Design Studies and Intelligence Engineering
L.C. Jain et al. (Eds.)

doi:10.3233/FAIA231443

A Review on Vascular Biometrics for Finger Vein Authentication System

D Jude HEMANTH[1] and Nisha Joy THOMAS
Department of ECE, Karunya Institute of Technology & Sciences, Coimbatore, India Corresponding

Abstract. In the area of biometric authentication, vascular biometrics has been highlighted off late due to its much-appreciated list of advantages which promotes more efficient person identification and authentication. Finger Vein Recognition Systems (FVRS) is an emerging biometric technology gaining much attention throughout the world especially in the banking sector, cashless/ cardless money transfer, ATM systems and soon. Finger vein authentication systems have the threat of spoof attacks or presentation attacks (PA) which affects the security measures in a serious manner. Since vascular biometrics is receiving more attention in the field of financial transfer, being aware of the possible security attacks is a necessity. This paper presents a review of selected literature on presentation attacks in finger vein authentication systems. Also listing the pros and cons of the presentation attack detection methods and certain ways to prevent PA. The pros and challenges of dealing with FVRS have also been listed here.

Keywords. vascular biometrics, finger vein authentication, presentation attack, fake vein attack, biometric security, spoofing.

1. Introduction

Identity identification is now a big part of how people live their lives. Logging into computers or online accounts, using ATMs, and getting permission to enter a bank or a certain area are just some of the most common times when name verification is needed. There are many ways to find out who someone is. Most people use passwords, but they are becoming less common because biometrics seem to be the best way to identify a person [8].

A biometric authentication system measures specific physical characteristics or behaviors in real-time to verify a person's identity. As a result, algorithms used in biometric authentication systems may be used to identify or validate the person by comparing the data to other biometric records in the database. [1]. Finger vein biometrics, also called vascular biometrics is coined as such because of the authentication performed by verifying the unique pattern of blood vessels (veins) under the skin in the fingertips. This physical trait is different for every human being on earth. Compared to other biometric modalities like fingerprint, face recognition, iris recognition etc., vascular biometrics stands out with the greater number of benefits such as:

- difficult to forge compared to other biometric modalities.

[1] Corresponding Author: judehemanth@karunya.edu

- contactless authentication.
- this pattern of veins seems not to evolve with time and contains enough discriminant information to be used as a person recognition method [4] .
- multiple fingers can be used to acquire sufficient vein information for finger vein recognition, and finger vein capture devices are smaller in volume [21].
- in addition, customers can register one of their fingers as a "stress finger" to use when under stress. For instance, if a criminal makes an individual to take out currency, the customer's stress finger can be detected by the bank, which can then implement an automatic countermeasure, such as closing the ATM and displaying an "out of service" notification [27].
- finger vein recognition is a major biometric method that is thought to be safer, reliable, and on the rise [3].
- less time-consuming and simpler to use for the end user [10] . Only roughly 400 bytes of data need to be sent, so the user's name can be validated in a few seconds [27].

Identification and verification are the two main ways that biometric security systems work. In the recognition mode, the data that is put in can be compared to all the patterns that are already in the database. Using this method, it is possible to find out if this person is in the database. In verification mode, biometric data is matched to the unique pattern of a single person. If they aren't the same individual, it stops many people from using the same name [2]

Despite the advantages mentioned above, finger vein recognition system has challenges associated with it as well, since the effects of environmental illumination, ambient temperature, and scattering of light during the acquisition of finger vein images can lead the vein patterns to be confusing and incoherent [6]. A further consideration is that extremely cold and 'dead' fingers (such as those of individuals with Raynaud's syndrome) are difficult to read using finger vein pattern recognition [10]. Information about the person’s health issues can be leaked [13].

Late strange of applications using vascular biometrics [28]:

- Application of pay-by-finger in retail industry.
- Finger Vein Authentication using visible light smartphone cameras. Infrared light is usually used for the sensor to acquire the vein image.
- Public Biometrics Infrastructure (PBI) technology also allows the utilization of electronic data with digital signatures in lieu of traditionally signed paper transaction docs. It allows branches to conduct processes electronically, thus boosting the productivity of banking work (paperless procedures).
- At present, finger vein recognition technology is mostly used for identity authentication, financial transactions, and information security. It is expected to be used in other sectors soon. In the smart healthcare sector, finger vein recognition can enhance patient identity identification and medical data access control, enhancing security and privacy. Finger vein recognition technology can be used in smart transport to authenticate drivers and improve traffic safety by allowing only authorized drivers to drive vehicles.

