PRNU-based Detection of Finger Vein Presentation Attacks

Babak Maser*
Department of Computer Science
University of Salzburg
5020 Salzburg, Austria

Dominik Söllinger*
Department of Computer Science
University of Salzburg
5020 Salzburg, Austria

Andreas Uhl
Department of Computer Science
University of Salzburg
5020 Salzburg, Austria
uhl@cosy.sbg.ac.at

***Abstract*—In this work, we evaluated the effectiveness of the Photo Response Non-Uniformity (PRNU) to detect presentation/spoofing attacks for finger vein imagery. The performance is evaluated on two publicly-available finger vein presentation/spoofing attack datasets (IDIAP and SCUT-FVD). Maximum likelihood estimation (MLE) is used to estimate the sensor's PRNU. To decide whether a query image is real or spoofed, we compare its residual to the estimated sensor PRNU using PCE and NCC as similarity measures. We observe that the classification performance is heavily dependent on the set of images used for PRNU estimation. We assume different degrees of variability in image content caused by distinct light scattering properties in real tissue and artifacts to be one of the main reasons for the differences in classification performance.**

***Index Terms*—Photo Response Non-Uniformity, PRNU, image residual, source camera identification, presentation attack detection, spoofing detection, finger vein**

I. Introduction

Biometric systems deal with traits taken from a physical or behavioral characteristic of a human used for authentication purposes. In the last decade, biometric systems have become popular and have started to cover a wide range of governmental (e.g., border control), commercial (e.g., securing ATMs or home banking), and private (front-door fingerprint authentication) applications. Specifically, biometrics are used in authentication to complement or replace traditional authentication techniques like passwords or tokens as biometric techniques exhibit certain advantages. These advantages include higher security, but also user convenience.

There are many different biometric modalities: E.g., face, fingerprint, palmprint, voice, gait, signature, and iris. All of them reflect unique personal characteristics and can (eventually) be used to identify a person. A modality of recent interest is finger vein recognition, due to its (claimed) advantages as compared to fingerprints, e.g., being independent of finger surface conditions and difficult to be acquired covertly, respectively. Also, the widespread usage of finger vein systems to secure ATM cash withdrawals render this modality of current interest.

A common way to compromise biometric systems is the fabrication of a biometric trait's copy and subsequent presentation of this artifact to the sensor. This type of attack is called presentation attack, aka sensor spoofing attack. Thus, the biometric community came up with solutions to detect this type of vulnerabilities and prevent such attacks. Corresponding techniques are termed presentation attack detection (PAD) methods, aka anti-spoofing techniques [1].

In [2], a review on PAD techniques for finger vein data is provided. In general, PAs can be mounted using printouts of the biometric trait, placing monitors/displays in front of the sensor, or fabricating an artifact mimicking the biometric trait. Corresponding PAD methods can be categorized into liveness-based, motion-based, and texture-based ones, respectively. The aim of all mentioned techniques to resolve the spoofing is to discriminate the real biometric data from spoofing variations.

In this work, we apply photo response non-uniformity (PRNU) methodology for PAD. PRNU is a digital hardware fingerprint which is caused by pixel non-uniformity (PNU) [3]. PRNU is an intrinsic property of the digital sensor. Each silicon wafer which represents pixels has a slightly different ability to convert photons to electrons. The mentioned inhomogeneity and imperfection caused by the sensor manufacturing process lead us to a unique noise pattern for each sensor type. Thus the noise-like pattern is cast onto every image it captures. Thus, the PRNU methodology has been used to identify imaging sensors, enabling discrimination at the sensor instance level. In biometrics, most work has been done on iris sensor identification [4]–[8], but also fingerprint sensors have been addressed [9]. However, it has been demonstrated that the PRNU can be forged [4] even maintaining recognition performance [10].

However, PRNU-related techniques have been additionally used to detect and localize image manipulations like image splicing, copy-move attacks, among other malicious forgeries (see, e.g. [11], [12]). In the biometric context, PRNU properties have recently been used to detect morphing in facial imagery [13].

