COMPARISON OF PRNU ENHANCEMENT TECHNIQUES TO GENERATE PRNU FINGERPRINTS FOR BIOMETRIC SOURCE SENSOR ATTRIBUTION

Luca Debiasi, Andreas Uhl

Department of Computer Sciences
University of Salzburg
Salzburg, Austria

ABSTRACT

Identifying the source camera which acquired a given image using the cameras PRNU is a well established task in image forensics, known as camera or device identification. Since digital image sensors are widely used to acquire biometric data, it is eligible that this task can also be performed with biometric sensors and the respective data. This has already been studied in literature.

In this paper we focus on a slightly different task, which consists in clustering images acquired with the same sensor in a data set possibly containing images from an unknown number of biometric sensors. Previous work showed unclear results that have been difficult to interpret because of the low quality of the extracted PRNU. In this paper we compare the use of a PRNU enhancement technique to the use of special uncorrelated images acquired with known biometric sensors in this clustering context. We additionally propose extensions of existing source sensor attribution techniques using data from known sensors. Finally, the results of the enhancement approaches and the results using the uncorrelated data acquired with the known sensors are compared and an assessment on whether multiple sensor instances have been used in the different investigated data sets is given.

Index Terms— Biometric sensor forensics, PRNU, Source sensor classification

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 present in all digital imaging sensors. Every digital image sensor adds this weak, noise-like pattern into every image acquired with it. This pattern, which enables the identification of this 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. The sensor identification can be performed at different levels, as described by Bartlow *et al.* [2]: Technology, brand, model, unit. In this work we focus on the unit level, which corresponds to a differentiation of instances of sensors of the same model and brand.

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 work on this application by Höller *et al.* [3] performed 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. Other work by Kalka *et al.* [4] regarding the differentiability of iris sensor showed varying results, while studies conducted on fingerprint sensors by Bartlow *et al.* [2] showed more satisfactory results. The question raised, that if PRNU fingerprints are being applied as an authentication measure for biometric databases, it is not clear where the poor differentiation results for some sensors come from. On one hand it was assumed that this high variation could be caused by the correlated data that was used to generate the sensors PRNU fingerprint, since all images investigated in [3] have a very similar image content. On the other hand Kalka *et al.* [4] concluded that the variations are caused by the absence of the PRNU in saturated pixels (pixel intensity $= 255$) or under saturated pixels (pixel intensity $= 0$) for different images in the data sets. Furthermore Höller *et al.* [3] 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. An alternative method to deal with the correlated 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 [5] 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.

In the previously described sensor identification task the PRNU fingerprints are usually pre-calculated using images from sensors available to the investigators. However this is not always the case in a realistic scenario, because the images under investigation could be part of an image set containing images from an unknown number of different cameras. Hence, before a source identification can be performed, images acquired with the same camera need to be identified and grouped together first. This task is known as source camera attribution in an open set scenario [6]. This has already been investigated by other researchers, who proposed Hierarchical Agglomerative Clustering (HAC) [7, 8] or Multi-Class Spectral Clustering (MCSC) for this scenario [6] 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 the ground truth for the data sets is usually not available in this scenario, these approaches are not considered in this work. Other related work by Bloy [9] 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 source sensor attribution techniques used in [10] are used in this work together with the previously mentioned approach of Bloy [9].

In this paper we perform a source sensor attribution on different biometric data sets to investigate if multiple sensors have been used during the acquisition of the images in a completely blind manner without a priori knowledge of the data sets described in Section 4. To enhance the quality of the extracted PRNU, we make use of a PRNU enhancing technique to be able to reduce the influence of the image content on the results as described in Section 2. Furthermore special uncorrelated data has been acquired with available sensors to generate PRNU fingerprints and the performance of using these fingerprints is compared to the use of the PRNU enhancement technique. To be able to use the uncorrelated data specifically acquired with the available sensors, alterations of the previously mentioned techniques used in [10] are proposed in Section 3. Section 5 explains the experimental set-up and in Section 6 the experimental results are presented. Finally Section 7 concludes the paper.

2. PRNU EXTRACTION AND ENHANCEMENT

The extraction of the PRNU noise residuals is performed by using the algorithm described by Fridrich [13]. 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 [14], because it is producing good results in filtering out the PRNU. The PRNU noise residual is then normalized in respect to the L_2-norm because its embedding strength is varying between different sensors as explained by [3]. As additional post processing steps a zero mean operation has been applied to each extracted PRNU noise residual to suppress artifacts with regular grid structure and a Wiener filtering is performed in the Discrete Fourier Transform (DFT) domain to suppress periodic artifacts in the calculated PRNU fingerprints.

