# Biometric Authentication System

Amit D Mishra

Academic Research Student, Department of Information Technology,

B.K. Birla college of Arts, Science and Commerce (Autonomous) Kalyan, Thane, India

Mishramit823@gmail.com

**Abstract:**

**Smart devices are gaining popularity and becoming a key platform for accessing business and personal information in this industry.to access this sensitive data requires a good quantity of authentication and identification. The focus of this paper will be to discuss the limitations of a single biometric system and suggest the need to overcome the limitations to enhance the system performance. Biometrics provides better security solutions than conventional authentication systems because it uses certain physiological or behavioral traits associated with the person.**

Key Words:

Biometrics, Authentication, Pattern recognition, Humans, Ear Artificial intelligence

## Introduction of Biometric System

Mobile computing is quickly starting gaining popularity and mobile device are becoming the main key platform for accessing business and personal information in this industry. For Access this information requires identification, verification and authentication for secure transaction .The Identification can be done in different forms. It may be in the form of authentication or recognition. Biometric traits can be divide into two categories which is shown below:

A. **Physiological biometrics:** it is based on direct measurements of a part of the human body. Fingerprint, iris, retina, face recognition is part of physiological biometrics.
B. **Behavioral biometrics:** it is based on measurements and data derived from an action performed by the known user, and that indirectly measures the some characteristics of the human body for verification. Signature, gait and gesture are part of behavioral biometrics.

There are six basic criteria for biometric security system:.

1. **Uniqueness:** It will Show how different and unique the biometric security system will able to recognize each user among all the user.

2. **Universality:** Universality is the secondary criteria for the biometric security system. This parameter show the requirement for different characteristics of each person in the database, which cannot be duplicate.
3. **Collectability:** The collectability parameter need the collection of each and every characteristic from the system in order to store in database.
4. **Performance:** The accuracy and robustness are two factors for the biometric system. These two factors will decide the performance of the biometric system.
5. **Acceptability:** The acceptability parameter will choose fields in which biometric technologies are acceptable.
6. **Circumvention:** circumvention will decide how easily every characteristic and each trait given by the user can lead to the failure of the verification process in biometric system.


Figure: Basic Criteria for Biometric Security System

## Research Objectives

1) The good thing for using biometric security system for verification and identification is that the modern biometric system are built and designed to be easy and safe to use.
2) The object of our project is use biological characteristics like fingerprints and iris scans, which offer you unique and accurate identification method. These feature cannot be easily duplicated, which means only the known user get access to biometric security system.

3) Passwords and pins are easy to forget making people to write them down and can be stolen, and can be hacked. With biometrics security technology, like fingerprints cannot be lost and cannot be copied by someone aiming to illegally gain access

## Literature Review

**1)** We is able to highlight the biometric authentication in critical environments like military or industry. The future work is on biometric template security. This is fact that a biometric template which can lead to the construction of artificial biometric authentication template using reverse engineering if such a template gets into the hands of a wrong user.

**2)** To provide a good survey we categorize existing recognition techniques and also presented detailed description of representative methods within each and every category. In extra part topic like psychophysical studies and pose variation are covered in biometric system.

**3)** The Face Recognition Technology in a biometric authentication system is a large database of facial images, divided into two main part which is development and sequestered portion. The development portion is available to researchers and the second sequestered portion is available for testing face recognition algorithms.

**4)** We provide a survey of face recognition, including the age estimation discussion. The research outlines several challenges faced in face recognition which has been explored. This paper also provide a landscape mapping based on integrating into a critical taxonomy.

**5)** We discussed four widely used face detection tool, which are Face++, IBM visual recognition, AWS recognition, and Microsoft Azure face API, using multi database to determine their accuracy in inferring user attributes, including gender, face, and age.

**6)** A recent survey of iris biometric authentication from its inception from 2007, total 15 years of research, lists total 180 publication. This new survey is for update the previous one, and covers iris biometric authentication research over the period of 2008-2010 in biometric system.

**7)** Multi-biometric is an interesting research topic. It is used to recognizing individual for many security reason, to increase security level. The recent research trends to next biometric system in real-time applications.

**8)** As biometric template are stored in the database, due to many security threats biometric template may be found by the attacker. To deal with this type of issue visual cryptography schemes can be applied to make more secure to the iris template.

**9)** A method and system generates biometric information by capture an image of retinal vessel pattern and simultaneously capturing an image of an iris pattern. Retinal biometric data and iris biometric data is generated by the images. The retinal biometric data and the iris biometric data combined to maintain the co-relation between the two biometric.

**10)** We proposed a finger vein database captured by a portable device. Which is established with participation of 100 user, coming from 20 country. It contains images acquired from different person with different skin colors.

