BLIND BIOMETRIC SOURCE SENSOR RECOGNITION USING ADVANCED PRNU FINGERPRINTS

Luca Debiasi, Andreas Uhl

Multimedia Signal Processing and Security Lab
University of Salzburg
Salzburg, Austria

ABSTRACT

Previous device identification studies on the iris sensors of the CASIA-Iris V4 database using PRNU fingerprints showed high variations regarding the differentiability of the sensors. These variations may have been caused by the usage of multiple sensors of the same model for the image acquisition. Since no specific documentation on this exists we investigate the presence of multiple image sensors in the data sets. The images under investigation, furthermore, show a strong correlation regarding their content, therefore we make use of different PRNU enhancements approaches based on weighting the PRNU depending on the image content. The enhanced PRNU is used in conjunction with different forensic techniques to detect the presence of multiple sensors in the data sets.

Finally, the results of the enhancement approaches and the results without any PRNU enhancement are compared and an assessment on whether multiple sensor instances have been used in the data sets is given.

Index Terms— Digital image forensics, Biometric sensor forensics, PRNU, Sensor identification

1. INTRODUCTION

In the field of digital image forensics the photo response non-uniformity (PRNU) of an imaging sensor emerged as an important tool for the realization of different forensic tasks like device identification, device linking, recovery of processing history and the detection of digital forgeries.

Slight variations of individual pixels during the conversion of photons to electrons in digital image sensors are the source of the PRNU, thus it is considered an intrinsic property which is contained in all digital imaging sensors. Every digital image sensor adds this weak, noise-like pattern into every image that has been acquired with it. This pattern, which enables the identification of a specific image sensor, is essentially an unintentional stochastic spread-spectrum watermark that survives processing, such as lossy compression or filtering and it meets essential criteria like dimensionality, universality, generality, stability and robustness [1] that make it well suited for forensic tasks.

Beyond that, the PRNU fingerprint of a sensor can also be used to improve a biometric systems security by ensuring the authenticity and integrity of images acquired with a biometric sensor. Previous studies on this application by Höller *et al.* [2] have conducted a feasibility study on the CASIA-Iris V4 database. The differentiability of the sensors in the CASIA-Iris V4 database using PRNU fingerprints has been tested with the conclusion, that the EERs and respective thresholds vary highly. Some sensors showed satisfying results while others did not, some subsets even showed EERs of over 20%. The question raised, that if PRNU fingerprints are being applied as an authentication measure for iris databases, it is not clear where the poor differentiation results for some sensors come from.

It was assumed that this high variation could be caused by the correlated data that was used to generate the sensors PRNU fingerprint. Further investigation from Debiasi *et al.* [3] showed that using uncorrelated data to generate the PRNU fingerprint does not improve the results for this data set and hence is not causing the high variation. An alternative method to deal with the uncorrelated data is to further separate the PRNU from the image content. Since the PRNU covers the high frequency components of an image, it is contaminated with other high frequency components from the images, such as edges. Li [4] proposed an approach for attenuating the influence of details from scenes on the PRNU so as to improve the device identification rate of the identifier. Caldelli *et al.* [5] considered this approach and developed a new kind of enhancer.

On the other hand, Höller *et al.* [2] suspected that multiple sensors may have been used for the acquisition of the CASIA Iris-V4 subsets. If a PRNU fingerprint is generated using images of different sensors, it will match with images acquired with all of these sensors and hence lead to a decreased differentiability. Unfortunately, neither the meta data of the images in the CASIA-Iris V4 database, nor the database description, denoting solely the sensor model without any additional information, can reveal the number of sensors instances used during the acquisition. Even the researchers involved in the acquisition cannot determine the number of sensors any more. Debiasi *et al.* [6] investigated the case of multiple sensors and

978-0-9928626-3-3/15/$31.00 ©2015 IEEE

came to the conclusion that one data set might be acquired with more than one sensor, while the other have been acquired with a single sensor only. No PRNU enhancement was used to overcome the problem of the correlated data in the investigation.

