DOI: 10.1109/IWBF50991.2021.9465091

Confronting a Variety of Finger Vein Recognition Algorithms With Wax Presentation Attack Artefacts

Johannes Schuiki ♦ Bernhard Prommegger ♦ Andreas Uhl

Department of Computer Sciences, University of Salzburg, Austria

Abstract

Presentation attacks for finger vein recognition systems has emerged to be a widely researched topic. For this reason, a previously published, shown to be non-functional, approach for presentation attack artefact generation has been redesigned and used as a basis to generate a new publicly available finger vein presentation attack database. In order to assess the threat emitted by those artefacts from a broad perspective, an extensive vulnerability analysis including twelve finger vein recognition algorithms, that can be grouped into three meta categories of algorithms, was conducted. Experiments on the group of vein structure-based recognition algorithms, that also includes the de facto standard feature extraction method for vulnerability analysis, indicate a high level of threat by Impostor Attack Presentation Match Rates up to 90%. However, fundamentally different approaches (i.e. more relying on the entire finger texture under NIR illumination) show little to no susceptibility at all. This indicates that the actual threat level represented by presentation attack artefacts has to be re-considered in the light of these results.

Contents

This work has been partially supported by the Austrian Science Fund, project no. P32201.

1 Introduction

There are various reasons for using biometric traits as a method for authentication instead of well-established methodologies. Forgotten passwords, stolen keys and fraudulently imitated signatures are probably among the most popular shortcomings of classical authentication systems. Biometric traits can be any physiological or behavioural characteristic as long as it has the property of being unique per person in order to have a high level of distinctiveness. Eligible options include fingerprint, facial images or vascular pattern. This work focuses on finger vein images, which is a specific example of the latter category. Since vein structures are invisible to the naked eye, special hardware for capturing such images is almost inevitable. The demand for extra hardware and the fact that no latent prints are left behind, as it is the case with fingerprints, yields additional levels of security since forgery becomes more challenging. However, the last decade has brought forward several publications that presented multiple ways to potentially fool finger vein authentication systems. One type of such attempts to deceive a biometric system are known as presentation attacks and can be generated as easily as printing a previously captured finger vein image on a piece of paper and presenting this printout to the sensor. Table 1 aims to give an overview (i) about related works that use existing finger vein presentation attack databases or generate new attack samples and also (ii) how the vulnerability of finger vein recognition systems to those corresponding attack samples was determined and measured.

Most of the existing work uses either ink- and laserprints on different paper types or on overhead projector film. There is very scarce literature on different approaches: [1] utilized a smartphone display where vein images were shown, in [2], the goal was to create a sort of master sample that exploits a weakness in a matching algorithm, [3] used a prosthetic finger and a rubber cap with printed finger vein images glued onto it to test a hardware based liveness detection and [4] used a variation of presentation attacks that employ wax and silicone casts but no successful matching was reported.

In order to demonstrate the actual functionality of created presentation attacks, some authors utilize what is known as a ”2 Scenario Protocol” which is described in Section 3. Nearly all use Maximum Curvature [25] finger vein template generation together with cross correlation template comparison for such a vulnerability analysis. One recent publication [21] tests Wide Line Detector [26] and Repeated Line Tracking [27] as template generation algorithms in addition to the aforementioned Maximum Curvature. All three methods belong to the category of vein pattern based recognition schemes (which finally store a binary pattern of the vascular structure). Most related works however just assume that their created spoofs would be a threat to finger vein recognition systems based on related work.

Currently, only two of the related publications made their collected databases accessible to public: The Idiap Research Institute VERA Fingervein Database (IDIAP VERA) [7] and South China University of Technology Finger Vein Database (SCUT-FVD) [12].

From this description of the related work the novelty and contribution of this work can be derived as:

- Finger vein presentation attack generation recipe that employs beeswax together with prints of extracted vein structures in order to simulate a human finger, overcoming the limitations of [4] to successfully spoof the sensor described in [28].
- Generation of a corresponding publicly available finger vein presentation attack dataset.
- Testing 12 finger vein recognition algorithms on their vulnerability to the newly generated presentation attack samples, that include vein pattern based, keypoint based and texture based approaches.

