Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.777654

BIOMETRIC RECOGNITION: CHALLENGES AND OPPORTUNITIES

Mudunuru Suneel[1], Dr T. Ranga Babu[2]

[1.] Ph.D Research Scholar, Department of ECE, University College of Engineering, Acharya Nagarjuna University (ANU), Guntur, AP, India.

[2.] Professor & HoD, Department of ECE, RVR & JC College of Engineering, Guntur, AP, India.

*Correspondence E-Mail: suneel007@gmail.com

ORCID: 0009-0002-1200-9830

Abstract: The study has discussed the implication of the biometric system and the related advantages and disadvantages of the system. Additionally, the study has helped to highlight the different implications of biometric systems in a systematic manager. Thus, such discussion helped to understand the advantages and disadvantages related to biometrics. At the time of implementing biometric systems have some specific problems which hinder the process of the implication of biometric systems. Therefore, such implication is related to the security of collected data. It has been seen that there is a problem with security thus implementing mimetic is simplified. At the same time, the discussion related to the implication of biometric is discussed in the analysis. Additionally, the discussion of biometrics is discussed with an appropriate model and with a related problem. Therefore, the implication of biometric devices and their challenges provide a detailed discussion of the topic.

Keywords: Biometric Recognition, Biometric devices, Biometric information.

1. Introduction

Biometric recognition is the process of identifying or verifying the identity of an individual based on unique physiological or behavioral traits such as fingerprints, face, voice, iris, gait, and others. Biometric recognition has been widely adopted in various fields such as security, law enforcement, finance, healthcare, and others. The advancement of biometric recognition technology has brought about numerous opportunities and benefits, but it also poses various challenges that need to be addressed. This review paper aims to explore the challenges and opportunities of biometric recognition. Advancements in technology have presented different opportunities to the lives of humans at the same time three there are different challenges of modern technology [1]. Moreover, such challenges hinder the process of implication for modern technology. Thus, this study has focused on the technology of Biometric identification and the advantages of the smart [3]. In addition, an advantage of the same is discussed in the study which helped to understand the implication of biometrics in different uses. At the same time, opportunities and challenges help to understand the overall solution that can improve the implication of biometrics. Additionally, appropriate models and theories are used in the study in order to describe the appropriate use of the biometric system [2].

1.1. Challenges:

One of the primary challenges of biometric recognition is the accuracy and reliability of the technology. Although biometric recognition has a higher accuracy rate than traditional identification methods such as passwords and PINs, it is not 100% accurate. Factors such as lighting conditions, image quality, and physiological changes can affect the accuracy of biometric recognition. Another challenge is privacy and security concerns. The collection, storage, and use of biometric data raise privacy concerns, and the potential misuse of biometric data can lead to identity theft and fraud. Moreover, biometric recognition systems can be vulnerable to hacking and cyber-attacks, which can compromise the security of the system.

Another significant challenge of biometric recognition is the potential for bias and discrimination. Biometric recognition technology can be biased towards certain demographic groups, leading to false positives or false negatives. For instance, facial recognition technology has been shown to have higher error rates for people of color and women. Such biases can result in discrimination and lead to unfair treatment.

1.2. Opportunities:

Despite the challenges, biometric recognition technology has numerous opportunities and benefits. One significant opportunity is enhancing security and safety. Biometric recognition systems can be used to secure facilities and prevent unauthorized access, reduce fraud in financial transactions, and aid in criminal investigations.

Another opportunity is improving the efficiency of various processes. Biometric recognition can streamline processes such as voter registration, healthcare access, and transportation systems. Moreover, biometric recognition can aid in providing personalized and convenient services such as unlocking phones and making payments.

Additionally, biometric recognition technology has the potential to contribute to public health by identifying infectious diseases and tracking outbreaks. Biometric recognition can be used to detect early signs of diseases such as COVID-19 by monitoring symptoms and temperature.

