Vulnerability Assessment and Presentation Attack Detection Using a Set of Distinct Finger Vein Recognition Algorithms

Johannes Schuiki, Georg Wimmer, Andreas Uhl
Department of Computer Sciences
University of Salzburg
{jschuiki, gwimmer, uhl}@cs.sbg.ac.at

Abstract

The act of presenting a forged biometric sample to a biometric capturing device is referred to as presentation attack. During the last decade this type of attack has been addressed for various biometric traits and is still a widely researched topic. This study follows the idea from a previously published work which employs the usage of twelve algorithms for finger vein recognition in order to perform an extensive vulnerability analysis on a presentation attack database. The present work adopts this idea and examines two already existing finger vein presentation attack databases with the goal to evaluate how hazardous these presentation attacks are from a wider perspective. Additionally, this study shows that by combining the matching scores from different algorithms, presentation attack detection can be achieved.

1. Introduction

The human body provides various features that have been found to be well suited for the task of distinguishing persons, *i.e*. have a high inter class variability. In the field of biometrics such features are known as biometric traits and include physiological as well as behavioural characteristics. Popular examples of such traits are fingerprints, properties of voice recordings, keystroke dynamics, facial images or vascular pattern. This research focuses on vascular pattern in the human finger. Finger vein structures are captured using special hardware that operates on the near infrared wavelength spectrum. That is due to the observation that the oxygen saturated hemoglobin in the blood has a relatively high molar extinction coefficient for this particular part of the wavelength spectrum. The veins in the finger therefore absorb the light, resulting in dark lines in the acquired image. Although the need for special hardware adds an extra layer of security, researchers in this area [16, 23] shed light on the fact that finger vein recognition systems can potentially be fooled with forged samples. Maliciously forged samples that are intended to interfere with the operation of the biometric system are known as presentation attacks. Such presentation attacks can be created as easy as printing previously captured finger vein images on a piece of blank white paper [23].

978-1-6654-3780-6/21/$31.00 ©2021 IEEE

Countermeasures for such attacks are referred to as presentation attack detection (PAD). Presentation attack detection methods in general operate either on single images (the interested reader is referred to table 14.1 in [10] which provides a comprehensive overview including hand crafted methods that employ image quality, generic texture and spatial frequency components as well as convolutional neural network based methods), on consecutive images (*i.e*. video sequences) [18] or utilize more than one biometric trait, therefore increasing the effort to deceive every single biometric capturing device [4].

In order to evaluate the effectiveness of such PAD algorithms, either private data sets or publicly available databases are used. Currently, three finger vein presentation attack databases are available for the research community: The Idiap Research Institute VERA Fingervein Database (IDIAP VERA) [22], the South China University of Technology Finger Vein Database (SCUT-SFVD) [17] and the Paris Lodron University of Salzburg Finger Vein Spoofing Data Set (PLUSVein-Spoof) [19].

For the sake of demonstrating the actual level of threat emitted from created presentation attack data sets, a common threat evaluation methodology is what is known as ”2 scenario protocol” which is described in section 3.1. Most authors that utilize this protocol use Maximum Curvature [15] finger vein template generation together with cross correlation template comparison. For the IDIAP VERA set, one recent publication [2] tests Wide Line Detector [5] and Repeated Line Tracking [14] as template generation algorithms in addition to the aforementioned Maximum Curvature. In case of the SCUT-SFVD, a publication [26] reports a pass rate that is defined as successful attacks di-

vided by the total attacks using a recognition method that is not further described. The publication that introduced the PLUSVein-Spoof database [19] contains a vulnerability analysis that employs twelve different finger vein recognition schemes in order to evaluate how hazardous the presentation attacks are from a broader perspective.
This research aims to re-evaluate the threat emitted by SCUT-SFVD & IDIAP VERA by considering a greater pool of feature extraction and matching schemes, such as in [19]. Additionally, experiments are carried out whether score level fusion from various matching schemes could be used as PAD. Therefore the remainder of this paper is structured as follows: Section 2 presents a description of the databases used in the later sections. In section 3, the scheme for a comprehensive vulnerability analysis is adopted from [19] and performed on the IDIAP VERA and SCUT-SFVD databases. In section 4 various combinations of the similarity scores from the matching schemes in section 3 are evaluated for their applicability as PAD method. Section 5 reports the conclusion of this research.