The remainder of this work is structured as follows: Section 2 describes the generation of the artefact samples, in section 3 a vulnerability analysis with various finger vein recognition algorithms is conducted and section 4 reports the conclusion of the paper.

2 Artefact Generation

The presentation attack (PA) database introduced in this section uses a subset of the *PLUSVein-FV3* [22] data set as a starting point. This subset comprises of six fingers (index, middle and ring finger of both hands) from 22 subjects in two illumination variants (LED and Laser). Every sample in the reference database was acquired in five distinct capturing sessions. Three of which are used for the PA generation, making a total of 660 bona fide and 396 presentation attack samples per light source. For 16 of the subjects, new bona fide acquisitions were made. Note that the newly acquired sample images have not been captured under supervision thus the acquisition can

Table 1: Overview recent publications that used or generated finger vein attack samples; The term ”2 Scenario Protocol” refers to the same protocol as the one described in section 3.

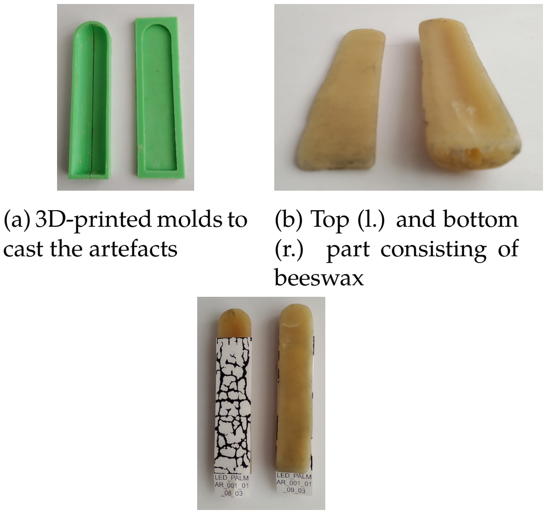
Year	Ref.	Database	Artefact type	Vulnerability Analysis
2013	[5]	Custom DB (private)	Laser printed on 2 types of paper and overhead projector film; 300, 1200 & 2400 dpi	Comparison of 2 Cases: (i) Enrollment Live & Recognition Fake and (ii) Enrollment Fake & recognition Fake; LBP + Hamming Distance
2014	[6]	IDIAP VERA (subset, spoof extension introduced here)	Laser printed on 200gr. paper; contours enhanced w/ blackboard marker	2 Scenario Protocol; Maximum Curvature + Correlation; SFAR (IAPMR) 86%
2015	[7]	IDIAP VERA (full set introduced here)	See [6]	–
	[8]	IDIAP VERA [6]	See [6]	–
	[1]	Custom Image Presentation Attack Database (private)	InkJet printed on 200gr. normal paper, Laser printed on 300gr. glossy paper & presented on smartphone display	2 Scenario Protocol; Maximum Curvature + Correlation; SFAR (IAPMR) 78%, 76.4% & 100%, respectively
	[9]	Custom Video Presentation Attack Database (private)	InkJet printed on 200gr. normal paper, Laser printed on 300gr. glossy paper	2 Scenario Protocol; Maximum Curvature + Correlation; SFAR (IAPMR) 90.62% & 91.87%, respectively
2016	[10]	IDIAP VERA [6]	See [6]	–
	[2]	Custom DB (private)	Single ”wolf attack” sample, that is supposed to match with every enrolled template	2 Scenario Protocol; Maximum Curvature; Success probability (IAPMR) 51.6%
2017	[11]	Custom DB from [5]	See [5]	–
		IDIAP VERA [6]	See [6]	–
	[12]	SCUT-FVD (introduced here)	Sandwiched printed artefact on overhead projector film - white paper 200gr. - printed artefact on overhead projector film	–
		IDIAP VERA [6]	See [6]	–
	[13]	Custom DB from [9]	See [9]	–
		Custom DB from [1]	Subset: Inkjet printed and Laser printed from [1]	–
	[14]	IDIAP VERA [6]	See [6]	–
2018	[15]	SCUT-FVD [12]	See [12]	–
		IDIAP VERA [6]	See [6]	–
	[3]	Custom DB (private)	Paper print, prosthetic finger & rubber cap with finger vein image pasted onto it on the latter two	–
	[16]	Custom DB from [9]	See [9]	–
		Custom DB from [1]	Subset Inkjet printed and Laser printed from [1]	–
	[17]	IDIAP VERA [6]	See [6]	–
2019	[18]	Custom DB (private)	Printed with high resolution printer on paper	–
	[19]	Custom DB (private)	Laser printed on glossy paper, algorithmically enhanced	–
	[20]	SCUT-FVD [12]	See [12]	–
		IDIAP VERA [6]	See [6]	–
	[21]	IDIAP VERA [6]	See [6]	2 Scenario Protocol in 4 self defined sub versions; Maximum Curvature, Repeated Line Tracking & Wide Line Detector; IAPMR (full protocol) 89%, 34% and 80%, respectively
2020	[4]	Subset from PLUS-Vein-FV3 [22] Data set (private)	Laser printed, enhanced using permanent marker & by software; Sandwiched into top & bottom made from silicone and wax, respectively	Comparison of average genuine and average impostor scores per artefact; Maximum Curvature + Correlation
	[23]	SCUT-FVD [12]	See [12]	Pass rate := #successful attacks / #total attacks; 22% and 100% on a system that is not further described
		IDIAP VERA [6]	See [6]	–
2021	[24]	SCUT-FVD [12]	See [12]	–