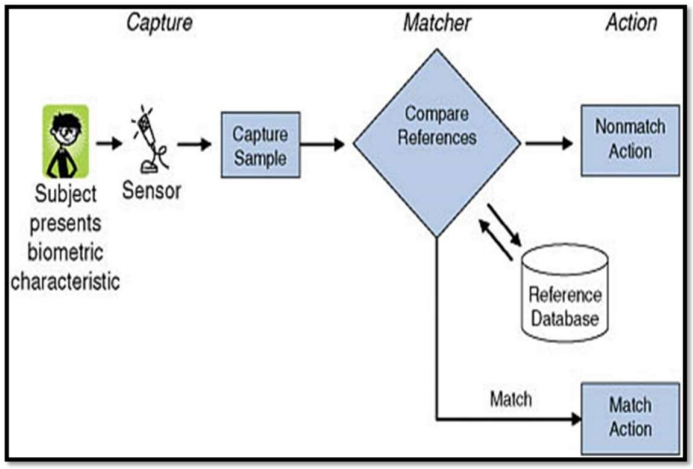

Figure 1: Different aspects of Biometric recognition data base **[3]**

2. OBJECTIVES

For the development of the study, a proper guideline was required. Therefore, the following objectives were created that guided the study:

- To analyse the importance of biometrics in the modern world
- To discuss different use of biometric
- To observe biometric with the help of modern theories and model
- To analyse opportunities for biometric technology
- To describe the challenges of using biometric
- To analyse the related problems of biometric technology

In addition to the above objectives Biometric recognition is also having following points to be considered

The study was guided by a set of objectives to provide a framework for development. These objectives included:

1. To examine the significance of biometric recognition in contemporary society.
2. To explore various applications of biometric recognition technology.
3. To investigate biometric recognition using modern theories and models.
4. To assess potential opportunities for biometric recognition technology.
5. To identify challenges associated with the implementation of biometric recognition technology.
6. To analyze related issues and concerns surrounding the use of biometric recognition technology.

These objectives were intended to guide the study and provide a comprehensive understanding of biometric recognition technology, including its importance, potential applications, opportunities, challenges, and related concerns.

3. METHODOLOGY

For the development of a study, there are different steps that help to reach the final results. Such steps combine to form the methodology of a study. In addition, the methodology of a study helps to formulate an ethical basis and helps to maintain the Interiority of the study [2]. In addition, the methodology of a study plays an important role for discusses the results and appropriately following the set objectives of the study. Thus in order to discuss the opportunity and threats presented by the use of the biometric secondary qualitative method was used [6]. In order to collect data secondary sources were analysed. Furthermore, for analysing the collected data qualitative method was used. The secondary qualitative method of analysis further helps to implement a rational analysis through observing fractal data for the research. Thus secondary qualitative methods of analysis are used for the development of the study.

Biometric recognition refers to the process of identifying individuals based on their unique biological traits, such as fingerprints, facial features, iris patterns, or voiceprints. There are several different biometric recognition methods, each with their own unique methodology.

Fingerprint recognition: This is one of the most widely used biometric recognition methods. It involves capturing an individual's fingerprint image, which is then converted into a digital template. The template is compared with a database of known fingerprints to identify the individual.

Facial recognition: This method involves capturing an image of an individual's face, which is then analyzed to extract unique facial features. These features are compared with a database of known faces to identify the individual.

Iris recognition: This method involves capturing an image of an individual's iris, which is then analyzed to extract unique iris patterns. These patterns are compared with a database of known irises to identify the individual.

Voice recognition: This method involves capturing an individual's voice sample, which is then analyzed to extract unique voiceprints. These voiceprints are compared with a database of known voiceprints to identify the individual.

Retina recognition: This method involves capturing an image of an individual's retina, which is then analyzed to extract unique retina patterns. These patterns are compared with a database of known retinas to identify the individual.

Hand geometry recognition: This method involves capturing an image of an individual's hand, which is then analyzed to extract unique hand geometry features, such as finger length and hand size. These features are compared with a database of known hand geometries to identify the individual.

In general, the methodology of biometric recognition involves capturing a sample of the individual's unique biological trait, processing the sample to extract relevant features or patterns, comparing those features or patterns with a database of known samples, and then making a determination of identity based on the degree of similarity between the samples. The specific details of each method may vary depending on the technology used and the application in which it is being used.