In this paper, we investigate if PRNU-based algorithms can be used for the discrimination of real and spoofed finger vein imagery. We used subsets of images from two publicly-available finger vein presentation/spoofing attack datasets. The classification performance is evaluated by applying two different similarity measures: Normalized-Cross-Correlation (NCC)

* Both authors contributed equally

and Peak-Correlation-Energy (PCE). These approaches seem to be contradictory at first sight, as both real and spoofed data are acquired by the same sensor. Thus the PRNU should not be affected, and real and spoofed data could not be discriminated. On the other hand, it is well known that the PRNU is massively influenced by image content and the quality of PRNU sensor fingerprints does rely on the availability of proper uncorrelated data to average out image content related properties. This is where our proposed techniques have its foundation: Spoofed data exhibit a much lower variability compared to real data as the artifacts do not model the variations in human tissue (except for the vein structure layout). Thus, light scattering is expected to be much more homogeneous for spoofed data, resulting in low quality and different sensor fingerprints as compared to fingerprints from real data, which we exploit in this work. Consequently, we assume that our method delivers best results when "training" on the real data (i.e., in fact, we do not train, but we only generate the PRNU fingerprint from training data). Thus, there is potential that this approach also could work on unseen spoofing data types (which is not investigated in this work).

This paper is structured as follows: Section II is dedicated to the discussion of PRNU-based algorithms and describes how to extract image residuals and compute the PRNU. In Section III we discuss the workflow and PRNU enhancement methods. We also introduce the datasets which are used in this paper. In Section IV we discuss the experimental result, followed by a conclusion in Section V.

II. Methodology

To extract the PRNU fingerprint we use the method proposed by *Fridrich* in [14] which is based on maximum likelihood estimation (MLE). For each image I_i the noise residual R_i gets estimated as follows:

$$R_i = I_i - F(I_i) \tag{1}$$

$F(I_i)$ is a denoised version of the original image obtained by applying an adaptive Wiener filter in the wavelet domain. As a result, $F(I_i)$ mainly contains low frequencies. After subtracting the denoised version from the original image, we obtain a high-frequency image containing the residual noise. This method has originally been proposed by Mihcak *et al.* in [15]. Since the noise residual might be contaminated with undesired artifacts often referred to as non-unique artifacts (NUAs) [16], two different enhancement techniques are applied. Zero-Mean (ZM) as proposed in [17] as well as Wiener filtering [5] to suppress periodic artifacts. Both applied methods are described in II-B.

A maximum likelihood estimator [14] is used to obtain the PRNU factor K using the following equation:

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

$\hat{K}$ is our zero-mean noise-like signal responsible for the PRNU and I_i corresponds to images of the same sensor with $i = 1...N$ where N denotes the total number of images in the dataset.

To evaluate the similarity between the PRNU fingerprint $\hat{K}$ and the residual noise R_I of a query image I two different metrics are used: Normalized Cross Correlation (NCC) as shown in (3) and Peak Correlation Energy (PCE) as proposed in [18]. Note that, X and Y denotes two image patches of the size $W \times H$. $X(i,j)$ and $Y(i,j)$ denotes the pixel value at position (i,j), $\bar{X}$ and $\bar{Y}$ denotes the arithmetic mean of all pixel values.

$$NCC(X,Y) = \frac{\sum_{i=1}^{W}\sum_{j=1}^{H}\Big(\big(X(i,j)-\bar{X}\big)\cdot\big(Y(i,j)-\bar{Y}\big)\Big)}{||X-\bar{X}||\cdot||Y-\bar{Y}||} \tag{3}$$

The presence of the PRNU fingerprint in the query image I can be estimated by measuring the correlation between the noise residual R_I of a query image I and the PRNU factor $\hat{K}$ weighted by the image content of I.

$$\rho_{[R_I, I\hat{K}]} = NCC(R_I, I\hat{K}) \tag{4}$$

Peak Correlation Energy (5) is an alternative measure to attenuate the influence of periodic noise contamination. It has been shown to yield more stable results in scenarios where images have been geometrically transformed and scaled [19]. Although Kang *et al.* [20] showed that PCE might increase the false-positive rate if images have not been geometrically transformed, we test PCE as a second metric in this work.