be labelled as being “unattended”. The capturing device in use is the *PLUS OpenVein finger vein sensor* (LED and Laser version) [28].

The presentation attack artefacts are designed to work for sensors with transillumination (camera and illumination module are on opposite sites of the finger). Their design follows the idea presented in [29]: The body of the artefacts are made of beeswax whereas the vein pattern itself is printed on white paper using a using a laser printer (’HP LaserJet 500 colour M551’). The body of the artificial wax finger is made up of two parts. The bottom part, which is presented towards the illumination module, has an elliptic shape with width 20 mm and height 8 mm (ratio of major to minor axis is 1:0.8 as assumed by Huang *et al*. in [30]). Its task is to diffuse the penetrating light and thus ensure uniform illumination. The upper part is a rectangular shaped strip with a height of 2 mm and is responsible for the blurring of the vein pattern. During acquisition, the top part is aligned towards the camera. Both parts can be seen in figure 1b. The lid (on the left side) has a rectangular cross section and is thinner (2 mm) than the elliptic bottom part (8 mm). Both parts are cast of yellow beeswax using the moulds shown in figure 1a. In figure 1c one can see the usage of the printed vein

Table 2: Overview number of images in data set

Sample Type	Unique Fingers	Samples	Images
PLUS-FV3 Bona Fide LED	132 (22 * 6)	5	660
PLUS-FV3 Bona Fide Laser	132 (22 * 6)	5	660
Unattended Bona Fide LED	96 (16 * 6)	5	480
Unattended Bona Fide Laser	96 (16 * 6)	5	480
Presentation Attack LED thick	132 (22 * 6)	3	396 [1]
Presentation Attack LED thin	132 (22 * 6)	3	396
Presentation Attack Laser thick	132 (22 * 6)	3	396 [1]
Presentation Attack Laser thin	132 (22 * 6)	3	396



(a) 3D-printed molds to cast the artefacts

(b) Top (l.) and bottom (r.) part consisting of beeswax

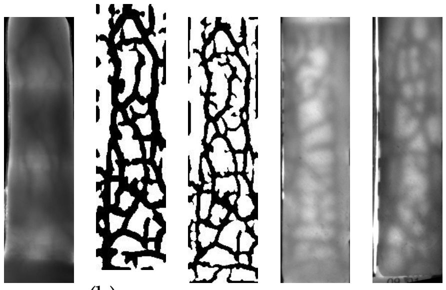
(c) Use of artefact with printed vein pattern

Figure 1: Generation and use of beeswax artefacts

image: it is placed on the bottom piece and covered with the lid.

