Techniques for a Forensic Analysis of the CASIA-Iris V4 Database

UNIVERSITÄT SALZBURG

Luca Debiasi and Andreas Uhl
Multimedia Signal Processing and Security Lab
University of Salzburg
Salzburg, Austria
{ldebiasi,uhl}@cosy.sbg.ac.at

WAVELAB
Multimedia Signal Processing and Security Lab

Abstract

The photo response non-uniformity (PRNU) of a sensor can be useful to enhance a biometric systems security. Previous studies regarding the feasibility of this application have been conducted on the CASIA-Iris V4 database by studying the differentiability of the sensors PRNU fingerprints. The results showed a high variation among the different subsets of the database. To investigate these variations we perform a forensic investigation on the CASIA-Iris V4 database by applying an existing forensic technique and proposing several novel forensic techniques to establish a ground truth of the number sensors used to a acquire a digital image data set in a blind manner and without any a priori knowledge.

Introduction

The **PRNU fingerprint** of a sensor can be used to **improve a biometric systems security**, for instance by ensuring the authenticity and integrity of images acquired with a biometric sensor. **Some sensors in the CASIA-Iris V4 DB showed satisfying results regarding their differentiability, while others did not**.

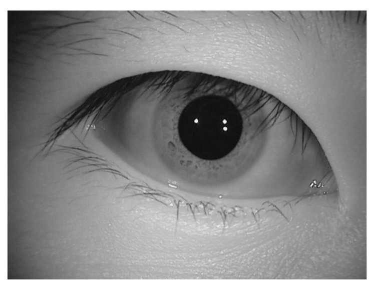
The question raised, that if the PRNU fingerprint is going to be applied as an **authentication measure for iris databases**, it is not clear if the poor differentiation results for some sensors come from the image's special content with low variance between the images, or that **multiple sensors may have been used for the acquisition of the subsets** (**not documented for the CASIA-Iris V4 DB**).

Data Sets

Test data sets:

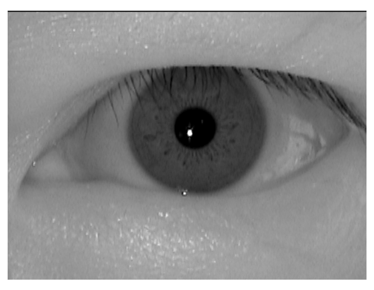
- Sensors: OKI IRISPASS-h0 (A) and Irisguard H100 IRT (B)
- ***test-sequential*** **(TS)**: 500 images from A, 500 from B.
- ***test-mixed*** **(TM)**: alternated blocks of 100 images from A and B (1000 in total).

(1)



(2)

(3)



(4)

OKI IRISPASS-h0 (1) and Irisguard H100 IRT (2) sensors with respective sample images (3) and (4).

CASIA Iris-V4 subsets with sensors:

- ***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 if each subset has been acquired using a single sensor or multiple sensor instances of the same model**.

PRNU extraction and Set-up

All the the **forensic investigation techniques** in this work are **based on the sensors PRNU**.

Because the **image size is varying between the data sets**, the PRNU is extracted from 4 patches located in the corners with a size of 128 × 128 pixels each, resulting in a total **noise residual size of** 256 × 256 pixels.

Forensic Investigation Techniques

- Blind Fingerprinting and Image Clustering (**BFAIC**) by Greg J. Bloy [1]
- K-Means clustering (**KM**)
- PCA K-Means Clustering (**PCA-KM**)
- Sliding window fingerprinting (**SW**)
- Device identification on dataset partitions (**DIODP**)

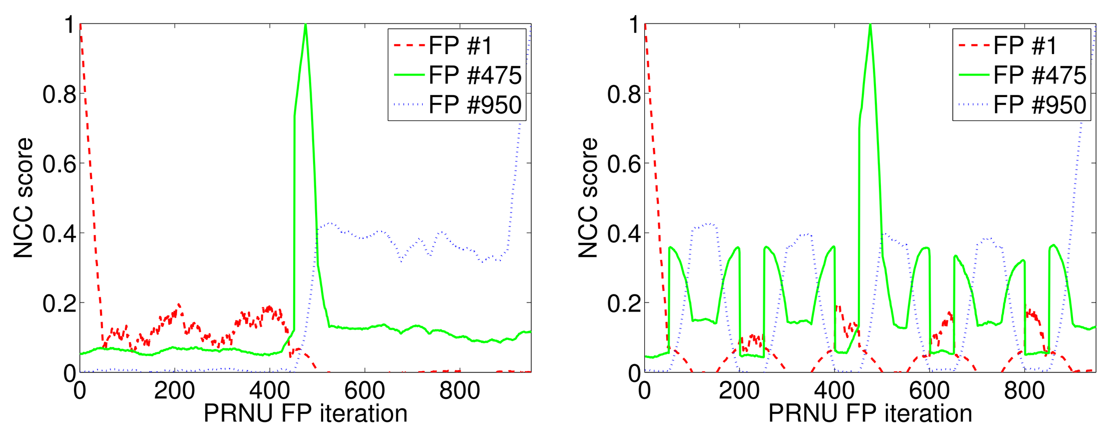
A more detailed description of the forensic techniques can be found in the paper.