As in this work, only image patches of the same size are compared, image transformations like scaling and cropping are not taken into account. Consequently, the formula for PCE simplifies as follows [17]:

$$PCE = \frac{CNCC(0,0)^2}{\frac{1}{WH-|A|}\sum_{i,j\neq A} CNCC(i,j)^2} \tag{5}$$

$CNCC$ is the circular normalized cross correlation between R_I and $I\hat{K}$. A is a small area around the peak located at position $(0,0)$ and $|A|$ represents the cardinality of the area.

$$CNCC(x,y) = \frac{1}{WH}\sum_{i=1}^{W}\sum_{j=1}^{H}(X(i,j)-\bar{X})\cdot(Y_{(i,j)\oplus(x,y)}(i,j)-\bar{Y}) \tag{6}$$

A. *Wavelet-based residual extraction*

Low-pass filters applied in Wavelet domain [15] have been shown to be a well-suited tool for image denoising and residual extraction. Denoising is typically achieved by applying a Wiener filter like attenuation on high-frequency sub-bands (incl. local variance estimation). Subtraction of the denoised image from the original image (1) returns a high-frequency signal containing the residual noise.

1) Apply 4-Level Wavelet decomposition using Daubechies 8-tap WMF. Coefficients in the horizontal, vertical and

diagonal high-frequency sub-bands are denoted $v(i,j)$, $h(i,j)$ and $d(i,j)$.

2) For each sub-band: Estimate the local variance by applying local MAP estimation using different window sizes W where $W \in \{3,5,7,9\}$.

$$\hat{\sigma}^2{}_w(i,j) = max\left[0, \frac{1}{W^2}\sum_{(i,j)\in N} h^2(i,j) - \sigma_0^2\right] \quad (7)$$

Choose the minimum local variance as final estimate:

$$\hat{\sigma}^2(i,j) = min\left[\sigma_3^2(i,j), \sigma_5^2(i,j), \sigma_7^2(i,j), \sigma_9^2(i,j)\right] \quad (8)$$

3) Obtain the denoised coefficients by applying the Wiener filter like attenuation for each coefficient $C(i,j)$. $\sigma_0 = 3$ has been chosen empirically.

$$C_{Den}(i,j) = C(i,j)\frac{\sigma^2(i,j)}{\sigma^2(i,j) + \sigma_0^2} \quad (9)$$

4) Extract the noise residual by subtracting both images in the wavelet domain and transforming it back into the spatial domain. WF denotes the Wiener filter as described in the previous steps. $IDWT$ and DWT denote the (inverse) discrete wavelet transformation.

$$R = IDWT\Big(DWT(I) - WF\big(DWT(I)\big)\Big) \quad (10)$$

B. *Enhancement Techniques*

In this work, we applied two different post-processing techniques to further improve the extracted residuals and PRNU fingerprints.

Wiener filter: Noise residuals might be contaminated with undesired artifacts. A Wiener filter [8] applied in the frequency domain allows to suppress these artifacts.

Zero-Mean filter: Noise residuals might also be contaminated with non-unique artifacts (NUAs) introduced by demosaicing algorithms that depend on the CFA (Color Filter Array). Zero-mean filtering as proposed in [8] can remove these periodic artifacts.

III. Experimental Setting

A. *Datasets*

In this work, the applicability of PRNU fingerprints for presentation attack detection was tested on a subset of images from the following publicly-available datasets.