In this work we apply a PRNU enhancement approach which aims at filtering out scene details using 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. The enhancement function *ELi* used corresponds to the Model 3 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 $i = 1...N$.

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

To enhance the PRNU fingerprints a Wiener filter is applied in the DFT domain, to suppress periodic artifacts as described in [1].

The peak correlation energy (PCE), as proposed in [1], is used to detect the presence of a PRNU fingerprint $\hat{K}$ in an Image I with

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

where ρ indicates the PCE score between the PRNU residual W_i of the image I and the fingerprint $\hat{K}$ weighted by the content of I.

3. SOURCE SENSOR ATTRIBUTION TECHNIQUES

For the source sensor attribution we use two different techniques: the *Blind Camera Fingerprinting and Image Clustering* (BCFAIC) proposed in [9] and the *Sliding Window Fingerprinting* (SWFP) proposed in [10]. Additionally we propose extensions of these methods for the case that the sensor is available to the investigators and uncorrelated data is used to generate the PRNU fingerprint (KSBCFAIC and KSSWFP), which are described in the following section. These is done by acquiring images with high saturation (but not over saturated) and smooth content, according to Fridrich [1]. The novel extensions of the existing methods are presented below.

3.1. KSBCFAIC

In [9] Bloy proposed the Blind Fingerprinting and Image Clustering (BFAIC) technique, which performs an agglomerative clustering to construct PRNU fingerprints from a mixed set of images, enabling identification of each images source camera without any prior knowledge of source. This technique solely depends on a pre-calculated threshold function. Using this threshold function t an automatic clustering algorithm performs the following steps:

1. Randomly select pairs of images until a pair is found whose noise correlation exceeds $t(1)$; average the PRNU of this pair to form a fingerprint.
2. Perform the first pass: for each remaining image, correlate the PRNU with the fingerprint. When the correlation value exceeds t(# of images in fingerprint cluster), average (cluster) it into the fingerprint. When $n = 50$ images have been averaged into the fingerprint or all images have been tried, stop and go to Step 3.
3. Perform the second pass: loop over all the unclustered images a second time, correlating with the current fingerprint and adding those that exceed the threshold. (Do not average more than 50 images into the fingerprint but allow more than 50 to be associated with the fingerprint.)
4. Repeat Step 1. Give up when Step 1 has tried 1000 pairs without success.

To be able to use the uncorrelated data, the first step (Step 1) is modified so that in the first iteration a PRNU Fingerprint is calculated from the uncorrelated data and the selection of two random images is skipped. After that each remaining image is correlated to this fingerprint as described in Step 2 and 3. After correlating all images, Step 1 is repeated as in the original algorithm by selecting two random images. We call this extension *Known Sensor Blind Camera Fingerprinting and Image Clustering* (KSBCFAIC).

3.2. KSSWFP

The Sliding Window Fingerprinting (SWFP) technique proposed in [11] consists of a so called "sliding window" with an arbitrary but fixed size n that moves over a data set image by image. This novel forensic technique uses an iterative algorithm which performs the following steps:

1. Start at image with index $i = 0$.
2. Gather images inside the sliding window with size n, hence the images with index $i \dots i + n$.
3. Extract the PRNU noise residual for each image.
4. Compute a PRNU fingerprint using the images inside the window.
5. Increment the index i by 1.
6. Repeat step 2 until all the images have been used to calculate a PRNU fingerprint.

Moving the window over the whole data set yields a list of PRNU fingerprints, which have been computed using sequential overlapping windows. For a data set containing m images, $m - n$ PRNU fingerprints are generated. After generating the fingerprints, the similarity of a PRNU fingerprint FP_i from the iteration i with all other fingerprints FP_j where $i \neq j$ is computed by calculating the PCE score of each fingerprint pair. This leads to a similarity matrix with size $(m - n) \times (m - n)$ containing all the pairwise PCE scores.

For the *Known Sensor Sliding Window Fingerprinting* (KSSWFP) a PRNU fingerprint is calculated with the uncorrelated data and then its PCE score to all sequentially overlapping PRNU fingerprints generated from the data set under investigation is calculated, which leads to a $(m - n)$ sized vector. High PCE scores in this vector indicate that the current PRNU fingerprint matches to the known sensor used to generate the uncorrelated data.

