# GENERATION OF IRIS SENSOR PRNU FINGERPRINTS FROM UNCORRELATED DATA

*Luca Debiasi, Andreas Uhl*

Department of Computer Sciences
Multimedia Signal Processing and Security Lab
University of Salzburg
Jakob-Haringer-Str. 2,
5020 - Salzburg, Austria

*Zhenan Sun*

Center for Biometrics and Security Research
National Laboratory of Pattern Recognition,
Institute of Automation,
Chinese Academy of Sciences,
P.O. Box 2728, Beijing, 100080, P.R. China

## ABSTRACT

The photo response non-uniformity (PRNU) of a sensor can be used for various forensic tasks, such as source device identification, source device linking, classification of images taken by unknown cameras, integrity verification, authentication. To ensure good results a high quality PRNU fingerprint of the sensor is needed. This can be achieved by acquiring images with uncorrelated content and high saturation, which are then used to calculate the fingerprint.

Generating the desired data with iris sensors is not trivial, since they mostly have limited configuration options. These limitations come either by the sensor itself or by the software used to acquire the data. We describe how the desired images can be acquired with different iris sensors and illustrate the challenges and problems faced during the acquisition process. Finally the impact of the PRNU fingerprints calculated from the uncorrelated data on the device identification results is evaluated in respect to the usage of correlated data.

***Index Terms***— Digital image forensics, Biometric sensor forensics, iris sensor identification, photo response non-uniformity

## 1. INTRODUCTION

Biometric recognition is becoming more and more popular, because possession and knowledge based authentication techniques are error-prone, since e.g. smart-cards can be lost or PINs and passwords can be forgotten. Biometric authentication systems are able to resolve many of these issues, since biometric features are distinct for different persons. These features cannot be lost or forgotten. However, biometric features can be stolen or adopted and various other ways to circumvent the integrity of a biometric authentication system exist.

To ensure the integrity of biometric systems watermarks have been proposed. As watermarks represent additional data that is inserted into sample data, impact on recognition accuracy may be expected. In fact, literature reports on corresponding effects in case of iris recognition [1], speech recognition [2], and fingerprint recognition [3]. Hence, an other way of ensuring media security is needed. This is where passive media security techniques comes into play, also known as digital image forensics [4]. Sensor fingerprints, a methodology used in digital image forensics, are based on a sensors photo response non uniformity (PRNU) [5, 6]. They provide image integrity and also authenticity by identifying the source sensor uniquely, even various sensors from the same make and model can be distinguished. To ensure good results a high quality PRNU fingerprint of the sensor is needed.

As shown in previous work [7] this methodology was applied to iris biometric datasets in order to investigate its usefulness. The discriminability of the fingerprints of the sensors in the CASIA Iris V4 database was tested with the conclusion, that the EERs and respective thresholds vary highly. Some sensors show satisfying results while others yield EERs over 20% which is not acceptable. The question raised, that if the PRNU fingerprint is going to be applied as an authentication measure for iris databases, it is not clear if the poor EER values in some sensors result from the images special content with low variance between the images, or from the sensor properties.

In this work, we describe how we used the biometric sensor equipment (sensors used to generate the CASIA Iris V4 database) to acquire uncorrelated iris sensor data. For this purpose uncorrelated images have been acquired with the specific sensors, which were afterwards used to generate PRNU fingerprints for the sensors. In section 2 we describe how to acquire uncorrelated and high saturated images for high quality PRNU fingerprint generation. Besides, the challenges and problems faced at doing so are also described. Section 3 explains how a iris-sensor PRNU fingerprint is generated from uncorrelated data. In Section 4 we present our experimental study, where we evaluate the results using the PRNU fingerprints calculated from uncorrelated data, while section 6 concludes the paper.