2. Databases

This section describes the finger vein presentation attack databases used in the later parts of this research:

A) *The Idiap Research Institute VERA Fingervein Database (IDIAP VERA):* The IDIAP VERA finger vein database consists of 440 bona fide images that correspond to 2 acquisition sessions of left and right hand index fingers of 110 subjects. Therefore considered as 220 unique fingers captured 2 times each. Every sample has one presentation attack counterpart. Presentation attacks are generated by printing preprocessed samples on high quality paper using a laser printer and enhancing vein contours with a black whiteboard marker afterwards. Every sample is provided in two modes named *full* and *cropped*. While the full set is comprised of the raw images captured with size 250x665, the cropped images were generated by removing a 50pixel margin from the border, resulting in images of size 150x565.

B) *South China University of Technology Spoofing Finger Vein Database (SCUT-SFVD):* The SCUT-SFVD database was collected from 6 fingers (*i.e*. index, middle and ring finger of both hands) of 100 persons captured in 6 acquisition sessions, making a total of 3600 bona fide samples. For presentation attack generation, each finger vein image is printed on two overhead projector films which are aligned and stacked. In order to reduce overexposure, additionally a strong white paper ($200g/m^2$) is put in-between the two overhead projector films. Similar to the IDIAP VERA database, the SCUT-SFVD is provided in two modes named *full* and *roi*. While in the full set every image sample has a resolution of 640x288 pixel, the samples from the roi set are of variable size. Since the LBP and the ASAVE matching algorithm can not be evaluated on variable sized image samples, a third set was generated for this study named *roi-resized* where all roi samples have been resized to 474x156 which corresponds to the median of all heights and widths from the roi set as can be seen in figure 1.

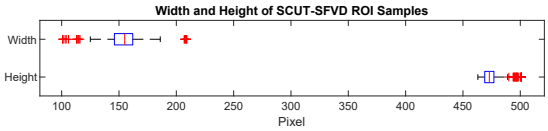

Figure 1: The image resolutions of the SCUT-SFVD roi samples vary, therefore all roi samples have been resized to the median resolution.

C) *Paris Lodron University of Salzburg Finger Vein Spoofing Data Set (PLUSVein-Spoof):* The PLUSVein-Spoof database uses a subset of the *PLUSVein-FV3* [7] database as bona fide samples. For the collection of presentation attack artefacts, binarized vein images from 6 fingers (*i.e*. index, middle and ring finger of both hands) of 22 subjects were printed on paper and sandwiched into a top and bottom made of beeswax. The binarization was accomplished by applying Principal Curvature [3] feature extraction in two different levels of vessel thickness, named *thick* and *thin*. The original database was captured with two types of light sources, namely *LED* and *Laser*. Therefore, presentation attacks were created for both illumination variants. While the original database was captured in 5 sessions per finger, only three of those were reused for presentation attack generation. Summarized, a total of 396 (22*6*3) presentation attacks per light source (LED & Laser) and vein thickness (thick & thin) with corresponding to 660 (22*6*5) bona fide samples are available. Every sample is of size 192x736.

3. Threat analysis

This work follows the idea from a previous publication [19] in which a new finger vein presentation attack database (database C from section 2) is examined for the actual level of threat which its presentation attacks emit to a variety of recognition algorithms. In order to do so, an evaluation protocol which is described in section 3.1 is used. The goal from the experiments in this section is to transfer this threat analysis and apply it on two additional publicly available finger vein presentation attack databases (databases A and

B from section 2). In total, this study includes twelve different finger vein recognition schemes that can be categorized into three classes of algorithms, based on the type of feature they extract from acquired finger vein samples:

- *Binarized vessel images*: Seven feature extraction schemes are used which finally store a binary image of the extracted vessel structures as feature. The overall goal for these kind of feature extractors therefore is the separation of vein structures from the remaining parts of the finger as well as from the background. *Maximum Curvature (MC) [15]* and *Repeated Line Tracking (RLT) [14]* try to achieve this by looking at the cross sectional profile of the finger vein image. Other methods such as *Wide Line Detector (WLD) [5]*, *Gabor Filter (GF) [11]* and *Isotropic Undecimated Wavelet Transform (IUWT) [21]* also consider local neighbourhood regions by using filter convolution. A slightly different approach is given by *Principal Curvature (PC) [3]* which first computes the normalized gradient field and then looks at the eigenvalues of the hessian matrix at each pixel. All so far described binary image extraction methods use a correlation measure to compare probe and template samples which is often referred to as *Miura-matching* due to its introduction in Miura *et al*. [14]. One more sophisticated vein pattern based feature extraction and matching strategy is *Anatomy Structure Analysis-Based Vein Extraction (ASAVE) [25]*, which includes two different techniques for binary vessel structure extraction as well as a custom matching strategy.

- *Keypoints*: The term keypoint refers to an interesting point in an image, where the term *interesting* strongly depends on the given application. This research uses three keypoint based feature extraction and matching schemes. One such keypoint detection method, known as *Deformation Tolerant Feature Point Matching (DTFPM) [13]*, was especially tailored for the task of finger vein recognition. This is achieved by considering shapes that are common in finger vein structures. Additionally, modified versions general purpose keypoint detection and matching schemes, *SIFT* and *SURF*, as described in [8] are tested in this research. The modification includes filtering such that only keypoints inside the finger are used while keypoints at the finger contours or even in the background are discarded.

- *Texture information*: This study includes two methods that can be counted to texture-based approaches. One being a *Local Binary Pattern [12]* descriptor that uses histogram intersection as a similarity metric. The second method is a *convolutional neural network (CNN)* based approach that uses triplet loss as presented in [24]. Similarity scores for the CNN approach are obtained by computing the inverse Euclidean distance given two feature vectors corresponding to two finger vein samples.

3.1. Evaluation protocol

In order to evaluate the threat emitted by the databases under question, a scheme that is known as "2 scenario protocol", which was also used for threat analysis in [19], is adopted for this research. The two scenarios are briefly summarized hereafter:

- **Licit Scenario (Normal Mode)**: The first scenario employs two types of users: Genuine (positives) and zero effort impostors (negatives). Therefore, both enrollment and verification is accomplished using bona fide finger vein samples. Through varying the decision threshold, the False Match Rate (FMR, *i.e*. the ratio of wrongly accepted impostor attempts to the number of total impostor attempts) and the False Non Match Rate (FNMR, *i.e*. the ratio of wrongly denied genuine attempts to the total number of genuine verification attempts) can be determined. The normal mode can be understood as a matching experiment which has the goal to determine an operating point for the second scenario. The operating point is set at the threshold value where the FMR = FNMR (i.e. Equal Error Rate).

- **Spoof Scenario (Attack Mode)**: The second scenario uses genuine (positives) and presentation attack (negatives) users. Similar to the first scenario, enrollment is accomplished using bona fide samples. Verification attempts are performed by matching presentation attack samples against their corresponding genuine enrollment samples or templates. Given the threshold from the licit scenario, the proportion of wrongly accepted presentation attacks is then reported as the Impostor Attack Presentation Match Rate (IAPMR), as defined by the ISO/IEC 30107-3:2017 [1].

3.2. Experimental results

Table 1 contains the outcomes from the evaluation protocol described in section 3.1 for every matching algorithm described earlier in section 3. Horizontal lines indicate a change of algorithm category. The first seven rows correspond to feature extraction schemes that extract a binary vessel image as feature, the intermediate three algorithms represent keypoint based schemes and the last two are generic texture based methods. Similar to the reference paper [19], all feature extraction schemes except for the CNN based matching scheme are evaluated using the *PLUS OpenVein Toolkit* [9]. Matching is achieved using

