Proceedings of the Joint Austrian Computer Vision and Robotics Workshop 2020 DOI: 10.3217/978-3-85125-752-6-16

Presentation Attacks and Detection in Finger- and Hand-Vein Recognition

Luca Debiasi, Christof Kauba, Heinz Hofbauer, Bernhard Prommegger, Andreas Uhl
Department of Computer Sciences, University of Salzburg
{ldebiasi,ckauba,hhofbaue,bprommeg,uhl}@cs.sbg.ac.at

Abstract. *Biometric recognition systems, especially vascular pattern based ones, are becoming more popular. However, these systems are still susceptible to so called presentation attacks, where a forged representation of the original biometric is presented to the system trying to mimic the original biometric and fool the system. We propose a presentation attack approach for finger- and hand-vein recognition systems using paper prints as well as wax and silicone artefacts. We further develop a suitable presentation attack detection (PAD) scheme based on natural scene statistics and acquire a corresponding hand vein presentation attack dataset. Evaluating the PAD scheme on the dataset confirmed its success in the detection of the forged samples.*

1. Introduction

In our modern world there is an ever growing need for personal authentication. Biometric authentication systems are one way to overcome the typical problems of classical authentication methods, e.g. disclosed or forgotten passwords, lost or stolen keys and forged signatures. Biometric authentication systems are based on so called biometric traits, which are unique behavioural or physiological characteristics of a person. These are inherently linked to a person and cannot get lost, be forgotten or be stolen. The most prominent examples of biometric traits include fingerprints, face and iris. Recently, vascular pattern based biometrics (usually denoted as vein recognition based systems) gain more attention as well, with finger- and hand-vein based systems being the most widely used ones [27]. Vein based systems exhibit some advantages over other biometric systems, e.g. fingerprint and face recognition ones. They rely on the structure of the vascular pattern formed by the blood vessels inside the human body tissue, i.e. it is an internal biometric trait. This pattern only becomes visible in near-infrared (NIR) light, as the haemoglobin in the blood absorbs NIR light, rendering the blood vessels (veins) visible as dark lines in the captured images. Vein based systems are more resistant to forgery and they are neither susceptible to abrasion nor skin surface conditions [11].

Despite the advantages mentioned above, biometric recognition systems are far from being perfect. Almost all of the currently employed systems are susceptible to spoofing or presentation attacks (PAs). A PA is defined as *presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system* according to the ISO/IEC 30107-1 standard [4]. This corresponds to the creation of a forged representation mimicking the original biometric trait (also called a spoofing artefact) that is used to spoof/fool the biometric system. PAs are posing a severe problem in practical applications as a genuine user may be impersonated. By launching a successful PA, an adversary is able to gain illegitimate access to the system. In contrast to passwords and tokens, a biometric trait can neither be replaced nor revoked. Hence, if a system is prone to PAs, it can no longer be considered as secure. Fortunately, there are counter-measures which aim to detect PAs by equipping the biometric system with either additional hardware or software performing presentation attack detection (PAD).

In this work we focus on PAs and PAD for finger- as well as hand-vein recognition systems. We propose several approaches to create spoofing artefacts using different materials replicating the vein pattern of genuine subjects. Furthermore, corresponding PA datasets are acquired and a PAD approach, tested on hand veins, is presented.

The rest of the paper is organised as follows: Section 2 gives an overview on PAs and PAD schemes for finger- and hand-vein recognition. In Section 3 the generation of the spoofing artefacts is explained.

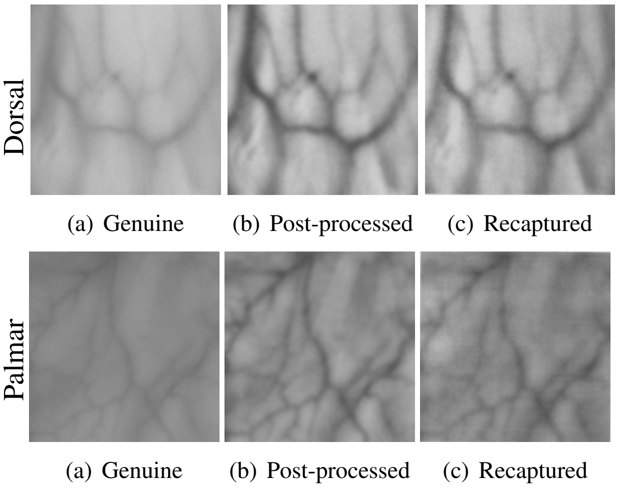
Section 4 presents our proposed PAD approach. The experimental evaluation is described in Section 5. Section 6 concludes this paper and gives an outlook on future work.