## 2. ACQUISITION OF UNCORRELATED IRIS SENSOR DATA FOR PRNU FINGERPRINT GENERATION

Previous work regarding Iris-Sensor Authentication using Camera PRNU Fingerprints [7] came to the conclusion that low variance between images used to generate the PRNU fingerprint of the imaging sensors might result in a poor fingerprint. To obtain high-quality PRNU fingerprints, images with uncorrelated content and high saturation are needed. Generating the desired data with the biometric sensors is not trivial, since these sensors are not like cameras in a common way. The configuration options are often limited either by the sensor itself or by the software used to acquire the data. Usually these sensors are optimized to only take specific types of images and have a built-in quality assessment, which ensures that the acquired image satisfies defined constraints.

As noted by Fridrich [8], the best images for estimating the fingerprint are those with high luminance (but not saturated) and small $\sigma^2$ (images with a smooth content). If the camera under investigation is available to the analyst, unsaturated out-of-focus images of bright cloudy sky would be the best.

The sensors used for the image acquisition are the CASIA long-range iris camera, OKI IRISPASS-h, Irisguard AD100 and Irisguard H100 IRT. To capture the data different materials, like paper sheets and plastic foil, were used to obtain uncorrelated out-of-focus images with high luminance.

### 2.1. CASIA long-range iris camera

The CASIA long-range iris camera operates with near infrared illumination and has a lens, which allows manual focusing and aperture control. Therefore the acquisition of the desired data was not challenging, since high luminance could be achieved by using a large aperture and the focus could be easily set to obtain out-of-focus images. The image acquisition software did not contain any quality assessment preventing the images to be taken. A total of 38 images have been acquired with this sensor. Examples are presented in figure 1.

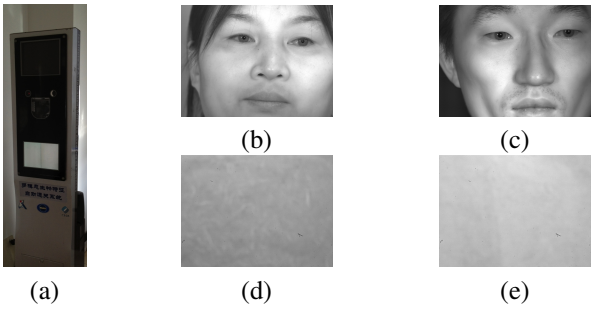



**Fig. 1**. (a) CASIA long-range iris camera. (b),(c) Examples from CASIA-Iris-Distance data set. (d),(e) Examples from uncorrelated data acquisition.

### 2.2. OKI Irispass-h (1)

The OKI Irispass-h sensor is also operating with near infrared illumination and is a small hand held device, which does not allow any manual changes of exposure or focus and the acquisition software has a quality threshold. This threshold can be set to a minimum, where it it possible to take lightly blurred images, but all images must contain a dark filled circle (the pupil) in order to be acquired. The image content could be blurred by holding plastic foil between the sensor and the eye, where the amount of blur could be controlled by adjusting the distance of the foil from the sensor. The larger the distance between the eye and the foil was set, the higher the amount of blur became. The foil had also to be hold in a 45 degree angle, to avoid reflections of the NIR illumination. We were able to acquire lightly blurred images, but it was very challenging because the quality assessment allowed only a certain amount of blur. Therefore the acquisition process with this sensor was very time consuming, resulting in a total of 65 images. Examples are presented in figure 2.