Data set name	Sensor	Modality
casiaLamp	OKI Irispass-h	Iris
stsmH100_2009	Irisguard H100 IRT	Iris
stsmH100_2013	Irisguard H100 IRT	Iris
stsmIPH_2009	OKI Irispass-h	Iris
stsmIPH_2013	OKI Irispass-h	Iris
casiaFP	Digital Persona UrU4000	Fingerprint
stsmURU_1	Digital Persona UrU4000 #1	Fingerprint
stsmURU_2	Digital Persona UrU4000 #2	Fingerprint

Table 1: Data set name, sensor model and according biometric modality.

4. BIOMETRIC DATA SETS

The data sets used in this paper consist of images for two different biometric modalities, iris and fingerprints, and are illustrated in table 1. The *casiaLamp* data set corresponds to the *CASIA-Iris-Lamp* data set present in the CASIA-Iris V4 database [1]. The *casiaFP* data set corresponds to the CASIA Fingerprint V5 database [1]. The remaining data sets have not been published, however the iris and fingerprint data sets starting with "stsm" and ending with "2013" have been acquired during a COST STSM as described in [12], while data sets ending with "2009" have been provided by the host institution during the STSM. The ground truth on the number of sensor instances used for the acquisition is only known for the *stsmH100_2013*, *stsmIPH_2013*, *stsmURU_1* and *stsmURU_2* data sets, which consists of 1 sensor instance. For all other data sets only the sensor model is known, but not how many instances of this model have been used.

All images are 8 bit grey-level JPEG files. The iris data has been collected under near infrared illumination, while the fingerprint sensors used red LEDs. The uncorrelated data used in this work to acquire the PRNU fingerprints for the known sensors has been acquired according to [12] for the sensors: *OKI Irispass-h*, *Irisguard H100 IRT*, *Digital Persona*

[1]CASIA Iris Image Database and CASIA Fingerprint V5 Database, `http://biometrics.idealtest.org/`

BCFAIC *ELi*	casiaLamp	stsmH100_2009	stsmH100_2013	stsmIPH_2009	stsmIPH_2013	casiaFP	stsmURU_1	stsmURU_2
Images	16213	908	1451	1620	970	19958	1000	1000
Total partitions	7	2	1	3	3	3	2	2
Partitions > 500	2	1	1	1	1	1	1	1
Partitions < 10	3	1	0	1	1	1	1	0
KSBCFAIC	casiaLamp	stsmH100_2009	stsmH100_2013	stsmIPH_2009	stsmIPH_2013	casiaFP	stsmURU_1	stsmURU_2
Total partitions	8	2	1	3	3	3 / 3	2	2
Partitions > 500	3	1	1	1	1	2 / 2	1	1
Partitions < 10	4	0	0	1	1	0 / 0	0	0
KSBCFAIC *ELi*	casiaLamp	stsmH100_2009	stsmH100_2013	stsmIPH_2009	stsmIPH_2013	casiaFP	stsmURU_1	stsmURU_2
Total partitions	7	3	1	3	3	3 / 3	2	2
Partitions > 500	2	1	1	1	1	2 / 2	1	1
Partitions < 10	2	2	0	2	2	0 / 0	0	0

Table 2: Clustering Results of the BCFAIC technique with applied *ELi* PRNU enhancement (top) compared to the KSBCFAIC technique using uncorrelated data (middle) and a combination of the *ELi* PRNU enhancement and the use of uncorrelated data for KSBCFAIC (bottom).

UrU4000 #1 and *Digital Persona UrU4000 #2*. To obtain high-quality PRNU fingerprints according to Fridrich [1], images with uncorrelated content and high saturation have been acquired. *Irisguard H100 IRT* sensor had no built-in quality assessment for the acquired images, hence the uncorrelated could be acquired as desired. For all other sensors the quality assessment partially prevented to acquire such images.

5. EXPERIMENTS AND SET-UP

All the data sets described in section 4 are investigated independently. Since the image size is varying between the data sets, the PRNU noise residual of each image is extracted from a single patch with a size of 256×256 pixels from the image centre. First we compare the use of PRNU enhancements for the ordinary source attribution techniques, BCFAIC and SWFP, to the extended techniques KSBCFAIC and KSSWFP without any further enhancements, to evaluate if the use of uncorrelated data helps to clarify the results for known sensors. Second, the use of PRNU enhancements and uncorrelated data are combined.

After the extraction of the PRNU noise residuals the enhancement of Li [5] (denoted as *ELi*) is applied to the PRNU as described in section 2. A threshold value of $\alpha = 6$ was used for the enhancement function for both enhancement approaches. The Wiener filtering in DFT is applied after each PRNU fingerprint calculation, while the zero mean operation is applied after the PRNU extraction for each image.