**11)** The experiment result shows that the method of Wm and Wt –(2D)2pca ha high and unique recognition rate, and the disadvantage of low recognition rate through single feature recognition.

**12)** Image capturing technique based on infrared to capture vein pattern images for biometric is introduced. Experiments involving 30 test subjects. Comparison between the data collected with other biometric techniques show that this hardware method is good to obtain a high quality vein image.

**13)** The human-biometric-sensor-interaction (HBSI) method that uses the simple quality variables for the overall biometric authentication system performances.

**14)** The general approach to application-dependent, testing and reporting of device performance prediction based on test is also discussed in biometric system.

**15)** We present a practical view of biometric authentication system attack vectors, placing them in the risk based systems to approach the security in biometric authentication systems.

## Methodology

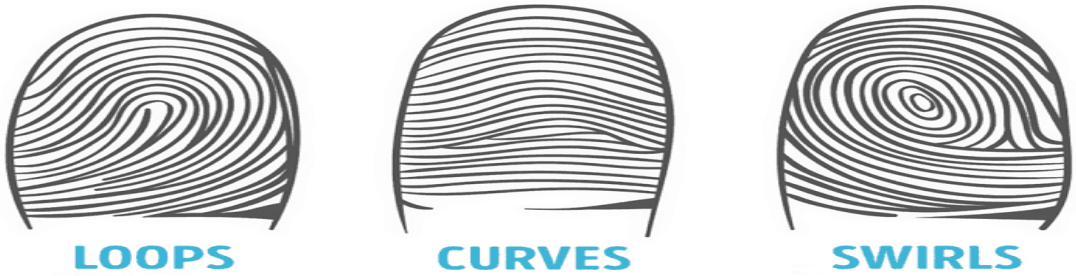
You will see number of biometrics some are rather impractical even if that is technically interesting. The popular biometrics seem to present around the following methodologies which is shown below:

1. **Facial Recognition Detector:**
   The human face verification is the easiest way that can be used in biometric security system to identify a user. It will calculate the overall structure, shape and proportion of features on the user face such as: distance between two eyes, nose, mouth shape, ears shape, jaw shape, size of eyes, and other facial expressions.

**Example of Facial Recognition Scan**

2. **Fingerprint reader:**

Human fingerprint is made from the many number of ridges and valley on the upper surface of the finger that are unique for each human. To successfully capture the upper surface of the fingerprint for verification during the identification of user, new technology are designed with new tools such as: optical and ultrasound.




**Fingerprint Types**

3. **Voice Recognition:**

There are two important factors which makes a person's voice unique. First it is the physiological component which is define as the voice tract. Second, it is a behavioral component which is define as the voice accent. Voice recognition systems are easy to install and it requires a cheap amount of equipment it is low in cost.

4. **Iris Scanner & Recognition:**

. It will analyze all 200 points of the human iris including: ring, furrow, freckle, the coronas and other characteristics. it will store the information in a system database for any future use for comparing it every time a user want to access to the system.

5. **Veins Recognition:**

One of the recent and famous biometric technology is invented in the recent days that is vein recognition system. Veins are blood vessels who carry blood to the heart for blood circulation. Each person's veins have unique physiological and behavioral trait. Compared to the other biometric scanning system, the user's veins are hide inside the human skin. For that reason the vein recognition system will capture images of the vein patterns inside of users' fingers by transmitting light to each and every finger.

**Veins Recognition System**

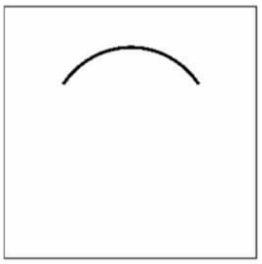
6. **DNA Biometrics System :**
   DNA Biometrics System is one of the recent and famous technology which can be used in biometric security systems. It is hard to fake this type of biometric because each and every person have unique DNA.

7. **2D Barcode Scanner :**

   2-D Barcode Scanner technology is a 2-dimesional method of presenting digital security data which is provide by the biometric technology systems. By combining 2D barcode data and biometric data, it will generate a better security level which can be accessed easily and faster for any future uses.

## Experiment: Template generation

In order to create the template, 64 fingerprints image of eight individual are form a training set. These image are captured using a fingerprint scanning sensor LSI. LSI is manufactured by the NTT Electronic Corporation. The sensor produce each and every image with a size of 224×256 pixels with 8 bits per pixel, the size is increased to 256 ×256 pixels from 224×256 by adding zero-value pixels in order to perform a fast transform. One of the fingerprint images of each and every individual is used for enrollment of fingerprint and the others are used for verification or identification. The optimized template image is shown in Figure. (a) the given parameters is as follows A = 82, B = 86, θ = 57 [Degree], and W = 3, and an image exhibiting the core is shown in Figure .(b) It is consider that this type of template can determine the position of the core even the fingerprint image is shifted significantly to different position.