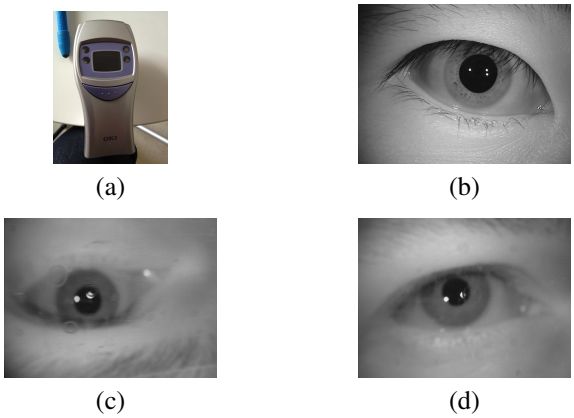
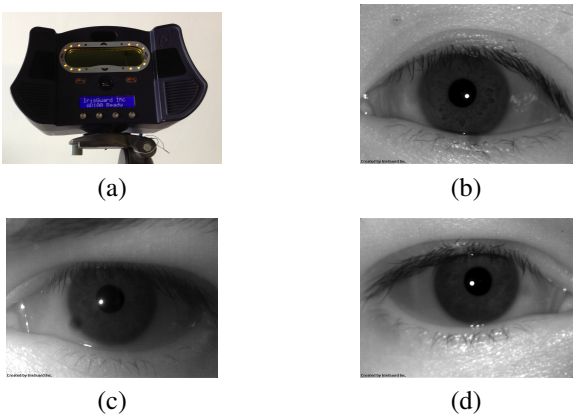



**Fig. 2**. (a) OKI Irispass-h (1) sensor. (b) Example from CASIA-Iris-Lamp data set. (c),(d) Examples from uncorrelated data acquisition.

### 2.3. Irisguard AD100

The Irisguard AD100 sensor is an auto-focus iris camera and features native built-in passive, behavioural and dynamic countermeasures like liveness detection, Cosmetic contact lenses spoofing detection, replay attacks and their denial using a built-in flash illumination tickler and advanced software countermeasures mechanics. Further countermeasures detect severe head tilting, abnormal pupil dilation in order to reduce vulnerability to malign attacks. These quality assessments could not be disabled and therefore made it impossible to acquire out-of-focus images with uncorrelated content and high

saturation. Blurring the images with plastic foil did not work because the quality assessment did not capture any blurred images. Hence, for this sensor uncorrelated images could not be acquired. Examples can be seen in figure 3.



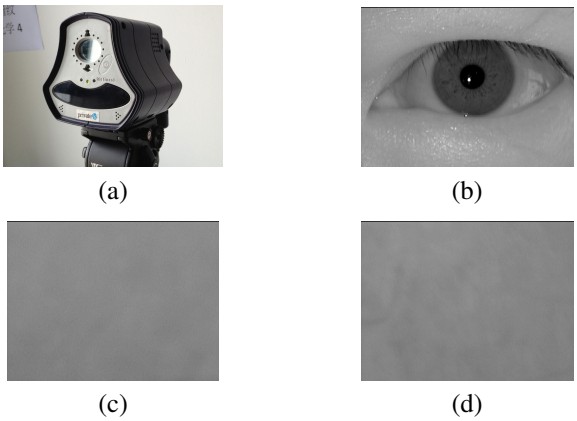
(a) (b)

(c) (d)

**Fig. 3**. (a) Irisguard AD100 sensor. (b) Example from subject captured in the AD100-2013 data set. (c),(d) Examples from attempted uncorrelated data acquisition.

### 2.4. Irisguard H100 IRT

The Irisguard H100 IRT sensor, a hand held device, also features near infra-red illumination and offers no manual controls. The quality assessment of its acquisition software can be deactivated, which allows to acquire the desired images using different sheets of paper to obtain uncorrelated out-of-focus images. By holding the sheets at a closer distance to the sensor than its near focus limit, blurred images could be captured. A total of 400 images have been acquired with this sensor. Examples can be seen in figure 4.



(a) (b)

(c) (d)

**Fig. 4**. (a) Irisguard H100 IRT sensor. (b) Example from subject captured in the H100-2013 data set. (c),(d) Examples from uncorrelated data acquisition.

## 3. IRIS-SENSOR FINGERPRINT GENERATION FROM UNCORRELATED DATA

For an estimation of each sensors PRNU fingerprint, the algorithm described by Fridrich [7] was used to calculate the PRNU. The PRNU is represents the noise intrinsically inserted into an image during the acquisition process. For each image $I$ the noise residual $W_I$ is estimated

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

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 [9] , because it is producing good results in filtering out the PRNU.