In this paper we conduct a forensic analysis on the CASIA-Iris V4 database to investigate if multiple sensors have been used during the acquisition of the images in a completely blind manner with no a priori knowledge of the data set and make use of two PRNU enhancing techniques to be able to reduce the influence of the correlated data. The paper is organized as follows: Section 2 briefly describes the related work regarding this scenario, section 3 gives a short description of the CASIA-Iris V4 database and section 4 gives an overview of the PRNU extraction and the PRNU enhancements. Section 5 describes the forensic techniques used for the investigation and the experiment set-up. In section 6 the experimental results are presented and section 7 concludes the paper.

2. RELATED WORK

Blind classification of image source in an open set scenario has already been investigated by other researchers, who proposed Hierarchical Agglomerative Clustering (HAC) [5, 7] or Multi-Class Spectral Clustering (MCSC) for this scenario [8, 9] by formulating the classification task as a graph partitioning problem. These approaches rely on a known training or test set to determine special criteria, e.g. the stop criterion for the clustering. Because we do not have a ground truth for the CASIA-Iris V4 DB, these approaches are not considered in this work. Other related work [10] relies on an iterative algorithm that consecutively "constructs" a sensor fingerprint from images with similar PRNU using a pre-calculated threshold function. Some of the forensic techniques proposed in [6] are used in this work together with the previously mentioned approach of Bloy [10].

3. CASIA-IRIS V4 DATA SET

The CASIA-IrisV4 contains a total of 54,601 iris images of more than 1,800 genuine subjects. All iris images are 8 bit grey-level JPEG files, collected under near infrared illumination. The five subsets investigated in this work, with the corresponding sensors (as described in the database specification), are:

- *intv*: CASIA close-up iris camera
- *lamp*: OKI IRISPASS-h1
- *twin*: OKI IRISPASS-h2
- *dist*: CASIA long-range iris camera
- *thou*: Irisking IKEMB-100

For the CASIA Iris V4 data sets it is not clear, whether the single data sets have been acquired with a specific sensor or if multiple instances of the same sensor model have been used. This question is substantiated by the fact that the same sensor model was used for two different data sets (*lamp* and *twin*).

4. PRNU EXTRACTION AND ENHANCEMENT

For all the forensic investigation techniques used in this work the PRNU from the images under investigation is extracted. This process is further described in the following section.

The extraction of the PRNU noise residual is performed by using the algorithm described by Fridrich [11]. The PRNU represents the noise intrinsically inserted into an image during the acquisition process. For each image I the noise residual W_I is estimated as described in equation 1,

$$W_I = I - F(I) \tag{1}$$

where F is a denoising function filtering out the sensor pattern noise. We used the wavelet-based denoising filter as described in Appendix A of [12], because it is producing good results in filtering out the PRNU. The PRNU noise residual it then normalized in respect to the L_2-norm because its embedding strength is varying between different sensors as explained by [2].

In this work two different PRNU enhancement approaches are used, which both aim to filter out scene details by the following idea: Scene details contribute to the very strong signal components in the wavelet domain, so the stronger a signal component in the wavelet domain, the more it should be attenuated. For the enhancement the PRNU is transformed into the discrete wavelet transform (DWT) domain, where an enhancement function is applied to the coefficients. We use two different enhancement functions: *EnhLi3* that corresponds to the Model 3 from [4] and *EnhCald* that is proposed in [5]. After the application of the respective function, the resulting coefficients are transformed back into the spatial domain by performing an inverse DWT (IDWT).

The PRNU fingerprint $\hat{K}$ of a sensor is then estimated using a maximum likelihood estimator for images I_i with $i = 1...N$.

$$\hat{K} = \frac{\sum_{i=1}^{N} W_I^i I^i}{\sum_{i=1}^{N} (I^i)^2} \tag{2}$$

The normalized cross correlation (NCC) is used to detect the presence of a PRNU fingerprint $\hat{K}$ in an Image J with

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

where ρ indicates the correlation between the PRNU residual W_j of the image J and the fingerprint $\hat{K}$ weighted by the image content of J.