Similar beeswax casts have already been used in [4]. While in [4] the authors acquire the artefacts using different printed versions of the original vein image (image space: no enhancement, CLAHE [31], tracing with black marker), which have been reported not to be useful for a successful presentation attack, this work uses printouts of the already extracted vein patterns (feature space) inside the beeswax artefact. The vein patterns are extracted using principal curvature (PC) [32] feature extraction in two thicknesses, denoted *thick* and *thin*

Figure 2 shows the original image, the corresponding feature images and two randomly selected resulting LED and Laser presentation attacks. Table 2 gives the numbers on the acquired images per acquisition type. The data set is publicly available for research purposes and can be downloaded at `http://wavelab.at/sources/PLUS-FV3-PALMAR-Image-Spoof/`



(a) orig. (b) thick (c) thin (d) (e)

Figure 2: a) Bona fide sample b) & c) PC features d) Example PA LED thin e) Example PA Laser thick

3 Artefact Threat Evaluation

This section describes the evaluation process of the wax presentation attacks introduced in Section 2. In order to get a comprehensive overview of how hazardous these particular presentation attacks are, 12 feature extraction schemes are tested on their vulnerability which are briefly described:

First, this study uses seven vein pattern based feature extraction methods, six of which generate a binary feature image as a result of extracting vein structures from the background. *Maximum Curvature (MC) [25]* and *Repeated Line Tracking (RLT) [27]* achieve this by looking at the cross sectional profile of the finger vein image, *Wide Line Detector (WLD) [26]*, *Gabor Filter (GF) [33]* and *Isotropic Undecimated Wavelet Transform (IUWT) [34]* also consider local neighbourhood regions via filter convolution and *Principal Curvature (PC) [32]* first computes the normalized gradient field and then looks at the eigenvalues of the Hessian matrix at each pixel. The resulting binary images are compared using a correlation measure. One more advanced vein pattern based feature extraction and matching strategy is given by *Anatomy Structure Analysis-Based Vein Extraction (ASAVE) [35]*. This technique extracts two binary vessel structures, differing by the extent of used context in creating these.

Second, three keypoint based schemes are used, two of which being filtered versions of the general purpose keypoint detection and matching schemes *SIFT* and *SURF* as described in [36]. The third keypoint based method is *Deformation Tolerant Feature Point Matching (DTFPM) [37]* which was tailored especially for vein pattern by also looking at curvature and vein directions.

[1] Due to image acquisition errors, the presentation attack database part with thick lines consists only of 387 images for LED and 393 images for Laser illumination

Table 3: Vulnerability of various finger vein template matching schemes to the proposed artefact samples reported as Impostor Attack Presentation Matching Rate (IAPMR) and corresponding Equal Error Rate (EER) obtained via 2 scenario protocol.

Method	Bona Fide: PLUS-FV3						Bona Fide: Unattended New Captures					
	LED			Laser			LED			Laser		
	EER	IAPMR thick	IAPMR thin	EER	IAPMR thick	IAPMR thin	EER	IAPMR thick	IAPMR thin	EER	IAPMR thick	IAPMR thin
MC	0.61	72.29	89.52	1.29	58.37	75.00	4.24	43.03	54.86	13.81	48.50	56.77
PC	0.62	71.24	80.93	1.90	55.17	64.27	4.68	43.74	59.72	17.38	48.68	56.08
WLD	1.13	69.28	84.22	2.80	57.73	78.66	4.48	51.50	70.31	15.21	40.21	58.85
RLT	4.91	43.40	36.49	6.59	23.75	17.30	11.98	46.74	33.16	26.34	47.80	39.93
GF	1.06	37.78	60.98	2.65	31.80	53.41	5.84	32.10	47.92	15.92	30.16	46.35
IUWT	0.53	79.35	90.03	1.97	79.82	84.34	3.86	69.84	74.83	14.38	67.55	67.36
ASAVE	2.35	24.31	19.07	2.59	8.81	1.89	7.84	4.41	2.26	19.16	21.69	13.19
DTFPM	2.20	16.99	16.16	2.64	5.62	6.31	6.97	23.99	21.35	11.99	35.98	37.15
SURF	3.43	0.00	0.00	3.49	0.00	0.00	6.57	0.35	0.00	15.21	5.11	3.47
SIFT	0.96	0.00	0.00	0.91	0.00	0.13	2.42	0.35	0.17	11.19	0.71	1.04
LBP	3.79	0.00	0.38	4.24	0.00	0.00	10.18	0.88	0.69	15.33	3.88	6.42
CNN	2.89	0.67	0.35	6.8	0.0	0.05	6.36	0.7	0.83	10.62	0.48	0.62

