its field of view. 

Fig 10.

Appropriate features like joint angles, stride length, speed and silhouettes are extracted and stored accordingly as gait signatures. Steps involved in gait recognition biometrics are shown in Fig 10. The gate signatures are then compared to a pre-registered gait signature to verify the identity of the person. The algorithm then recognizes the gait data, processes it and looks for contours and detects segments of individual human features. The algorithms may vary as some of them are designed to process video signals whereas others use data from sensors [17]. Again, this is a new technology and still needs improvement and is subjected to changes with different footwears, clothing or health conditions.

1. **Odour**

Body odour biometrics is a contactless physical biometric system which attempts to confirm a person’s identity with the help of olfactory property analysis. This technology uses an electronic nose or mass spectrometers to figure out the smell of every user being enrolled and it can be dynamic and can account for changes in environment. The analysis is based on the composition and concentration of several chemical compounds in one’s scent. The unique template is created for everyone which is known as “odour print” [18].

In fact, body odour as a biometric has been recently studied, and there is plenty of opportunity for researchers to explore. However, developing a complete system that is new requires a lot of investment in terms of resources and time.

1. **DNA**

DNA (Deoxyribonucleic acid) is a chemical substance which is found in each of the approximately 100 trillion cells within the human body. It contains a lot of information like genetic code for replica formation and protein construction required to sustain life. Every strand of DNA contains entire biological information about the individual which is known as “genome”. This information can be exploited (Fig 11.) for a person’s identity just like DNA testing for blood relations.

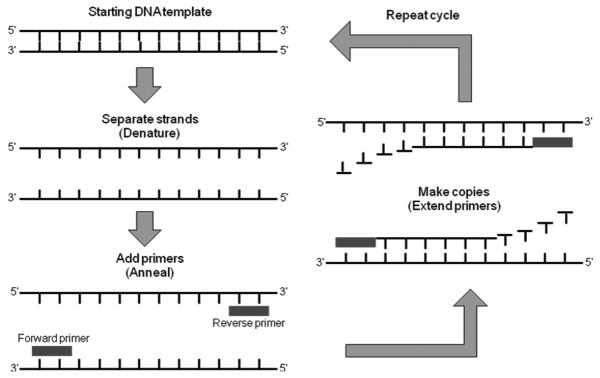


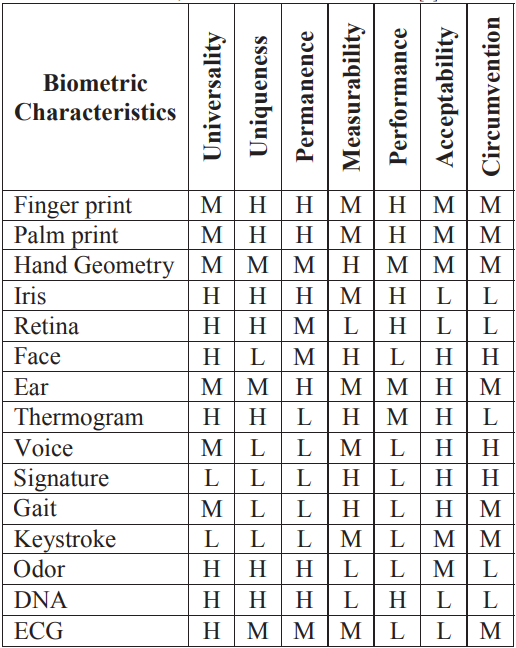
Fig 11.

[19] This information of DNA is just enough to identify even a disease or for security. This is in beta phase but researches show that scientists are looking for unusual patterns in DNA to pin point an individual. If we are able to achieve that, we can use a small database to store a huge number of people record and find their details with a click. Much of this is still in investigation and experimental stages and nothing concrete can be inferred as of now but in the future, it could be one of the life changing developments in both medical science and cybersecurity with cryptography.

1. **Multimodal biometrics**

Multimodal biometrics as the name suggests, is related to combining several above-mentioned techniques to exploit the overall advantages and get better security and results. The below table (Table 1) shows a comparison of different types of attributes used in biometric authentication system: [20].

Table 1



There are high chances to crack a particular code like microphone or gait signatures. Even, the accuracy and reliability of digital signatures are questionable but it is highly impossible for someone to copy all those at once, thus providing an extra layer of privacy protection. On the other hand, modalities can lead to increased processing time and latency, which can be problematic in certain applications. An example is mentioned below.

In an experiment, the scientists and researchers had developed a multimodal biometric system by combining iris, face and voice at match score level using simple sum rule. The match scores were normalized by min-max normalization. The identity established by that system was much more reliable and precise than the individual biometric systems. Experimental evaluations were performed on a public dataset demonstrating the accuracy of the proposed system. The effectiveness of proposed system regarding FMR (False Matching Rate) and FNMR (False Non-Matching Rate) is demonstrated with the help of MUBI (Multimodal Biometrics Integration) software [21].