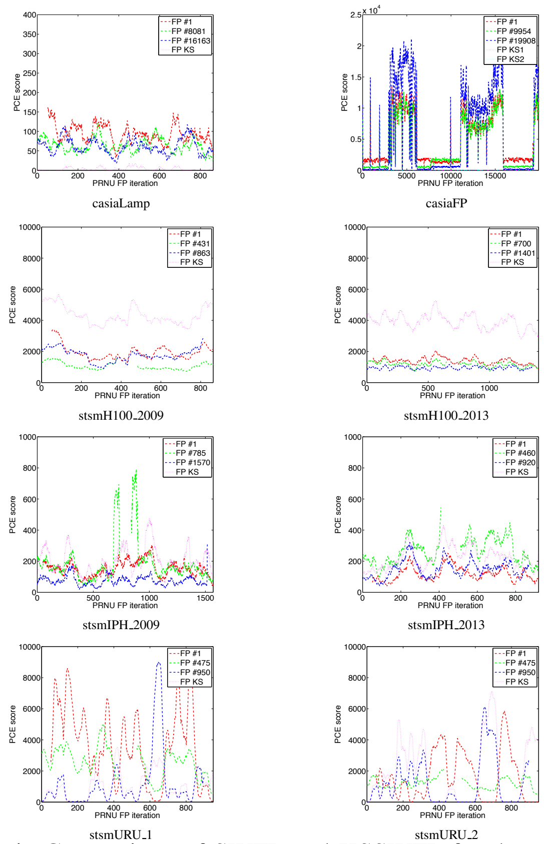

Fig. 1: Comparison of SWFP and KSSWFP for the various data sets: FP #x denotes the similarity of the PRNU fingerprint with iteration x to all other fingerprints for the SWFP technique, FP KS denotes the similarity of the PRNU fingerprint generated from uncorrelated data in the KSSWFP technique.

6. RESULTS

In the following section we first compare the use of PRNU enhancements for the ordinary source attribution techniques, BCFAIC and SWFP, to the extended techniques KSBCFAIC and KSSWFP without any further enhancements and afterwards, we compare the results of using PRNU enhancements and uncorrelated data in combination to the previous results. For the *casiaFP* data set it was not clear which of the two sensors, *Digital Persona UrU4000 #1* or *Digital Persona UrU4000 #2*, has been used for the data acquisition, hence the uncorrelated data from both sensors was used independently for the experiments.

6.1. Uncorrelated data versus PRNU enhancements

First the Blind Camera Fingerprinting and Image Clustering (BCFAIC) using the *ELi* technique was applied to the different data sets and compared to the KSBCFAIC technique using data from the sensors assumed to have been used to acquire the data as shown in table 2. These techniques create clusters of associated images (images with a high PCE score) and partition the data sets. The resulting partitions are reflecting the number of distinct sensors used in the data set. The results do not show any clear improvement of using uncorrelated data for the sensors in respect to the PRNU enhancement, almost all data sets show one cluster containing almost all of the images and a small number of small clusters containing only a few images. Only the *casiaLamp* and *casiaFP* data sets show each two partitions both containing a large amount of images. This could be an indicator that the dataset is containing images from multiple sensors.

The (Known Sensor) Sliding Window Fingerprinting (KS)SWFP 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 scores. 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 or have at least a PCE score of 50 or above. The results for the *casiaLamp* and *casiaFP* data set show many jumps in the PCE scores, which could indicate the presence of multiple sensors. It is to note that the PRNU fingerprint generated produces very low PCE scores (around 0), meaning that the uncorrelated data has not been acquired with the same sensor. The use of uncorrelated data does not lead to any improvement for the score interpretation here. Contrary to the previous results, for both *stsmH100* and both *stsmIPH* data sets, the results using the uncorrelated data show a high improvement in the PCE scores, which leads to the assumption that this sensor was exclusively used for their acquisition. For the remaining *stsmURU* data sets the scores have a high variation and the use of uncorrelated data does not help to clarify the scores either because the results are very similar to the PRNU enhancement results.

6.2. Combination of Uncorrelated data and PRNU enhancement

As it can be seen in table 2, the results of combining the *ELi* PRNU enhancement and uncorrelated data acquired also used to acquire the images in the respective data sets almost does not change the results for the KSBCFAIC technique. The only change that can be seen is that it shifts some images from the clusters containing between 500 and 10 images towards the larger clusters, which leads to a higher amount of small clusters with less than 10 images in some cases.

