EasyChair Preprint

№ 9155

Finger Vein Biometric Authentication: Accurate, Secure, and Contact Less Biometric Authentication - a Comparative Analysis

Faizee Razee Anwar and Abullais Nehal Ahmed

October 26, 2022

Finger Vein Biometric Authentication: Accurate, Secure, and Contactless Biometric Authentication - A Comparative Analysis

FAIZI RAZI ANWAR[a,1], ABULLAIS N. AHMED[b]
[a] *Assistant Professor, Dept. of Computer Sci., JAT Arts, Science & Comm. College*
[b] *Assistant Professor Dept. of Physics, JAT Arts, Science and Comm. College*

Abstract. Biometric authentications like fingerprint, face recognition, iris recognition and finger vein recognition , as compare to username/password or rfid card based authentication are convenient and secure authentication method because it is impossible for a person to forget or lose his/her biological characteristics. In the current pandemic COVID-19 situation, a secure and contactless biometric authentication system's need has been arising instead of a touch based biometric authentication systems. In this paper, we will try to find which biometric authentication system can be called as "Accurate, secure and contactless biometric authentication" by discussing fingerprint, face recognition, iris recognition and finger vein recognition biometric authentication systems. The paper not only includes vulnerabilities, and protections but also comparison of all these popular biometric methods, specially draw attention to security and accuracy. As the conclusion, the comparative study indicates that the finger vein authentication is most accurate, secure and contactless authentication because the finger vein authentication is able to detect the liveness of a person and it is impossible to make copy of finger vein pattern.

Keywords. Authentication System, Biometric Authentication, Biological feature, COVID-19, Contactless biometric authentication, Fingerprint, Face recognition Iris recognition, Vein Recognition, Vulnerabilities

1. Introduction

In current society, several biometric based identity authentication methods are used in various fields such as e-governance, banking and finance, e-commerce, justice, education and so on. In India, the Unique Identity Authority of India, the UIDAI for short, is established for issuing unique identity card to the entire population of India base on the biometric identification. [1] Due to COVID-19 pandemic a secure and contactless biometric authentication become more important than ever before. [2]

[1] Faizee Razee Anwer
Department of Computer Science .,J.A.T. Arts, Science and Comm. College (for Women), Malegaon, Dist. Nashik, Maharashtra, India, Pin-423203
email : faizeerazee@gmail.com

Juniper Research forecasts that biometric authentication will increase from an estimated 429 million in 2018 to over 1.5 billion in 2023. [3]

In Biometric authentication system biometric characteristics such as fingerprint, face, iris, and finger vein are used for identification. [4] Since these biometric characteristics are unique to individual and cannot be lost or forget, the authentication systems become more secure and accurate than traditional forms of multi-factor authentication.

But there are so many security issues related to biometric authentication system such as figure print, face recognition and iris recognition suffer from presentation attack and these methods do not detect the liveness of a person.

To overcome these security issues, finger vein recognition can be used because unlike figure print, face and iris images, it is not possible to make copies of someone's vein structures. So the chance of presentation attack is reduced. Also, unlike figure print, face and iris images, vein recognition can detect the liveness of a person, as the vein pattern disappears just as soon as blood-flow disappears. [5]

2. Types of Biometric Authentication

A variety of biometrics methods are now being used in a variety of applications. As shown in Figure 1, biometric method can be classified into physiological biometrics (also known as anatomical or morphological) which include images of the ear, face, hand geometry, iris, retina, palm print or fingerprint, and behavioural biometrics including voice, written signature, gait or key stroking.