From Equation 1 it can be seen that the PRNU covers the high frequency components of the Image $I$. Hence it interferes with high frequency components of the image content,like edges, which leads to a less accurate estimation of the PRNU. If images with high luminance (but not saturated) and smooth content are used to calculate the PRNU fingerprint as proposed by Fridrich in [8] then estimation accuracy is higher. 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 images used in our work have not been geometrically transformed, therefore 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 $\rho$ 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 $\rho$ is calculated between each image from a sensor $S_i$ and the PRNU fingerprint $\hat{K}_i$ of the sensor $S_i$, where only images are used that have not been part of the PRNU fingerprint estimation. Additionally the correlation $\rho$ 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.

We chose the EER to measure the discriminative performance of the PRNU extracted from the images of the different sensors under investigation. It relies on 2 different types of errors, the false match rate (FMR) and the false-non-match rate (FNMR). Let $I$ be an image captured with sensor $S_I$, $J$ is an image captured with sensor $S_J$ and $\hat{K}$ is the PRNU fingerprint estimate for the sensor $S_I$, where $S_I \neq S_J$.

A false match (FM) is given, if

$$\rho_{[J,\hat{K}]} \geq min(\rho_{[I,\hat{K}]}) \tag{4}$$

Equation 4 implies that the PRNU fingerprint of sensor $S_I$ is more likely present in the image $J$ although it has been acquired with the sensor $S_J$ and the NCC score $\rho_{[J,\hat{K}]}$ is higher

than the minimal matching NCC score$\rho_{[I,\hat{K}]}$, which leads to an identification error because no NCC score threshold can be found either exclude the NCC score of image $J$ from the matches without also excluding the NCC score of image $I$. The more images $J$ from sensor $S_J$ have a higher correlation score with the PRNU fingerprint $\hat{K}_I$ then images $I$ taken with sensor $S_I$, the higher the FMR becomes.

This brings us to the other error type, the false non match (FNM), which is given if

$$\rho_{[I,\hat{K}]} \leq max(\rho_{[J,\hat{K}]}) \tag{5}$$

Equation 5 implies that the PRNU fingerprint of sensor $S_I$ is less likely present in the image $I$ although it has been acquired with the same sensor $S_I$ and the NCC score $\rho_{[I,\hat{K}]}$ is lower than the maximal non-matching NCC score$\rho_{[J,\hat{K}]}$, which leads to an identification error because no NCC score threshold can be found either exclude the NCC score of image $I$ from the non-matches without also excluding the NCC score of image $J$. The more images $I$ from sensor $S_I$ have a lower correlation score with the PRNU fingerprint $\hat{K}_I$ then images $J$ taken with sensor $S_J$, the higher the FNMR becomes. The EER rate describes the point where the FMR and FNMR are equal and can therefore be used to measure the discriminability between two different sensors, where a lower EER implies better discrimination performance.

We calculated the equal error rate (EER) from all correlation values $\rho$ by comparing the sensors pairwise. To estimate the real variability of these values, the interval of confidence at 95% was estimated, because only a finite set of values was used to calculate the EER. To do so, the calculation of EER and threshold was repeated 1000 times on the respective set of $m$ matching and $n$ non-matching $\rho$ values, by drawing $m$ correlation values from the matching-data set and $n$ correlation values from the non-matching data set, making use of sampling with replacement. As a result, we obtained 1000 EERs and the range containing 95% of these values is the interval of confidence. This range excludes the 2.5% lowest and 2.5% highest measures, hence the most extreme values.

## 4. EXPERIMENTS

In the following experiments we used images from six different iris sensors. The six sensors are: CASIA close-up iris camera, OKI IRISPASS-h (1), OKI IRISPASS-h (2), CASIA long-range iris camera, Irisking IKEMB-100, and Irisguard H100 IRT.

The first experiment, subsequently denoted as CASIA Iris V4 experiment, has been conducted with the first five sensors from the CASIA Iris V4 database. The respective data sets are: CASIA-Iris-Interval, CASIA-Iris-Lamp, CASIA-Iris-Twins, CASIA-Iris-Distance and CASIA-Iris-Thousand. 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 sensors of the same model have been used.

