 DOI: 10.3217/978-3-85125-663-5-38

# PRNU-based Finger Vein Sensor Identification in the Presence of Presentation Attack Data

Babak Maser[1,*], Dominik Söllinger[1,*] and Andreas Uhl[1]

*Abstract*— **We examine the effectiveness of the Photo Response Non-Uniformity (PRNU) in the context of sensor identification for finger vein imagery. Experiments are conducted on eight publicly-available finger vein datasets. We apply a Wiener Filter (WF) in the frequency domain to enhance the quality of PRNU estimation and noise residual, respectively, and we use two metrics to rank PRNU similarity, i.e. Peak-to-Energy (PCE) and Normalized Cross Correlation (NCC). In the experiments, we include a dataset consisting of both real finger vein data and captured artifacts produced to assess presentation attacks. We investigate the impact of this situation on sensor identification accuracy and also try to discriminate spoofed images from non-spoof images varying decision thresholds. Results of sensor identification for finger vein imagery is encouraging, the obtained scores for classification accuracies are between 97% to 98% for different settings. Interestingly, selecting particular decision thresholds, it is also possible to discriminate real data from artificial data as used in presentation attacks.**

## I. INTRODUCTION

Human identification is one of the main goals of biometric technology and the corresponding research area. Biometric systems utilize a human's physical or behavioral characteristics for authentication. Not only companies or governmental organizations do rely on biometric technology to provide secure authentication, but also everyday technology (e.g. smartphones, laptops, entrance systems) applies this technology to an increasing extent. Nevertheless, biometric traits also set new challenges in terms of maintaining the security and integrity of biometric data. While the (cryptographic) key material used in traditional authentication methods like PINs, passwords, smart-cards etc. can usually be changed once compromised, a person's biometric trait usually remains stable. Therefore, once biometric features are leaked, stolen or adopted many different attack scenarios become realistic and many corresponding attack vectors have been identified.

In order to capture a certain biometric trait, we need digital hardware which is typically termed "sensor" that has the technological capability to acquire the corresponding data suited to uniquely identify humans, which is a near-infrared (NIR) camera used with NIR illumination to visualize the structure and vascular pattern of human finger veins. The underlying imaging principle relies on NIR light absorption of human blood, thus, vessels appear dark in such images. For the security of a biometric system, the integrity of the authentication process is of vital interest. In this context, it is required to ascertain that imagery used for authentication has been indeed captured by the proper sensor, and has not entered the system in the context of an injection attack. At this point, we encounter passive media security techniques termed "digital image forensics" which can be used for this purpose. Similar to bullet scratches that allow forensic experts to match a bullet to a particular barrel with high reliability to be accepted even in court, these techniques can be eventually used to identify a sensor which has captured a finger vein image.

In this paper, we use an approach which is based on the photo-response non-uniformity (PRNU) [1] method. PRNU is an intrinsic property of every digital sensor caused by different sensitivity of pixels to light due to inhomogeneity of silicon wafers and imperfections during the sensor manufacturing process. PRNU can be interpreted as the telltale of "scratches" in images which can identify the originating sensor and discriminates images taken by different sensor instances.

Prior work in biometric sensor identification has shown that the PRNU method can be considered a well-suited method to identify a sensor in different fields of biometrics, so far considered for fingerprint [2] as well as iris [3], [4], [5], [6] sensors, respectively.
Prior work shows that the PRNU method can be considered a well-suited method to identify a sensor in different fields of biometric, e.g. Bartlow *et al.* studied the application of hardware fingerprinting based on PRNU noise analysis of biometric fingerprint devices for sensor identification [2], also PRNU has been used in the context of iris sensors in [3], [7], [8]. Alternatively to PRNU, also classical texture-oriented features have been used to identify a particular sensor model in the context of iris recognition [4], [5], [6]. Finally, in [9], Schuch *et al.* studied the applicability of a CNN-based and conventional approach on database bias as distinguishing property for the origin of a fingerprint. Also Marra, Francesco, *et al.* in [10] proposed a CNN-based algorithm improve the iris sensor model identification for benefit of the sensor interoperability.

