wjert, 2021, Vol. 7, Issue 4, 162-176. Review Article ISSN 2454-695X

World Journal of Engineering Research and Technology

WJERT

www.wjert.org

SJIF Impact Factor: 5.924

STUDY OF PHYSIOLOGICAL AND BEHAVIORAL BIOMETRIC AUTHENTICATION SYSTEMS

***[1]Dr. Jageshwar K. Keche, [2]Amitabh A. Halder, [3]Prof. Mahendra P. Dhore**

[1]Department of Computer Science, SSESA's Science College, Congress Nagar, Nagpur-12(MS), India.

[2]Department of Computer Science, SSESA's Science College, Congress Nagar, Nagpur-12(MS), India.

[3]Principal, SSESA's Science College, Congress Nagar, Nagpur-12(MS), India.

Article Received on 06/05/2021 **Article Revised on 27/05/2021** **Article Accepted on 17/06/2021**

***Corresponding Author**
Dr. Jageshwar K. Keche
Department of Computer Science, SSESA's Science College, Congress Nagar, Nagpur-12(MS), India.

ABSTRACT

Biometric Authentication Systems plays a vital role in data security. It is widely adopted and accepted technology everywhere to authenticate unique personal identification based on his or her physiological or behavioral traits. Physiological biometrics involves the face, finger-prints, hand geometry, palm-prints, iris, retina patterns, ear, and DNA, while behavioral biometrics includes the signature, voice/speech, keystroke, and gait/walking style. By using biometric authentication system a person could be identified based on "who he/she is" rather than "what he/she has" (id card, token, key) or "what he/she knows" (password or PIN). The various applications of biometric authentication system are now cost-effective, reliable and highly accurate and the need to be addressed form making biometric systems an effective tool for providing information security. This paper have been discussed the various biometrics authentication system, characteristics, challenges and their applications in concern with the human interface.

KEYWORDS: Biometrics, Authentication, Physiological and Behavioral classification.

1. INTRODUCTION

The term "biometrics" is derived from the Greek words 'bio' (life) and 'metric' (to measure). Biometrics[1-6] is the science of identifying or verifying the identity of a person and is receiving growing interest from both academia and industry.[5] Every human being possesses certain unique features in terms of both physiological and behavioral characteristics that are different from everybody. These characteristics are unique to individuals hence the main purpose of biometric authentication system or, simply biometrics is to uniquely identify or verify an individual human.[6,9] Biometric systems verify a person's identity by analyzing his/her physical features like face recognition, fingerprint identification, iris identification, ear identification, hand geometry, palm print identification, retina identification, DNA sequence matching or behavioral feature like signature, keystroke, voice, walking style(gait), etc.

The first and most common thing that comes to mind when speaking of unique features is the fingerprint, which is a physiological characteristic. But there are other characteristics that are more of behavioral in nature, like the way we speak, typing style on a keyboard, the way we write our signature, and several others.[7-8] In the literal and most simple sense, biometrics means the "measurement of the human body". Together, these sets of characteristics are used to identify an individual with a reasonable level of confidence, and can dramatically improve the level of security than the traditional ones. The second things are that the passwords, PINs, smart keys, smart cards and the like are widely used forms of authentication, but have limitations and vulnerabilities. Passwords and PINs can be easily forgotten, hard to remember, or stolen. Smart keys can be easily lost or duplicated/replicated. Smart cards with magnetic strips can be forged. In biometrics these drawbacks exist only in small scale.[1] But a person's biometrics or behavioral traits cannot be stolen, forgotten, or misplaced. As a result, they provide a much more secure and reliable way to authenticate an individual when compared to the traditional methods.

The rest of the paper have been discussed the various biometrics standards, authentication system, characteristics, challenges, advantages and their applications in detail. Concluding remarks are given in the last section.

2. BIOMETRIC AUTHENTICATION SYSTEMS

2.1 Biometric Standard

Biometric plays a very important role to identify and verify (to confirm the identity of a claimant) an individual's identity.[10] As mentioned by A. K. Jain et al.[2], the following standards are applicable identifiers of any human physiological or behavioral traits can be used as a biometric characteristic in terms of related parameters described in table 1.