Method	IDIAP VERA				SCUT-SFVD					
	Full		Cropped		Full		ROI		ROI Resized	
	EER	IAPMR	EER	IAPMR	EER	IAPMR	EER	IAPMR	EER	IAPMR
MC	2.66	93.18	17.72	53.79	4.01	86.33	25.43	26.21	22.59	27.14
PC	2.73	90.45	20.91	49.24	4.79	84.67	25.86	25.73	23.41	26.08
WLD	6.03	93.48	13.18	63.48	7.60	74.21	21.18	21.34	16.96	18.83
RLT	30.00	41.67	27.19	38.64	14.01	40.36	5.34	14.07	2.94	9.46
GF	6.83	85.76	24.55	53.94	9.40	54.90	27.70	24.33	25.05	23.96
IUWT	4.95	93.18	13.30	64.24	6.29	74.06	17.70	20.69	11.87	16.51
ASAVE	9.11	72.58	19.10	68.79	11.56	74.98	–	–	6.03	59.88
DTFPM	10.45	26.21	6.69	81.97	8.90	73.75	5.20	52.31	5.63	55.08
SURF	11.39	0.91	11.62	14.24	5.49	4.18	9.69	6.27	9.41	7.42
SIFT	4.54	14.24	5.43	44.55	2.37	30.43	1.75	32.72	1.92	34.93
LBP	7.38	26.82	6.91	73.33	8.78	45.43	–	–	3.51	55.36
CNN	6.35	17.57	10.18	8.63	0.74	69.8	–	–	0.83	55.69

Table 1: Equal Error Rates (EER) and Impostor Attack Presentation Match Rates (IAPMR) evaluated for IDIAP VERA and SCUT-SFVD databases using twelve matching schemes. Note that for the CNN approach, the samples are being resized to a custom size anyway, therefore only values for ROI Resized are reported for SCUT-SFVD.

the 'FVC' matching mode which performs all possible genuine comparisons but only compares one sample of each subject to the one sample of all the remaining subjects as impostor comparisons. While the number of impostor comparisons is therefore drastically reduced, it is still ensured that every subject is matched against every other subject at least once. Symmetric comparisons are omitted in both cases. This toolkit also provides the option to set hyper parameters for the feature extraction and the matching process. These settings have been adopted from the reference paper as well. Since a related publication [2], by authors from the same research institute that published the IDIAP VERA database, also reported EER and IAPMR values for MC (1-2% EER, 77-89% IAPMR), RLT (11-19% EER, 32-38% IAPMR) and WLD (3-7% EER, 70-80% IAPMR) using varying matching protocols, one can verify that the used hyper parameters can be considered satisfactory. Unfortunately, for the SCUT-SFVD no such results for the methods used in this research have been reported so far that could be used as a reference. The CNN based approach was implemented in python. Due to the fact that this is a learning based approach, 2-fold-cross validation is applied for the results seen in table 1. Since such learning is non deterministic, the feature vectors from different folds must be evaluated separately meaning that EER and IAPMR reported are the arithmetic mean of both splits.

Binary vessel pattern based matching schemes reach IAPMRs as high as 93.18% for the case of the IDIAP VERA and 86.33% for the SCUT-SFVD database, which signalizes that in the worst case scenario 9 out of 10 presentation attacks would be a treated as a bona fide sample. When dealing with non-cropped versions of the databases, meaning that background is also visible on the finger vein images, one can often observe a lower EER as compared to the cropped or ROI versions. This indicates that the contour of the finger plays a significant role in recognition.

For the database that was introduced in the reference work, little to no susceptibility at all was reported when using keypoint based or generic texture based matching schemes. In this study however, the IAPMRs for the keypoint and texture based algorithms are very inhomogeneous, ranging from 0.91% (IDIAP VERA full, SURF) up to 81.97% (IDIAP VERA cropped, DTFPM). Interestingly, even though one would expect SIFT and SURF to achieve very similar results, a discrepancy can be observed. While SIFT in general obtains a lower EER, SURF occurs to be less prone to presentation attacks. Therefore it can be concluded that both the IDIAP VERA and the SCUT-SFVD presentation attacks samples in many cases pose a threat to the evaluated matching schemes, however future considerations should not disregard the fact that exceptions such as RLT (9.46% IAPMR on SCUT-SFVD ROI Resized) or SURF (consistently low IAPMRs) also exist.