As biometric authentication becomes a standard replacement for the traditional way of authentication in many areas, various attacks have been used to fool sensors with prerecorded data or artifacts. One of the approaches to mislead and deceive biometric sensors is the so-called "presentation attack" or sensor spoofing [11].

[1] Babak Maser, Dominik Söllinger, and Andreas Uhl are with the Department of Computer Sciences, University of Salzburg, Jakob-Haringer-Str. 2, 5020 Salzburg, Austria uhl@cosy.sbg.ac.at
[*] Both authors contributed equally

In this attack, a copy of a biometric trait is fabricated artificially and presented to the sensor. Intensive work has been done to develop techniques to detect presentation attacks [12], and for evaluation purposes, datasets consisting of artificial biometric data resulting from sensing such artifacts have been established and published.

This work is organized as follows: Section II gives an overview of techniques used for PRNU extraction and enhancement. Section III introduces the datasets, explains the different experimental settings as well as the evaluation workflow in detail. Finally, experimental results are provided in section V followed by a conclusion (section VII).

## II. Technical Approach

There are different ways how to compute the PRNU, we used a method proposed by Fridrich in [13], the method describes how to estimate the PRNU image from set of images taken by the same camera, the PRNU estimator is derived using maximum likelihood estimator (MLE),the MLE is modeled from the simplified sensor output model [13]. Thus the PRNU factor is obtained as follow:

$$\hat{K} = \sum_{i=1}^{N} R_i I_i \Big/ \sum_{i=1}^{N} I_i^2 \tag{1}$$

where PRNU factor is denoted by $\hat{K}$ which is noise-like signal responsible for the PRNU. $I_i$ is an image and $R_i$ is the noise residual of an image which is obtained by (eq. 2), note that $i$ stands for the $i$ *th* image out of N images which have been taken from a particular sensor.

The residual image $R_i$ can be calculated by subtracting an original image from a denoised image obtained using e.g. a wavelet denoising filter from an original image:

$$R_i = I_i - F(I_i) \tag{2}$$

where F denotes the denoising method, in our case the denoised image is obtained in the wavelet domain applying a 4-Level Wavelet decomposition using the Daubechies 8-tap wavelet filter, we empirically set $\sigma_0 = 3$. Eventually, a Wiener Filter (WF) [14] is applied additionally.

To detect whether the Residual of an image I ($R_I$) is taken by the sensor with PRNU estimator $\hat{K}$, we use normalized cross-correlation (NCC):

$$\rho_{[R_I, I\hat{K}]} = NCC(R_I, I\hat{K}) \tag{3}$$

NCC has been also proposed in [13]. Apart from NCC, we investigate the effect of using the Peak Correlation Energy (PCE) as another similarity metric [13] in this paper.

## III. Experimental Design

### A. Datasets

In this paper, we have assembled the following publicly available datasets to evaluate the performance and effectiveness of the proposed approach. The number of images in each dataset is not equal, thus to keep the sample dataset balance we choose an equal number of images from each dataset. Hence we have chosen the first 120 images from each dataset for our experiments. The following listing provides a description of the datasets.