Table 1: Properties of Physiological or Behavioral traits.

Sr. No.	Parameters	Descriptions
1	Universality	Each person should have unique characteristic.
2	Uniqueness	Any two persons must be different when compared to others in terms of characteristic.
3	Permanence	Biometric features that remains constant over a period of time.
4	Collectability	The characteristic can be quantitatively measureable.
Practically in biometric authentication system, the following important issues should be considered:		
5	Performance	Robustness of techniques used which refers recognition accuracy and speed.
6	Acceptability	It should be user friendly and convenient in everyday life.
7	Circumvention	Which indicates how easily to cheat or fooled the system or use of a substitute.

2.2. Modes of Biometric system

A biometric system is a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database. When the first time user uses a biometric system called as enrolment. During this, biometric information from an individual is captured and stored in the database. Then biometric information is detected and compared with the stored information at the time of enrolment. The sensor is the interface between the real world and the system. Any biometric system includes two different modes: verification mode and identification mode.

Verification mode

Biometrics can also be used to verify a person's identity. In the verification process, the system compares the captured biometric data with the template stored in the database. For example, an individual who desires to be verified claims an identity, usually via a PIN (Personal Identification Number), a user name, a smart card, etc. Another example, one can grant physical access to a secure area in a building by using finger scans or can grant access to a bank account at an ATM by using retinal scan, and the system performs a one-to-one

comparison to validate the veracity of the claim. This mode is typically used for positive recognition where the aim is to prevent multiple people from using the same identity.

Identification mode

Biometrics can be used to determine a person's identity even without his knowledge or consent. Scanning a crowd with a camera and using face recognition technology, one can determine matches against a known database or using a fingerprint/face as part of the login process to a computer is an example of biometric identification. In identification mode, the system recognizes the user by searching the templates of all users in the database. In this case, the comparison is one-to-many. This mode is typically a negative recognition application. The main purpose of negative recognition is to prevent a single person from using multiple identities.

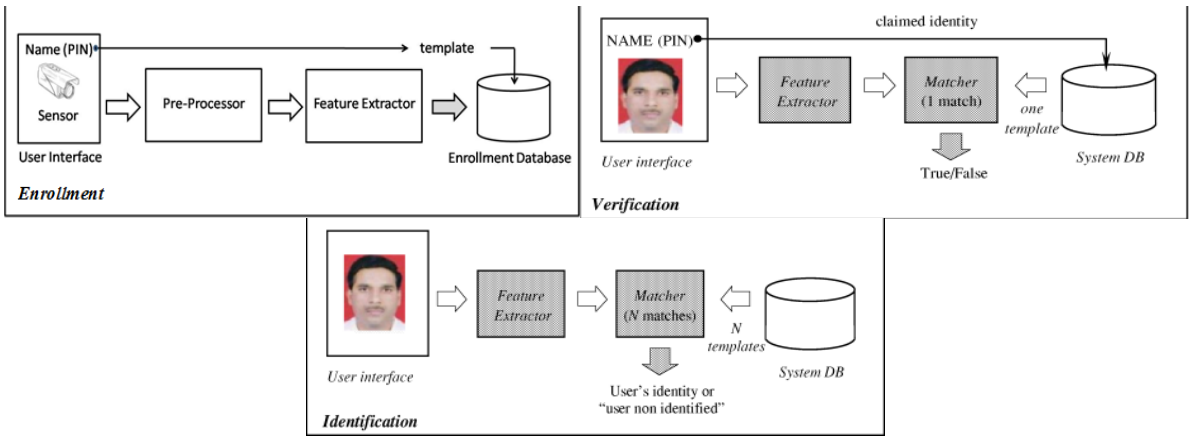

Figure 1: Block diagram of a biometric system.[2]

3. BIOMETRIC CLASSIFICATION

Biometrics authentications are classified into two types Physiological and Behavioral. Physiological biometrics used for identification or verification purposes. Identification refers to determining who a person is. This method is commonly used in criminal investigations. Behavioral biometrics is used for verification purposes. Verification is determining if a person is who they say they are. This type of biometric looks at patterns of how certain activities are performed by an individual.