The correlation ρ is calculated between each image from a sensor S_i and the PRNU fingerprint $\hat{K}_i$ of the sensor S_i,

NoEnh	intv	lamp	twin	dist	thou
images	1307	6858	1095	1566	2000
partitions	143	212	20	1	6
partitions > 100	2	11	1	1	1
partitions < 10	128	157	18	0	4
unassociated images	0	0	0	0	0

EnhLi3	intv	lamp	twin	dist	thou
images	1307	6855	1095	1566	2000
partitions	186	266	24	1	14
partitions > 100	1	12	1	1	2
partitions < 10	168	129	19	0	12
unassociated images	0	0	0	0	0

EnhCald	intv	lamp	twin	dist	thou
images	1307	6855	1095	1566	2000
partitions	6	2867	307	1	193
partitions > 100	1	0	3	1	3
partitions < 10	4	260	254	0	188
unassociated images	928	0	0	0	0

Table 1: BFAIC experiment results on the CASIA-Iris V4 data sets for *NoEnh* (top), *EnhLi3* (middle) and *EnhCald* (bottom).

where only images are used that have not been part of the PRNU fingerprint estimation. Additionally the correlation ρ between all images from the other sensors S_j, $i \neq j$, and the PRNU fingerprint $\hat{K}_i$ of the sensor S_i is also calculated.

5. EXPERIMENTS AND SET-UP

All the subsets from the CASIA-Iris V4 DB are investigated independently. Since the image size is varying between the data sets, the PRNU noise residual of an image is extracted from 4 patches located in the corners with a size of 128x128 pixels each for all of the forensic techniques. Hence we obtain a total noise residual size of 256x256 pixels.

After the extraction of the PRNU noise residual, either no enhancement, the enhancement of Li [4] (denoted as *EnhLi3*) or the enhancement of Caldelli *et al.* [5] (denoted as *EnhCald*) is applied to the PRNU as described in section 4. A threshold value of $\alpha = 6$ was used for the enhancement function in both enhancement approaches.

After the extraction and optional enhancement, three different forensic techniques are applied to investigate the data sets:

- Blind Camera Fingerprinting and Image Clustering (*BCFAIC*) by Bloy [10]
- Sliding Window Fingerprinting (*SWF*) by Debiasi *et al.* [6]
- Device Identification on Dataset Partitions (*DIODP*) by Debiasi *et al.* [6]

6. RESULTS

In the following section the results of the ivestigation of the CASIA-Iris V4 DB with the before mentioned forensic techniques and PRNU enhancements are presented.

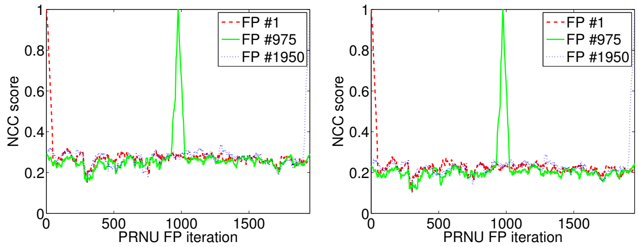

Fig. 1: Results of SW experiment *thou* data set without PRNU enhancement (left) and the *EnhLi3* enhancement (right).