Results test data sets

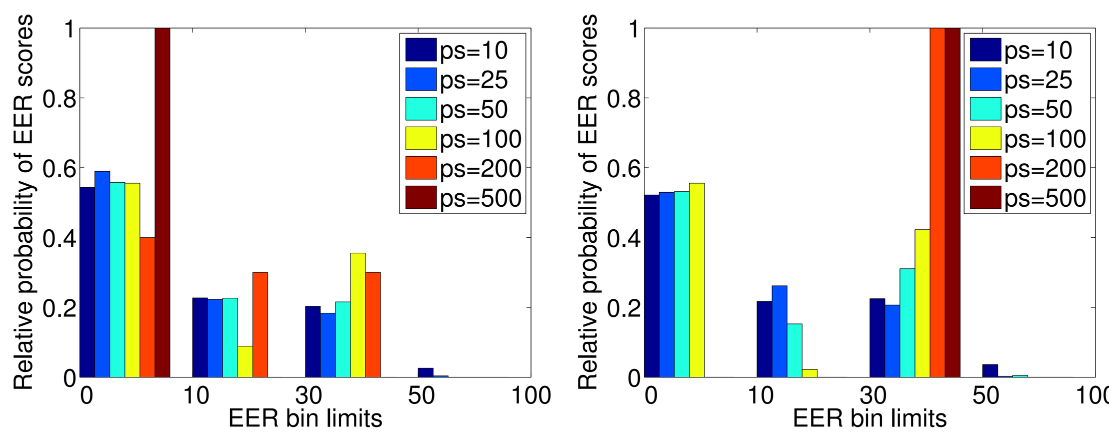
BFAIC	TS	TM
Images	1000	1000
Partitions	**10**	**12**
Unassociated images	0	0

	K-Means		PCA K-Means	
k	TS	TM	TS	TM
1	0.0230	0.0235	0.0112	0.0111
2	**0.0384**	**0.0388**	**0.0381**	**0.0370**
3	0.0161	0.0257	0.0271	0.0269
4	0.0030	0.0037	0.0150	0.0245
5	0.0042	0.0035	0.0140	0.0134

SW experiment with a window size of 50:



DIODP with varying partion sizes (ps):



Results CASIA-Iris V4 I

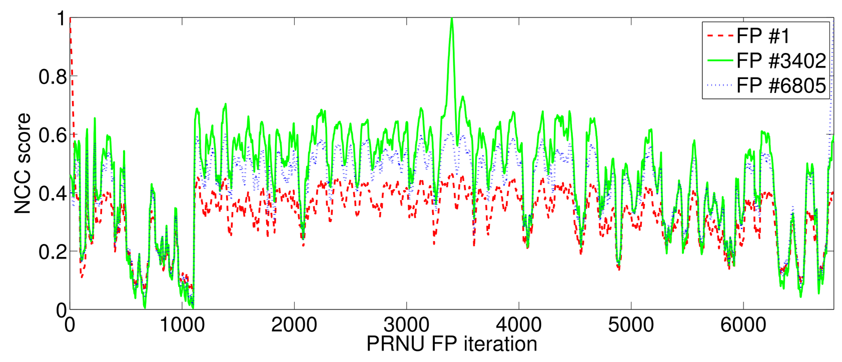
BFAIC	intv	lamp	twin	dist	thou
Images	1307	6855	1095	1566	2000
Partitions	**36**	**64**	**31**	**1**	**3**
Unassociated images	0	0	0	0	0

K-Means results:

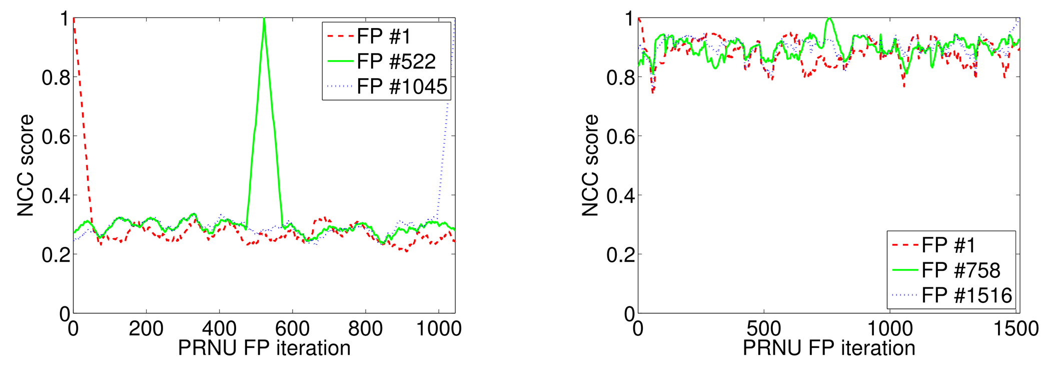
k	intv	lamp	twin	dist	thou
1	0.0024	**0.0391**	**0.0398**	**0.3821**	**0.0121**
2	0.0034	0.0100	0.0052	0.0632	0.0074
3	0.0031	0.0004	0.0063	-0.0076	0.0064
4	0.0032	0.0003	0.0057	-0.0069	0.0045
5	0.0030	0.0001	0.0053	-0.0071	0.0042

Results CASIA-Iris V4 II

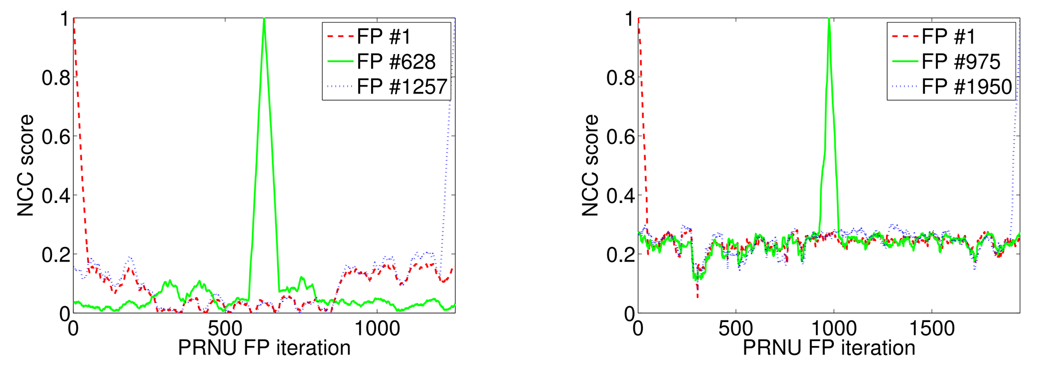
SW with window size 50 on ***lamp***:



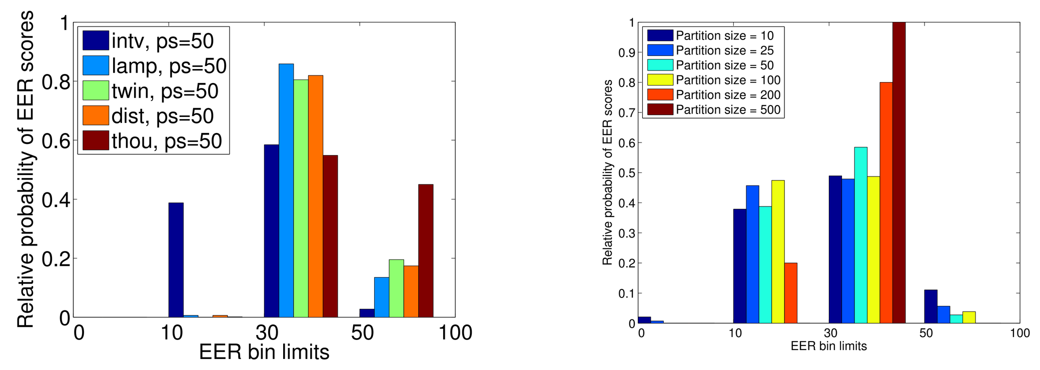
SW with window size 50 on ***twin*** and ***dist***:



SW with window size 50 on ***intv*** and ***thou***:



DIODP with partition size 50 **on all CASIA subsets** and different partition sizes on ***intv***:



Conclusion

Test data sets:

- **All proposed forensic techniques detect the presence of multiple sensors**
- Some even pointed out the **exact number of different sensors**
- **Reimplemented related technique (BFAIC) was outperformed**

CASIA-Iris V4 subsets:

- Results **not as clear as with test sets**
- ***intv*** might contain images from **multiple sensors**
- All **other subsets** have been acquired using **one sensor**

Unknown factors could affect the quality of the PRNU noise residuals and hence tamper the results. Further studies on factors that interfere with the PRNU have to be conducted to be able to use sensor fingerprints to improve a biometric systems security.

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

References

[1] 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.