- **SDUMLA-HMT (SDUMLA)** - Images are selected from the first 20 clients, images of the dataset [15] are stored in BMP format with 320×240 pixels in size.
- **IDIAP VERA (IDIAP-REAL)** - Images of the dataset [16] are stored in PNG format with a size of 250×665. The images are taken from 60 clients of the IDIAP-REAL sub-dataset.
- **IDIAP VERA (IDIAP-SPOOF)** - Images of the dataset [16] are stored in PNG format with a size of 250×665. The images are taken from 60 individuals of the IDIAP-Spoof sub-dataset.
- **FV-USM** - Images of the dataset [17] are stored in JPEG format with a size of 480×640. The selected subset is taken from the first 30 clients.
- **MMCBNU_6000 (MMCBNU)** - Images of the dataset [18] are stored in BMP format with a size of 640×480. The selected subset is chosen from the first 20 clients.
- **PLUS-FV3-Laser-Palmar (Palmar)** - Images of the dataset [19] are stored in PNG format with a size of 600×1024. The selected subset has been chosen from the first 20 clients.
- **THU-FVFDT** - Images of the dataset [19] are stored in PNG format with a size of 600×1024. The selected subset is composed of images from the first 20 clients.
- **UTFVP** - Images of the dataset [20] are stored in PNG format with a size of 672×380. The selected subset is composed of images of the first 20 clients.
- **HKPU-FV** - Images of the dataset [21] are stored in BMP format with a size of 513×256. The selected subset is composed of images of the first 60 clients.

### B. Cropping

The primary goal of this work is not only to study the general applicability of PRNU-based sensor identification for finger vein images but also to investigate the effect of the presence of spoofed images resulting from a presentation attack on the sensor identification performance.

We assume that fingerprints generated from uncorrelated data (in order to facilitate the out-averaging of image-content related high-frequency content) are better suited for sensor identification than fingerprints generated from

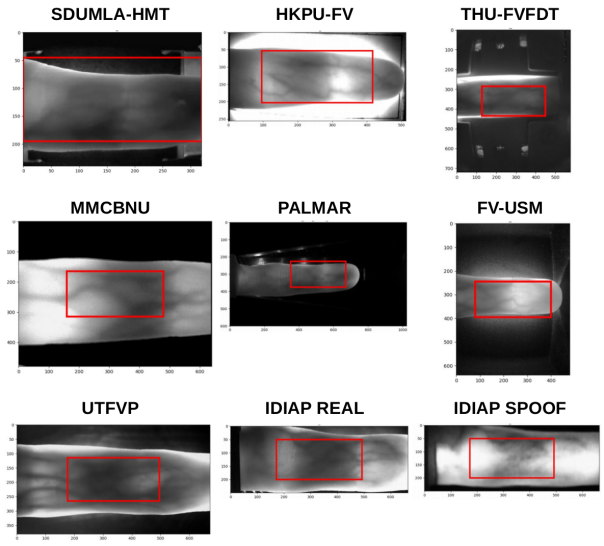


Fig. 1. Sample Patches: Center 320×150

correlated data. Therefore, we expect good performance for regions containing the biometric trait due to a better variability of the image content instead of image regions covered by sensor parts only. Thus, we decided to focus our experiment on a region which contains the biometric trait. The selected cropping is termed as **Center 320×150** as the image region was taken from the center and contains mostly finger vein texture (except for some data sets like SDUMLA-HMT and PALMAR, see Figure 1 for example croppings).

## IV. Workflow and Scenario

We applied a 4 fold cross-validation framework for all eight datasets to examine the proposed methods. In each fold, we feed $3/4$ of the query dataset (i.e. 90 images) to the model to determine the PRNU estimation by MLE ($\hat{K}$), subsequently, the estimated PRNU will be enhanced by WF or no enhancement will be applied. The images of the other datasets, as well as $1/4$ of the query dataset, are fed into the model to compute the residuals ($R_i$), and again, either WF is applied to the residuals or *No Enhancement* is considered. The estimated PRNU, as well as the residuals, are fed into the classification unit, and as it is mentioned in Section II we use two similarity metrics for sensor identification (NCC and PCE).

Recall that IDIAP-Real dataset and IDIAP-Spoof dataset are captured with the same sensor, the difference is that for the former, human fingers are imaged, while for the latter, presentation artifacts are imaged. The AUC-ROC score and the Precision-Recall score for the IDIAP-Real data are obtained by estimating $\hat{K}$ from images of the IDIAP-Real dataset only, while the residuals are taken from both the IDIAP-Real dataset and the IDIAP-Spoof dataset respectively. The IDIAP-Spoof results are generated in the same manner, but $\hat{K}$ is computed from IDIAP-Spoof data only.

