

A Comprehensive Study on Biometric Systems

Nisha Charaya¹ , Ashima Narang² 

¹ Assistant Professor, Electronics and Communication Engineering, Amity University, Gurugram, Haryana, India

² Assistant Professor, Department of Computer Science & Engineering, Amity University, Gurugram, Haryana, India

Correspondence should be addressed to Nisha Charaya;

charayanisha.1010@gmail.com

Received: 3 March 2025

Revised: 16 March 2025

Accepted: 29 March 2025

Copyright © 2025 Made Anvesha Katti et al. This is an open-access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

ABSTRACT- Biometrics has become an essential part of our lives. It has evolved significantly over past few decades. From unlocking of phone to marking attendance in office and making bank transactions, everything has been automated with the use of biometrics. A lot of biometric attributes are in use with each having its own pros and cons. This paper presents a study of different biometrics and their features.

KEYWORDS: Biometrics, Security, Forgery, Signature, Hand Vein, Fingerprint.

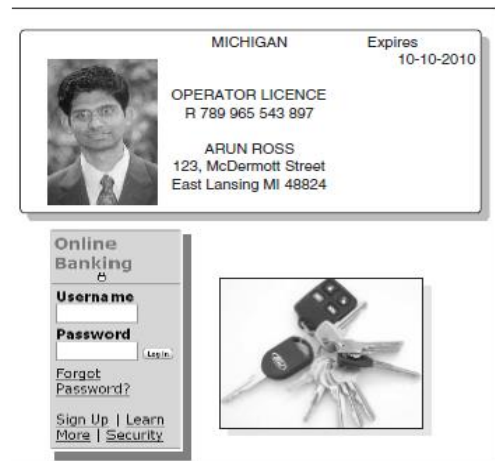
I. INTRODUCTION

Security has become an attention seeking concern these days with an advent in the area of information technology. It's an era of secure automations with so much dependency on technology that a small error may lead to loss of personal data. All of these automations require user confirmations to provide the access which can be accomplished by using some sort of keywords or passwords [1]. Traditional methods fail to provide the desired security level for highly important and confidential data. So, it was the need of an hour to switch to some other attribute for identification of a person which assures better security along with user convenience.

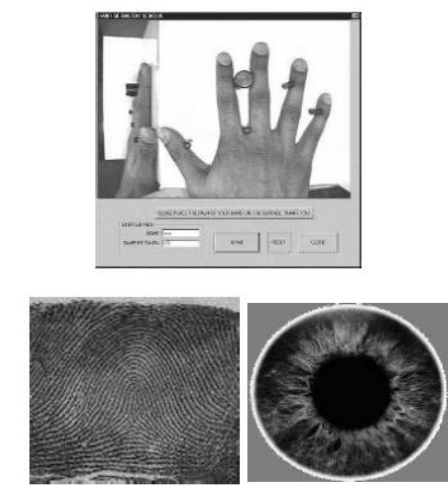
The best way to improve security is by identifying or verifying the person with some technique. The science of identifying or verifying a person based on physiological or behavioral trait is known as biometrics. Fingerprints, iris, face, veins come under physiological biometrics and gait, voice, DNA comes under behavioral biometrics.

The necessity of biometrics has been imposed by access management system which requires accurate identification of a person for several large scale applications. The most important step in this is the verification of claimer's identity. This is done to protect the important resources from impostors. Traditionally an identity card or password was used for this purpose but it came with the shortcoming of being lost, stolen, shared or forged. Mere forgetting the password or losing the identity card may deny the genuine user to forbid the access. Biometric has emerged as a reliable and automated authentication attribute that can't be shared, stolen, forged or forgotten [2]. Figure 1 shows the traditional and biometrics based authentication system.

In addition to these, biometric system is user-convenient as any identity card or password need not be kept safe or remembered all the times.



(a)



(b)

Figure 1: Authentication Systems (a) Traditional system using ID card and Password (b) Biometric based Authentication System [2]

II. BIOMETRIC BASED AUTHENTICATION SYSTEM

An authentication system based on biometric attribute acquires the data from an individual, extracts unique features from it and compares the extracted features with the ones preserved in its database. The decision regarding authenticity of a person is made based upon the comparison result. So, a general authentication system consists of four major

modules: data acquisition module, feature extraction module, matching module and database module.