2. Related Work

Finger- and hand-veins have been shown to be susceptible to spoofing [26, 24]. PAD approaches help in detecting presentation attacks and can be categorised into liveness-based (rely on signs of vitality, e.g. capturing the heartbeat), motion-based (analyse movements during the capturing process and try to detect unnatural ones) and texture-based methods (detect and analyse textural artefacts present in the image). While the first two categories require a video or a sequence of consecutive images to be captured, texture-based methods can be applied to single images. One liveness based approach is presented in [19], which applies motion magnification techniques. The majority of the proposed PAD schemes are texture-based ones, e.g. a Fourier, Haar and Daubechies wavelet transform based one [16], exploiting differences in the bandwidth of vertical energy signals. A binarised statistical image features based one and some others based on Riesz transform, local binary patterns (LBP), local phase quantisation and Weber local descriptors are presented in [25]. Another approach [23] uses a windowed dynamic mode decomposition (W-DMD) to detect spoofed finger vein images. Even baseline LBP [20] and some LBP variants and extensions of LBP [10] proved to be effective for the task of finger vein PAD. Several other approaches are utilising image quality assessment methods (IQA), e.g. [15] and [1] which detection accuracy turns out to be highly dependent on the particular dataset. In [22] the authors showed that the classification accuracy can be improved by incorporating natural scene statistics (NSS) [13]. A very different approach for PAD detection is to use a photo-response non-uniformity (PRNU) technique to differentiate PA data from genuine samples [12]. Furthermore, a CNN-based approach has been proposed in [17].

3. Presentation Attack Approaches

Capturing the vein pattern using an appropriate capturing device forms the basis of vein recognition in general and finger- and hand-vein PA evaluation in particular. Therefore, we utilise the PLUSVein finger vein scanner [7] and the PLUS hand vein scanner [8] as capturing devices to prepare our finger- and hand-vein spoofing artefacts as well as for recapturing the artefacts. The interested reader is referred to the authors original publications for more details about those capturing devices. In the following, the production of the hand and finger vein spoofing artefacts is described. These spoofing artefacts are then again presented to the capturing devices mentioned above.



(a) Genuine (b) Post-processed (c) Recaptured

(a) Genuine (b) Post-processed (c) Recaptured

Figure 1. Hand vein PA artefacts for 950 nm reflected light illumination captured with the PLUS hand vein scanner [8]: genuine image (a), post-processed image for printing (b) and re-acquired printed image (c).

3.1. Hand Vein Spoofing Artefacts

The hand vein capturing device is used to acquire reflected light images in two different wavelengths (850 and 950 nm). Since printouts of finger vein patterns have shown to yield successful presentation attacks [26], we decided for this approach as an attack scenario for the hand vein recognition system as well. Our spoofing attack samples are derived from samples contained in the publicly available PROTECTVein dataset, which is part of the PROTECT Multimodal Biometric Database [21].

The hand vein spoofing attack samples are created by first selecting 100 images based on the visibility of the vein pattern (5 dorsal and 5 palmar for one hand of 10 users). Afterwards, a region of interest (ROI) is manually cropped from the images. These ROIs are then post-processed using a Contrast Limited Adaptive Histogram Equalisation (CLAHE) and Gauss filtering, to enhance the visibility of the vascular pattern and remove the skin texture and hair to eventually obtain smooth images. Afterwards, the post-processed images are scaled to approximately match

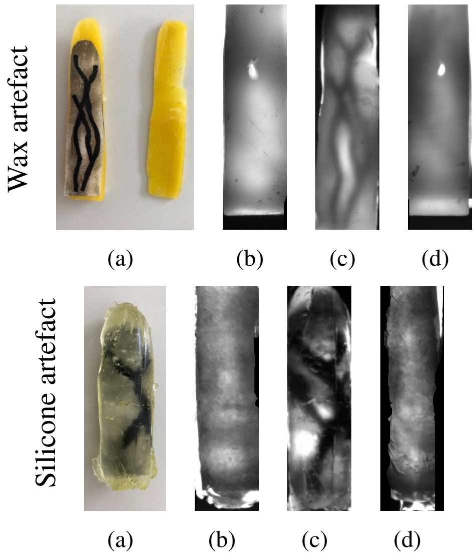


Figure 2. Wax and silicone artefacts (a) and image as captured by the PLUSVein finger vein scanner [7] using different enhancements for the vein pattern: no enhancement (b), tracing with black marker (c), local contrast enhancement (CLAHE) (d).