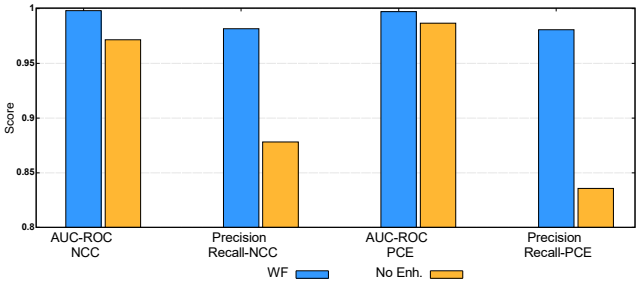


Fig. 2. Impact of applying Wiener filter and No Enhancement on AUC-ROC and Precision-Recall scores using NCC and PCE similarity metrics

| Similarity metric | Performance measurement | WF | No Enh. |
|---|---|---|---|
| NCC | AUC ROC | 0.998 | 0.971 |
| NCC | AUC Precision Recall | 0.982 | 0.878 |
| PCE | AUC ROC | 0.997 | 0.986 |
| PCE | AUC Precision Recall | 0.980 | 0.835 |

TABLE I
IMPACT ON AUC ROC AND PRECISION RECALL USING NCC AND PCE BY APPLYING WF AND NO ENH.

## V. Experiments and Results

Our aim is to investigate the following topics as our primary interest:

- Feasibility of PRNU-based sensor identification using the proposed method for finger vein imagery,
- Comparison between PCE and NCC as similarity assessment methods in the context of finger vein data,
- Assessment of the influence of applied WF and
- Investigation of the influence of the presence of presentation attack data.

To evaluate and analyze the proposed method we provide the AUC-ROC score and the Precision-Recall score for all sensors/data sets.
In Figure 2 and Table I, we display the achieved AUC-ROC and the Precision-Recall scores by taking the average over all sensor class scores.

We find that the Wiener Filter plays a significant role in sensor identification accuracy[1]. This behavior was somehow expected because the WF suppresses periodic artifacts and it has been observed on other data that the resulting PRNU and residuals have higher quality. We observe the same behavior in Figures 3, 4, 5, 6 which show non-averaged but per-sensor results.

When comparing PCE and NCC we find that for data after the application of WF there is hardly any difference. When considering non-enhanced data, there are some differences, but these are not consistent when considering AUC-ROC scores and Precision-Recall scores.

[1]In this paper, we use the term *accuracy* for the AUC ROC score and the AUC ROC Precision-Recall score

Figures 3, 4, 5, 6, now detailing results per dataset, confirm that the PRNU-based approach is well suited to identify sensors overall. However, there are some results where certain configurations turn out not to deliver satisfying performance.

Figure 3 displays stable results with excellent accuracy in case of WF application, while scores are down to 0.75 for one sensor (i.e. THU-FVFDT) in case no enhancement is applied.