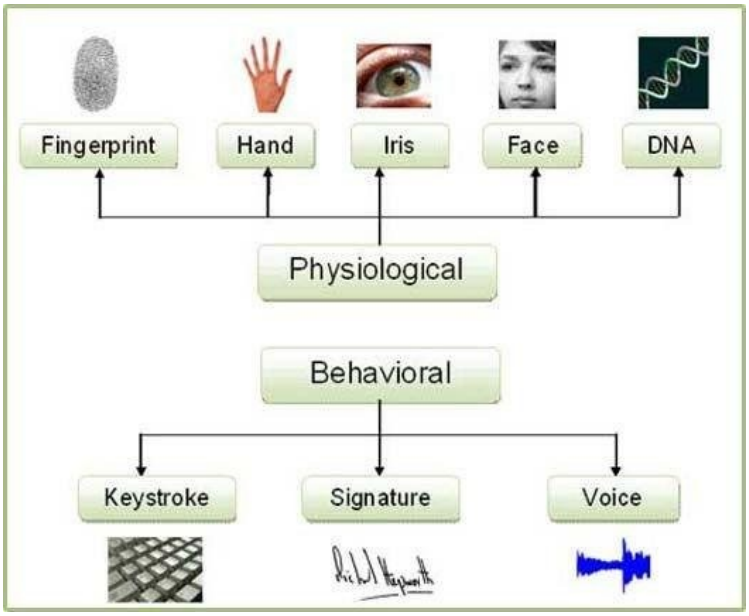

Figure 1. Classification of Biometrics

3. Related Works

In this paper, we concentrated on two areas of biometrics research where new contributions have been made: i) Vulnerability evaluation to direct attacks, ii) Proposal of new countermeasures.

3.1 Direct Attacks

It has been shown in several works, not always in a systematic and replicable way that a biometric system can be fooled by means of presenting a synthetic trait to the sensor. Although special emphasis has been made in the study of spoofing techniques for fingerprint-based recognition systems, [6] different contributions can be found describing direct attacks to biometric systems based on iris, [7] face [8] and vein [9] pattern.

3.1.1 Direct Attacks on Finger Print

The least sophisticated attackers might simply place their own fingers on the sensor and hope to be recognized as an enrolled data subject. The chance of success is then determined by the *false match rate* of the system and should be low enough for success to be very rare. More determined attackers may attempt to produce an artefact, a false fingerprint, which matches the finger of an enrolled user. Older fingerprint sensors can be hacked by a "gummy finger" created by casting the fingerprint on clay. It is clearly easy to obtain a fingerprint image with the co-operation of an enrolled *data subject* but it is also possible to obtain such an image covertly. [6]

This is because of major vulnerability of fingerprint biometrics is that latent fingerprints are sometimes left when a finger comes into contact with a surface. Sometimes, this makes it possible to obtain a fingerprint image from which an artefact can be produced.

3.1.2 Direct Attacks on Iris

A Presentation attack requires capturing an image of an individual's iris with sufficient detail to allow the creation of an appropriate artefact. Capture of a suitable image is easiest with iris recognition camera and subject cooperation - though attacks have been shown using a general-purpose camera. [10]

Germany's Chaos Computer Club (CCC), a well known group of white-hat hackers, claims to have figured out a comparatively easy way to trick the iris-recognition system on Samsung's flagship Galaxy S8 smart phone.

3.1.3 Direct Attacks on Face

For a presentation attack, covert acquisition of a suitable face image of the target is likely to be fairly easy. The physical presentation of the resulting image in a presentation attack is likely to involve a photograph, a mask, or a computer/tablet display.

An attack may be more sophisticated than simply presenting a photograph of the target face or a static face mask. The attacker may enhance their artefact in a bid to

overcome liveness or spoof detection protections. Figure 2 illustrates the process of creating a facial model using personal photographs collected from the internet. With the use of expression animations, this model not only duplicates the face but also provides mimics of liveness. [11]

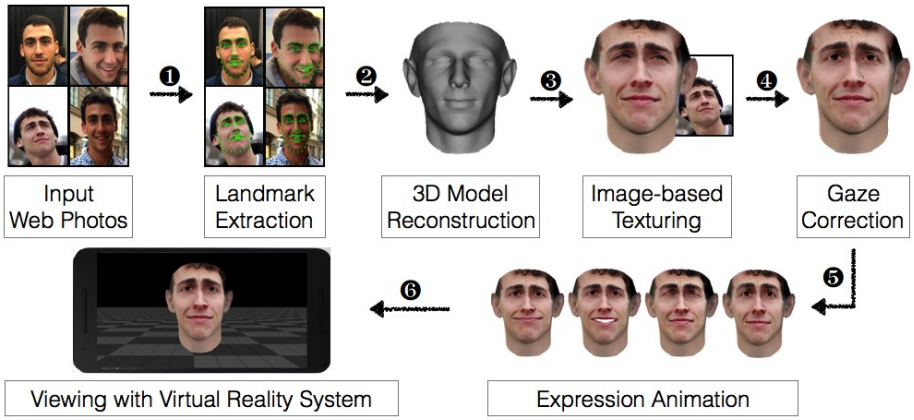

Figure 2. Process of preparing facial models for the presentation attack

3.1.3 Direct Attacks on Finger Vein

Although the finger-vein recognition method has been used as an alternative for traditional methods, it is still vulnerable to attackers. Capturing the vein pattern using an appropriate capturing device forms the basis of vein recognition in general and finger PA evaluation in particular. Therefore, we utilise the PLUSVein finger vein scanner as capturing devices to prepare our finger spoofing artefacts as well as for recapturing the artefacts. [12]