4. PAD using score level fusion

With the observation from the previous section that different matching schemes vary in their behaviour when confronted with presentation attacks, the question arises whether one could combine multiple matching methods to achieve presentation attack detection. Therefore this section describes various experiments in order to do so. Combining

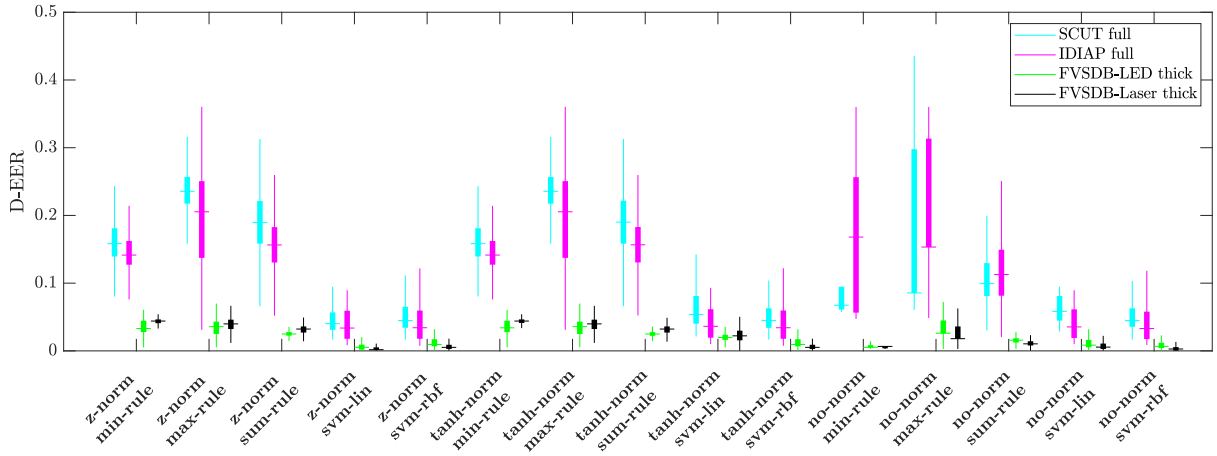

Figure 2: Cross combination of every normalization technique and every fusion method for at least one mode of every presentation attack database used in this work. Note that every histogram incorporates 4095 detection error rates corresponding to 4095 possible method constellations possible with 12 matching methods.

similarity scores from multiple matching schemes is generally referred to as *score level fusion*. In total, five techniques for the fusion of similarity scores are evaluated in this research. Let the similarity score from the ith recognition algorithm be denoted as S_i, where i is in the range from 1 to the number of considered matching algorithms N. Using simple fusion methods described below, a resulting fusion score f is obtained. With every comparison attempt now being described as a combined matching score f, the biometric probe sample can then be classified as either bona fide or presentation attack sample using simple thresholding. Three fusion methods have been adopted from [20]:

- *Simple Sum-Rule Fusion*

$$f = \sum_{i=1}^{N} S_i \tag{1}$$

- *Min-Rule Fusion*

$$f = min(S_1, ..., S_N) \tag{2}$$

- *Max-Rule Fusion*

$$f = max(S_1, ..., S_N) \tag{3}$$

Another approach follows the idea of forming a feature vector $\vec{x} = (S_1, ..., S_N)$ by concatenation of similarity scores. Doing so these new feature vectors are then classified using a *Support Vector Machine (SVM)* by applying k-fold cross validation. Experiments in section 4.1 provide results for using a linear kernel as well as radial basis function kernel.

Arguably, similarity scores from different classifiers do not necessarily need to be in the same range. Therefore, two popular score normalization schemes [6], *tanh-norm* and *z-norm*, are evaluated together with the option of omitting score normalization (*no-norm*). The formula for the calculation of *z-norm* is given by

$$S' = \frac{S - \mu}{\sigma} \tag{4}$$

and *tanh-norm* by

$$S' = 0.5 * \left(tanh\left(0.01 * \frac{S - \mu}{\sigma}\right) + 1 \right) \tag{5}$$

where σ is the standard deviation and μ is the arithmetic mean over all the similarity scores obtained from the same matching algorithm. S' here denotes the normalized similarity score S. The *z-norm* is well suited for Gaussian distributed data, which is often the case for similarity scores in biometric systems.