Data Acquisition Module: An appropriate sensor that may be a scanner or camera is used to obtain the original biometric data of an individual. Figure 2 shows most commonly used biometric attributes for authentication systems.

The quality of data depends upon the characteristics of sensor technology used. Now-a-days, camera is being used to acquire most of the physiological attribute as the data is required in form of images. So, a good quality camera resolves the problem of obtaining a fine data from an individual. Sometimes, a pre-processing algorithm is applied to improve the quality of data. However, in few cases where the quality of data is compromising, the biometric data is collected again from the user.

Feature Extraction Module: The pre-processed biometric data is then processed using some algorithm and a set of unique features is extracted from it. The feature set varies from attribute to attribute and even different feature sets may be extracted from the same attribute by different researchers. For example, in a signature verification system, height, width and area are extracted as features[3]. These feature sets are then stored as template in database during the enrolment phase.

Matching Module: It matches the feature set of presented data with the stored templates and calculates a similarity index between them. This similarity index is used to validate a person's identity.

Database Module: The database module stores all the biometric information. During the enrolment phase, the feature set extracted from the raw samples are stored as templates along with some personal information like name, address, contact number etc.

So, every user needs to get enrolled first so that his/her template and personal information gets stored in the database module. After enrolment, he/she may be authenticated to get the desired access.

III. COMMONLY USED BIOMETRIC ATTRIBUTES

A lot of physiological and behavioral attributes are used for biometric system. Figure 2 depicts some of the majorly used biometric attributes. The major characteristics of some of these are explained as under:

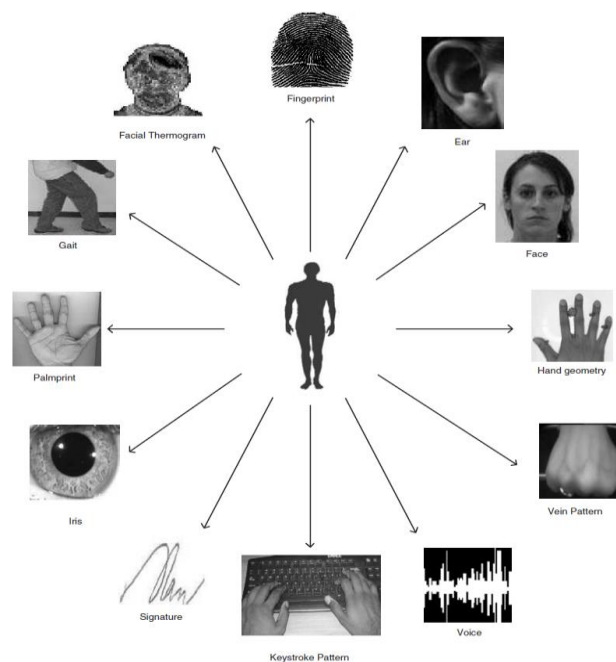


Figure 2: Commonly Used Biometric attributes [2]

A. Fingerprint

Fingerprint is the most widely used biometric attribute. It is preferred due to its uniqueness, ease to capture, performance and cost effectiveness. It is extensively used for forensic applications but it is widely used in other applications like access control, financial transactions, adhaar card etc. With its popularity and demand, it has become an identity card which people carry all the time. This creates a huge demand of automatic fingerprint identification systems. However, it needs to be combined with other biometric traits to increase its reliability at a cost of increased complexity and price [4]. A simple cut or moisture in the skin may lead to its

failure. The major problem associated with it is forgery. It can be replicated easily which leads to security issues [11].

B. Ear

Ear-based biometrics is a relatively new and innovative technique. Ear geometry can be captured easily using a smart phone camera even from a distance and without user's co-operation as it is large [5]. The ear structure is unique and stable over age and facial expressions or all individuals and can be used as a biometric attribute for authentication purpose [6]. This technique is not very well known yet because it is at initial stages of research. Further, the system faces difficulty if the hair covers the ear [7].