Third, two generic texture-based techniques are considered. A *Local Binary Pattern* [38] descriptor that uses histogram intersection as comparison method and a *convolutional neural network (CNN)* based approach using triplet loss as presented in [39] are evaluated. For network training, the finger vein images from the PROTECT [40] data set have been used, since these descend from a similar sensor. With the exception of the CNN based matching scheme, all feature extraction schemes are evaluated using the *PLUS OpenVein Toolkit* [41].

In order to be in the same format as the *PLUSVein-FV3* database, every finger of the new presentation attack dataset was aligned with the horizontal axis by applying an appropriate rotation transformation. Afterwards a 192x736 pixel region of interest was extracted. The same preprocessing steps have been applied to the images from the PROTECT dataset.

3.1 Evaluation Protocol

For the experiments, the subsequent test scenarios were adopted in order to analyze the vulnerability of the biometric system to the printed wax artefacts [42]. These two scenarios are performed for both thicknesses of the presentation attack veins, both lighting variants of the sensor and every feature extraction scheme respectively:

- **Licit Scenario (Normal Mode)**: In this scenario, both enrollment and verification is accomplished using bona fide finger vein samples. Doing so, a set of genuine matching scores (positives) and zero effort impostor matching scores (negatives) in order to compute the False Match Rate (FMR, *i.e.* the ratio of wrongly accepted impostor attempts to the number of total impostor attempts) and False Non Match Rate (FNMR, *i.e.* the ratio of wrongly denied genuine attempts to the total number of genuine verification attempts) are acquired. An operating point is set at the threshold value where the FMR = FNMR (i.e. Equal Error Rate).

- **Spoof Scenario (Attack Mode)**: In the second scenario, similar to the first scenario, enrollment is accomplished using bona fide samples. Verification attempts are performed using presentation attack samples. By pretending that the presentation attack samples are bona fide samples, the set of "quasi-genuine" matching scores (positives) can be evaluated to compute the Impostor Attack Presentation Match Rate (IAPMR) as defined by the ISO/IEC 30107-3:2017 [43], i.e. the proportion of wrongly accepted presentation attacks given the threshold from the fist scenario.

3.2 Experimental Results

Table 3 contains the results of the experiments. Through horizontal lines, the feature extraction methods are split into three categories of methods: The first seven methods are vein pattern based, the intermediate methods are keypoint based and the two last methods can be classified as texture based. On the left hand side the results can be seen where finger vein images from the original *PLUSVein-FV3* database were used as bona fide samples while on the right table the newly acquired unattended images were used as bona fide samples. We observe