- **IDIAP VERA (REAL & SPOOF)** - The dataset [21] consists of index fingers of 110 subjects. All images are stored in PNG format with a size of 250×665. Additionally, presentation-attacks were created for each image by printing on high-quality paper and presenting it to the same sensor. In our experiments, we take two subsets (real and spoof). Each of them is composed of 120 images from 60 different subjects obtained by selecting two non-cropped images of the subject's left and right index finger. The images were taken from the first 60 subjects in the dataset (subject id 001-072; some ids have been skipped by the creators of the dataset)

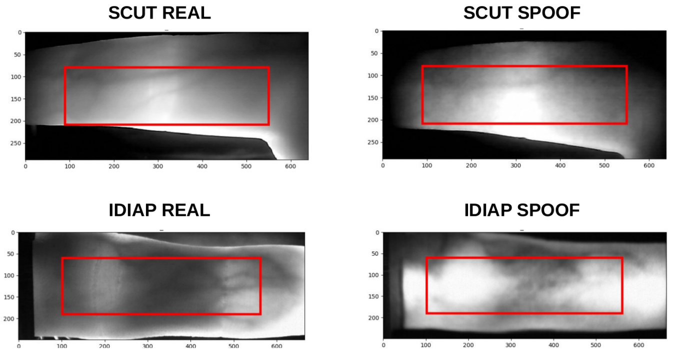

Figure 1: Samples of finger vein images of all datasets. The red bounding box denotes the region used for residual extraction.

- **SCUT FVD (REAL & SPOOF)** -The dataset [22] consists of 3600 real and 3600 spoofed images. All images are stored in BMP format with a size of 158×467. Images were taken from 100 subjects. From each subject, images of his/her index, middle and ring finger are provided. In our experiments, we take two subsets of real and spoofed images out of the dataset's non-cropped train-subset. We only keep the first shot of each finger. As the train-subset consists of 20 clients, we collect a subset of 120 images for our evaluation.

B. *Workflow*

To assess the performance of our PRNU-based model we used subject-wise 4-fold cross-validation. Out of 120 images from each dataset, we used 90 images to estimate the sensor's PRNU in each fold. Thus, 150 images remained for testing in each fold. As images of the SCUT dataset were provided in portrait mode, we rotated them by 90 degrees. Finally, to obtain image patches of the same size, we cropped a 460×130-sized image region (containing biometric trait) from the center of each image. This choice is motivated by our previous experiments which showed that regions mainly containing biometric trait should be preferred in the course of PRNU estimation. Samples of all datasets are shown in Figure 1.

The PRNU estimation has already been explained in the previous section. To estimate the residual we picked each query image and calculated its similarity to the PRNU of the same dataset using PCE or NCC. Considering the distribution of similarity scores, we aimed to find a threshold that separates real from spoofed images of the *same* dataset. For instance, the threshold should separate IDIAP REAL from IDIAP SPOOF images. The model's classification capability was assessed concerning AUC ROC (Area under the ROC curve) and AUC Precision-Recall (Area under the Precision-Recall curve) scores since these metrics do not require a fixed decision threshold. However, as the quantitative performance of the developed models should also be compared according to the metric developed in ISO/IEC 30107-3 in terms of (i) attack presentation classification error rate (APCER), (ii) normal presentation classification error rate (NPCER) and (iii) average classification error rate (ACER), we have also chosen a threshold to report the aforementioned metrics. This threshold has been chosen based on the estimated EER and is specific to the dataset/enhancement method, but remained the same across all four folds. To decide on an appropriate threshold, we calculate the EER for each fold and finally run the metric computation (APEC, NPCER, ACER) using the averaged threshold as the decision boundary. Note that the error rates capture the capability of the model to distinguish between real and spoofed images of the *same* dataset. We do not compare, for instance, an IDIAP REAL fingerprint with SCUT images, but we compare the IDIAP fingerprint with IDIAP REAL and IDIAP SPOOF images.