C. Face

Face is the most common physical identity of any individual. It is unique and easily accessible. Even the face of identical twins which can't be differentiated by naked eye differs in terms of minute things like placement of eyebrows, breadth of nose and size of eyes etc. These are the distinguished features which can be utilized by a biometric system to identify an individual[8]. If the face image is captured using a high quality camera and used for matching purpose, it can be used for authentication or verification of a person by using pattern matching techniques. It suffers problems with different pose, background, expressions, and lightning [7].

D. Hand geometry

The spatial geometry of hand is unique for every person and is used for the authentication purpose. The hand or finger dimensions can be utilized for the same. However, owing to the storage requirements, two or three fingers are accessed and measured for matching[7]. This can be done with 2D or 3D images of the hand. The dimension parameters like length, width, thickness and surface area are measured and stored as a template[9]. This method is not widely used and suffers problems with hardware requirements.

E. Retina

The blood vessel pattern in the retina of a person is unique for all individuals and even among identical twins. The retinal style gets altered due to some diseases like diabetes, glaucoma etc but retina remains the same [8]. This strengthens the capabilities of retina as a biometric attribute. This means, the image of retina (blood vessel pattern) can be captured, stored and used as a template for further processing to distinguish the individuals [7]. It is reliable and accurate but it fails to identify or authenticate people having cataracts, astigmatism; people wearing glasses or lens and is not user-friendly in terms of cost and convenience[7], [8].

F. Hand Veins

The veins pattern present in hand of an individual is unique and possesses characteristics to be used as a biometrics. It can be captured using infra red camera. The captured images can be used for matching process. However, it should be more reliable to seek attention [7]

G. Signature

Signature in general is the way, a person signs his name. It is a behavioral characteristic of that individual which represents unique variations in hand geometry. Signatures based authentication system is well-known and widely used with numerous applications like bank cheque clearance [3]. This technology extracts features like direction, speed and shape of a signature and uses it for the matching purpose. However, it is not reliable in long term and needs improvement in accuracy [7].

H. Palm print

Just like the fingerprint, the palm print of an individual is unique. It contains unique information like indents and symbols which can be used to match palm print of two individuals. It can be utilized for forensic, criminal and commercial applications. But it doesn't remain stable over time, working conditions or profession of a person[8]. Further the presence of moisture and wrinkles may affect the accuracy of the system [7].

I. Gait

It is a behavioral biometric to identify people based on their unique way of walking. Human motion involves movements of many muscles and joints in a synchronized manner. Though the basic movement pattern remains the same, gait varies among individuals in terms of magnitude and timing. Slight variations in gait can be used as a biometric attribute for identification or authentication of a person. The features like step-length, step-width, speed and rotation of various joint like hip, knee and ankle etc are measured and used as features for matching [10].

IV. SELECTION OF A BIOMETRIC ATTRIBUTE

A number of biometric attributes each having its own pros and cons are proved to be and are being used as an attribute for authentication purpose. For a particular application, the choice of a biometric attribute is made based upon its characteristics which determine its suitability. These characteristics are:

- (a) Universal: Every person should possess that attribute.
- (b) Unique: The given selected attribute should be unique to each individual among the huge population.
- (c) Permanent: The selected biometric attribute should remain permanent or stable over a period of time.
- (d) Easy to acquire: It should be possible to acquire the biometric attribute without causing any harm or inconvenience to the user.
- (e) Performance: The system should be accurate and compatible with the application specific constraints.
- (f) Acceptable: The target individuals should not have any objection to present their biometric attribute.
- (g) Forgery: The biometric attribute selected should be difficult to forge.

All of these characteristics are hard to find in any one attribute. However, a suitable attribute can be selected based upon the requirements of application.

V. CONCLUSION

Different biometric systems are available these days each being good at one or other parameters like user convenience, cost, forgery and accuracy. A particular biometric attribute can be selected and implemented for authentication as per the application. For daily life applications fingerprint is mostly used due to its user-convenience, however for highly secure applications retina is preferred.

Hand-veins are drawing attention of researchers as it is user convenient as well as secure against forgery. A lot of work needs to be done before it being used in commercial biometric applications.