Biometrics uses characteristics[2][6][11-12] that can be physiological such as face, fingerprint, hand geometry, palm-print, iris, retina scan, ear, and DNA. Biometrics use characteristics that are behavioral traits such our signature, keystroke, walking style (gait), speech or voice the way we speak or use a computer. Biometric is not optimal to meet the requirements of all the

applications. The match between a specific biometric and an application is determined depending upon the operational mode of the application and the properties of the biometric characteristic.[2]

3.1. Physiological Biometrics

Face: Face is one of the most acceptable biometrics because of most common method of identification which use in their visual interaction. There are two primary approaches to the identification based on face recognition. The first approach is Transform approach.[13-14] The facial attributes like eyes, eyebrows, nose, mouth, shape of the face, shape of the mouth, etc are extracted from the face images for the identity of a person. The invariance of geometric properties among the face features is used for recognizing the face. The various face databases such as ORL, JAFFE, Yale, Face94, FERET database etc., are used to obtain the recognition rates. As mentioned by Anil K. Jain et al., the two most popular recognition approaches are[2]:

- Measuring the location and shape of facial attributes;
- Analyzing the overall face image as "a weighted combination of a number of canonical faces".

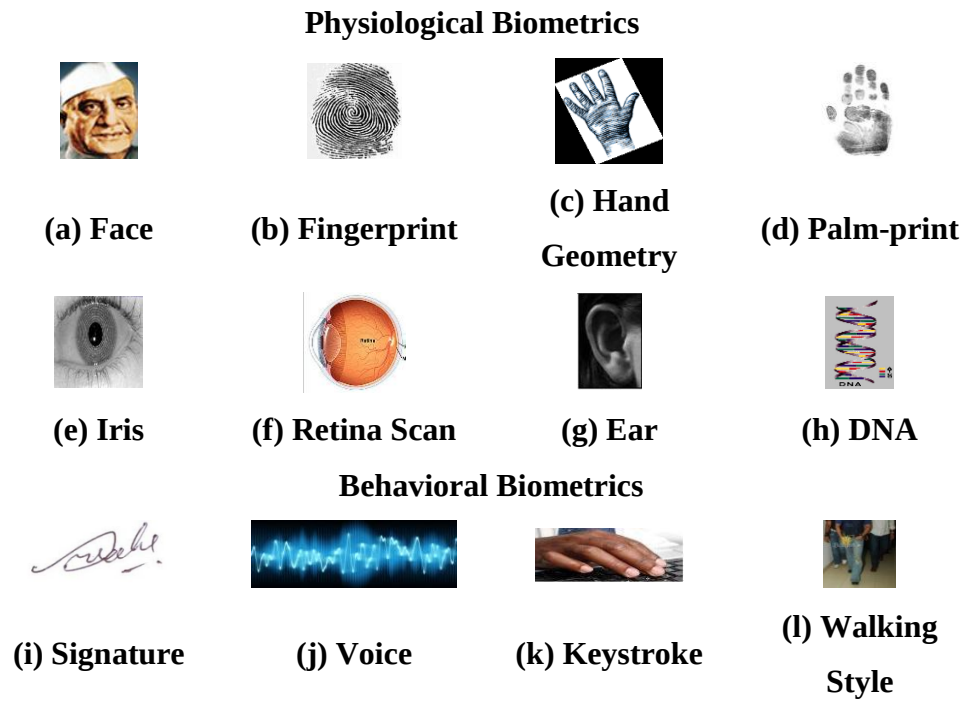

Figure 2: Biometric Classification.

Fingerprint: Fingerprint identification is well established and a mature science. It has also been extensively tested in various legal systems and is accepted as an international standard for identification. The law enforcement agencies are principle users of fingerprints; various

electronic readers are now commonly available and are used for authentication purposes, mainly in access control applications. No two individuals have been found to have identical fingerprints. Smooth and clean surfaces record better quality fingerprints but fingerprints can also be found on irregular surfaces such as paper. There are three basic categories of fingerprint:[15]

- Visible prints or patent made in oil, ink or blood
- Latent prints which are invisible under normal viewing conditions; and
- Plastic prints which are left in soft surfaces such as new paint.