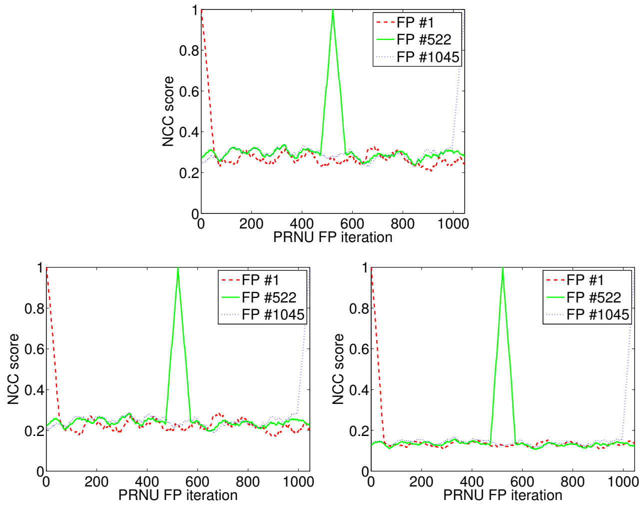

Fig. 2: Results of SW experiment for the *twin* data set with *NoEnh* (top), *EnhLi3* (left) and *EnhCald* (right).

6.1. Blind Camera Fingerprinting and Image Clustering

First the Blind Camera Fingerprinting and Image Clustering (BCFAIC) technique was applied to the different subsets of the CASIA-Iris V4 database. This technique creates clusters of associated images (images with a high NCC score) and partitions the data set. The resulting partitions should reflect the number of distinct sensors used in the data set. Unassociated images have a very low NCC score among each other, so that they are classified as being all from different sensors because they could not be clustered properly. Table 1 shows the results without any PRNU enhancement applied (*NoEnh*) as well as the results with the *EnhLi3* and *EnhCald* PRNU enhancement.

The results show a high cluster fragmentation for all subsets, except for the *dist* data set, where all images have been clustered together with all enhancement approaches. The *EnhLi3* enhancement produces slightly more clusters then *NoEnh*, but the results are comparable. The *EnhCald* enhancement, on the other hand, produces a much higher amount of clusters for all data sets (except *dist*) compared to the other enhancements and also leads to unassociated images in the *intv* data set.

The results of the BCFAIC experiments indicate that the *dist* dataset has been acquired with a single sensor, while the results are unclear for the other data sets. It can also be seen that the *EnhLi3* produces comparable results to the PRNU enhancement being omitted.

6.2. Sliding Window Fingerprinting

The Sliding Window Fingerprinting (SWP) moves a window with a defined size over the data image after image and a PRNU fingerprint from the data within this window is calculated in each step. The presence of images from multiple sensors in the data set should express in a sudden increase or decrease of the correlation score. If only images from one sensor are present in the data set, the correlation scores among all images should be quite stable around a certain level. The high spikes with a peak value of 1 occur when fingerprints that have one or more common images in their generation are compared.

As this experiment shows in figure 1, the *EnhLi3* enhancement produces comparable results as if no enhancement is applied for all data sets. There is only a very small offset in the correlation scores between the two configurations, where the *EnhLi3* scores are slightly lower, but the transitions are equal for both configurations. An example is given in figure 1 for the *thou* data set. Hence only the *EnhLi3* and *EnhCald* configurations are compared in the following figures.

In the results of the *dist*, *twin* and *thou* data sets no transitions in the correlation scores can be identified. They are comparable for *EnhLi3*, *EnhLi3* and *EnhCald*, therefore these data sets have probably been acquired with a single sensor according to this experiment. The only difference is an offset in the correlation scores for the individual enhancement configurations, as it can be seen in figure 2.

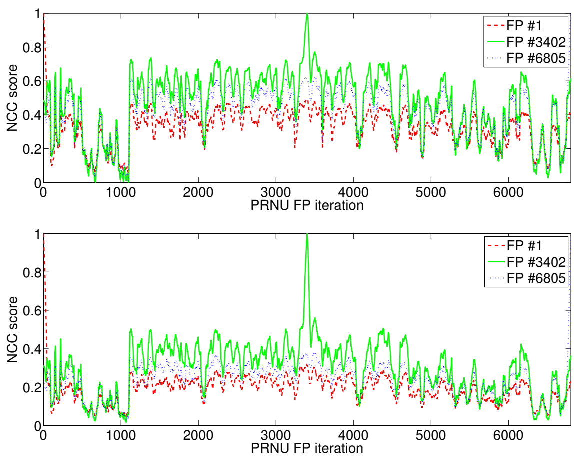

Fig. 3: Results of SW experiment for the *lamp* data set with *EnhLi3* (left) and *EnhCald* (right).