the real-life genuine samples and printed to paper. Multiple printers and print configurations have been tested to find an appropriate solution in regard to the absorption of NIR light. In the end, using a ‘HP LaserJet 500 colour M551’ laser printer in grey-scale printing mode yielded satisfactory results. Some examples of the hand vein PA artefact generation and recapturing are shown in Figure 1.

3.2. Finger Vein Spoofing Artefacts

For the light transmission based finger vein modality, the establishment of working PA artefacts is less trivial than in the reflected light case seen for hand veins. Following an idea as exhibited in a recent Chaos Computer Club video based on a sliced wax artefact and a silicone model as proposed in [18] we finally came up with two different types of artefacts, as shown in Figure 2. These artefacts are derived from samples contained in the publicly available PLUSVein-FV3 finger vein data set [6]. These two materials exhibited the best properties in regard to appropriate illumination in the light transmission case among several other considered materials.

For both types of artefacts, wax and silicone, the first step in creating the artefacts is to obtain a mould with a finger-like shape. We use a 3D-printer to create the moulds, consisting of two parts: base and top. Afterwards the vein pattern is printed using a ‘HP LaserJet 500 colour M551’ laser printer in grey-scale printing mode (similar to hand vein artefacts). The paper sheet containing the vein pattern is placed between the bottom and top finger artefact parts, as shown in Figure 2. The same finger artefact could be used for all spoofs by simply substituting the piece of paper containing the vein pattern.

In order to improve the visibility of the vein pattern, different techniques are employed: no enhancement, enhancing the image (CLAHE and Gauss filtering) as well as tracing the veins with a black permanent marker. Furthermore, various types of paper are tested. The tracing of the vein pattern yields the visually most pleasing results. In total, 42 finger artefacts (2 materials, 7 types of paper, 3 vein pattern enhancements) are generated for 3 fingers of an exemplary user. Figure 2 illustrates the created artefacts and images recaptured with the sensor.

4. Presentation Attack Detection

The PAD system applied in this work uses natural scene statistics as described in [13] and is based on the framework presented in [2], which was adapted to presentation attack detection in [22]. In brief, the features used for detection are the parameters of (asymmetrical) generalised Gaussian distributions, (A)GGD, fit to statistics of characteristics derived from samples & artefacts using a multi-scale approach.

The features are fed into a support vector machine (SVM) for classification, two-class ‘genuine’ and ‘spoofed’, using a radial basis function. First of all, the available genuine and spoofed data is randomly separated on a user basis into two equally sized training and test sets.

For training, in order to cleanly separate training and evaluation data, learning is done using a ‘leave one label out’ cross-fold technique. All images of a user’s hand are defined as having the same label, i.e. the right and left hand have different labels for each user. Furthermore, also the perspective (dorsal or palmar) is split into different labels. To evaluate on the whole training dataset each label is left out in turn, the SVM is trained on the relevant training data, then the left-out label is evaluated. The final training evaluation data is the union of the individually evaluated labels. The parameters are optimised for the overall training database, where the search is done non-exhaustively on a grid with logarithmic drill-down, presenting closed set learning. The spoofing detection accuracy serves as learning function for the parameter optimisation.

The trained SVM is then applied to the previously unseen test data and yields an output class and a confidence, which represents the difference between class probabilities.

5. Experimental Evaluation

This section describes the experimental set-up for the evaluation of the hand- (HV) and finger-vein (FV) spoofing artefacts as well as the spoofing artefact's quality and PAD performance.

5.1. Experimental Set-Up

The software used to process the finger- and hand-vein data is the OpenVein Toolkit [9]. The ROI extraction has been done manually and the visibility of the vein pattern is improved by applying different post-processing techniques from the toolkit. The vascular patterns are extracted using Maximum Curvature (MC) [14] and the comparison of the resulting binary feature vectors is performed using a correlation based approach [14].