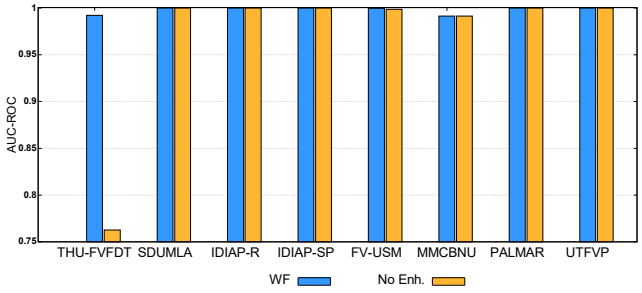


Fig. 3. AUC ROC for NCC

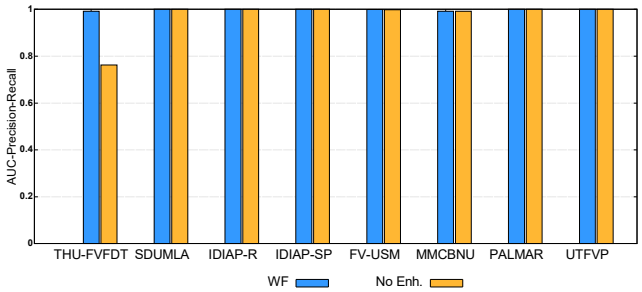


Fig. 4. AUC Precision-Recall for NCC

This result is confirmed in Figure 4, which shows the results of AUC-Precision-Recall for all sensors. Again the worst result is seen for sensor THU-FVFDT in case of no enhancement is applied. We observe that the score for the MMCBNU sensor is slightly improved compared to AUC-ROC scores in Figure 3.

When looking at PCE results (Figure 5 and Figure 6), these seem to less stable as compared to their NCC counterparts at first sight. However, in Figure 5 the scale on the y-axis is fairly different as the minimum score value is 0.965. So basically all these results are excellent and the differences do not matter. Figure 6 reveals a very poor result in case of UTFVP and no enhancement applied. Here is the score is down to 0.3! In this setting again the superiority of applying WF is confirmed.

Overall, we note that there are some lower score values in all settings but applying WF enhancement and using NCC as similarity measure prevents significant inaccuracies in any case.

## VI. Detection of Spoofed Images

As described in section III-A, the IDIAP dataset consists of real finger vein images as well as of spoof images which

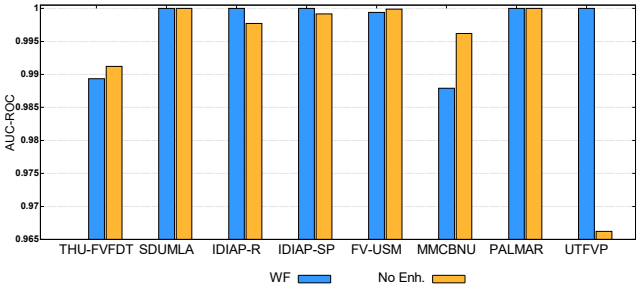


Fig. 5. AUC ROC for PCE

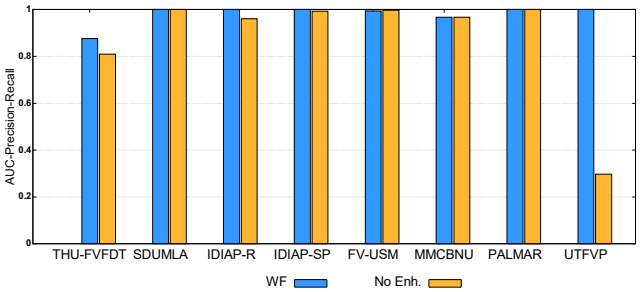


Fig. 6. AUC Precision-Recall for PCE

were generated by imaging presentation attack artifacts with the same sensor. The results of the previous section clearly demonstrate that these spoof images do not prevent a correct classification of the sensor as both, real and spoof images can be discriminated well from finger vein images acquired by one of the other sensors. However, there might still be subtle differences present, which might lead to slight differences in the PRNU which could be exploited to detect a presentation attack using corresponding artifacts. To understand whether PRNU can be also used for this purpose, we analyze if there is a certain NCC-threshold that allows us to discriminate between IDIAP-Real and IDIAP-Spoof images.

Table II shows the accuracy of assigning IDIAP-Real and IDIAP-Spoof images to the appropriate class for different thresholds. The PRNU computed from IDIAP-Real images is computing NCC to the respective residuals. We can observe that for a low threshold, all IDIAP-Real images are classified correctly. When we increase the threshold to 0.5, we classify 98% of IDIAP-Real images correctly and IDIAP-Spoof images are still hardly correctly classified (7%). For threshold 0.6, IDIAP-Real images achieve 92% accuracy while IDIAP-Spoof accuracy is 48%. When increasing the threshold further, accuracy for IDIAP-Real images are further reduced while IDIAP-Spoof image classification accuracy is almost perfect.