The figures 3 and 4 show the results for the *lamp* and *intv* data sets. In the *lamp* and *intv* data sets the previously described correlation score transitions can be observed at approximately iteration 700 and 1050 (*lamp*) and iteration 250 and 800 (*intv*).

Summing up, this technique suggests that all data sets, with the exception of *lamp* and *intv*, have been acquired with a single sensor. Regarding the PRNU enhancements it can be observed that the two PRNU enhancements *EnhLi3* and *EnhCald* exhibit decreased mean correlation scores.

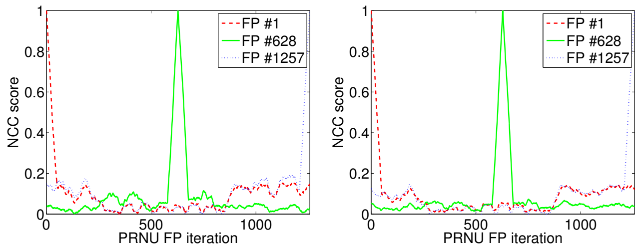

Fig. 4: Results of SW experiment for the *intv* data set with *EnhLi3* (left) and *EnhCald* (right).

6.3. Device Identification on Dataset Partitions

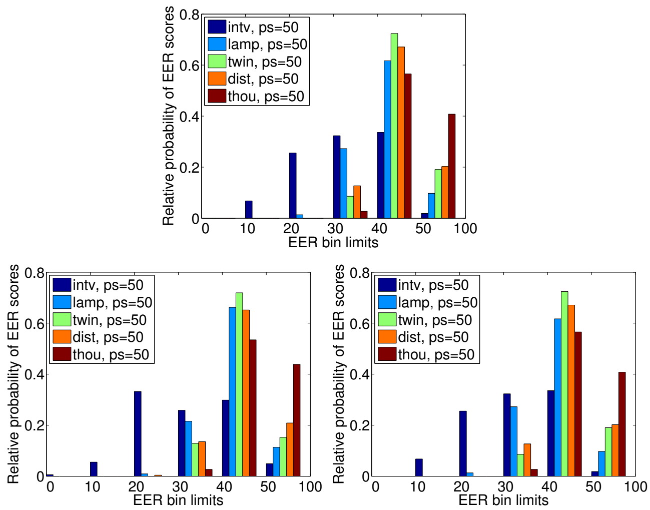

Fig. 5: Results of DIODP experiment on all CASIA-Iris V4 data sets with a partition size of 50.

The Device Identification on Dataset Partitions (DIODP) experiment divides the data sets into n partitions with the same size and treat the disjoint partitions as n different sensors. After calculating the pairwise EER scores for all partition combinations P_i and Pj, where $i \neq j$, the EER score distribution is evaluated. If the distribution contains mostly high EER scores, the data set probably contains images from a single sensor. On the other hand, if the distribution contains very low EER scores, the data set is suspicious of containing images from multiple sensors. To be able to clearly represent the resulting EER scores we performed a binning of the scores into six bins with the following limits: scores below 10%, between 10% and 20%, between 20% and 30%, between 30% and 40%, between 40% and 50%, and scores above 50%, where the lower bounds are inclusive and the upper bounds are exclusive.

Similar to the previous forensic techniques, the results for the two PRNU enhancement approaches are quite similar to the unenhanced ones, as represented in figure 5. This figure also indicates that the score distribution for the *intv* data set shows some low EER scores. For all other data sets it can be observed that the EER scores are mostly larger than 30%, which indicates that these data sets might be acquired with a single sensor. Having a closer look at the *intv* data set with different partition sizes in figure 6 indicates that this set might have been acquired with multiple sensors, because the distribution of the EER scores contains most of the scores in the range between 10% and 40% for almost all partition sizes under investigation.