The second experiment, subsequently denoted as 2013 iris data sets experiment, has been conducted only for the OKI IRISPASS-h (1) and Irisguard H100 IRT sensors with the corresponding data sets Irispass-2013 and H100-2013. These data sets have reliably been completely acquired with a specific sensor each.

The following steps have been executed for the two experiments mentioned above.

Because the image size is varying between the data sets, we decided to extract the PRNU of every image from 4 patches located in the corners of the image with a size of 128x128 pixels each.

From each of the data set, 180 images were randomly chosen, resulting in a total of 1080 images. From this 180 images 30 were used to calculate the PRNU fingerprint for the respective sensor and the other 150 were used to calculate the correlation scores. At this, the presence of the PRNU fingerprint $\hat{K}$ in images taken with a sensor $S$ is examined to obtain the correlation scores.

This leads to 150 matching (fingerprint $\hat{K}$ comes from the same sensor as the images in the data set under investigation) and 5x150 non-matching correlation scores (fingerprint $\hat{K}$ comes from an other sensor as the images in the data set under investigation) for each sensor. From this correlation scores the EER was calculated for each sensor pair $S_i$ and $S_j$, where $i \neq j$.

The steps described above was repeated twice, first with the PRNU fingerprints generated using images from the respective data sets and then with PRNU fingerprints generated using the uncorrelated data acquired as described in section 2 for the sensors OKI IRISPASS-h (1), CASIA long-range iris camera, and Irisguard H100 IRT.

## 5. RESULTS

### 5.1. CASIA Iris V4 experiment

Table 1 shows the first iteration of the CASIA Iris V4 experiment, where the images used to calculate the PRNU fingerprint for each sensor are taken from the data set of the given sensor, which contains correlated data.

Table 2 shows the second iteration of the CASIA Iris V4 experiment , where the images used to calculate the PRNU fingerprint for the sensors OKI IRISPASS-h (1) and CASIA long-range iris camera are the acquired uncorrelated data according to section 2. For all other sensors, the PRNU fingerprint was calculated as before from images of the respective data set.

Table 3 shows the the absolute difference for the EER values between the first experiment iteration and the second. The values were calculated by subtracting the EER result of a specific sensor pair $(S_i, S_j)$ , $i \neq j$, from the first iteration from the EER value of same sensor pair $(S_i, S_j)$ of the second iteration. Therefore positive values indicate that the EER has

(a) Equal error rates.

| Data set | Interval | Lamp | Twins | Distance |
|---|---|---|---|---|
| Thousand | 24.67 | 14.67 | 4.33 | 5.33 |
| Distance | 17.67 | 11.33 | 1.33 | |
| Twins | 17.67 | 15.33 | | |
| Lamp | 25.33 | | | |

(b) Confidence Intervals.

| Data set | Interval | Lamp | Twins | Distance |
|---|---|---|---|---|
| Thousand | (21.54-27.54) | (11.68-16.62) | (2.98-6.02) | (3.50-6.96) |
| Distance | (14.88-20.34) | (8.62-13.47) | (0.68-2.48) | |
| Twins | (14.69-20.52) | (12.65-17.52) | | |
| Lamp | (21.95-27.98) | | | |

**Table 1**. EERs (a) and CI (b) for all possible sensor combinations. PRNU fingerprints generated from respective data sets.