Hand Geometry: The recognition of human hand based on the many measurements including its shape, size of palm, and length and width of the fingers.[16] The actual shape and dimensions of your hand are sometimes used for access control and time-and-attendance operations in the workplace. That shape of a person's hand (after a certain age) does not significantly change its shape. As compared to some other biometric identification (fingerprints), hand geometry does not produce a large data set. The physical size of a hand geometry-based system is large, and it cannot be embedded in certain devices like laptops.[17] Therefore a large number of records, hand geometry biometrics may not be able to distinguish one individual from another who has similar hand characteristics.

Palm-print: The palm is a pattern of ridges and valleys as like the fingerprints. The study of palm print is an ancient practice to know the personal details of a person and also for the astrologers. Palm features[18] are unique for an individual with rich information on it like principal lines and wrinkles, textures and ridges are used for identifying a person. Palm features are extracted using high or low resolution cameras. The features of the palm such as geometry of hand, ridge and valley features, principal lines, and wrinkles may be combined to build a highly accurate biometric system. Latent palm print is of growing importance in forensic applications.

Iris: Iris biometrics is the unique feature characteristics of human iris because it remains unchanged individuals lifetime. The iris is the annular region of the eye bounded by the pupil and the sclera (white of the eye). The complex iris texture carries very distinctive information useful for personal recognition.[19-20] Early iris-based recognition technique required considerable user participation and were expensive. The newer systems have become more users friendly and cost effective. While iris system have a very low false Accept Rate (FAR)

compared to other biometrics traits, the False Reject Rate (FRR) of these systems can be rather high.[21]

Retina Scan: Retinal scan is the example of secure biometrics because it is not easy to change or replicate the retinal vasculature.[22] Basically the retina is a thin nerve on the back of the eye. It is a part of eye which senses light and transmits impulses through the optic nerve to the brain. Blood vessels used for identification which are located along the neural retina. This technique involves using a low-intensity infrared light source through an optical coupler to scan the unique patterns of retina. The reflection of vascular information is being recorded. Retina scanning works for identification as well as verification. The additional advantages include the small template size and good operational speed.

Ear: The shape of an ear is different from person to person. An ear biometric is based on matching the distance of salient points on the pinna from a landmark location on the ear. The features of ear are very distinctive in establishing the identity of an individual user.[23] A sensor such as a camera collects a side profile image of the user's head, from which the system automatically locates the ear and isolates it from the surrounding hair, regions of the face, and the user's clothes. A combination of color and depth analysis algorithm is used to localize the ear pit and then generates an outline of the visible ear region.

DNA: DNA (Deoxyribonucleic Acid) provides the most reliable form of identification of all the biometric identification systems. It is powerful digital and unchangeable during a human's life and even after death. Deoxyribonucleic acid (DNA) can be collected from various sources such as blood, finger nails, hair, mouth swabs, saliva, straws, etc., that has been attached to the human body. DNA is currently used mostly in forensics applications for identifying people. DNA biometrics differs from standard biometrics in several ways[24]:

- DNA requires a tangible physical sample as opposed to an impression, image, or recording.
- DNA matching is not done in real-time, and currently not all stages of comparison are automated.
- DNA matching does not employ templates or feature extraction, but rather represents the comparison of actual samples.

DNA matching has become a popular use in criminal trials. There are many complexities surrounding the issue of biometrics of DNA, such as biometrics and health issues, private information, access to DNA and data. The process of DNA is slowly and costly.[25-26]

3.2. Behavioral Biometrics

Signature: Signature verification uses behavioral biometrics of a hand written signature to confirm the identity of a person. A person does not make a signature in a fixed manner; hence the data obtained from any one signature from an individual has to allow for a range of possibilities. Signature recognition is based on the dynamics of making the signature like acceleration rates, directions, pen pressure, stroke length, etc., rather than a direct comparison of the signature after it has been written.[27] The major difficulty with this technology is to differentiate between the consistent parts of a signature. These are the characteristics of the static image and the behavioral parts of a signature which vary with each signing.