As defined in ISO/IEC 19795-1 [3], the EER, FMR1000 and ZeroFMR are used to quantify the verification performance, where all samples are compared against each other (full comparison). The experiments are performed separately for fingers/hands, orientations (dorsal/palmar) and illumination types where applicable.

The PAD approach is evaluated using the metrics defined in the ISO/IEC 30107-3 [5] standard: detection equal error rate (D-EER), where APCER=BPCER, attack presentation classification error rate (APCER, equivalent of FAR) which is the proportion of attack presentations using the same spoofing artefact species incorrectly classified as bona fide (true) presentations in a specific scenario, bona fide presentation classification error rate (BPCER, equivalent of FRR) representing the proportion of bona fide presentations incorrectly classified as presentation attacks in a specific scenario and a corresponding Detection Error Trade-off (DET) curve.

5.2. Results: Quality of Spoofing Artefacts

In order to assess the PAD performance, it is essential to evaluate the quality of the spoofed artefacts first. This is done by comparing the recaptured images of the spoofed artefacts against bona fide images. The main goal in creating the spoofed artefacts is to have as little as possible impact on the matching performance. If that is the case, the quality of the spoofed artefacts can be considered as satisfactory.

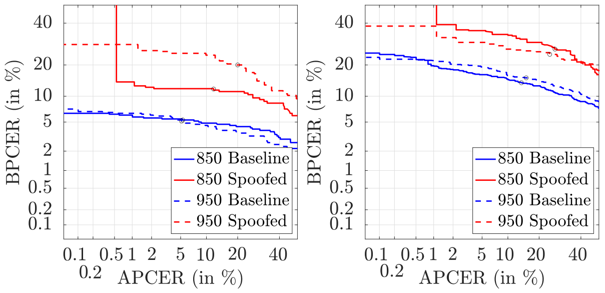


Figure 3. HV Verification results obtained when comparing bona fide samples only (baseline) and with presentation attacks (spoofed) for dorsal (left) and palmar (right) view.

		EER	FMR1000	ZeroFMR
Baseline	Dorsal 850	3.01	3.00	4.00
	Dorsal 950	4.99	6.00	6.00
	Palmar 850	16.99	30.00	32.00
	Palmar 950	18.16	32.00	33.00
Spoofed	Dorsal 850	10.80	94.80	98.00
	Dorsal 950	11.20	15.60	16.40
	Palmar 850	20.82	100.00	100.00
	Palmar 950	23.22	38.00	41.20

Table 1. Performance values (in %) obtained when verifying bona fide samples only (baseline) compared to verifying bona fide samples against PAs (spoofed) for reflected light HV recognition.

The results for the HV artefacts (reflected light) are shown in Figure 3 and the corresponding performance values are reported in Table 1. In general, we notice a matching performance degradation with spoofing artefacts, however the resulting EER degradation is still acceptable. It can be observed that the quality of the 950 artefacts (dorsal and palmar) is consistent for all spoofed patterns, since the FMR1000 and ZeroFMR remain quite stable in this case. For the 850 spoofs on the other hand, a large degradation in the FMR1000 and ZeroFMR can be observed, which indicates that some of the created artefacts did not have sufficient quality. Furthermore, the baseline performance is much lower for the palmar view compared to the dorsal one (3.01% vs. 16.99%), while the relative EER degradation using spoofed artefacts behaves stably and ranges approximately between 4% and 7% for all modalities.

Table 2 illustrates the comparison scores (genuine and impostor) of the created FV spoofing artefacts compared to the baseline, where only bona fide

Artefact Type	aGen	aImp
Baseline	0.2346	0.1257
Wax	0.1222	0.1236
Wax traced	0.1199	0.1220
Wax CLAHE	0.1252	0.1199
Silicone	0.1285	0.1297
Silicone traced	0.1250	0.1250
Silicone CLAHE	0.1274	0.1283

Table 2. Average genuine (aGen) and impostor (aImp) FV comparison scores obtained when verifying bona fide samples only (baseline) compared to verifying bona fide samples against PAs using different artefact types for light transmission FV recognition.

images have been used. The scores have been averaged over all three fingers and paper types for illustration purposes because of the small variation in their scores. It is immediately noticeable that none of the spoofing artefacts is meeting the quality requirements, since the obtained genuine and impostor scores are not differentiable. This is also true for the visually promising traced wax artefacts. Therefore, a further refinement of these artefacts is necessary to come up with a dataset of sufficient quality as required for a sensible PAD evaluation.