IV. Result

In this section, we report the real-spoof classification results achieved by means of the PRNU-based classification approach described in Section II. More precisely, we are interested in the following aspects:

- Applicability of PRNU-based algorithms to discriminate between real and spoofed images
- Effect of different enhancement techniques and similarity measures (NCC/PCE) on the classification performance

Table I shows the AUC ROC scores obtained when performing real-spoof classification for the IDIAP and SCUT dataset using different enhancement techniques and NCC as similarity measure. The ”FP Dataset” column denotes the set of images used to estimate the PRNU fingerprint. The result is also graphically visualized in Figure 2. It can be observed that classification of images in the IDIAP dataset exhibits better performance than for the SCUT dataset since the NCC AUC ROC scores for IDIAP are superior to the scores for SCUT (true for all enhancement methods). Furthermore, it is interesting to see that for both datasets the obtained classification results are not symmetric. For instance, a PRNU fingerprint generated from real images of the SCUT datasets achieves an AUC ROC score of 0.77 (without enhancement), while the classification efficiency decreases to 0.39 when generating the fingerprint from the dataset’s spoofed images. The same behavior can also be observed in the case of the AUC Precision-Recall scores which are shown in Table II as well as in Figure 3.

Surprisingly, the result also shows that fingerprints generated from real images do not always lead to better classification performance. For instance, we observe that fingerprints generated from IDIAP SPOOF outperform fingerprints generated from REAL. This at least contradicts with our expectation that real fingerprints always work better for classification. In the case of spoofed images we expected that the captured paper does not exhibit varying texture as it is seen when generating images from human tissue. Therefore, the light scattering in a paper should be quite homogeneous, while scattering should vary extremely due to locally changing properties of human tissue like density. Consequently, this low extent of variability in spoofed data (and thus higher correlation), should degrade the quality of the PRNU fingerprint and thus impacts on the classification performance. Nevertheless, fingerprints generated from real images show good overall performance (AUC ROC 0.792 for SCUT REAL / AUC ROC 0.903 for IDIAP REAL) (using WF enhancement).

Table III / Figure 4 and Table IV / Figure 5 show the classification performance using PCE as similarity measure. In general, the PCE results show a similar characteristic as the NCC results. The PRNU-based spoofing attack detection achieves better results on the IDIAP dataset than on the SCUT dataset. Also, we are not able to identify a clear winner among both similarity measures in terms of their classification performance.

Table V and VI report the performance of the different models in terms of APCER, NPCER and ACER (see Section III-B). Again, the ”FP Dataset” column denotes the set of images used to estimate the PRNU fingerprint. As explained in Section III-B, these metrics only capture the model’s capability to distinguish between real and spoofed images of the *same* dataset, but not between different datasets.

FP Dataset	**No Enh.**	**WF**	**WF+ZM**
SCUT REAL	0.770 (±0.017)	0.792 (±0.023)	0.713 (±0.024)
SCUT SPOOF	0.390 (±0.031)	0.479 (±0.005)	0.516 (±0.005)
IDIAP REAL	0.866 (±0.010)	0.903 (±0.015)	0.904 (±0.014)
IDIAP SPOOF	0.966 (±0.007)	0.984 (±0.005)	0.982 (±0.006)

Table I: **NCC: AUC ROC** (using diff. enhancement techniques)

FP Dataset	**No Enh.**	**WF**	**WF+ZM**
SCUT REAL	0.680 (±0.016)	0.620 (±0.026)	0.445 (±0.043)
SCUT SPOOF	0.159 (±0.013)	0.190 (±0.001)	0.218 (±0.004)
IDIAP REAL	0.661 (±0.028)	0.796 (±0.031)	0.793 (±0.029)
IDIAP SPOOF	0.904 (±0.016)	0.952 (±0.011)	0.945 (±0.012)

Table II: **NCC: AUC Precision-Recall** (using diff. enhancement techniques)