Identifier	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	High	Low	Medium	High	Low	High	Low
Fingerprint	Medium	High	High	Medium	High	Medium	Medium
Hand Geometry	Medium	Medium	Medium	High	Medium	Medium	Medium
Hand Vein	Medium	Medium	Medium	Medium	Medium	Medium	High
Iris	High	High	High	Medium	High	Low	High
Retinal scan	High	High	Medium	Low	High	Low	High
Signature	Low	Low	Low	High	Low	High	Low
Voice print	Medium	Low	Low	Medium	Low	High	Low
F.Thermo grams	High	High	Low	High	Medium	High	High

Table 1: Comparison of different biometric recognition systems [10]

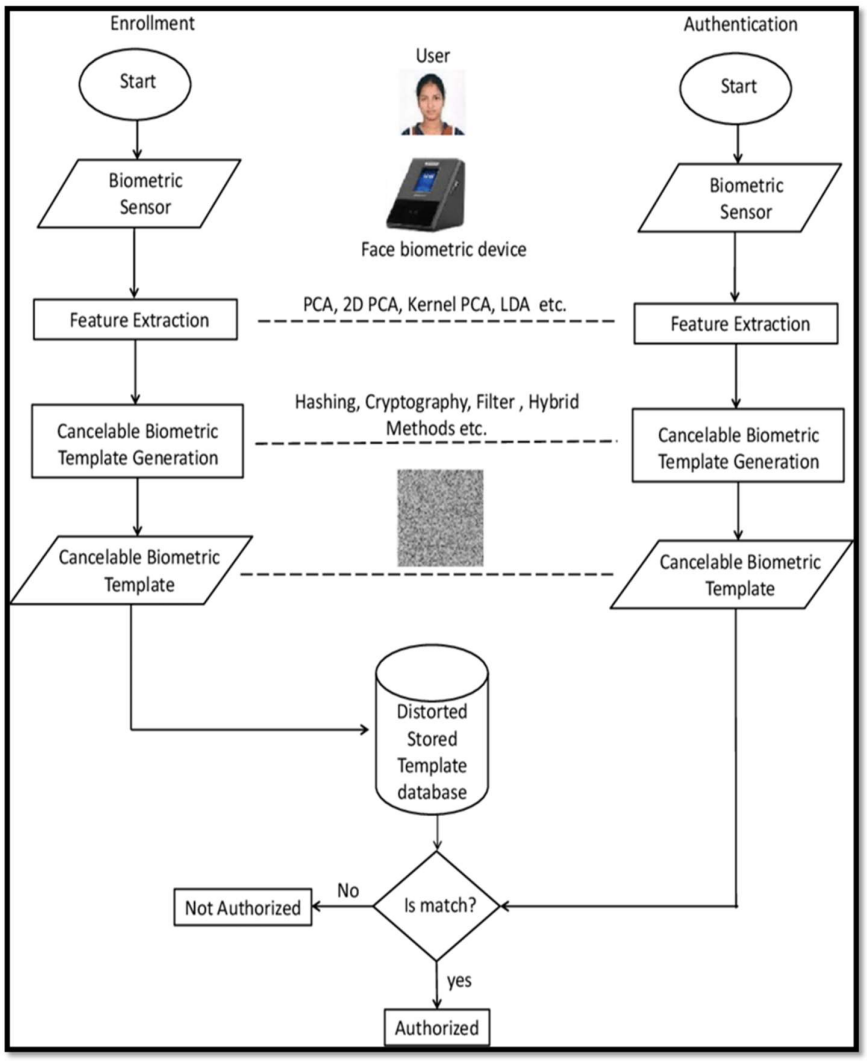

Figure 2: Flowchart of using biometric recognition system [5]

4. ADVANTAGES OF USING BIOMETRIC DEVICES

A biometric device is related to individual data. For instance, biometric identification is related to the Irish, fingerprints or other biometric details. Thus it can be more secure than other ways. For instance, a lock can have a different key, or a password can be shared. However biometric information cannot be shared with other.

Biometric recognition has several advantages over traditional forms of identification and authentication methods:

Accuracy: Biometric recognition systems have a high level of accuracy since they are based on unique physical or behavioral characteristics of an individual. This makes it difficult for others to impersonate or cheat the system.

Security: Biometric recognition provides high security since the biometric traits are difficult to fake or reproduce, making it harder for unauthorized individuals to access secured areas or information.

Convenience: Biometric recognition eliminates the need for physical tokens, such as keys or cards, or memorizing passwords or PINs, making it convenient for users to access their devices or secure areas.

Efficiency: Biometric recognition systems can process large volumes of users quickly, making it useful in high-traffic areas or situations where rapid identification is required.

User-friendly: Biometric recognition is user-friendly since it eliminates the need for users to remember passwords or carry physical tokens, which can be lost or stolen.

Scalability: Biometric recognition can be easily scaled up to accommodate more users or to cover a larger area, making it ideal for organizations with rapidly growing user bases.