(a)

(b)

**Result:**

We evaluated the performance of the created templates images by giving it another 50 test images of the eight individual. The result revealed an average estimation error of 7.7 pixels in template creator.

## CONCLUSION

Biometrics refers to an automatic authentication of a user based on his physiological or behavioral characteristics. The biometric uses for authentication is currently gaining momentum, thou the industry is still evolving and emerging. We have presented all the necessary details of each emerging biometric systems to help new researches in this area to choose a particular and unique topic of their interest for researches in this area. We also discussed enough details about future trends of biometric systems and new biometric technology. This work shows a review of biometric system which was done as part of our literature review on biometric authentication. As a continuation to this work the future plan for biometric system is to study and analyze facial recognition system as it is suffering from many difficult challenges.

## GLOSSARY

1. **Biometric data:** a sample taken from individual which is special and unique to their own person. Common biometric data is like fingerprint, voice and iris scans, palm vein and facial pattern.
2. **Behavioral Biometric:** Biometric pattern that is established after amount of time. this biometric is not necessarily a physiological trait in biometric authentication.
3. **Authentication:** Biometric data is considered to be correct and valid for user to verification of the identity. Validation is the preferred term.
4. **Enrolment:** Gathering and processing of biometric data to store into a database.

## Acknowledgements for an Academic Research paper:

This paper and the research behind it would not have been possible without the exceptional support of my supervisor, Swapna Augustine Nikale. And a special gratitude to Amit d mishra Student in Department of Information Technology of B.K. Birla College of Arts, Science and Commerce (Autonomous) Kalyan, Thane Mumbai.

## References


1) Wu, W., Elliott, S. J., Lin, S., Sun, S., & Tang, Y. (2020). Review of palm vein recognition. IET Biometrics, 9(1), 1–10. https://doi.org/10.1049/iet-bmt.2019.0034
2) Syazana-Itqan, K., Syafeeza, A. R., Saad, N. M., Hamid, N. A., & Bin Mohd Saad, W. H. (2016). A Review of Finger-Vein Biometrics Identification Approaches. Indian Journal of Science and Technology, 9(32), 1–8. https://doi.org/10.17485/ijst/2016/v9i32/99276
3) Yu, X., & Wang, H. (2013). Recognition and Matching of ROI Region Finger-Vein Based on NMI Feature. Advanced Materials Research, 760–762, 1447–1451. https://doi.org/10.4028/www.scientific.net/amr.760-762.1447
4) Singh, B. (2016). Iris Recognition Using Curve let Transformation Based on Gabor Filter& SVM. International Journal Of Engineering And Computer Science, 1–5. https://doi.org/10.18535/ijecs/v5i8.32
5) Ma, L., Tan, T., Wang, Y., & Zhang, D. (2004). Efficient Iris Recognition by Characterizing Key Local Variations. IEEE Transactions on Image Processing, 13(6), 739–750. https://doi.org/10.1109/tip.2004.827237
6) Iris recognition. (2015). Biometric Technology Today, 2015(8), 12. https://doi.org/10.1016/s0969-4765(15)30142-9
7) Senaratne, R., Halgamuge, S., & Hsu, A. (2009). Face Recognition by Extending Elastic Bunch Graph Matching with Particle Swarm Optimization. Journal of Multimedia, 4(4), 775–779. https://doi.org/10.4304/jmm.4.4.204-214
8) GU, R. U. I. (2018). Overview of Occlusion Face Recognition Technology. DEStech Transactions on Computer Science and Engineering, ceic, 1–8. https://doi.org/10.12783/dtcse/ceic2018/24539
9) Liu, T., Mi, J.-X., Liu, Y., & Li, C. (2016). Robust face recognition via sparse boosting representation.Neurocomputing,214,944–957. https://doi.org/10.1016/j.neucom.2016.06.071
10) Face recognition. (2008). Biometric Technology Today, 16(10), 9–11. https://doi.org/10.1016/s0969-4765(08)70210-8

11) Darwaish, S. F., Moradian, E., Rahmani, T., & Knauer, M. (2014). Biometric Identification on Android Smartphones. Procedia Computer Science, 35, 832–841. https://doi.org/10.1016/j.procs.2014.08.250

12) Ma, L., Tan, T., Wang, Y., & Zhang, D. (2004). Efficient Iris Recognition by Characterizing Key Local Variations. IEEE Transactions on Image Processing, 13(6), 739–750. https://doi.org/10.1109/tip.2004.827237

j