Table III again shows the accuracies of classifying IDIAP-Real and IDIAP-Spoof images for different thresholds, respectively. However, in this case, IDIAP-Spoof images are used to compute the PRNU.

As we can see, when choosing a low threshold at 0.3, 0.4 and 0.5, IDIAP-Spoof images are correctly classified, but the accuracy for IDIAP-Real images is almost 0. However, once

| Threshold (NCC) | IDIAP-REAL | IDIAP-SPOOF |
|---|---|---|
| 0.3 | 1.0 | 0.0 |
| 0.4 | 1.0 | 0.01 |
| 0.5 | 0.98 | 0.07 |
| 0.6 | 0.92 | 0.48 |
| 0.7 | 0.34 | 0.99 |
| 0.8 | 0.0 | 1.0 |
| 0.9 | 0.0 | 1.0 |

TABLE II
DISCRIMINATION AMONG IDIAP-REAL AND IDIAP-SPOOF IMAGES FOR DIFFERENT THRESHOLDS BASED ON IDIAP-REAL PRNU

the threshold increases to 0.6, it can be observed that most (99%) IDIAP-spoof images are still treated correctly, while also 74% of the IDIAP-Real images are correctly classified. Furthermore, if we increase the threshold to 0.7 we can see that 100% of IDIAP-Real images are correctly classified while 44% of the IDIAP-Spoof images are detected correctly as spoof images. Increasing the threshold further entirely disables classification for IDIAP-spoof images. Overall, we cannot find any threshold in Tables II and III to perfectly discriminate both datasets, but for some settings, a PRNU-based distinction seems to be realistic.

| Threshold (NCC) | IDIAP-REAL | IDIAP-SPOOF |
|---|---|---|
| 0.3 | 0.00 | 1.00 |
| 0.4 | 0.00 | 1.00 |
| 0.5 | 0.02 | 1.00 |
| 0.6 | 0.74 | 0.99 |
| 0.7 | 1.00 | 0.44 |
| 0.8 | 1.00 | 0.00 |

TABLE III
DISCRIMINATION AMONG IDIAP-REAL AND IDIAP-SPOOF IMAGES FOR DIFFERENT THRESHOLDS BASED ON IDIAP-SPOOF PRNU

## VII. CONCLUSION

This work studies the applicability of PRNU-based sensor identification methods for finger vein images in the context of biometric systems. The result clearly shows that this approach is well-suited, in particular, the Wiener filter is used as an enhancement technique. Finally, we observe that the PRNU-based approach might be also suited for presentation attack, aka sensor spoofing, detection.

## ACKNOWLEDGEMENTS

This work has received funding from the European Union's Horizon 2020 research and innovation program under grant agreements No. 700259 (PROTECT) and No. 690907 (IDENTITY), respectively. The work was also funded by the Austrian Research Promotion Agency, FFG KIRAS project AUTFingerATM under grant No. 864785.

## REFERENCES

[1] Jan Lukas, Jessica Fridrich, and Miroslav Goljan. Digital camera identification from sensor pattern noise. *IEEE Transactions on Information Forensics and Security*, 1(2):205–214, 2006.

[2] Nick Bartlow, Nathan Kalka, Bojan Cukic, and Arun Ross. Identifying sensors from fingerprint images. In *Computer Vision and Pattern Recognition Workshops, 2009. CVPR Workshops 2009. IEEE Computer Society Conference on*, pages 78–84. IEEE, 2009.

[3] Luca Debiasi and Andreas Uhl. Blind biometric source sensor recognition using advanced prnu fingerprints. In *Signal Processing Conference (EUSIPCO), 2015 23rd European*, pages 779–783. IEEE, 2015.

[4] Christof Kauba, Luca Debiasi, and Andreas Uhl. Identifying the origin of iris images based on fusion of local image descriptors and prnu based techniques. In *Biometrics (IJCB), 2017 IEEE International Joint Conference on*, pages 294–301. IEEE, 2017.