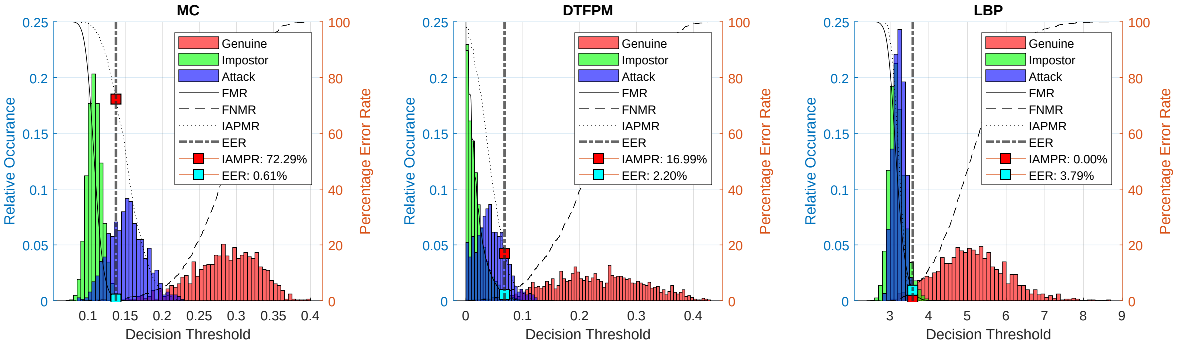


Figure 3: Depiction of the matching score distributions and the error rates acquired in the first and second scenario. One representative method for each category: MC for vein pattern based, DTFPM for keypoint based & LBP for texture based. The IAPMR and EER correspond to the case LED thick from the matching against the original *PLUSVein-FV3* in table 3.

a huge drop of EER which can be explained by the fact that these images were captured without supervision. This circumstance caused various lighting artefacts in the acquired finger vein images and thus we observe differences in the IAPMR as well. However the overall trend remains the same: We observe a vulnerability of vein pattern based feature extraction methodologies being, with the exception of RLT and ASAVE, always above 30% IAMPR meaning that at least every third presentation attack matches its corresponding bona fide finger. The overall highest false acceptance rate exhibits IUWT on the LED thin attacks with more than 90% IAMPR.

The general purpose keypoint descriptor and matching algorithms (i.e. filtered SIFT and SURF) on the other hand seem to be not prone at all to the generated wax artefacts. Having a maximum IAPMR of little above 5% for the case of the unattended bona fide samples but most of the experiments below 1% even reaching 0.00% sometimes. An exception represents the DTFPM scheme: Here we observe higher IAMPRs, which can be explained through the fact that this keypoint description scheme is a vein tailored one. The LBP and CNN achieve, similar to the general purpose keypoint schemes, error rates just above zero, sometimes even reaching 0.00% meaning that they are unsusceptible to the proposed presentation attacks.

These differences in attack vulnerabilities can be explained by the larger contexts that are used to created feature point and texture-based finger vein templates, respectively. While the vein pattern based schemes focus merely on the binary vessel layout only, the two other feature types also include the vincinity of the vessels and the inter-vessel texture in the template comparison process. Obviously, the artefacts do not model these sample image parts sufficiently similar to the original samples.

Three exemplary score distributions are shown in figure 3, representing one category of feature extraction schemes each.

4 Conclusion

In this study, a previously published non-functional finger vein presentation attack recipe, that employs a top and bottom cast made of beeswax together with a printed vein structure sandwiched in between, was reworked and tested on its level of threat to finger vein recognition systems. In order to do so, a database with two sightly different types of vein structure prints, captured with LED and laser illumination, was created and publicly released. As a starting point, a subset of an already existing finger vein database was used. Additionally, a second set of bona fide samples was acquired. The recording for the newly acquired bona fide finger vein samples has not been supervised thus representing a test case that simulates a real world environment where image recordings are not captured under laboratory conditions.

An extensive vulnerability analysis was conducted on 12 finger vein recognition schemes that includes vein pattern based, keypoint based and generic texture based feature extraction methodologies. Experimental results show that the new presentation attacks emit a high level of threat to vein pattern based schemes, while being relatively innoxious to recognition schemes from the other two categories. Thus, the actual threat level represented by certain presentation attack artefacts has to be re-evaluated in the context of the type of recognition scheme used in the targeted system.

Future work will include the transfer of this extensive test to other publicly available finger vein presentation attack databases such as IDIAP VERA and SCUT-FVD .

References

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

[2] A. Otsuka, T. Ohki, R. Morita, M. Inuma, and H. Imai, *Security evaluation of a finger vein authentication algorithm against wolf attack*, 37th IEEE Symposium on Security and Privacy, San Jose, CA, 2016.

[3] A. Krishnan, T. Thomas, G. R. Nayar, and S. Sasilekha Mohan, "Liveness detection in finger vein imaging device using plethysmographic signals", in *Intelligent Human Computer Interaction*, Springer International Publishing, 2018.