5.3. Results: PAD Performance

Following the evaluation of the produced spoofing artefacts' quality, this section covers the detection performance of the PAD system described in section 4. The evaluation of the PAD system is only performed for presentation attacks using HV artefacts due to insufficient quality of the FV artefacts. The available genuine and spoofed data was split 50/50 on a user basis for training and testing.

The PAD detection performance under different illumination conditions in terms of D-EER, BPCER @ APCER<=0.001 (BPCER1000) and BPCER @ APCER=0 (BPCER0) is reported in Table 3. It becomes apparent that the artefacts are harder to detect under 950nm NIR than under 850nm one. This might be due to varying reflectivity and absorption properties of the vein pattern prints for different NIR wavelengths. The PAD system has some problems in correctly classifying the palmar 950nm artefacts, however the PAD performance can be considered good to excellent across all HV artefacts.

	D-EER	BPCER1000	BPCER0
Dorsal 850	0.22	0.43	0.43
Dorsal 950	0.33	0.65	0.65
Palmar 850	0.00	0.00	0.00
Palmar 950	6.04	30.43	30.43

Table 3. Performance values (in %) for hand veins PAD evaluation

6. Conclusion

Presentation attacks are still a major problem in many applications of biometric recognition systems. Recent publications have shown that even vascular pattern based systems are susceptible to this kind of attack. In this work, we investigated two approaches to produce presentation attack artefacts, one for finger veins and one for hand veins. We also developed a suitable presentation attack detection scheme for vein recognition systems based on a natural scene statistics framework. We established a hand vein presentation attack dataset, consisting of 100 presentation attack samples and the corresponding original samples, which is publicly available as part of the PROTECT MMDB v2[1].

The PAD evaluation results on the established dataset showed that the proposed PAD approach achieves a good performance in detecting the fake representations. The verification experiment further revealed that if the fake representations are not detected, they achieve a rather high verification rate, i.e. that there is a good chance that a presentation attack is successful if no suitable PAD approach is employed.

Our future work will include tests with other types of presentation attack artefacts for the hand veins and the establishing of a presentation attack dataset for finger veins as well.

References

[1] A. P. S. Bhogal, D. Söllinger, P. Trung, J. Hämmerle-Uhl, and A. Uhl. Non-reference image quality assessment for fingervein presentation attack detection. In *Scandinavian Conference on Image Analysis*. Springer, 2017.

[2] H. Hofbauer and A. Uhl. Applicability of no-reference visual quality indices for visual security assessment. In *Proceedings of the 6th ACM Workshop on Information Hiding and Multimedia Security*, 2018.

[1] Will be released at `http://projectprotect.eu`

[3] ISO/IEC JTC1 SC37 Biometrics. ISO/IEC IS 19795-1:2006, it – Biometric performance testing and reporting – Part 1: Principles and framework.

[4] ISO/IEC JTC1 SC37 Biometrics. *ISO/IEC IS 30107-1:2016, IT – Biometric presentation attack detection – Part 1: Framework.*

[5] ISO/IEC JTC1 SC37 Biometrics. *ISO/IEC IS 30107-3:2017, IT – Biometric presentation attack detection – Part 3: Testing and Reporting.*

[6] C. Kauba, B. Prommegger, and A. Uhl. Focussing the beam - a new laser illumination based data set providing insights to finger-vein recognition. In *2018 IEEE 9th Int. Conference on Biometrics Theory, Applications and Systems (BTAS)*, Los Angeles, California, USA, 2018.

[7] C. Kauba, B. Prommegger, and A. Uhl. Openvein - an open-source modular multipurpose finger vein scanner design. In A. Uhl, C. Busch, S. Marcel, and R. Veldhuis, editors, *Handbook of Vascular Biometrics*, chapter 3. Springer Nature Switzerland AG, Cham, Switzerland, 2019.

[8] C. Kauba and A. Uhl. Shedding light on the veins - reflected light or transillumination in hand-vein recognition. In *Proceedings of the 11th IAPR/IEEE Int. Conference on Biometrics (ICB'18)*, Gold Coast, Queensland, Australia, 2018.

[9] C. Kauba and A. Uhl. An available open-source vein recognition framework. In A. Uhl, C. Busch, S. Marcel, and R. Veldhuis, editors, *Handbook of Vascular Biometrics*, chapter 4. Springer Nature Switzerland AG, Cham, Switzerland, 2019.