Voice: Our voices are uniquely different to each person, and cannot be exactly replicated. Voice is a combination of physiological and behavioral characteristics of a person. Speech or voice recognition systems can discriminate between two very similar voices, including twins. The features of individual's voice are based on the shape and size of vocal tracts, mouth, nasal cavities and lips that are used in the synthesis of sound.

The benefits of voice biometric systems are mostly used for telephone-based applications.[28] It can be automated and used with speech recognition. The weakness of the system is a high false non-matching rate. Speaker/voice verification focuses on the vocal characteristics that produce speech and not on the sound or the pronunciation of the speech itself. Voice verification is used for call centres, healthcare, government, electronic commerce, financial services, and customer authentication for service calls.

Keystroke: Keystroke biometrics or typing dynamics is the detailed timing information that describes exactly when each key was pressed and when it was released as a person is typing at a computer keyboard.[29] The behavioral biometric of keystroke dynamics uses the manner and rhythm in which an individual types characters on a keyboard or keypad. The keystroke rhythms of a user are measured to develop a unique biometric template of the users typing pattern for future authentication. Such type of technique is classified into two types like static and dynamic verification techniques. The static verification uses a neural network approach while the dynamic verification is using statistics.

Walking style (Gait): The walking style of a person is also known as the Gait of the person. Gait is a behavioral biometric and may not remain invariant, especially over a long period of time, due to fluctuations in body weight, major injuries involving joints or brain. It is more specific as a study of human motion, using the eye and the brain of observers, augmented by instrumentation for measuring body movements, body mechanics, and the activity of the muscles.[30] Gait is not supposed to be very distinctive, but is sufficiently discriminatory to allow verification in some low-security applications.

Table 2: Comparison of Biometrics based on Physiological & Behavioral parameters[31-32]

Biometrics	Circumvention	Permanence	Acceptability	Uniqueness	Universality	Collectability	Measurability
Face	Low	Medium	High	High	High	High	High
Fingerprint	High	Medium	Medium	High	Medium	Medium	High
Hand	Medium	Low	Medium	Medium	High	Medium	Medium
Palm Print	Medium	Medium	Medium	Medium	Medium	Medium	High
Ear	Low	High	High	High	Medium	High	High
Iris	Low	Medium	Low	High	Medium	Low	High
Retina	Low	Medium	Low	High	Medium	Low	High
DNA	Low	Medium	High	High	Medium	Low	Low
Signature	High	Medium	Medium	High	Low	Medium	High
Voice	High	Medium	High	Medium	High	High	High
Keystroke	Medium	Medium	High	Medium	Medium	Medium	Medium
Gait	Low	Medium	High	Medium	High	High	Medium

4. CHALLENGES, ADVANTAGES AND APPLICATIONS

4.1 Challenges

Some of the possible challenges/difficulties in Physiological and Behavioral Authentication for a machine are listed below.

- Face recognition is an eminent biometric trait offers several challenging tasks. Some of them are pose variation; illumination-different lighting conditions; persons wearing collusions such as hat, scrap, eye glasses, etc.; aging effect; various facial expressions degrades the performance of the system.
- The recognition rate of biometric profile degrades when the finger is wet and wrinkled. Research needs to be focused to address when the finger is wet and wrinkled towards development of system.
- The research should be advanced to reduce the hardware requirements.
- The recognition rate degrades, when the human eyes are covered by some occlusions and if the face images with various facial expressions are captured from the device.
- Research in this area needs to be more improved to assure its reliability against important factors namely contact lenses, eye glasses, watery eyes etc.
- In retinal scan, it has to be developed to distinguish and identify individual wearing glasses or lens.
- DNA approach is not automatic and the method of acquisition of samples needs to be developed.
- Keystroke technology has to be developed more to increase the accuracy.
- Long term reliability and lack of accuracy are the main issues to be focused in signature approach.
- In speech recognition, the technology needs to be advanced to store the unique digital code by decreasing the space. And also, the accuracy degrades, when the person's voice changes.

4.2 Advantages & Applications

The advantages of adopting biometrics for authentication of an individual are listed below.