[4] L. Debiasi, C. Kauba, H. Hofbauer, B. Prommegger, and A. Uhl, "Presentation attacks and detection in finger- and hand-vein recognition", in *Proceedings of the Joint Austrian Computer Vision and Robotics Workshop (ACVRW'20)*, 2020.

[5] 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*, vol. 23, no. 5, 2013.

[6] P. Tome, M. Vanoni, and S. Marcel, "On the vulnerability of finger vein recognition to spoofing", in *2014 International Conference of the Biometrics Special Interest Group (BIOSIG)*, 2014.

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

[8] 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 International Workshop on Information Forensics and Security (WIFS)*, 2015.

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

[10] D. Kocher, S. Schwarz, and A. Uhl, "Empirical evaluation of lbp-extension features for finger vein spoofing detection", in *Proceedings of the International Conference of the Biometrics Special Interest Group (BIOSIG'16)*, 2016.

[11] D. Nguyen, H. Yoon, T. Pham, and K. Park, "Spoof detection for finger-vein recognition system using nir camera", *Sensors*, vol. 17, 2017.

[12] X. Qiu, S. Tian, W. Kang, W. Jia, and Q. Wu, "Finger vein presentation attack detection using convolutional neural networks", in *Biometric Recognition*, Springer International Publishing, 2017.

[13] R. Raghavendra, S. Venkatesh, K. B. Raja, and C. Busch, "Transferable deep convolutional neural network features for fingervein presentation attack detection", in *2017 5th International Workshop on Biometrics and Forensics (IWBF)*, 2017.

[14] 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 *Proceedings of 20th Scandinavian Conference on Image Analysis (SCIA'17)*, ser. Springer Lecture Notes on Computer Science, vol. 10269, 2017.

[15] 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*, vol. 13, no. 2, 2018.

[16] R. Raghavendra, K. B. Raja, S. Venkatesh, and C. Busch, "Fingervein presentation attack detection using transferable features from deep convolution neural networks", in *Deep Learning in Biometrics*, CRC Press, 2018, ch. 12.

[17] D. Söllinger, P. Trung, and A. Uhl, "Non-reference image quality assessment and natural scene statistics to counter biometric sensor spoofing", *IET Biometrics*, vol. 7, no. 4, 2018.

[18] J. Bok, K. Suh, and E. C. Lee, "Detecting fake finger-vein data using remote photoplethysmography", *Electronics*, vol. 8, 2019.

[19] J. M. Singh, S. Venkatesh, K. B. Raja, R. Ramachandra, and C. Busch, “Detecting finger-vein presentation attacks using 3d shape diffuse reflectance decomposition”, in *2019 15th International Conference on Signal-Image Technology Internet-Based Systems (SITIS)*, 2019.

[20] B. Maser, D. Söllinger, and A. Uhl, “Prnu-based detection of finger vein presentation attacks”, in *Proceedings of the 7th International Workshop on Biometrics and Forensics (IWBF’19)*, 2019.

[21] A. Anjos, P. Tome, and S. Marcel, “An introduction to vein presentation attacks and detection”, in *Handbook of Biometric Anti-Spoofing: Presentation Attack Detection*, Springer International Publishing, 2019.

[22] 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 International Conference on Biometrics Theory, Applications and Systems (BTAS)*, 2018.

[23] W. Yang, W. Luo, W. Kang, Z. Huang, and Q. Wu, “Fvras-net: An embedded finger-vein recognition and antispoofing system using a unified cnn”, *IEEE Transactions on Instrumentation and Measurement*, vol. 69, no. 11, 2020.

[24] W. Q. J. Lee, T. S. Ong, T. Connie, and H. T. Jackson, “Finger vein presentation attack detection with optimized lbp variants”, in *Advances in Cyber Security*, Springer Singapore, 2021.

[25] N. Miura, A. Nagasaka, and T. Miyatake, “Extraction of finger-vein patterns using maximum curvature points in image profiles”, *IEICE - Trans. Inf. Syst.*, vol. E90-D, no. 8, 2007.

[26] B. Huang, Y. Dai, R. Li, D. Tang, and W. Li, “Finger-vein authentication based on wide line detector and pattern normalization”, in *2010 20th International Conference on Pattern Recognition*, 2010.