[5] Luca Debiasi, Christof Kauba, and Andreas Uhl. Identifying iris sensors from iris images. *Iris and Periocular Biometric Recognition*, 5:359, 2017.

[6] Susan El-Naggar and Arun Ross. Which dataset is this iris image from? In *WIFS*, pages 1–6, 2015.

[7] Nathan Kalka, Nick Bartlow, Bojan Cukic, and Arun Ross. A preliminary study on identifying sensors from iris images. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops*, pages 50–56, 2015.

[8] Andreas Uhl and Yvonne Höller. Iris-sensor authentication using camera prnu fingerprints. In *Biometrics (ICB), 2012 5th IAPR International Conference on*, pages 230–237. IEEE, 2012.

[9] Patrick Schuch, Jan Marek May, and Christoph Busch. Estimating the data origin of fingerprint samples. In *2018 International Conference of the Biometrics Special Interest Group (BIOSIG)*, pages 1–6. IEEE, 2018.

[10] Francesco Marra, Giovanni Poggi, Carlo Sansone, and Luisa Verdoliva. A deep learning approach for iris sensor model identification. *Pattern Recognition Letters*, 113:46–53, 2018.

[11] Amrit Pal Singh Bhogal, Dominik Söllinger, Pauline Trung, Jutta Hämmerle-Uhl, and Andreas Uhl. Non-reference image quality assessment for fingervein presentation attack detection. In *Scandinavian Conference on Image Analysis*, pages 184–196. Springer, 2017.

[12] Sébastien Marcel, Mark S. Nixon, and Stan Z. Li, editors. *Handbook of Biometric Anti-Spoofing - Trusted Biometrics under Spoofing Attacks*. Advances in Computer Vision and Pattern Recognition. Springer, 2014.

[13] Jessica Fridrich. Digital image forensics. *IEEE Signal Processing Magazine*, 26(2), 2009.

[14] M Kivanc Mihcak, Igor Kozintsev, and Kannan Ramchandran. Spatially adaptive statistical modeling of wavelet image coefficients and its application to denoising. In *Acoustics, Speech, and Signal Processing, 1999. Proceedings., 1999 IEEE International Conference on*, volume 6, pages 3253–3256. IEEE, 1999.

[15] Y. Yin, L. Liu, and X. Sun. SDUMLA-HMT: A Multimodal Biometric Database. In *The 6th Chinese Conference on Biometric Recognition (CCBR 2011)*, volume 7098 of *Springer Lecture Notes on Computer Science*, pages 260–268, 2011.

[16] Pedro Tome, Matthias Vanoni, and Sébastien Marcel. On the vulnerability of finger vein recognition to spoofing. In *IEEE International Conference of the Biometrics Special Interest Group (BIOSIG)*, September 2014.

[17] M. S. M. Asaari and B. A. Rosdi S. A. Suandi. Fusion of band limited phase only correlation and width centroid contour distance for finger based biometrics. *Expert Systems with Applications*, 41(7):3367–3382, 2014.

[18] Yu Lu, Shan Juan Xie, Sook Yoon, Zhihui Wang, and Dong Sun Park. An available database for the research of finger vein recognition. In *Image and Signal Processing (CISP), 2013 6th InternationalCongress on Image and Signal Processing (CISP 2013)*, volume 1, pages 410–415. IEEE, 2013.

[19] Christof Kauba, Bernhard Prommegger, and Andreas Uhl. Focussing the beam - a new laser illumination based data set providing insights to finger-vein recognition. In *Proceedings of the IEEE 9th International Conference on Biometrics: Theory, Applications, and Systems (BTAS2018)*, pages 1–9, Los Angeles, California, USA, 2018.

[20] B.T. Ton and R.N.J. Veldhuis. A high quality finger vascular pattern dataset collected using acustom designed capturing device. In *International Conference on Biometrics, ICB 2013*. IEEE, 2013.

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