3.2 Direct Attack Protection

Researchers have focused in the design of specific countermeasures that permit biometric systems to detect fake samples and reject them, improving this way the robustness of the systems against direct attacks. Among the studied anti-spoofing approaches, special attention has been paid to those known as liveness detection techniques, which use different physiological properties to distinguish between real and fake traits.

3.2.1 Direct Attack Protection of Finger Print

The biometric sensor and controlling software may perform checks to detect a presentation attack. These can happen in several ways, including: Deformation effects when the finger is presented to the sensor, Optical spectrum analysis to identify the distinctive texture of skin, Conductivity/capacitance of the skin, Oxygen levels of the blood in the finger, Pulse or ECG measurements. [13]

3.2.2 Direct Attack Protection of Iris

Liveness detection methods may involve observing the location of reflections as illumination angles are changed, or movements of the pupil are measured. In addition, the fact that an iris system will need to locate the face region and subsequently the eye region adds a certain amount of difficulty to an attacker trying to present an artificial image. [14]

3.2.3 Direct Attack Protection of Face

Liveness checks look for a simple, measurable test that there is a real person in front of the camera. This could, for example, require specific movements in response to challenges e.g. blinking, nodding, and shaking the head or by continual assessment of small-scale movements of the head while the biometric measurement is taking place, using video capture of the face.[15]

With the advent of deep learning face recognition solutions; there is a parallel development of presentation attack detection, where a dedicated network is trained to identify known attacks, with the aim that such training will also detect new and unseen attacks.

Video sequences can also be used to protect against replay attacks. Although it is possible to simply capture a video sequence and replay it when prompted to authenticate, information can be added to the sequence that makes it either very difficult or impossible, to re-use the sequence. [16]

3.2.4 Direct Attack Protection of Finger Vein

To protect the finger-vein recognition from attackers, we propose a new PAD method for the finger-vein recognition system based on feature extraction by CNN and post-processing by PCA and SVM methods for dimensionality reduction of feature space and classification, respectively. [17]

4. Finger Vein Recognition the Proposed modality

Finger vein recognition is contactless and most secure biometric authentication system. [18] Since vein features are hard to be copied and changed even by surgery, it makes finger vein recognition the most reliable authentication method. The properties of the blood vascular network are used in finger vein recognition methods. [19]

4.1 Working of Finger Vein

When a finger is positioned across near infra-red-light rays of 760 nm wavelength, finger vein patterns in the subcutaneous tissue of the finger are scanned because deoxygenated haemoglobin in the vein absorbs the light rays. [20] The resultant vein image appears darker than the other regions of the finger because only the blood vessels absorb the rays. Figure 3 shows the working of finger vein recognition with the help of near infrared light and CCD camera.