[27] N. Miura, A. Nagasaka, and T. Miyatake, “Feature extraction of finger-vein patterns based on repeated line tracking and its application to personal identification”, *Machine Vision and Applications*, vol. 15, 2004.

[28] C. Kauba, B. Prommegger, and A. Uhl, “Openvein - an open-source modular multipurpose finger vein scanner design”, in *Handbook of Vascular Biometrics*, Springer Nature Switzerland AG, 2019, ch. 3.

[29] J. Krissler and Julian, *Venenerkennung hacken - Vom Fall der letzten Bastion biometrischer Systeme*, Chaos Computer Club e.V. https://doi.org/10.5446/39201, last accessed: 21 Jan 2021, 2018.

[30] B. Huang, Y. Dai, R. Li, D. Tang, and W. Li, “Finger-vein authentication based on wide line detector and pattern normalization”, in *Pattern Recognition (ICPR), 2010 20th International Conference on*, IEEE, 2010.

[31] K. Zuiderveld, “Contrast limited adaptive histogram equalization”, in *Graphics Gems IV*. Academic Press Professional, Inc., 1994.

[32] J. H. Choi, W. Song, T. Kim, S.-R. Lee, and H. C. Kim, “Finger vein extraction using gradient normalization and principal curvature”, in *Image Processing: Machine Vision Applications II*, vol. 7251, 2009.

[33] A. Kumar and Y. Zhou, “Human identification using finger images”, *IEEE Transactions on Image Processing*, vol. 21, no. 4, 2012.

[34] J. Starck, J. Fadili, and F. Murtagh, “The undecimated wavelet decomposition and its reconstruction”, *IEEE Transactions on Image Processing*, vol. 16, no. 2, 2007.

[35] L. Yang, G. Yang, Y. Yin, and X. Xi, “Finger vein recognition with anatomy structure analysis”, *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 28, no. 8, 2018.

[36] C. Kauba, J. Reissig, and A. Uhl, “Preprocessing cascades and fusion in finger vein recognition”, in *Proceedings of the International Conference of the Biometrics Special Interest Group (BIOSIG’14)*, 2014.

[37] Y. Matsuda, N. Miura, A. Nagasaka, H. Kiyomizu, and T. Miyatake, “Finger-vein authentication based on deformation-tolerant feature-point matching”, *Machine Vision and Applications*, vol. 27, 2016.

[38] E. C. Lee, H. C. Lee, and K. R. Park, “Finger vein recognition using minutia-based alignment and local binary pattern-based feature extraction”, *Int. J. Imaging Syst. Technol.*, vol. 19, no. 3, 2009.

[39] G. Wimmer, B. Prommegger, and A. Uhl, “Finger vein recognition and intra-subject similarity evaluation of finger veins using the cnn triplet loss”, in *Proceedings of the 25th International Conference on Pattern Recognition (ICPR)*, 2020.

[40] C. Galdi, J. Boyle, L. Chen, V. Chiesa, L. Debiasi, J.-L. Dugelay, J. Ferryman, A. Grudzień, C. Kauba, S. Kirchgasser, M. Kowalski, M. Linortner, P. Maik, K. Michoń, L. Patino, B. Prommegger, A. F. Sequeira, Ł. Szklarski, and A. Uhl, "Protect: Pervasive and user focused biometrics border project – a case study", *IET Biometrics*, vol. 9, no. 6, 2020.

[41] C. Kauba and A. Uhl, "An available open-source vein recognition framework", in *Handbook of Vascular Biometrics*, Springer Nature Switzerland AG, 2019, ch. 4.

[42] I. Chingovska, A. Mohammadi, A. Anjos, and S. Marcel, "Evaluation methodologies for biometric presentation attack detection", in *Handbook of Biometric Anti-Spoofing: Presentation Attack Detection*, Springer International Publishing, 2019.

[43] I. J. S. B. I. 30107-3, "Information technology — biometric presentation attack detection — part 3: Testing and reporting", International Organization for Standardization, ISO ISO/IEC 30107-3:2017, 2017.