Overall, biometric recognition offers a secure, convenient, and accurate way to identify individuals, making it an increasingly popular choice for authentication and identification purposes.

4.1. CONVENIENCE OF USING BIOMETRIC DEVICES

Biometric information is a convenience as there is no key or other elements that need to be carried similarly there is no password to remember [5]. A person's individual data is related to the identification of a person. Therefore, the implication of biometric is convenient. Improvements in technology have presented different implications of the technology. In addition improvement in technology further helps to reduce the time for different processes. Additionally, security is directly related to the implication of biometrics.

The COVID-19 pandemic has led to a significant increase in the adoption of biometric recognition systems, and there are several advantages of these systems in this situation:

1. Touchless identification: Biometric recognition systems, such as facial recognition, fingerprint recognition, or iris recognition, enable touchless identification, eliminating the need for physical contact and reducing the risk of infection transmission.
2. Improved security: Biometric recognition systems provide a more secure and reliable way of verifying an individual's identity, reducing the risk of fraud or identity theft.
3. Contact tracing: Biometric recognition systems can be used for contact tracing, helping to track and identify individuals who have been in close contact with an infected person.
4. Health screening: Biometric recognition systems can be used for health screening, such as temperature checks, to detect potential COVID-19 symptoms and prevent infected individuals from entering premises.
5. Efficient data collection: Biometric recognition systems can efficiently collect and store data on individuals, allowing for quick and accurate identification and tracking of potential COVID-19 cases.

Overall, biometric recognition systems have several advantages in the COVID-19 situation, providing a safer and more secure way of identifying individuals while minimizing the risk of transmission.

4.2. FRAUD RESISTANCE

One of the major elements of biometrics is that they are individual to each person [7]. Thus it can be understood that fraud resistance is a major advantage of biometric. Therefore, some

government uses biometrics as a major technology to keep an account of their citizens. Spoofing detection and fraud presentation attack detection of biometric systems is also an additional advantage.

Fraud detection is an important aspect of biometric recognition technology, as it helps to ensure the accuracy, reliability, and security of biometric data. The following are some of the ways in which fraud detection is used in biometric recognition:

Spoofing detection: Spoofing involves presenting a fake biometric sample to the recognition system, such as a fake fingerprint or face image. Fraud detection algorithms are used to detect such spoofing attempts by analyzing the biometric data for unusual patterns or anomalies.

Liveness detection: Liveness detection is a method used to ensure that the biometric sample being presented to the system is from a living person and not a fake representation. This can be achieved by analyzing various physiological or behavioral characteristics of the person, such as eye movements or changes in skin colour.

Data integrity checks: Fraud detection algorithms can be used to check the integrity of the biometric data being used, such as detecting any tampering or manipulation of the data.

Multi-factor authentication: Biometric recognition can be combined with other authentication factors, such as passwords or smart cards, to provide an additional layer of security and fraud detection.

Overall, fraud detection is a critical component of biometric recognition technology, as it helps to ensure the accuracy and reliability of biometric data and prevent unauthorized access or fraudulent activities.

5. DISCUSSIONS & CONCLUSION

During the analysis it was observed that cost of a biometric system installation is a major drawback. Moreover, the cost of an overall biometric system and the cost of installation are hindering the implication [9]. In addition, it can be said that the cost of biometric systems is the major reason that is not allowing small businesses to implement biometrics. On the other hand, issues related to data breaches are there which major issues [8]. A biometric system generally is used as a security device and attendance device for different office offices. Similarly, some country uses biometric for the identification of their cities. Therefore, a data breach is a major issue that can cause harm at the time of implementing biometric for a business [10].

At the same time, tracking of data stored in a biometric system is a major problem. Further, it was seen that lack of knowledge is an issue hindering the implication of biometric. Additional security is a major issue related to the implication of biometrics.