(a) Equal error rates.

| Data set | Interval | Lamp | Twins | Distance |
|---|---|---|---|---|
| Thousand | 24.67 | 23.67 | 4.33 | 49.17 |
| Distance | 52.33 | 58.17 | 46.00 | |
| Twins | 17.67 | 24.83 | | |
| Lamp | 30.83 | | | |

(b) Confidence Intervals.

| Data set | Interval | Lamp | Twins | Distance |
|---|---|---|---|---|
| Thousand | (21.22-26.96) | (20.87-26.70) | (3.01-6.01) | (44.41-53.59) |
| Distance | (48.63-55.82) | (54.32-61.63) | (41.60-49.76) | |
| Twins | (14.62-20.32) | (22.20-27.83) | | |
| Lamp | (27.69-34.02) | | | |

**Table 2**. EERs (a) and CI (b) for all possible sensor combinations. PRNU fingerprints for Dist and Lamp generated with uncorrelated data.

| Data set | Interval | Lamp | Twins | Distance |
|---|---|---|---|---|
| Thousand | 0.00 | +9.00 | 0.00 | +43.84 |
| Distance | +34.66 | +46.84 | +44,67 | |
| Twins | 0.00 | +9.50 | | |
| Lamp | +5.50 | | | |

**Table 3**. Absolute differences of EERs between PRNU fingerprints generated from the data sets and PRNU fingerprints generated from the uncorrelated data.

increased and negative values that it has decreased.

It can be seen that the generation of the PRNU fingerprints from the uncorrelated data has brought a general increase in the EER between all the different sensor combinations. The increase varies a lot between the different sensors. The sensor pairs having '0' as value used the same fingerprints as in the first iteration.

For the CASIA long-range iris camera respectively the Distance data set there has been an increase of up to almost 50%. Looking at the correlation scores from this sensor using the PRNU fingerprint estimated by the uncorrelated data, it can be seen that they are very low. This could indicate, that the images used to generate the fingerprint and the images in the Dist data set have been acquired with a different sensor. Another explanation for this behaviour is that the two generated PRNU fingerprints do not correlate at all, which could also indicate that this might be different sensors. Taking a closer look at the images from both the data set and the uncorrelated data shows that both contain pixel defects, but the positions of these defects do not match as illustrated in figure 5. Furthermore the defects from the image from the dataset (acquired in 2009) cannot be found in the image with uncorrelated content (acquired in 2013), which excludes ageing effects since pixel defects do not recover over time. All these hints lead to the assumption, that the sensor used to acquire the uncorrelated data was not the same as the one used to acquire the Dist data set and therefore explains the very high EERs. The OKI IRISPASS-h (1) sensor used for the Lamp data set had an increase of the EER of about 9-10%. Because the EER is already relatively high for the Lamp data set (see table 1), Hoeller and Uhl [7] assumed that maybe the data set could have been acquired with different sensors. The increase of the EER could intensify this assumption. On the other hand the uncorrelated data acquired with this sensor could have been insufficient to improve the quality of the sensors PRNU fingerprint. Using the fingerprint generated from the uncorrelated data, where it is verified that the exact same sensor has been used to acquire all the images, it could be investigated if the Lamp data set was acquired with different sensors.

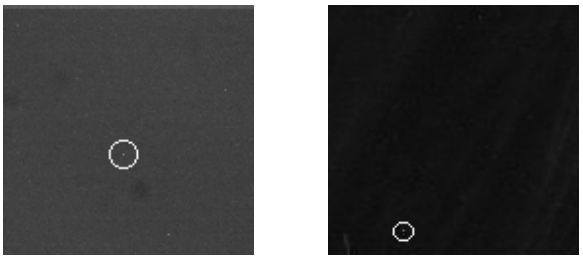
### 5.2. 2013 iris data sets experiment

Table 4 shows the first iteration of the 2013 iris data sets experiment. It can be seen from table 4 that using correlated data

| Data set pair | Irispass-2013 , H100-2013 |
|---|---|
| EER corellated data | 0.00 |
| EER uncorellated data | 0.00 |
| CI corellated data | (0.00-0.00) |
| CI uncorellated data | (0.00-0.00) |
| EER absolute difference | 0.00 |

**Table 4**. EERs, CI and absolute EER difference of the comparison of the Irispass-2013 and H100-2013 data sets.

to calculate the PRNU fingerprints already leads to a EER of 0 for this two data sets. Using uncorrelated data to generate the PRNU fingerprints for both sensors does not change the EER in this experiment and therefore the general increase from ex-