Experimental results are reported in compliance with the ISO/IEC 30107-3:2017 standard [1], which defines metrics for presentation attack detection such as Attack Presentation Classification Error Rate (APCER) and Bona Fide Presentation Classification Error Rate (BPCER):

- *Attack Presentation Classification Error Rate (APCER)*: Proportion of attack presentations incorrectly classified as bona fide presentations in a specific scenario
- *Bona Fide Presentation Classification Error Rate (BPCER)*: Proportion of bona fide presentations incorrectly classified as presentation attacks in a specific scenario

Database	D-EER	BPCER20	BPCER100	Fusion	Norm	MC	PC	WLD	RLT	GF	IUWT	ASAVE	DTFPM	SURF	SIFT	LBP	CNN
IDIAP VERA full	1.67	1.36	2.27	svm-lin	z-norm			✓			✓	✓	✓	✓	✓	✓
IDIAP VERA cropped	4.02	4.09	15.91	svm-lin	z-norm		✓			✓	✓	✓	✓	✓		✓
SCUT-SFVD full	0.75	0.24	0.71	svm-rbf	z-norm	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓
SCUT-SFVD roi-resized	1.09	0.41	1.21	svm-rbf	tanh-norm		✓		✓		✓		✓	✓	✓	✓
PLUS-LED thick	0.00	0.00	0.00	svm-rbf	z-norm									✓		✓
PLUS-LED thin	0.00	0.00	0.00	svm-lin	tanh-norm								✓	✓	✓	
PLUS-Laser thick	0.00	0.00	0.00	svm-lin	z-norm									✓		✓
PLUS-Laser thin	0.00	0.00	0.00	svm-lin	z-norm		✓					✓		✓		✓

Table 2: Selection of best working method constellations in terms of detection error rate.

The PAD performance is reported in table 2 in terms of detection equal error rate D-EER (BPCER = APCER), BPCER20 (BPCER at APCER $<= 0.05$) and BPCER100 (BPCER at APCER $<= 0.01$). For this research, also the database introduced in [19] is included in the experiments.

4.1. Experimental results

For this experiment, results are obtained by evaluating exhaustive cross combination of all described normalization and fusion techniques. The number of possible recognition-method-constellations per fusion is given by $2^{12}-1 = 4095$ considering all twelve matching schemes from section 3. Similarity scores are split using 10 fold (for IDIAP VERA and SCUT-SFVD) and 11 fold (for the PLUS) splitting. The folds that are currently not evaluated are used for calculation of the μ and σ for *z-norm* and *tanh-norm* normalization as well as training set for the SVM approaches.

The boxplots depicted in figure 2 show the distributions from the D-EERs for all 4095 method constellations over one specific database. Outliers are omitted in this plot for better visibility of the overall trend. Also, only one mode was chosen per database to keep the figure perspicuous. It can be observed that finding fusion combinations that are suited for PAD for the PLUS databases is easier compared to the other two databases since most of the D-EERs are below 10% and very compact. Another observation is that the SVM based fusion approaches in general outperform the simple sum, max and min fusions, regardless of the normalization technique applied.

A selection of the best working fusion combinations per database is listed in table 2. Especially for the PLUS sets, sometimes multiple method constellations achieve similar results. Therefore the selection for the one method reported in table 2 also considered to require as few methods as possible. Arguably, the results for the IDIAP VERA and the SCUT-SFVD are not perfect but the overall trend shows that score level fusion still holds the potential to be used as PAD in the domain of finger vein biometrics.

Altogether, the frequent use of keypoint- and texture-based recognition methods in table 2 suggests that these are the key elements for the similarity score fusion. This observation coincides with the study from section 3.2 where the IAPMRs from these recognition algorithms were inhomogeneous and possibly contain complementary information.

5. Conclusion

Inspired by a previous publication, this research carried out an extensive threat analysis on two publicly available finger vein presentation attack databases. The vulnerability analysis consists of twelve finger vein feature extraction algorithms together with their corresponding template matching schemes that can be categorized into three meta types of algorithms based on the type of feature they extract. Through observation of the results, it can be concluded that both databases under test provide presentation attack samples that in most cases indeed proof hazardous to established matching schemes.