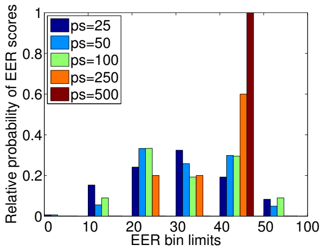

Fig. 6: Results of DIODP experiment with different partition sizes for the *intv* data set with the *EnhLi3*.

7. CONCLUSION

In this work we tried to establish a ground truth of the sensors used to acquire the various CASIA-Iris V4 data sets by using different PRNU enhancement techniques. This remains a challenging task for the CASIA-Iris V4 DB since this is a completely blind approach without any a priori knowledge of the sensors.

The PRNU enhancements did not clarify the previously obtained results from Debiasi *et al.* [6], where the results indicate that the *intv* data set might be acquired with more than sensor, while the other subsets have been acquired with one sensor. Actually, in this scenario, the impact of the evaluated PRNU enhancement approaches on the outcome of the applied forensic techniques is very low.

Unknown factors could have an impact on the quality of the PRNU noise residuals and hence tamper the results, therefore further studies have to be conducted to be able to use sensor fingerprints as an authentication measure for biometric systems.

8. ACKNOWLEDGMENTS

This work is partially funded by the Austrian Science Fund (FWF) under Project No. P26630.

REFERENCES

[1] Jessica Fridrich, "Sensor defects in digital image forensics," in *Digital Image Forensics: There is more to a picture than meets the eye*, H.T. Sencar and N. Memon, Eds., chapter 6, pp. 179–218. Springer Verlag, 2012.

[2] Andreas Uhl and Yvonne Höller, "Iris-sensor authentication using camera PRNU fingerprints," in *Proceedings of the 5th IAPR/IEEE International Conference on Biometrics (ICB'12)*, New Delhi, India, Mar. 2012, pp. 1–8.

[3] L. Debiasi, Z. Sun, and A. Uhl, "Generation of iris sensor PRNU fingerprints from uncorrelated data," in *Proceedings of the 2nd International Workshop on Biometrics and Forensics (IWBF'14)*, 2014.

[4] Ch.-T. Li, "Source camera identification using enhanced sensor pattern noise," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 280–287, 2010.

[5] R. Caldelli, I. Amerini, F. Picchioni, and M. Innocenti, "Fast image clustering of unknown source images," in *IEEE International Workshop on Information Forensics and Security (WIFS) 2010*, 2010, pp. 1–5.

[6] L. Debiasi and A. Uhl, "Techniques for a forensic analysis of the casia-iris v4 database," in *Proceedings of the 3rd International Workshop on Biometrics and Forensics (IWBF'14)*, 2015.

[7] Chang-Tsun Li, "Unsupervised classification of digital images using enhanced sensor pattern noise.," in *ISCAS*. 2010, pp. 3429–3432, IEEE.

[8] Shuhan Luan, Xiangwei Kong, Bo Wang, Yanqing Guo, and Xingang You, "Silhouette coefficient based approach on cell-phone classification for unknown source images.," in *ICC*. 2012, pp. 6744–6747, IEEE.

[9] I. Amerini, R. Caldelli, P. Crescenzi, A. Del Mastio, and A. Marino, "Blind image clustering based on the normalized cuts criterion for camera identification," *Signal Processing: Image Communication*, , no. 29, pp. 831–843, 2014.

[10] G. Bloy, "Blind camera fingerprinting and image clustering," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 30, no. 3, pp. 532–534, Mar. 2008.

[11] J. Fridrich, "Digital image forensic using sensor noise," *IEEE Signal Processing Magazine*, vol. 26, no. 2, March 2009.

[12] Jan Lukas, Jessica J. Fridrich, and Miroslav Goljan, "Digital camera identification from sensor pattern noise.," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 2, pp. 205–214, 2006.