- **Security:** The biometric systems offer a higher degree of security than conventional methods. Security is a primary concern at airports, harbor, ATM machines, border checkpoints, network security, control accesses to buildings, and e-mail authentication on multimedia workstations. Face recognition technology have been implemented at many airports around the world as a security purpose.

- **Accountability:** The biometric-based authentication systems are able to keep track of the user's activities. Better alternate of saving time and resources.
- **Scalability:** The biometric-based authentication systems are easily scalable. No remembering of passwords or login ID's is required. Elimination of need of carrying authorized documents.

Computer vision applications are universally used in digital camera, mobile phones, security areas, cars, toys, hospitals, airports. The primary applications of biometric authentication systems are person verification (matching) and person identification (one-to-many comparison). Some of the applications of biometric systems are[33-34] access control application can achieve high accuracy, surveillance, image database investigations, general identity verification, smart card applications, criminal analysis systems, automatic attendance and time monitoring in classes, banking systems, boarding pass for personal authentication, home security systems, electronic voting and ATM machine to secure an individual, military force to authenticate refugee; also schools, colleges, companies, government offices, and other private sectors to authenticate employees, Entry to high security places such as parliamentary house and defense zone.

5. CONCLUSION

Biometric Authentication System is widely adopted and accepted technology everywhere to authenticate an individual’s human identity. This paper makes a review study of the existing Physiological and Behavioral biometric methodologies, advantages, comparisons of various biometrics traits and applications. The advantages of adopting biometrics for authentication of an individual are meaningful for the society. The research needs to be more focused to address above challenges in order to implement reliable biometric recognition system. The biometric features can be easily acquired and measured for the processing only in the presence of a person. The biometric recognition systems have been proved to be accurate and very effective in different applications. The use of biometrics raises several privacy questions such as in case of face recognition privacy will be wiped out. In spite of all these, it is quite sure that in future biometric based recognition will have a great influence on our day-to-day life. Scientific work is very important for future applications and progress in the biometrics.

REFERENCES

1. Ratha, N.K., Senior, A., and Bolle, R.M., "Automated Biometrics in Proceedings of International Conference on Advances in Pattern Recognition", Rio de Janeiro, Brazil, March 2001.
2. Anil K. Jain, Arun Ross and Salil Prabhakar, "An Introduction to Biometric Recognition", IEEE Transactions on Circuits and Systems for Video Technology, January 2004; 14(1).
3. K P Tripathi, "A Comparative Study of Biometric Technologies with Reference to Human Interface", International Journal of Computer Applications (0975 – 8887), January, 2011; 14: 5.
4. Rhien-Lien Hsu, Mohamed Abdel-Mottabel, Anil K. Jain. "Face Detection in Color Images", IEEE Trans. Pattern Analysis and Machine Intelligence, May, 2002; 24(5): 696.706.
5. Special issue on Biometrics, Proceedings of the IEEE, September, 1997; 85(9).
6. J. K. Keche, Dr. M. P. Dhore. "An Overview of Biometric Technologies", UGC Sponsored National Conference on Emerging Trends in Information Technology & Business Computing (ITBC-2012), ISBN No: 978-81-921416-7-1. Organized by Department of Computer Education, Dhanwate National College, Nagpur, 369-379.
7. Kresimir Delac and Mislav Grgic, "A Survey of Biometric Recognition Methods," IEEE International Symposium on Electronics in Marine, 2004; 184-193.
8. Manuel R Freire, Julian Fierrez and Javier Ortega Garcia, "Dynamic Signature Verification with Template Protection using Helper Data," IEEE International Conference on Acoustics, Speech and Signal Processing, 2008; 1713-1716.
9. Jammi Ashok, vaka shivashankar,"An overview of Biometrics". International Journal of Computer Science and Engineering (IJCSE), 2010; 02(07).
10. Ashraf S Huwedi and Huda M Selem, "Face Recognition using Regularized Linear Discriminant Analysis under Occlusions and Illumination Variations", IEEE International Conference on Control Engineering and Information Technology, 2016; 1-5.
11. Joseph N. Pato and Lynette I. Millett, Editors; Whither Biometrics Committee; National Research Council (2010), "Biometric Recognition: Challenges and Opportunities".
12. National Science & Technology Council's (NSTC) Subcommittee on Biometrics, (September 2006) "Biometrics Frequently Asked Questions".
13. M. Turk and A. Pentland, "Eigenfaces for recognition", Journal of Cognitive Neuroscience, 1991; 3(1): 71-86.