Mr. Takeyuki Mayumi who is currently engaged in the facilitation of biometrics authentication deployment at Hitachi, says that “ The global need for biometric authentication has experienced a significant increase” [11].Certain countries including

Japan, China, South Korea has implemented finger vein systems in ATM systems and other countries like UAE, India, Brazil is exploring the use of this technology in ATM systems and banking sector. However, there are attacks that could weaken the level of protection provided by finger vein biometric systems [2].

Hence it is extremely important to be aware of the possible security threats, to prevent possible attacks. There is still a great deal of unknown territory in the field of presentation attacks (PA), studies of vulnerability, and attack detection, according to the published research content on biometric vein recognition [17].

1.1. Outline

The rest of this paper is organized as follows: Section 2 points out the motivation and problem statement. The different types of attacks in FVRS are mentioned in Section 3, focusing on the presentation attack. A review on certain chosen papers of presentation attacks is portrayed along with possible preventive measures. Section 4 gives an outline of the datasets used for FVRS and PA. Section 5 shows the parameters which justify the algorithms. Towards the end of the paper, section 6 gives the conclusion.

2. Motivation and Problem Statement

The main motivation is the threat to security in person authentication. Biometric protection gets more important as technology and electronic payment methods become more widely used [27]. Since vascular biometrics have been used in the banking sector for financial transfers and many other person authentication areas, vulnerability of PA to the FVRS is a major concern and PAD algorithms need to be tried and tested with various datasets to increase the features to withstand PA.

3. Different types of Attacks in FVRS

Finger vein pattern detection systems can be attacked in several different ways:

1. Direct Attack: A presentation attack refers to the deliberate action of an individual impersonating another person with the intention of gaining unauthorized entry into a system [17]. This kind of attack that belongs to the category of direct attacks[5] or physical attack. In this type of attack, the attacker shows the recognition system a captured biometric trait of the victim, like a picture of a finger vein, to make it think they are the victim. In a physical attack, a synthetic master vein image is used to make a real thing called a Presentation Attack Instrument (PAI) [25]. The PAI is then used to attack the recognition system with a presentation attack. [7]

2. Logical Attack: That means using a Trojan horse or another type of malware and virus to attack the parts of the biometric system, channel interception, replay attacks. Direct attacks on biometric systems are more interesting because the attacker doesn't need to know anything about the system being attacked. This kind of attack takes advantage of the flaws in the matching process [24].

In this paper, we focus only on presentation attacks. Presentation attacks, commonly referred to as spoofing, encompass the act of acquiring the biometric data of an individual through various means. This may involve capturing a high-quality image of the person's face, fingertip, or iris, or recording their voice. Subsequently, this acquired data is utilized to generate a replica image, either in two-dimensional or three-dimensional form. Such a replica can then be transformed into a mask or overlay, enabling an imposter to assume the identity of the victim [9]

3.1. Presentation Attack

The authors of [7] are evaluating the vulnerability of finger vein recognition (FVR) systems to master vein attacks. In these attacks, a manipulated image resembling a vein is used to match fraudulently with multiple identities. The findings highlight the significance of instituting increased security measures in FVR systems [7]. The authors explain two techniques for generating master veins in finger vein recognition systems. This method employs a pre-trained generative model and an evolutionary algorithm. The utilized generative model combines 2-VAE and WGAN-GP models. Typically, the LVE algorithm is used to generate master biometric samples; in this instance, it is used to generate master veins. This method employs an adversarial machine learning (AdvM) attack to target a robust CNN-based surrogate recognition system. The attack involves the creation of an image resembling a vein that can be used to impersonate multiple enrolled identities.

The researchers in [12] suggest a PAD [24] approach for a near-infrared (NIR) camera-based finger vein recognition system that uses a convolutional neural network (CNN) to improve the ability of handcrafted techniques to find veins. For dimensionality reduction and classification, they also employ principal component analysis (PCA) and support vector machine (SVM). The experimental results show that their proposed method is superior to other techniques for determining finger-vein images associated with presentation attacks.