# Biometric Authentication Challenges

Biometric authentication has become quite popular in recent years both in public and private sectors. As a result, it’s getting more integrated in our daily lives due to its performance and security factor. However, there are several challenges associated with biometric authentication that need to be addressed:

1. **Privacy**

Privacy is one of the major concern when it comes to biometrics where people might not provide consent to use any body feature. A covert or passive demand can be easily turned down by the audience leading to a bad market and can highly turn down the uses of biometrics. Moreover, biometrics are sensitive personal data of individuals which can fall into wrong hands and can be exercised for malicious purposes, spoofing and even harassment [22]. Therefore, it becomes necessary to ensure that the data is safe and protected from misuse. Lastly, we cannot enforce biometrics on people as the concept of privacy and consent varies between individuals and hence, we must be careful when dealing with people.

1. **Security concerns : Protecting Templates**

The BAS system must be secure to prevent any privilege escalation and unauthorized access of sensitive data from the system. Most existing privacy preserving biometric systems have focus on storing the biometric data in a modified version and keeping the original data safe. The modified data is transmitted which prevents any kinds of eavesdropping of sensitive data and the cases of compromised databases [23]. One solution to solve the above mentioned problem is to follow protection schemes like cancellable and bio hashing. Although bio hashing provide a quick authentication with low error rates, it can still be attacked and we need a robust security network to prevent data breaches.

1. **Accuracy**

Biometric authentication systems need to be more accurate in identifying individuals. Moreover, in image processing biometrics, we need to be make sure that the captured images are clear and in optimum resolutions otherwise the results could be contradicting. Biometrics are more inaccurate than we thought and a recent post by KnowBe4 states another angle of complexity of biometrics issue [23].

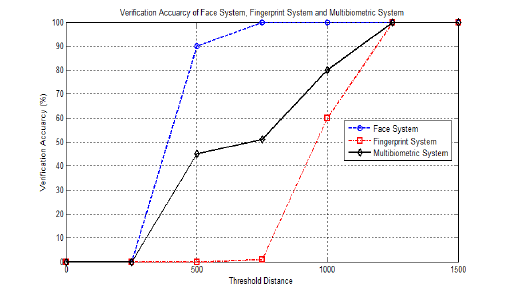


Fig 12.

The figure shows a comparison of accuracy for the three most prominent systems in biometrics [24]. An analysis by a defense evangelist at KnowBe4 stats that according to NIST evaluation ratings, it is aimed to have as less as 1 error per 100,000 tests which is an accuracy goal of 1:1000000. But as Grimes wrote, “So far, none of the submitted candidates come anywhere close”. The best results till now have an error of 1.9 % which is nearly 2 mistakes for every 100 tests [25]. Another key factor is theoretical accuracy vs real world accuracy. Because it can take into account a lot of different data points, facial recognition is theoretically much more discriminating. But in practice, finger print recognition wins the contest because it is not affected by factors like cosmetics, lighting, hair change etc. There is also distance issue and results can vary based on image size. Moreover, the biometrics technology isn’t a sole way of authentication and when it fails, the phone switches to default phone’s PIN.

1. **Cryptographic Primitives**

The direct employment of cryptographic primitives seems to be the most robust approach so far to tackle the challenging problem of privacy-preservation. If we instill cryptographic primitive techniques such as AES and RSA in biometrics then we can reduce the errors of Biometrics authentication results as cryptography is error intolerant. The main cryptographic tools used to combat the leakage of private information during biometric authentication are secure multiparty computation (SMPC) [23].

Homomorphic encryption, oblivious transmission, and mangled circuits are some of the cryptographic primitives that are frequently used in SMPC. 

Verifiable computation (VC) methods allow a client to safely outsource calculations to a distant server. After completing the computations, the server sends the client the outcome along with a proof that the computation was outsourced correctly (for the returned result).

# Conclusion

# Finally, the challenge of balancing security and privacy concerns in identity verification systems can be overcome by using privacy-preserving biometric authentication methods. Several methods for privacy-preserving biometric authentication have been highlighted in this study, including homomorphic encryption, secure multiparty computation, and biometric template protection. Although these methods have shown impressive results in preserving user privacy, they also have their own set of drawbacks, including a rise in computational complexity and a drop in recognition precision.

Multimodal biometric systems are likely to have a bright future since they solve some of the issues with unimodal biometric systems. The most common level of information integration for multimodal biometric systems is fusion at the matching score level. They not only enhance matching performance but also deal with spoofing and nonuniversality issues.