In the second part of this research, the observation that not all recognition methods perform equally prone to presentation attacks was used to perform presentation attack

detection by utilizing score level fusion. Experimental results verify that fusion of similarity scores from different recognition schemes is indeed capable of attaining a sound presentation attack detection.

References

[1] ISO/IEC JTC1 SC37 Biometrics: ISO/IEC 30107-3 . Information technology — biometric presentation attack detection — part 3: Testing and reporting. Iso, International Organization for Standardization, Geneva, CH, 2017.

[2] A. Anjos, P. Tome, and S. Marcel. An introduction to vein presentation attacks and detection. In S. Marcel, M. S. Nixon, J. Fierrez, and N. Evans, editors, *Handbook of Biometric Anti-Spoofing: Presentation Attack Detection*, pages 419–438. Springer International Publishing, Cham, 2019.

[3] 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*, volume 7251, pages 7251 – 7251 – 9, 2009.

[4] S. Crisan, B. Tebrean, and T. E. Crisan. Multimodal liveness detection system for hand vein biometrics. In *2018 IEEE International Symposium on Medical Measurements and Applications (MeMeA)*, pages 1–6, 2018.

[5] 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*, pages 1269–1272, 2010.

[6] A. Jain, K. Nandakumar, and A. Ross. Score normalization in multimodal biometric systems. *Pattern Recognition*, 38(12):2270–2285, 2005.

[7] 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)*, pages 1–9, Los Angeles, California, USA, 2018.

[8] C. Kauba, J. Reissig, and A. Uhl. Pre-processing cascades and fusion in finger vein recognition. In *Proceedings of the International Conference of the Biometrics Special Interest Group (BIOSIG'14)*, Darmstadt, Germany, Sep. 2014.

[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, pages 113–142. Springer Nature Switzerland AG, Cham, Switzerland, 2019.

[10] J. Kolberg, M. Gomez-Barrero, S. Venkatesh, R. Ramachandra, and C. Busch. *Presentation Attack Detection for Finger Recognition*, pages 435–463. Springer International Publishing, Cham, 2020.

[11] A. Kumar and Y. Zhou. Human identification using finger images. *IEEE Transactions on Image Processing*, 21(4):2228–2244, 2012.

[12] 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.*, 19(3):179–186, Sept. 2009.

[13] 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*, 27, 02 2016.

[14] 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*, 15:194–203, 10 2004.

[15] N. Miura, A. Nagasaka, and T. Miyatake. Extraction of finger-vein patterns using maximum curvature points in image profiles. *IEICE - Trans. Inf. Syst.*, E90-D(8):1185–1194, Aug. 2007.

[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):1401–1413, 2013.

[17] 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):465–477, 2018.

[18] 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)*, pages 1–7, 2015.

[19] J. Schuiki, B. Prommegger, and A. Uhl. Confronting a variety of finger vein recognition algorithms with wax presentation attack artefacts. In *Proceedings of the 9th IEEE International Workshop on Biometrics and Forensics (IWBF'21)*, pages 1–6, Rome, Italy (moved to virtual), 2021.

[20] R. Snelick, M. Indovina, J. Yen, and A. Mink. Multimodal biometrics: Issues in design and testing. In *Proceedings of the 5th International Conference on Multimodal Interfaces*, ICMI '03, page 68–72, New York, NY, USA, 2003. Association for Computing Machinery.

[21] J. Starck, J. Fadili, and F. Murtagh. The undecimated wavelet decomposition and its reconstruction. *IEEE Transactions on Image Processing*, 16(2):297–309, 2007.

[22] 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)*, pages 513–518, 2015.

[23] 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)*, pages 1–10, 2014.

[24] 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)*, pages 400–406, 2020.

[25] 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*, 28(8):1892–1905, 2018.

[26] W. Yang, W. Luo, W. Kang, Z. Huang, and Q. Wu. Fvrasnet: An embedded finger-vein recognition and antispoofing system using a unified cnn. *IEEE Transactions on Instrumentation and Measurement*, 69(11):8690–8701, 2020.