The work in [14] talks about the security problems with biometric systems, such as presentation attacks (PAs), in which fake biometric features or presentation attack tools are used to pretend to be someone else. The authors suggest a new method for detecting fingerprint presentation attacks (PAD) that uses a device that can take pictures in the short-wave infrared (SWIR) range. They test the method on a collection of more than 4,700 samples and show a low detection equal error rate (D-EER) of 1.35 percent, even in a situation where attacks are unknown.

The paper [15] talks about how fake finger vein pictures can be used to find presentation attacks. In this method, the pictures are broken down, the information is encoded, and a cascaded support vector machine model is used to classify the images. Experiments have shown that the proposed method works better than ways that are already in use. The paper talks about how important biometric techniques are in different situations, but it also says that they can be attacked by "presentation attacks."

The main goal of the study in [16] is to figure out how dangerous vein attack databases are in the field of biometrics for finger and hand veins. The study looks at how well different vein recognition methods can find attack specimens from a public database of attacks and a private database of dorsal hand veins. The goal is to figure out the Impostor Attack Presentation Match Rate, which is the number of attacks that were accepted when they shouldn't have been. The study also suggests a fusion method that detects presentation attacks by putting together comparison scores from different classification schemes.

Table 1. Highlights of the above review.

Ref.	Strengths	Limitations
[7]	Miura's system is readily corrupted by non-vein-appearing	CNN based FVRS could fool LVE method

	samples produced by a WGAN- GP model with vein-like. characteristics.[18][19]	
[12]	Employing a CNN-based approach, a suitable image feature extractor is found. Creates an extremely high degree of detection precision when compared to earlier techniques.	Needs an enormous number of computations and is more complicated than former techniques.
[14]	Use of SWIR images in combination with state-of-the-art CNNs offers a reliable and efficient solution to the threat posed by presentation attacks.	Unpredictable about the efficiency in attacks evolved in future
[15]	This is the first time that the amount of blurriness and the way noise is spread out in real and fake pictures are looked at as two different things.	Is applicable to large difference between real and forged images
[16]	Keypoint strategy SIFT is typically, highly resistant to PLUS, attacks.	The texture-based procedures LBP and CNN are typically. vulnerable to IDIAP and SCUT attack samples only.

3.2. Possible preventive measures

Presentation attacks can be stopped and made less dangerous in finger vein pattern recognition systems by using some of the countermeasures.

Here are some ways to approach the problem:

1. Liveness Detection: Using methods for liveness detection can help figure out if the finger vein pattern shown is from a real person or a fake one [25]. To make sure the picture is real, this can mean looking at things like blood flow or specific movements. [20]

2. Multimodal biometrics: Adding finger vein pattern recognition to other biometric methods, like fingerprint or iris recognition, can make the system more secure overall. When multiple biological traits are used together, it becomes harder for attackers to fool the system.[7][23]

3. Quality Assessment: Using quality assessment algorithms [26] can help find pictures of finger veins that look suspicious or aren't very good. By looking at things like picture resolution, focus, and noise levels, the system can get rid of images that don't meet the quality standards. This makes it less likely that a presentation attack will work.

4. Finger vein Datasets

1. Shandong University made the SDUMLA-HMT database, which is a biometrics library with many kinds of information. The finger vein database constitutes a

component of the SDUMLA-HMT collection. It has pictures of the veins in 6 fingers from 106 people. The index, middle, and ring fingers on both hands constitute the 6 fingers. The SDUMLA-HMT archive has six pictures for each finger of every individual[29].

2. Finger vein recognition and finger vein presentation assault detection (anti-spoofing) are both supported by the VERA Finger Vein dataset. The dataset includes 440 NIR bona fide photos from 110 clients that were taken using an open sensor. Additionally, the set of images comprises presentation assaults (spoofing attacks) on the same 440 images that can be studied to determine the vein identification systems' susceptibility as well as to create presentation attack detection methods [31][32].

3. The pictures in the archive, FV-USM came from 123 students and faculty at Universiti Sains Malaysia, 83 of whom were men and 40 of whom were women. Each subject gave four fingers: the index finger on the left, the middle finger on the left, the index finger on the right, and the middle finger on the right. This gave a total of 492 finger classes [33].