14. D. Swets and J. J. Weng, "Using discriminant eigen features for image retrieval", IEEE Trans. Pattern Analysis and Machine Intelligence, August, 1996; 18: 831-836.
15. Chris Roberts, "Biometric Technologies – Fingerprints", February 2006.
16. R. Zunkel, "Hand Geometry based Authentication".
17. Eric Kukula and Stephen Elliott, "Implementation of hand geometry an analysis of user perspectives and system performance", IEEE A&E Systems Magazine, Mar. 2006; 3-9.
18. Website: http://biometrics.cse.msu.edu/Publications/GeneralBiometrics/JainKumarNextGenBiometrics_BookChap10.pdf
19. J. G. Daugman, "High confidence visual recognition of persons by a test of statistical independence," IEEE Trans. Pattern Analysis and Machine Intelligence, 1993; 15(11): 1148-1161.
20. J. G. Daugman, "How Iris recognition works?" IEEE Trans. On circuits and systems for video technology, 2004; 14(1): 21-30.
21. Arun Ross and Anil K. Jain, "Human Recognition Using Biometrics: An Overview", Appeared in Annals of Telecommunications, Jan/Feb, 2007; 62(½): 11-35.
22. RAYCO Security, "Eyedentify retina biometric reader," http://www.raycosecurity.com/-hirsch/EyeDentify.html, 1997.
23. Kyong Chang, Kevin W. Bowyer, Sudeep Sarkar, and Barnabas Victor, "Comparison and combination of ear and face images in appearance-based biometrics", IEEE Transactions on Pattern Analysis and Machine Intelligence, Sep. 2003; 25(9): 1160-1165.
24. Sandra Maestre, and Sean Nichols, 'DNA Biometrics", ISM 4320-001.
25. De Santos Sierra, "A fuzzy DNA-based algorithm for identification and authentication in an iris detection system", ICCST, 2008; 226-232.
26. Federal Bureau of Investigation Educational Internet Publication, "DNA testing," http://www.fbi.gov/kids/dna/dna.htm, 1997.
27. Sourav Ganguly and Subhayan Roy Moulick, "A Review on Different Biometric Techniques", International Journal of Engineering Research & Technology (IJERT), July, 2012; 1(5). ISSN: 2278-0181.
28. Hong Kook Kim, Cox, R.V., and Rose, R. C., "Performance improvement of a bitstraem-based front-end for wireless speech recognition in adverse environments", IEEE Transactions on Speech and Audio Processing, Nov. 2002; 10(8): 591–604.
29. Checco, J. Keystroke Dynamics & Corporate Security. WSTA Ticker Magazine, 2003.

30. Whittle, Michael (2007). Gait Analysis: an Introduction (4th Ed.), Butterworth-Heinemann. ISBN 0-7506-8883-1. http://www.amazon.com/An-Introduction-Gait-Analysis-4e/dp/0750688831.
31. Gursimarpreet Kaur and Chander Kant Varma, "Comparative Analysis of Biometric Modalities", International Journal of Advanced Research in Computer Science and Software Engineering, 2014; 4(4): 603-613.
32. Sunil Swamilingappa Harakannanavar1, et. al., "Comprehensive Study of Biometric Authentication Systems, Challenges and Future Trends", Int. J. Advanced Networking and Applications, 2019; 10(04): 3958-3968. ISSN: 0975-0290.
33. Divyarajsinh N. Parmar, Brijesh B. Mehta, "Face Recognition Methods & Applications", Int. J. Computer Technology & Applications (IJCTA), Jan-Feb, 2013; 4(1): 84-86. ISSN:2229-6093.
34. J. K. Keche and Dr. M. P. Dhore, "Comparative Study of Feature Extraction Techniques for Face Recognition System", International Conference on Recent Trends in Computing, 7-8 April, 2012, Proceedings published by International Journal of Computer Applications® (IJCA), ISSN: 0975–8887.