FP Dataset	**No Enh.**	**WF**	**WF+ZM**
SCUT REAL	0.701 (±0.023)	0.728 (±0.025)	0.662 (±0.028)
SCUT SPOOF	0.483 (±0.021)	0.496 (±0.007)	0.516 (±0.007)
IDIAP REAL	0.618 (±0.053)	0.896 (±0.016)	0.902 (±0.015)
IDIAP SPOOF	0.856 (±0.014)	0.985 (±0.005)	0.982 (±0.006)

Table III: **PCE: AUC ROC** (using diff. enhancement techniques)

FP Dataset	**No Enh.**	**WF**	**WF+ZM**
SCUT REAL	0.626 (±0.015)	0.598 (±0.019)	0.485 (±0.010)
SCUT SPOOF	0.177 (±0.025)	0.173 (±0.008)	0.195 ±(0.006)
IDIAP REAL	0.403 (±0.053)	0.760 (±0.037)	0.794 (±0.028)
IDIAP SPOOF	0.604 (±0.035)	0.954 (±0.012)	0.943 (±0.011)

Table IV: **PCE: AUC Precision-Recall** (using diff. enhancement techniques)

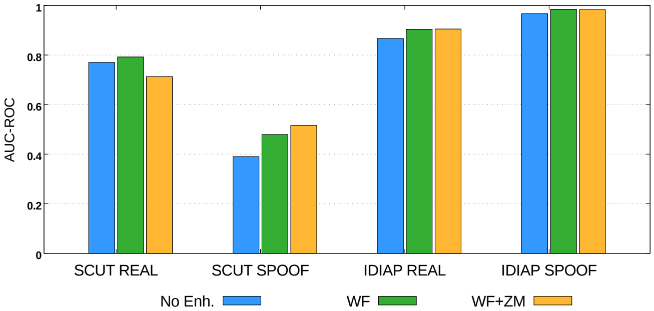

Figure 2: AUC ROC for NCC

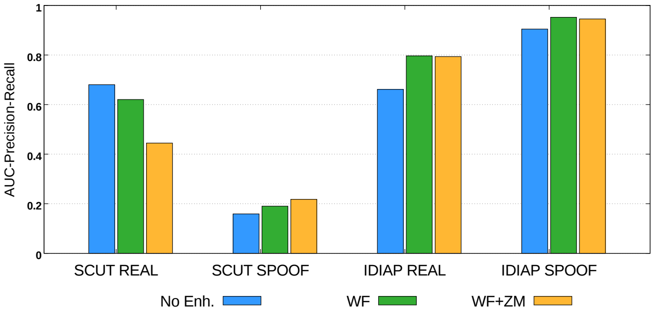

Figure 3: AUC Precision-Recall for NCC

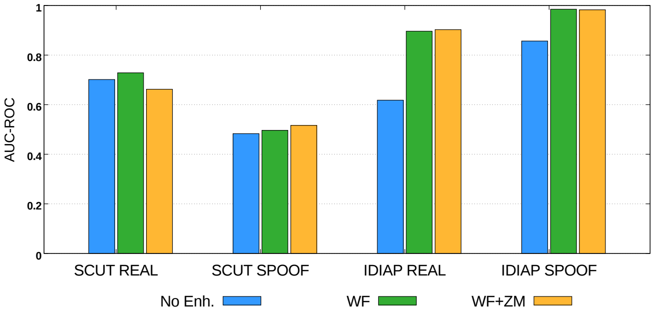

Figure 4: AUC ROC for PCE

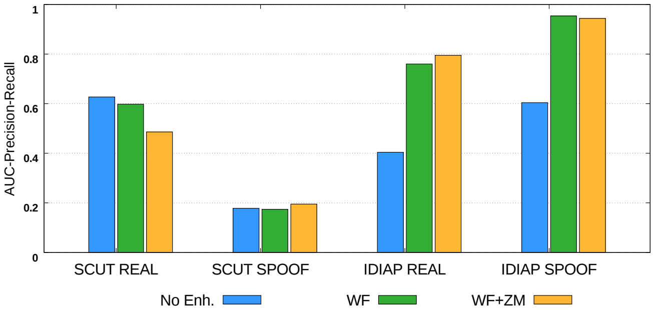

Figure 5: AUC Precision-Recall for PCE

FP Dataset	Threshold	ACER (%)	APCER (%)	NPCER (%)
SCUT REAL (No Enh.)	0.059368	28.53 (±1.07)	25.89 (±0.52)	31.18 (±1.67)
SCUT REAL (WF)	0.019746	26.16 (±2.06)	26.84 (±0.66)	25.49 (±3.79)
SCUT REAL (WF+ZM)	0.014821	33.24 (±1.26)	32.52 (±1.15)	33.96 (±2.72)
SCUT SPOOF (No Enh.)	0.057664	57.79 (±3.18)	58.26 (±5.51)	57.31 (±0.88)
SCUT SPOOF (WF)	0.020367	53.83 (±0.09)	54.44 (±0.68)	53.21 (±0.56)