4. The Finger Image Archive at HongKong Polytechnic University is made up of images of finger veins and finger surface textures taken at the same time from both male and female subjects. There are 6264 images from 156 people in the database [34].

5. The UTFVP Finger vein Database has 1440 pictures from 60 clients that can be used to recognize finger veins. The University of Twente in the Netherlands made this collection[36].

6. THU-FVFDT (Tsinghua University Finger Vein and Finger Dorsal Texture Database) is a collection that includes raw photos of 220 different subjects' finger veins and dorsal textures. Raw images have a resolution of 720 x 576 pixels [37].

5. Parameters for Evaluation

Shown below is a table displaying the parameters used for evaluating the efficiency of FVRS and PAD.

Ref.	Purpose	Parameters
[38][39]	FVRS	Equal Error Rate (EER), (True Acceptance Rate (TAR), False acceptance rate (FAR), False recognition rate (FRR)
[12][14][15][16]	PAD	Attack Presentation Classification Error Rate (APCER) Bona Fide Presentation Classification Error Rate (BPCER) SpoofFalse Acceptance Rate (SFAR) Average classification error rate (ACER)

6. Conclusion

In this paper, the advantages of vascular biometrics along with the challenges have been listed. The applications of vascular biometrics in various fields also have been

portrayed. There are attacks that can affect the performance of FVRS like the presentation attacks. Selected work on PA & PAD has been highlighted in a table. Also, some preventive measures that can be adopted have been mentioned. Certain available databases for FVRS and PA have also been listed out along with the parameters that decide the efficiency of the purpose.

References

[1] I. Boucherit et al., Finger vein identification using deeply-fused Convolutional Neural Network Journal *of King Saud University - Computer and Information Sciences* **34** (2022) 646-656.
[2] Finger Vein Recognition Using Deep Learning Technique Wasit Journal of Computer and Mathematic Science
[3] S. Shakilet al. An optimal method for identification of finger vein using supervised learning, *Measurement: Sensors* **25** (2023)
[4] Alexandre Sierro, Pierre Ferrez, Pierre Roduit, Contact-less Palm/Finger Vein Biometrics
[5] Pedro Tome and S´ebastien Marcel, On the Vulnerability of Palm Vein Recognition to Spoofing Attacks
[6] Kashif Shaheed et al., A Systematic Review of Finger Vein Recognition Techniques, *Information* **9** (2018)
[7] Huy H. Nguyen, Analysis of Master Vein Attacks on Finger Vein Recognition Systems, *IEEE* (2023)
[8] Shazeeda Shazeeda, Bakhtiar Affendi Rosdi, Finger vein recognition using mutual sparse representation classification*, IET Biom., The Institution of Engineering and Technology* (2018), Vol. 8 Iss. 1, pp. 49-58.
[9] A. Morales et al., Chapter 6, Introduction to Iris Presentation Attack Detection, *Handbook of Biometric Anti-Spoofing*, 2019.
[10] https://www.recogtech.com/en/knowledge-base/5-common-biometric-techniques-compared
[11] https://social-innovation.hitachi/en/article/pbi/
[12] Dat Tien Nguyen et al., Spoof Detection for Finger-Vein Recognition System Using NIR Camera, *Sensors,* 2017.
[13] A. Krishnan, T. Thomas, Finger Vein Recognition Based on Anatomical Features of Vein Patterns, IEEE
[14] Ruben Tolosana et al., Biometric Presentation Attack Detection: Beyond the Visible Spectrum IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 15, 2020.
[15] Xinwei Qiu et al., Finger Vein Presentation Attack Detection Using Total Variation Decomposition
[16] Johannes Schuiki et al., Extensive Threat Analysis of Vein Attack Databases and Attack Detection by Fusion of Comparison Scores.
[17] A. Anjos etal. Chapter 18, An Introduction to Vein Presentation, Attacks and Detection, Handbook of Biometric Anti-Spoofing pg.419
[18] Naoto Miura, Akio Nagasaka, and Takafumi Miyatake. Feature extraction of finger-vein patterns based on repeated line tracking and its application to personal identification. Machine Vision and Applications, 15(4):194-203, 2004.
[19] K. Shaheed et al., Recent advancements in finger vein recognition technology: Methodology, challenges and opportunities, Information Fusion 79 (2022), 84- 109
[20] KEVIN W. BOWYER, Presentation Attack Detection for Iris Recognition: An Assessment of the State of-the-Art ADAM CZAJKA, Research and Academic Computer Network (NASK),
[21] S. Dong, J. Yang, Y. Chen, C. Wang, X. Zhan, et al., Finger Vein Recognition Based on Multi-Orientation Weighted Symmetric Local Graph structure, KSII Trans. Internet Inf. Syst. 9 (10) (2015)
[22] https://social-innovation.hitachi/en/article/touchless-finger-vein/
[23] Ryszard S. Choras, Chapter Multimodal Biometrics for Person Authentication, *Security and Privacy from a Legal, Ethical, and Technical Perspective,* IntechOpen.
[24] R. Raghavendra, Presentation Attack Detection Algorithms for Finger Vein Biometrics: A Comprehensive Study, International Conference on Signal-Image Technology & Internet-Based Systems (2015)
[25] J. Galbally et al., Handbook of Biometric Anti-Spoofing: Trusted Biometrics Under Spoofing Attacks. Springer Publishing Company, Incorporated, 2014, page 4.
[26] Huafeng Qin et al., Quality Assessment of Finger-vein Image, IEEE Transactions on Information Forensics and Security
[27] https://social-innovation.hitachi/en-eu/case_studies/why-the-future-lies-in-fingerveinid/
[28] Zhou, L. (2023). Finger Vein Recognition Technology: Principles, Applications, and Future Prospects. International Journal of Biology and Life Sciences, 3(2), 45-48.