[10] D. Kocher, S. Schwarz, and A. Uhl. Empirical evaluation of lbp-extension features for finger vein spoofing detection. In *2016 Int. Conference of the Biometrics Special Interest Group (BIOSIG)*. IEEE, 2016.

[11] A. Kumar and Y. Zhou. Human identification using finger images. *Image Processing, IEEE Transactions on*, 21(4), 2012.

[12] B. Maser, D. Söllinger, and A. Uhl. Prnu-based detection of finger vein presentation attacks. In *2019 7th Int. Workshop on Biometrics and Forensics (IWBF)*, 2019.

[13] A. Mittal, A. K. Moorthy, and A. C. Bovik. No-reference image quality assessment in the spatial domain. *IEEE Transactions on image processing*, 21(12), 2012.

[14] N. Miura, A. Nagasaka, and T. Miyatake. Extraction of finger-vein patterns using maximum curvature points in image profiles. *IEICE transactions on information and systems*, 90(8), 2007.

[15] B. Mythily and K. Sathyaseelan. Measuring the quality of image for fake biometric detection: application to finger vein. In *National conference on research advances in communication, computation, electrical science and structures (NCRACCESS)*, 2015.

[16] D. T. Nguyen, Y. H. Park, K. Y. Shin, S. Y. Kwon, H. C. Lee, and K. R. Park. Fake finger-vein image detection based on fourier and wavelet transforms. *Digital Signal Processing*, 23(5), 2013.

[17] D. T. Nguyen, H. S. Yoon, T. D. Pham, and K. R. Park. Spoof detection for finger-vein recognition system using nir camera. *Sensors*, 17(10), 2017.

[18] X. Qiu, W. Kang, S. Tian, W. Jia, and Z. Huang. Finger vein presentation attack detection using total variation decomposition. *IEEE Transactions on Information Forensics and Security*, 13(2), 2017.

[19] R. Raghavendra, M. Avinash, S. Marcel, and C. Busch. Finger vein liveness detection using motion magnification. In *2015 IEEE 7th Int. Conference on Biometrics Theory, Applications and Systems (BTAS)*. IEEE, 2015.

[20] R. Raghavendra and C. Busch. Presentation attack detection algorithms for finger vein biometrics: A comprehensive study. In *2015 11th Int. Conference on Signal-Image Technology & Internet-Based Systems (SITIS)*. IEEE, 2015.

[21] A. F. Sequeira, J. Ferryman, L. Chen, C. Galdi, J.-L. Dugelay, V. Chiesa, A. Uhl, B. Prommegger, C. Kauba, S. Kirchgasser, A. Grudzien, M. Kowalski, L. Szklarski, P. Maik, and P. Gmitrowicz. PROTECT Multimodal DB: a multimodal biometrics dataset envisaging border control. In *Proceedings of the Int. Conference of the Biometrics Special Interest Group (BIOSIG'18)*, Darmstadt, Germany, 2018.

[22] D. Söllinger, P. Trung, and A. Uhl. Non-reference image quality assessment and natural scene statistics to counter biometric sensor spoofing. *IET Biometrics*, 7(4), 2018.

[23] S. Tirunagari, N. Poh, M. Bober, and D. Windridge. Windowed dmd as a microtexture descriptor for finger vein counter-spoofing in biometrics. In *2015 IEEE Int. Workshop on Information Forensics and Security (WIFS)*. IEEE, 2015.

[24] P. Tome and S. Marcel. On the vulnerability of palm vein recognition to spoofing attacks. In *The 8th IAPR Int. Conference on Biometrics (ICB)*, May 2015.

[25] P. Tome, R. Raghavendra, C. Busch, S. Tirunagari, N. Poh, B. Shekar, D. Gragnaniello, C. Sansone, L. Verdoliva, and S. Marcel. The 1st competition on counter measures to finger vein spoofing attacks. In *2015 Int. Conference on Biometrics (ICB)*. IEEE, 2015.

[26] P. Tome, M. Vanoni, and S. Marcel. On the vulnerability of finger vein recognition to spoofing. In *IEEE Int. Conference of the Biometrics Special Interest Group (BIOSIG)*, Sept. 2014.

[27] A. Uhl, C. Busch, S. Marcel, and R. Veldhuis. *Handbook of vascular biometrics*. Springer, 2020.