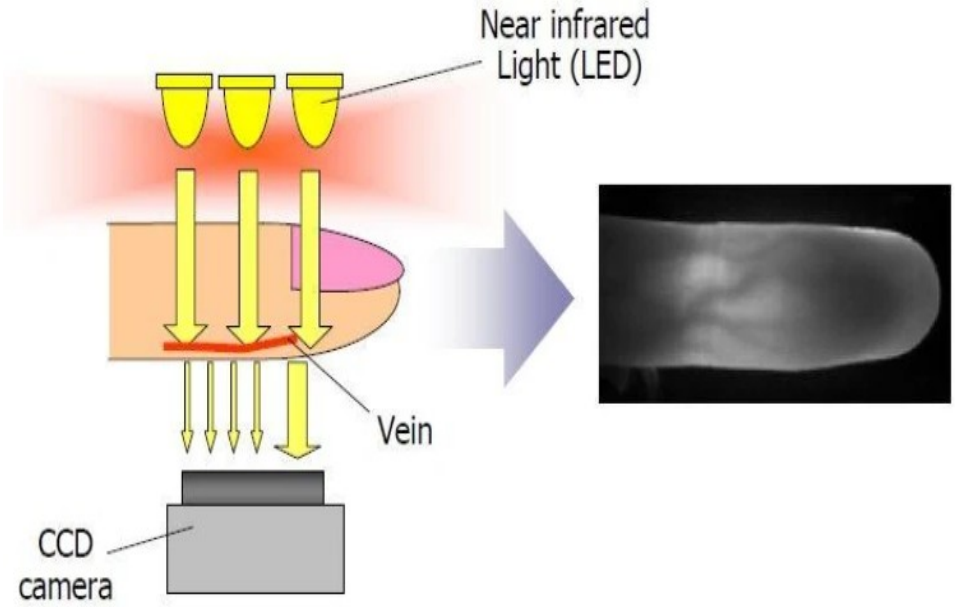

Figure 3. Working of Finger Vein Recognition

4.2 Advantages of Finger Vein Recognition

Table 1 provides a quick comparison of the biometric types presented in this paper. From the comparison it is cleared that finger vein authentication technology offers a number of distinguishing characteristics that distinguish it from other forms of biometrics as a highly secure and convenient method of personal identification.

Higher Level of Accuracy

The FRR (False Rejection Rate) is less than 0.01% for), the FAR (False Acceptance Rate) is less than 0.0001%, and FTE (Failure to Enrol) is 0%

Constant and Unique

The shape of finger veins has stability and uniqueness. Unlike fingerprints, finger veins remain constant through the mature years. Also not only the finger vein image of each person is unique, but also the vein image of the same person's other fingers are unique.

Contactless

Since near-infrared light is used which allows contactless imaging that ensures both handiness and hygiene for the user experience.

Fast Authentication Speed

It takes less than a second to do one-to-one authentication. Due to the small size of the fingers, the authentication device can also be compact.

Table 1. Comparison of Various Biometric authentication techniques

Recognition Technology	Recognition Technology	Authentication Mode	Outside Influence	Security Level	False Rejection rate	False Acceptance Rate
Fingerprint	Fingerprint pattern	Touch type	Intact surface, clean, and dry and wet environment	Low	0.1%	0.001%
Human Face	Information of human face	Non-touch type	Light, angle, and time for capturing human face	Low	2.6%	1.3%
Iris	Surface information of iris	Non-touch type, eyes irradiated by light	Camera lens, human body's physical condition, contact lens	High	0.01%	0.0001%
Finger Vein	Vein pattern in human body	Non-contact near infrared ray irradiation on finger	Internal features are not affected by the outside world	High	0.01%	0.0001%

4. Conclusion

This paper started with overview of biometric authentication systems as well as different issues and challenges related to implementation of such systems. It is found that each of biometric authentication system has advantages and disadvantages, but we can be concluded that, the finger vein based authentication provides understandable advantages compared with other biometric authentication systems due to contactless, liveness detection, in-body hidden characteristics, perfect and distinctive authentication and independence of external influence.

References

[1] Ursula Rao & Vijayanka Nair (2019) Aadhaar: Governing with Biometrics, South Asia: Journal of South Asian Studies, 42:3, 469-481, DOI: 10.1080/00856401.2019.1595343

[2] Uzoma I. Oduah, Ifeanyichukwu F. Kevin, Daniel O. Oluwole, Josephat U. Izunobi, Towards a high-precision contactless fingerprint scanner for biometric authentication, Array,Volume 11,2021,100083,ISSN 2590-0056, https://doi.org/10.1016/j.array.2021.100083.

[3] Nick Maynard, Susan Morrow ,Mobile Payment Security: Key Opportunities, Vendor Strategies & Market Forecasts 2021-2025,Published:01/02/2021,Juniper Research

[4] Shawkat, Shihab & Al-badri, Khalid & Turki, Ahmed. (2019). The New Hand Geometry System and Automatic Identification. 7. 996-1008. 10.21533/pen.v7i3.632.