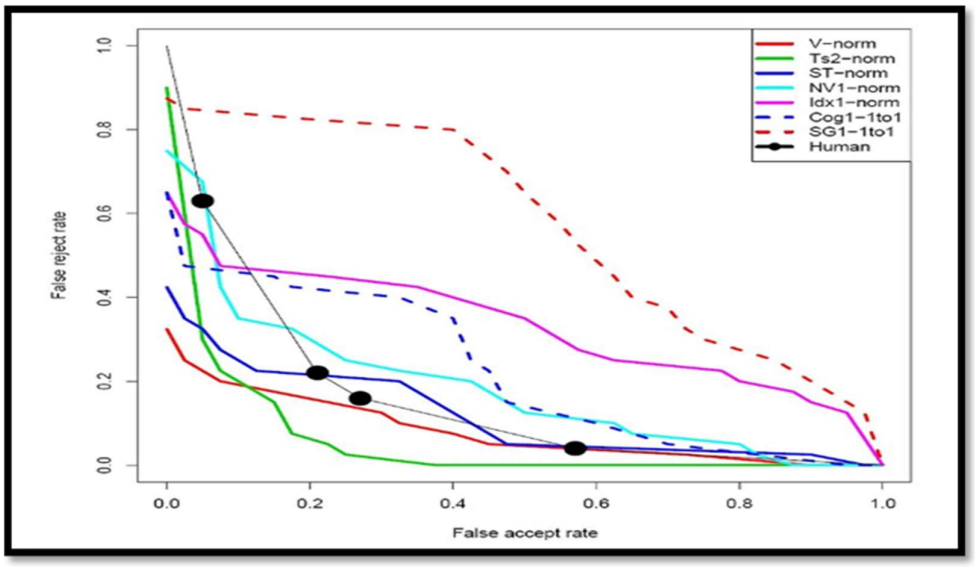

Figure 4: Graph showing the rate of facial recognition **[7]**

Thus, the study has discussed the implication of biometric systems at the same time the advantages and disadvantages are discussed in the study. In order to analyse the implications of the different biometric systems a secondary qualitative analysis method was used that helped to understand the challenge and opportunities from the use of secondary data. In addition, secondary sources like past literature and journals were used for the study. The advantages of using a biometric system are described in the study that helped to conduct a comparative analysis.

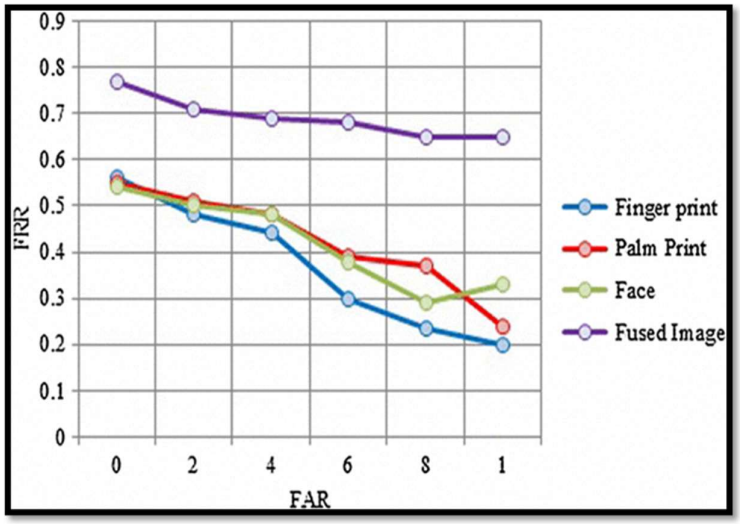

Figure 5: Different methods used for the recognition of biometrics **[7]**

Different use of biometric systems is described in the study that helped to understand factors related to implications. Additionally, the implication of biometric is analysed with appropriate models and theories thus a detailed discussion is conducted in order to describe

comparatively discuss the challenges and opportunities associated with the implication of biometric.

In this review we observed there are several advantages of using face biometric technology (that suits the prevention against COVID) compared to fingerprint and iris biometric technologies, some of which include:

Non-intrusive: Unlike fingerprint and iris biometric technologies, which require physical contact or close proximity, face recognition can be performed at a distance without any physical contact. This makes face recognition a non-intrusive and more convenient option.

High accuracy: Face recognition technology has made significant advancements in recent years, and its accuracy is comparable to that of fingerprint and iris recognition. Additionally, face recognition can recognize a person from a distance and in different lighting conditions, making it more accurate than other biometric technologies in certain situations.

Easy to use: Face recognition technology is very user-friendly and does not require any specialized training or equipment. It can be easily integrated into existing security systems and can be used by anyone without any difficulty.

Wide range of applications: Face recognition technology can be used in a wide range of applications, including security, surveillance, access control, and identification. It is also being used in various industries such as retail, banking, and healthcare, among others.

Cost-effective: Compared to other biometric technologies, face recognition technology is relatively cost-effective. It does not require specialized equipment or hardware, which makes it a more affordable option for businesses and organizations.