(a) (b)

**Fig. 5**. 128x128 pixel patch from the upper left corner of: (a) uncorrelated data acquired with CASIA long-range iris camera; (b) image from the CASIA Iris-Distance data set. The position of the pixel defects (marked by the circle) is different in both images.

periment 5.1 is not confirmed. This leads to the assumption that the increase in EER from the previous experiment might come from the usage of different sensors during the acquisition of the images in the data sets and that the fingerprints generated from uncorrelated data could further reveal this. To verify this assumption further investigation on the CASIA Iris V4 data set is needed.

## 6. CONCLUSION

High quality PRNU fingerprints are fundamental for good results in different forensic tasks. In this work we have acquired uncorrelated data with iris sensors and described different challenges and problems faced by doing so. Because of the nature of iris sensors of being developed for a special task, in most cases it is not trivial to successfully capture such kind of data, especially with iris sensors incorporating a highly sophisticated quality assessment. After the data acquisition we used the new images to generate PRNU fingerprints for various iris sensors and compared the device identification performance with the results obtained by using correlated data for the PRNU fingerprint generation. The use of uncorrelated data to generate the fingerprint yielded to an increase of the EER for the respective sensors, varying from negligible increase of 0-1% to an increase of up to almost 50%. Because it is not verified whether the CASIA data sets have been acquired each with a single sensor or if they have not, it is difficult to interpret the results, but hints have been found that the latter could apply. It is also possible that the usage of uncorrelated data does not bring any benefit in this case because the estimated fingerprints have already been accurate enough.

Future work will include the application of the method proposed by Chang-Tsun Li to enhance PRNU fingerprints [10] and its impact on both PRNU fingerprints calculated from correlated data and uncorrelated data is evaluated. Some forensic investigation on the CASIA iris database could also clarify if different sensors were used to acquire the images.

## 7. ACKNOWLEDGMENTS

This work has been partially supported by a COST 1106 Short Term Scientific Mission (STSM).

## 8. REFERENCES

[1] Jutta Hämmerle-Uhl, Karl Raab, and Andreas Uhl, "Experimental study on the impact of robust watermarking on iris recognition accuracy.," in *SAC*, Sung Y. Shin, Sascha Ossowski, Michael Schumacher, Mathew J. Palakal, and Chih-Cheng Hung, Eds. 2010, pp. 1479–1484, ACM.

[2] Andreas Lang and Jana Dittmann, "Digital watermarking of biometric speech references: impact to the eer system performance," *Proc. SPIE*, vol. 6505, pp. 650513–650513–12, 2007.

[3] M. Rajibul Islam, M. Shohel Sayeed, and A. Samraj, "Biometric template protection using watermarking with hidden password encryption," in *Information Technology, 2008. ITSim 2008. International Symposium on*, 2008, vol. 1, pp. 1–8.

[4] Hany Farid, "A survey of image forgery detection," *IEEE Signal Processing Magazine*, vol. 2, no. 26, pp. 16–25, 2009.

[5] Mo Chen, Jessica Fridrich, Miroslav Goljan, and Jan Lukáš, "Source digital camcorder identification using sensor photo response non-uniformity," *Proc. SPIE*, vol. 6505, pp. 65051G–65051G–12, 2007.

[6] Mo Chen, Jessica J. Fridrich, Miroslav Goljan, and Jan Lukás, "Determining image origin and integrity using sensor noise.," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 1, pp. 74–90, 2008.

[7] Andreas Uhl and Yvonne Höller, "Iris-sensor authentication using camera prnu fingerprints.," in *ICB*, Anil K. Jain, Arun Ross, Salil Prabhakar, and Jaihie Kim, Eds. 2012, pp. 230–237, IEEE.

[8] Jessica Fridrich, "Digital image forensics using sensor noise," *IEEE Signal Processing Magazine*, vol. 26, no. 2, pp. 26–37, 2009.

[9] 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.

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