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest

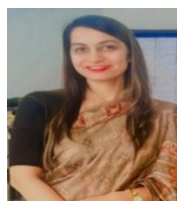
REFERENCES

- 1) J. N. Pato and L. I. Millett, Biometric Recognition: Challenges and Opportunities, Washington, DC: National Academies Press, 2010. Available: <https://nap.nationalacademies.org/catalog/12720/biometric-recognition-challenges-and-opportunities>
- 2) K. Jain, P. Flynn, and A. A. Ross, Handbook of Biometrics, New York, NY: Springer, 2007. Available: <https://link.springer.com/book/10.1007/978-0-387-71041-9>
- 3) Jain, P. Singh, and A. Chugh, "An Offline Signature Verification using Adaptive Resonance Theory 1 (ART1)," International Journal of Computer Applications, vol. 94, no. 2, pp. 8–11, May 2014. Available: <https://research.ijcaonline.org/volume94/number2/pxc3895542.pdf>
- 4) Z. Miklos and K. Vajna, "A Fingerprint Verification System Based on Triangular Matching and Dynamic Time Warping," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 22, no. 11, pp. 1266–1276, Nov. 2000. Available: <https://www.scrip.org/reference/referencespapers?referenceid=153764>
- 5) Querencias-Uceta, B. Rios-Sanchez, and C. Sanchez-Avila, "Principal Component Analysis for Ear-Based Biometric Verification," in Proc. 2017 International Carnahan Conference on Security Technology (ICCST), Madrid, Spain, Oct. 2017, pp. 1–6. Available: <https://oa.upm.es/79165/>
- 6) Tariq and M. U. Akram, "Personal Identification Using Ear Recognition," TELKOMNIKA, vol. 10, no. 2, pp. 321–326, Jun. 2012. Available: https://biomisa.org/uploads/2013/07/ear_1.pdf
- 7) K. Dharavath, F. A. Talukdar, and R. H. Laskar, "Study on Biometric Authentication Systems, Challenges and Future Trends: A Review," in Proc. 2013 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Enathi, India, Dec. 2013. Available: <https://shorturl.at/17JSJ>
- 8) K. CH, "Various Biometric Authentication Techniques: A Review," Journal of Biometrics & Biostatistics, vol. 8, no. 5, 2017. Available: <https://shorturl.at/tWgAN>
- 9) Bhattacharyya, R. Ranjan, F. A. A., and M. Choi, "Biometric Authentication: A Review," International Journal of Service Science, Management, Engineering, and Technology, vol. 2, no. 3, pp. 13–28, 2009.
- 10) R. King, "Explainer: Gait Recognition," Biometric Update, May 26, 2020. Available: <https://www.biometricupdate.com/202005/explainer-gait-recognition>
- 11) Narang A., Gupta D., Kaur A., "Biometrics-Based Un-Locker to Enhance Cloud Security Systems", *International Journal of Cloud Applications and Computing*, 10 (4), pp. 1 - 12, 2020. Available: <https://doi.org/10.4018/IJCAC.2020100101>

ABOUT THE AUTHORS



Dr. Nisha Charaya is a distinguished Academician working as an Assistant Professor, with extensive experience of more than 14 years in the field of Electronics and Communication Engineering. She has contributed significantly to the research Field in the various Areas including Biometrics, Security, Image Processing and Signal Processing. She has published various research papers, conference papers and book chapters and has been an active participant in various international conferences and a member of different professional bodies. Her ability to quickly adapt to new technologies, coupled with a creative approach to problem-solving, makes her an effective educator and mentor.



Dr. Ashima Narang is a distinguished Academician working as an Assistant Professor, with extensive experience of more than 13 years in the field of Computer Science and Engineering. She has contributed significantly to the research Field in the various Areas including Cloud Computing, Virtualisation and Artificial Intelligence. With a strong background in Academics in Computer Sciences, she has various research papers, conference papers and book chapters to her account and has been an active participant in various international conferences and a member of different professional bodies. Her ability to quickly adapt to new technologies, coupled with a creative approach to problem-solving, makes her an effective educator and mentor.