[5] Darwish S.M., Ismail A.A. (2021) An Evolutionary Biometric Authentication Model for Finger Vein Patterns. Proceedings of the International Conference on Advanced Intelligent Systems and Informatics 2020. AISI 2020. AISC, vol 1261. Springer, Cham. https://doi.org/10.1007/978-3-030-58669-0_25

[6] Diaa M. Uliyan, Somayeh Sadeghi, Hamid A. Jalab, Anti-spoofing method for fingerprint recognition using patch based deep learning machine,Engineering Science and Technology, an

International Journal,Volume 23, Issue 2,2020,Pages 264-273,ISSN 2215-0986,https://doi.org/10.1016/j.jestch.2019.06.005.

[7] Nguyen DT, Baek NR, Pham TD, Park KR. Presentation Attack Detection for Iris Recognition System Using NIR Camera Sensor. Sensors (Basel). 2018;18(5):1315. Published 2018 Apr 24. doi:10.3390/s18051315

[8] H. Wang, D. S. Zhang, and Z. H. Miao, "Face recognition with single sample per person using HOG–LDB and SVDL," Signal Image & Video Processing, vol. 13, no. 19, 2019.

[9] A. H. Mohsin et al., "Finger Vein Biometrics: Taxonomy Analysis, Open Challenges, Future Directions, and Recommended Solution for Decentralised Network Architectures," in IEEE Access, vol. 8, pp. 9821-9845, 2020, doi: 10.1109/ACCESS.2020.2964788.

[10] Boyd, A., Fang, Z., Czajka, A., & Bowyer, K. (2020). Iris Presentation Attack Detection: Where Are We Now? *Pattern Recognit. Lett., 138*, 483-489.

[11] Almeida WR, Andaló FA, Padilha R, Bertocco G, Dias W, Torres RdS, et al. (2020) Detecting face presentation attacks in mobile devices with a patch-based CNN and a sensor-aware loss function. PLoS ONE 15(9): e0238058. https://doi.org/10.1371/journal.pone.0238058

[12] Kashif Shaheed, Aihua Mao, Imran Qureshi, Munish Kumar, Sumaira Hussain, Xingming Zhang,Recent advancements in finger vein recognition technology: Methodology, challenges and opportunities,Information Fusion,Volume 79,2022,Pages 84-109,ISSN 1566-2535,https://doi.org/10.1016/j.inffus.2021.10.004.

[13] Wagh D.P., Fadewar H.S., Shinde G.N. (2020) Biometric Finger Vein Recognition Methods for Authentication. Computing in Engineering and Technology. AISC, vol 1025. Springer, Singapore.

[14] Y. Zhuang, J. H. Chuah, C. O. Chow and M. G. Lim, "Iris Recognition using Convolutional Neural Network," 2020 IEEE 10th International Conference on System Engineering and Technology (ICSET), 2020, pp. 134-138, doi: 10.1109/ICSET51301.2020.9265389.

[15] Salama AbdELminaam D, Almansori AM, Taha M, Badr E (2020) A deep facial recognition system using computational intelligent algorithms. PLoS ONE 15(12): e0242269. https://doi.org/10.1371/journal.pone.0242269

[16] Farah Deeba, Hira Memon, Fayaz Ali Dharejo, Aftab Ahmed, Abddul Ghaffar, LBPH-based enhanced real-time face recognition, Int J Adv Comput Sci Appl, 10 (5) (2019) 2019

[17] Kolberg J., Gomez-Barrero M., Venkatesh S., Ramachandra R., Busch C. (2020) Presentation Attack Detection for Finger Recognition. In: Uhl A., Busch C., Marcel S., Veldhuis R. (eds) Handbook of Vascular Biometrics. Advances in Computer Vision and Pattern Recognition. Springer, Cham. https://doi.org/10.1007/978-3-030-27731-4_14

[18] R. Ramachandra, K. B. Raja, S. K. Venkatesh and C. Busch, "Design and Development of Low-Cost Sensor to Capture Ventral and Dorsal Finger Vein for Biometric Authentication," in IEEE Sensors Journal, vol. 19, no. 15, pp. 6102-6111, 1 Aug.1, 2019, doi: 10.1109/JSEN.2019.2906691.

[19] Jain, A.K., Deb, D., & Engelsma, J.J. (2021). Biometrics: Trust, but Verify. *ArXiv, abs/2105.06625*.

[20] Racha Nikhil, Mohit Mirchandani, Dr.V.Kavitha. (2020). Finger Vein Authentication for Security Purpose. International Journal of Advanced Science and Technology, 29(06), 7669-7673. Retrieved from http://sersc.org/journals/index.php/IJAST/article/view/25127