Camera identification from sensor fingerprints: why noise matters

PS Multimedia Security 2010/2011

Yvonne Höller Peter Palfrader

Department of Computer Science
University of Salzburg

January 2011 / PS Multimedia Security

Outline

Outline

1. Introduction
   - Identification of source cameras
   - Recent work
2. Solution
   - Fingerprint Estimation
   - Fingerprint Detection
   - Evaluation
3. Discussion
4. Further Reading

Image Forensics

- detecting the fingerprint:
  - prove that a certain camera took a given image
  - prove that two images were taken by the same device
  - image is natural and not a computer rendering
- absence of the fingerprint in individual image regions
  - maliciously replaced parts of the image (integrity verification)

[Fridrich, 2009]

Image Forensics

- detecting the fingerprint:
  - prove that a certain camera took a given image
  - prove that two images were taken by the same device
  - image is natural and not a computer rendering
- absence of the fingerprint in individual image regions
  - maliciously replaced parts of the image (integrity verification)

[Fridrich, 2009]

Image Forensics

- strength or form of the fingerprint
  - reconstruct processing history
  - e.g. fingerprint as template to estimate geometrical processing (scaling, cropping, or rotation)
  - non-geometrical operations identified by influenced strength of the fingerprint
- spectral and spatial characteristics of the fingerprint
  - identify the camera model
  - distinguish between a scan and a digital camera image

[Fridrich, 2009]

Image Forensics

- strength or form of the fingerprint
  - reconstruct processing history
  - e.g. fingerprint as template to estimate geometrical processing (scaling, cropping, or rotation)
  - non-geometrical operations identified by influenced strength of the fingerprint
- spectral and spatial characteristics of the fingerprint
  - identify the camera model
  - distinguish between a scan and a digital camera image

[Fridrich, 2009]

Requirements on a camera identifier (fingerprint)

high dimensionality to cover large number of cameras

uniqueness no two cameras have the same fingerprint

stability over time and typical range of physical conditions under which cameras operate

robustness to common image processing

- brightness, contrast, and gamma correction
- filtering
- format conversions
- resampling and JPEG compression

universality virtually all digital cameras have it

[Goljan, 2008]

Outline

1. Introduction
   - Identification of source cameras
   - Recent work
2. Solution
   - Fingerprint Estimation
   - Fingerprint Detection
   - Evaluation
3. Discussion
4. Further Reading

Detecting forgeries - visual sensor classification

- detecting **duplicated image regions** [Popescu and Farid, 2004a]
- using **statistics** to reveal forgeries [Popescu and Farid, 2004b]
- detecting traces of **resampling** [Popescu and Farid, 2005a]
- forgeries in **scientific** images [Farid, 2006]
- intrinsic **lens radial distortion** [Choi et al., 2006]
- **color filter array interpolation** [Popescu and Farid, 2005b, Bayram et al., 2006, Swaminathan et al., 2007]
- imaging **sensor types** [Khanna et al., 2007a]
- **cell phone** cameras [Sankur et al., 2007]
- sensor **dust** characteristics [Dirik et al., 2007b]

Camera identification: Noise patterns

- sensor **imperfections** [Lukáš et al., 2005]
- sensor **noise** [Lukáš et al., 2006a, Lukáš et al., 2006b, Chen et al., 2007a, Khanna et al., 2007b, Chen et al., 2008]
- noise features [Gou, 2007]
- common source digital camera from **image pairs** [Goljan et al., 2007]
- CCD photo response non-uniformity (**PRNU**)[Chen et al., 2007b]
- improvements... [Sutcu et al., 2007]
- noise in **scaled** and **cropped** images [Goljan and Fridrich, 2008]
- **printed** images [Goljan et al., 2008]
- camera **model** identification [Filler and Fridrich, 2008]

Photo Response Non-Uniformity (PRNU)

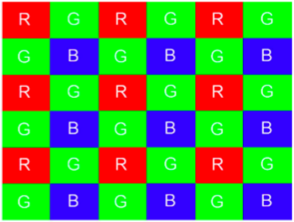
- (Main) research group: Lukáš, Chen et al., Goljan, Fridrich, Filler, et al.
- PRNU is injected into the image **during acquisition**
  - before the signal is quantized
  - before the image is processed in any manner

Photo Response Non-Uniformity (PRNU)

- (Main) research group: Lukáš, Chen et al., Goljan, Fridrich, Filler, et al.
- PRNU is injected into the image **during acquisition**
  - before the signal is quantized
  - before the image is processed in any manner

Sensor Output Model - Intuitive View

1. **light** cast by the camera optics projected onto pixel grid of the imaging sensor
2. **amplification** and **quantization**
3. **Color Filter Array**
   - interpolation (or demosaicking)
   - color correction, gamma correction

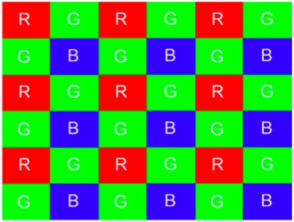


Finally:

- evt. filtering (de-noising, sharpening)
- JPEG: quantization

Sensor Output Model - Intuitive View

1. **light** cast by the camera optics projected onto pixel grid of the imaging sensor
2. **amplification** and **quantization**
3. **Color Filter Array**
   - interpolation (or demosaicking)
   - color correction, gamma correction

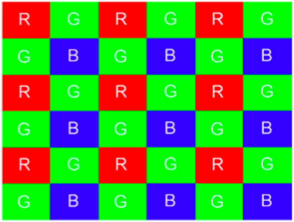


Finally:

- evt. filtering (de-noising, sharpening)
- JPEG: quantization

Sensor Output Model - Intuitive View

1. **light** cast by the camera optics projected onto pixel grid of the imaging sensor
2. **amplification** and **quantization**
3. **Color Filter Array**
   - interpolation (or demosaicking)
   - color correction, gamma correction



Finally:

- evt. filtering (de-noising, sharpening)
- JPEG: quantization

Sensor Output Model - Mathematic Model

$$I = g^{\gamma}[(1 + K)Y + \Omega]^{\gamma} + Q \qquad (1)$$

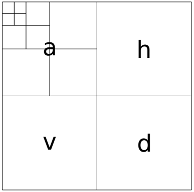
- I quantized signal before demosaicking
- g gain factor
- γ gamma correction factor
- K zero-mean noise-like signal - SENSOR FINGERPRINT
- Ω other noise sources
- Q distortion by quantization and/or compression
- Y scene light intensity

Outline

Fingerprint Estimation

- Sensor fingerprint is a noise-like signal.
- Sensor noise is … well, noise.
- How to find noise? Denoise the image, then diff it to the original.

Wavelet based Noise-Filter[Mihcak et al., 1999]



- Do a 4th-level wavelet decomposition (db8)
- For each high-frequency sub-band, and for each window size $w \in \{3, 5, 7, 9\}$, estimate local variance:

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

- Pick the smallest in each point, that's our $\hat{\sigma}^2[i,j]$.
- Apply a Wiener filter: $h_{\text{den}}[i,j] = h[i,j] \frac{\hat{\sigma}^2[i,j]}{\hat{\sigma}^2[i,j] + \sigma_0^2}$.
- Inverse the wavelet transform.

UNIVERSITÄT SALZBURG

Fingerprint Estimation, II

- Noise residual of one image is now $W = I - F(I)$.
- Fingerprint for many images? $\Rightarrow$ Average them.
- Observation: brighter regions contain more of the fingerprint. $\Rightarrow$ Weight them.

$$\widehat{K} = \frac{\sum_{i=1}^{n} W_i I_i}{\sum_{i=1}^{n} (I_i)^2}$$

- $\widehat{K}$ is our camera fingerprint.

[Goljan, 2008]

Fingerprint Estimation, II

- Noise residual of one image is now $W = I - F(I)$.
- Fingerprint for many images? $\Rightarrow$ Average them.
- Observation: brighter regions contain more of the fingerprint. $\Rightarrow$ Weight them.

$$\widehat{K} = \frac{\sum_{i=1}^{n} W_i I_i}{\sum_{i=1}^{n} (I_i)^2}$$

- $\widehat{K}$ is our camera fingerprint.

[Goljan, 2008]

Fingerprint Estimation, III

- PRNU is **unique** to the sensor.
- Other artifacts are **shared** among cameras of same model or sensor design.
- $\widehat{K}$ contains all **systematic** components in images, that is, artifacts introduced by:
  - color interpolation
  - JPEG compression
  - on-sensor signal transfer
  - sensor design

[Fridrich, 2009]

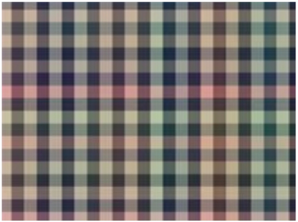
Suppress artifacts by camera model or sensor design

- Artifacts are periodic in row and column averages of $\widehat{K}$, while the PRNU is assumed to follow a zero-mean random distribution.
- Artifact suppression by subtracting row and column averages

$$
\begin{aligned}
\widehat{K}[i,j]' &= \widehat{K}[i,j] \\
&\quad - \frac{1}{m}\sum_{i=1}^{m}\widehat{K}[i,j] - \frac{1}{n}\sum_{j=1}^{n}\widehat{K}[i,j] \\
&\quad + \frac{1}{mn}\sum_{i=1,j=i}^{m,n}\widehat{K}[i,j]
\end{aligned}
$$