[29] Yilong Yin, Lili Liu, and Xiwei Sun. Sdumla-hmt: a multimodal biometric database. In Chinese Conference on Biometric Recognition, pages 260-268. Springer, 2011.
[30] K. Syazana-Itqan, A Review of Finger-Vein Biometrics Identification Approaches, Indian Journal of Science and Technology, Vol 9(32)
[31] Vanoni, Matthias, Tome, Pedro, & Marcel, Sébastien. (2014). VERA FingerVein [Data set]. https://doi.org/10.34777/8pkt-6z66
[32] Pedro Tome, Ramachandra Raghavendra, Christoph Busch, Santosh Tirunagari, Norman Poh, B. H. Shekar, Diego Gragnaniello, Carlo Sansone, Luisa Verdoliva and Sébastien Marcel: "The 1st Competition on Counter Measures to Finger Vein Spoofing Attacks", in Proceedings of the 8th IAPR International Conference on Biometrics (ICB), 2015
[33] Mohd Shahrimie Mohd Asaari, Shahrel A. Suandi, BakhtiarAffendi Rosdi, *Fusion of Band Limited Phase Only Correlation and Width Centroid Contour Distance for finger based biometrics*, Expert Systems with Applications, Volume 41, Issue 7, 1 June 2014, Pages 3367-3382, ISSN 0957- 4174, http://dx.doi.org/10.1016/j.eswa.2013.11.033.
[34] Ajay Kumar and Yingbo Zhou, "Human Identification using Finger Images", IEEE Trans. Image Processing, vol. 21, pp. 2228-2244, April 2012
[35] Ton, B. T., & Veldhuis, R. N. J. (2013). A high-quality finger vascular pattern dataset collected using a custom designed capturing device. In *Proceedings of the 2013 International Conference on Biometrics (ICB)* (pp. 1-5). (Proceedings International Conference on Biometrics (ICB); Vol. 2013). IEEE.
[36] Tome et al., On the Vulnerability of Finger Vein Recognition to Spoofing, IEEE International Conference of the Biometrics Special Interest Group, (2014)
[37] Yang W et al. Comparative competitive coding for personal identification by using finger vein and finger dorsal texture fusion. Information Sciences. 2014; 268:20–32
[38] Luo et al. FVCT: Finger Vein Authentication Based on the Combination of CNN and Transforme
[39] Kashif Shaheed et al., A Systematic Review of Finger Vein Recognition Techniques (2018)