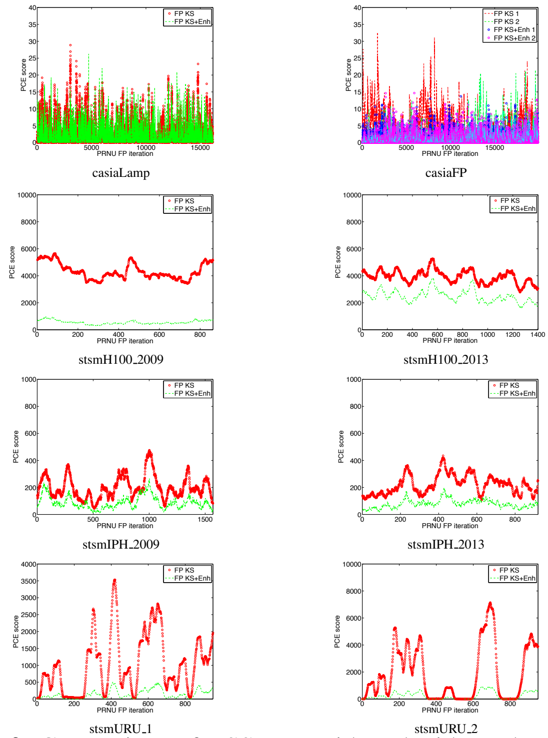

Fig. 2: Comparison of KSSWFP with and without the use of the *ELi* enhancement: FP KS denotes the use of uncorrelated data only, while FP KS+Enh denotes the additional use of the *ELi* enhancement. The two numerations for *casiaFP* denote the sensors for the uncorrelated data: 1 - UrU4000 #1, 2 - UrU4000 #2.

The results of the combination for the KSSWFP technique show highly variable very low PCE scores for the *casiaLamp* and *casiaFP* data sets, from which no conclusion on the number of sensors can be made. The only assessment that can be done is that the uncorrelated data must have been acquired with a different sensor than the images in the data sets, since the PCE scores are all very low. For the *stsmH100_2009* the PCE scores drop quite drastically after the combination, but they remain at a level where one could state that the images in the data set have been acquired using the sensor to acquire the uncorrelated data. Both *stsmIPH* data sets and also the *stsmH100_2013* also show a decrease in the PCE scores, but not as radical as in the *stsmH100_2009* data set. The *stsmURU* data sets also show variable PCE scores ranging from very low to very high values, which implies the presence of multiple sensors. Since both data sets have been acquired using a single sensor instance only, as noted in section 4, the extracted PRNU must have a low quality and hence distort the results. The combination of PRNU enhancement and uncorrelated data also lowers the PCE scores for these two data sets.

7. CONCLUSION

In this paper we compared the use of PRNU enhancement techniques to the use of uncorrelated data for PRNU fingerprint generation in the context of sensor attribution. We investigated data from biometric sensors of two different biometric modalities, iris and fingerprint, where some of the data sets have been known to be acquired with a single sensor instance, while this was not known for others. We additionally proposed novel extension, KSBCFAIC and KSSWFP, for two existing source attribution techniques and compared them to the original techniques. Summing up the results of the comparison between PRNU enhancement and uncorrelated data, it can be stated that for some sensors, like the *OKI Irispass-h* and *Irisguard H100 IRT* iris sensors, the use of uncorrelated data improved the similarity between images of the data set and the PRNU fingerprint of the sensor, which shows up in the results of the KSSWFP technique. For the other data sets either the sensor was different than the one used to acquire the images in the data set (*casiaLamp*), or, especially for the fingerprint sensors, the extracted PRNU did not have a sufficient quality to ensure reliable results. Further studies have to be performed in this regard, since previous results from literature showed that the PRNU extracted for fingerprint sensors has a comparable quality to the one extracted from sensors of other biometric modalities.

8. ACKNOWLEDGMENTS

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

9. 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] N. Bartlow, N. Kalka, B. Cukic, and A. Ross, "Identifying sensors from fingerprint images," in *Computer Vision and Pattern Recognition Workshops, 2009. CVPR Workshops 2009. IEEE Computer Society Conference on*, June 2009, pp. 78–84.

[3] 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.

[4] Nathan Kalka, Nick Bartlow, Bojan Cukic, and Arun Ross, "A preliminary study on identifying sensors from iris images," in *The IEEE Conference on Computer Vision and Pattern Recognition (CVPR) Workshops*, June 2015.

[5] 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.

[6] 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.

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

[8] 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.

[9] 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.

[10] 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'15)*, 2015.

[11] L. Debiasi and A. Uhl, "Blind biometric source sensor recognition using advanced prnu fingerprints," in *Proceedings of the 2015 European Signal Processing Conference (EUSIPCO 2015)*, 2015.

[12] 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.

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

[14] 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.