SCUT SPOOF (WF+ZM)	0.014674	50.87 (±0.68)	51.81 (±1.20)	49.93 (±0.32)
IDIAP REAL (No Enh.)	0.639553	18.39 (±1.13)	18.51 (±0.45)	18.26 (±2.36)
IDIAP REAL (WF)	0.642744	17.19 (±2.25)	16.81 (±0.51)	17.57 (±4.32)
IDIAP REAL (WF+ZM)	0.639613	16.88 (±2.14)	15.99 (±0.45)	17.78 (±4.08)
IDIAP SPOOF (No Enh.)	0.627337	9.97 (±1.05)	10.28 (±1.98)	9.67 (±1.21)
IDIAP SPOOF (WF)	0.642059	5.36 (±0.63)	5.97 (±1.82)	4.76 (±0.64)
IDIAP SPOOF (WF+ZM)	0.635989	4.39 (±1.02)	3.75 (±2.47)	5.03 (±0.48)

Table V: Error Rates for NCC

FP Dataset (Enh. Technique)	Threshold	ACER (%)	APCER (%)	NPCER (%)
SCUT REAL (No Enh.)	35.333797	35.37 (±2.10)	35.37 (±1.92)	35.37 (±2.47)
SCUT REAL (WF)	35.794293	32.24 (±1.08)	32.74 (±2.03)	31.73 (±3.69)
SCUT REAL (WF+ZM)	20.377283	37.30 (±1.34)	37.00 (±2.77)	37.61 (±4.62)
SCUT SPOOF (No Enh.)	55.654238	51.13 (±1.92)	49.93 (±4.87)	52.34 (±2.30)
SCUT SPOOF (WF)	37.527895	52.39 (±0.94)	52.15 (±2.18)	52.63 (±0.61)
SCUT SPOOF (WF+ZM)	19.628648	50.77 (±1.26)	50.59 (±2.18)	50.95 (±1.12)
IDIAP REAL (No Enh.)	28.934256	42.03 (±4.57)	41.35 (±2.69)	42.71 (±6.49)
IDIAP REAL (WF)	28149.56916	18.21 (±1.94)	18.44 (±0.85)	17.99 (±3.87)
IDIAP REAL (WF+ZM)	31731.80043	17.22 (±2.22)	16.88 (±0.47)	17.57 (±4.32)
IDIAP SPOOF (No Enh.)	41.487235	22.52 (±2.44)	23.47 (±4.31)	21.56 (±0.62)
IDIAP SPOOF (WF)	28575.26147	4.31 (±1.12)	4.03 (±2.47)	4.60 (±0.24)
IDIAP SPOOF (WF+ZM)	31550.43941	5.33 (±0.65)	5.97 (±1.82)	4.69 (±0.68)