Contactless identification: Face recognition systems are contactless, which means that there is no need for physical contact between the user and the system. This reduces the risk of spreading infections, such as COVID-19, through touch.

Hygienic: Face recognition systems do not require users to touch any surfaces, such as fingerprint scanners, which can be potential breeding grounds for viruses and bacteria. This reduces the risk of transmission of diseases through shared surfaces.

Scalability: Face recognition systems can be easily scaled up to handle large numbers of users, which makes them ideal for use in public places such as airports, train stations, and shopping malls.

Overall, face recognition biometric systems offer several advantages in the present COVID situation and can play a vital role in reducing the risk of spreading infections while ensuring efficient and accurate identification of people.

In conclusion, biometric recognition presents both opportunities and challenges. While it offers benefits, it also raises concerns that must be addressed. Robust regulations on privacy and security are essential to ensure the accuracy, reliability, and security of this technology. Additionally, it is crucial to prevent bias and discrimination in biometric recognition systems.

By implementing appropriate safeguards and regulations, we can maximize the opportunities and benefits of biometric recognition technology.

REFERENCES:

[1] Alsaadi, I. M. (2021). Study on most popular behavioral biometrics, advantages, disadvantages and recent applications: A review. Int. J. Sci. Technol. Res, 10, 15-21. Available at: https://www.researchgate.net/profile/Israa-Alsaadi-2/publication/348662448_Study_On_Most_Popular_Behavioral_Biometrics_Advantages_Disadvantages_And_Recent_Applications_A_Review/links/6009c63b299bf14088b188e8/Study-On-Most-Popular-Behavioral-Biometrics-Advantages-Disadvantages-And-Recent-Applications-A-Review.pdf

[2] He, J., & Jiang, N. (2020). Biometric from surface electromyogram (sEMG): Feasibility of user verification and identification based on gesture recognition. Frontiers in bioengineering and biotechnology, 8, 58. Available at: https://www.frontiersin.org/articles/10.3389/fbioe.2020.00058/full

[3] Acien, A., Morales, A., Vera-Rodriguez, R., Fierrez, J., &Tolosana, R. (2019, October). Multilock: Mobile active authentication based on multiple biometric and behavioral patterns. In 1st International Workshop on Multimodal Understanding and Learning for Embodied Applications (pp. 53-59). Available at: https://arxiv.org/pdf/1901.10312

[4] Tobji, R., Di, W., &Ayoub, N. (2019). FM net: Iris Segmentation and Recognition by Using Fully and Multi-Scale CNN for Biometric Security. Applied Sciences, 9(10), 2042. Available at: https://www.mdpi.com/2076-3417/9/10/2042/pdf

[5] Dargan, S., & Kumar, M. (2020). A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities. Expert Systems with Applications, 143, 113114. Available at: https://www.academia.edu/download/96674315/j.eswa.2019.11311420230102-1-l3gubk.pdf

[6] Krasniqi, G., &Filipi, K. (2019). Efficiency Comparison of Cryptographic Applications, Match-off-Card vs. Match-on-Card, Using National Biometric eID Card. Academic Journal of Interdisciplinary Studies, 8(1), 77. Available at: https://www.mcser.org/journal/index.php/ajis/article/download/10412/10041

[7] McAteer, I., Ibrahim, A., Zheng, G., Yang, W., &Valli, C. (2019). Integration of biometrics and steganography: A comprehensive review. Technologies, 7(2), 34. Available at: https://www.mdpi.com/2227-7080/7/2/34/pdf

[8] Mohammed, H. H., Baker, S. A., & Nori, A. S. (2021, February). Biometric identity authentication system using hand geometry measurements. In Journal of Physics: Conference Series (Vol. 1804, No. 1, p. 012144). IOP Publishing. Available at: https://iopscience.iop.org/article/10.1088/1742-6596/1804/1/012144/pdf

[9] Gerashchenko, M. S., Fateev, A. G., Markuleva, M. V., Astafyev, A. N., Zefirov, S. L., & Gerashchenko, S. I. (2020, November). Biometric identification and authentication based on a new method of a pulse wave contour forming. In Journal of Physics: Conference Series (Vol. 1679, No. 2, p. 022017). IOP Publishing. Available at: https://iopscience.iop.org/article/10.1088/1742-6596/1679/2/022017/pdf.

[10] Anil k. Jain, Lin Hong, Sharath Pankanti, " An ideintity based authentication system using fingerprints," IEEE proceedings, vol 85, n0-9 ,September 1997.