# Acknowledgement

Thanks to my instructor-in-charge Professor Dr. Abhishek Mishra and Professor Dr. Ashutosh Bhatia for giving me the chance to work on this project. Thanks to everyone involved for caring so much about my work, and for offering extremely valuable direction and feedback throughout the whole process.

I sincerely thank them for the giving me this opportunity to study about Privacy preserving biometrics techniques and challenges. Thanks to the Academic - Undergraduate Division, BITS Pilani for offering this course and giving me the chance to work on a project of this kind.

# References

1. Jain, A.K.; Bolle, R.; Pankanti, S., eds. (1999). Biometrics: Personal Identification in Networked Society. Kluwer Academic Publications. ISBN 978-0-7923-8345-1.
2. Atul N. Kataria1 , Dipak M. Adhyaru (Member IEEE)2 , Ankit K. Sharma3 , Tanish H. Zaveri4. A Survey of Automated Biometric Authentication Techniques pp. 1-2. 978-1-4799-0727-4/13/$31.00 ©2013 IEEE.
3. Qinghan Xiao. Biometrics—Technology, Application, Challenge And Computational Intelligence Solutions, May 2007 | Ieee Computational Intelligence Magazine.K. Elissa, “Title of paper if known,” unpublished.
4. January 2013 A Survey Paper on P aper on Palm Prints Based Biometric A alm Prints Based Biometric Authentication uthentication System Swati Verma, Pomona Mishra, CSIT Durg, C.G.
5. Naser Zaeri, Minutiae-based Fingerprint Extraction and Recognition, Biometrics, Edited by Jucheng Yang, ISBN 978-953-307-618-8.
6. Fingerprint Biometrics: Definition and How Secure It Is Learn why Top Industry Analysts consistently name Okta and Auth0 as the Identity Leader, Okta
7. Security and Accuracy of Fingerprint-Based Biometrics: A Review Wencheng Yang 1,\* , Song Wang 2 , Jiankun Hu 3 , Guanglou Zheng 1 and Craig Valli 1, symmetry
8. Iris Recognition For public safety market Japanese September 22, 2021 NEC iris recognition technology ranks first in NIST accuracy testing
9. Joe Bonino, Advisory Policy Board Joint Working Group Meeting. 24 April 2002
10. Hand Geometry Recognition Biometrics: All You Need to Know Danny Thakkar, biometric comparison, fingerprint recognition hand geometry.
11. Biometrics and Privacy – issues and challenges. OVIC office of the Victorian Information Commisioner.
12. Retinal Recognition: the Ultimate Biometric - Innovatrix, rootstrap
13. Facial Recognition: how it works and its safety Jul 28, 2022, Electronic identification, a signicat company.
14. What Is Voice Biometrics? By Dylan Teal plum | voice
15. Houmani, Nesmaa; A. Mayoue; S. Garcia-Salicetti; B. Dorizzi; M.I. Khalil; M. Mostafa; H. Abbas; J. Fabregas; M. Faundez-Zanuy; J. M. Pascual-Gaspar; V. Cardeñoso-Payo; C. Vivaracho-Pascual (March 2012). "BioSecure signature evaluation campaign (BSEC'2009): Evaluating online signature algorithms depending on the quality of signatures". Pattern Recognition
16. Gait Biometrics, Overview Rama Chellappa, Ashok Veeraraghavan & Narayanan Ramanathan
17. Gait Recognition System: Deep Dive into This Future Tech
18. Int J Environ Res Public Health. 2022 Dec; 19(24): 16777.Published online 2022 Dec 14. doi: 10.3390/ijerph192416777 PMCID: PMC9779205 PMID: 36554657 National Library of Medicine.
19. DNA biometrics written BY Masaki Hashiyada
20. HT - Croatian Telecom, Carrier Services Department, Kupska 2, Zagreb, CROATIA University of Zagreb, FER, Unska 3/XII, Zagreb, CROATIA
21. Multimodal Biometrics for user authentication IEEE R. Parkavi; K.R. Chandeesh Babu; J.Ajeeth Kumar Department of Information Technology, Thiagarajar College of Engineering, Madurai, Tamil Nadu
22. J. H. Connell, N. K. Ratha, and J. Zuo, “Salting system and method for cancelable iris biometric,” 2017, US Patent 9,633,261.View at: Google Scholar
23. Privacy-Preserving Biometric Authentication: Challenges and Directions Elena Pagnin1and Aikaterini Mitrokotsa.
24. Multibiometric Template Generation Using CS Theory and Discrete Wavelet Transform Based Fusion Technique Conference Paper Nov 2015 Dr. Rohit M. Thank
25. Biometrics are even less accurate than we thought By Evan Schuman, Contributing Columnist, Computerworld | 5 Decemeber 2022.