Table VI: Error Rates for PCE

V. Conclusion

In this work, we studied the applicability of PRNU-based methods (typically used for sensor identification) to detect image spoofing attacks for finger vein imagery. To accomplish this, PRNU fingerprints were generated from two publicly-available finger vein spoofing datasets and used to classify different query images either as a real or spoofed image versions. We observed that the effectiveness of the PRNU-based approach is heavily dependent on the set of images used to estimate the PRNU. For both datasets fingerprints generated from real images showed an adequate classification performance (AUC ROC 0.792 for SCUT / AUC ROC 0.903 for IDIAP). This is fortunate, as the availability of real data to generate a PRNU fingerprint is a realistic scenario in any case, while spoofed data might not be available at all in case of unseen attack types. Surprisingly, it turned out that fingerprints generated from real images did not always result in better classification performance. For instance, a fingerprint generated from IDIAP's spoofed images allowed to almost perfectly discriminate between real and spoofed data. We speculate that it might relate to the size of the spoofing artifacts. While in case of SCUT the spoofing artifacts had the same size as the finger, IDIAP's spoofed images were larger thus covering background parts of the sensor. Therefore, this might interfere with the PRNU generation. The results shown in this work strongly motivate further research on the effectiveness of PRNU-based techniques to detect image spoofing. More precisely, further investigations on how the finger vein PRNU is effected by light scattering, different tissue types and artifacts introduced during the process of spoofing need to be conducted, to better understand the effectiveness of such PRNU-based PAD approaches.

References

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

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

[7] 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.

[8] Luca Debiasi and Andreas Uhl. Prnu enhancement effects on biometric source sensor attribution. *IET Biometrics*, 6(4):256–265, 2017.

[9] 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.

[10] Sudipta Banerjee, Vahid Mirjalili, and Arun Ross. Spoofing prnu patterns of iris sensors while preserving iris recognition. *arXiv preprint arXiv:1808.10765*, 2018.

[11] Sujoy Chakraborty and Matthias Kirchner. Prnu-based image manipulation localization with discriminative random fields. In *Media Watermarking, Security, and Forensics 2017, Burlingame, CA, USA, 29 January 2017 - 2 February 2017*, pages 113–120, 2017.

[12] Giovanni Chierchia, Davide Cozzolino, Giovanni Poggi, Carlo Sansone, and Luisa Verdoliva. Guided filtering for prnu-based localization of small-size image forgeries. In *IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP 2014, Florence, Italy, May 4-9, 2014*, pages 6231–6235, 2014.

[13] Luca Debiasi, Ulrich Scherhag, Christian Rathgeb, Andreas Uhl, and Christoph Busch. Prnu-based detection of morphed face images. In *2018 International Workshop on Biometrics and Forensics (IWBF)*, pages 1–7. IEEE, 2018.

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

[15] 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.

[16] Thomas Gloe, Stefan Pfennig, and Matthias Kirchner. Unexpected artefacts in prnu-based camera identification: a'dresden image database'case-study. In *Proceedings of the on Multimedia and security*, pages 109–114. ACM, 2012.

[17] Xufeng Lin and Chang-Tsun Li. Preprocessing reference sensor pattern noise via spectrum equalization. *IEEE Transactions on Information Forensics and Security*, 11(1):126–140, 2016.

[18] Jessica Fridrich. Sensor defects in digital image forensic. In *Digital Image Forensics*, pages 179–218. Springer, 2013.

[19] Miroslav Goljan and Jessica Fridrich. Camera identification from cropped and scaled images. In *Security, Forensics, Steganography, and Watermarking of Multimedia Contents X*, volume 6819, page 68190E. International Society for Optics and Photonics, 2008.

[20] Xiangui Kang, Yinxiang Li, Zhenhua Qu, Jiwu Huang, et al. Enhancing source camera identification performance with a camera reference phase sensor pattern noise. *IEEE Transactions on Information Forensics and Security*, 7(2):393–402, 2012.

[21] 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.

[22] Xinwei Qiu, Wenxiong Kang, Senping Tian, Wei Jia, and Zhixing Huang. Finger vein presentation attack detection using total variation decomposition. *IEEE Transactions on Information Forensics and Security*, 13(2):465–477, 2018.