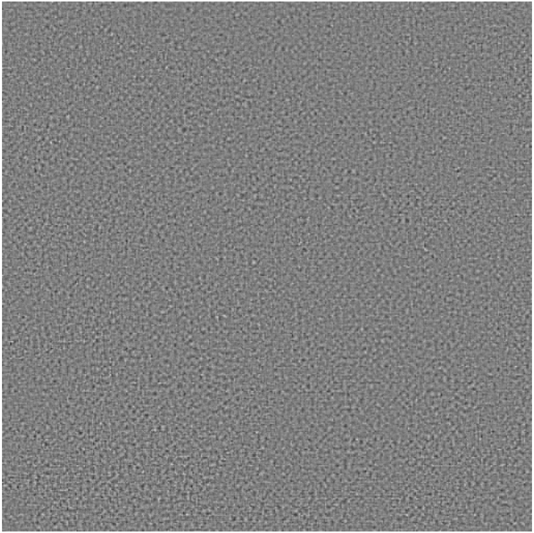
[Goljan, 2008]

Linear Pattern



- $\widehat{K} - \widehat{K}'$ is the linear pattern - used to classify camera model or brand for camera model identification see [Filler and Fridrich, 2008]
- In the presented work, the linear pattern is only a confounding factor, so from now on, $\widehat{K}'$ is our fingerprint.

Fingerprint



Outline

Fingerprint Detection

- Was image **taken with a given camera**?
- Does image noise residual **contain camera fingerprint**?
- noise residual of image I under question: $W = I - F(I)$
- binary **hypothesis test**:

  noise only hypothesis: $W = \Theta$

  fingerprint presence hypothesis: $W = I\widehat{K}' + \Theta$
- Θ denotes pure noise - sequence of **random** variables

Fingerprint Detection

- Was image **taken with a given camera**?
- Does image noise residual **contain camera fingerprint**?
- noise residual of image I under question: $W = I - F(I)$
- binary **hypothesis test**:

  noise only hypothesis: $W = \Theta$

  fingerprint presence hypothesis: $W = I\widehat{K}' + \Theta$
- Θ denotes pure noise - sequence of **random** variables

Decision

- **correlate** W of image I with $I\widehat{K}'$
- if $NCC \;\leq\; NCC_{threshold}$: **noise only**
- if $NCC \;>\; NCC_{threshold}$: **fingerprint present**

Outline

Setup

- database with images **sorted by model/camera**
- **split** the files into two sets
  - one for **estimating** fingerprints
  - the other for **evaluation** of detection performance
- randomly pick 50 images for each camera for fingerprint estimation

Determine $NCC_{threshold}$ - Step 1

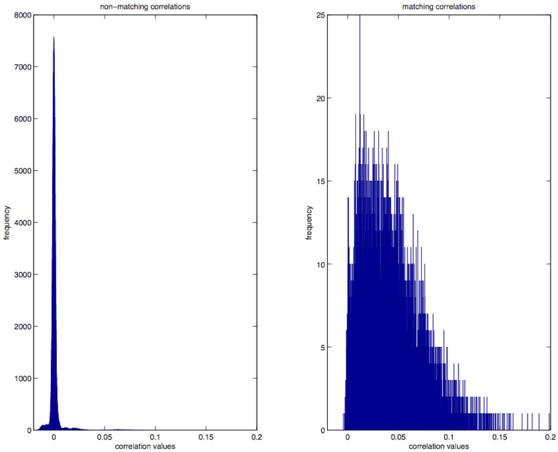
- 35 cameras, 7 brands, 16 models
- images which were **not used for fingerprint estimation**
- correlate:
  - all images taken with a source camera c_k with the respective source-camera-fingerprint $\widehat{K}'$ ("matches")
  - all images taken by a camera c_i with the fingerprints of cameras c_1, c_2, ... c_{i-1}, c_{i+1}, ... c_k

Determine $NCC_{threshold}$ - Step 1

- 35 cameras, 7 brands, 16 models
- images which were **not used for fingerprint estimation**
- correlate:
  - all images taken with a source camera c_k with the respective source-camera-fingerprint $\widehat{K}'$ ("matches")
  - all images taken by a camera c_i with the fingerprints of cameras c_1, c_2, ... c_{i-1}, c_{i+1}, ... c_k

Determine $NCC_{threshold}$ - Step 2

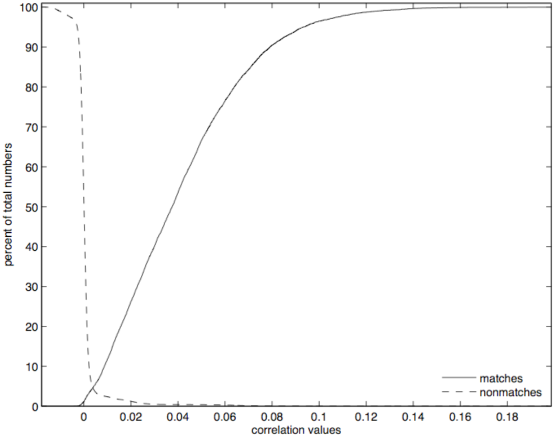
histograms of all correlations of images in database



UNIVERSITÄT SALZBURG

Determine $NCC_{threshold}$ - Step 3

what values are acceptable for false-positives and false-negatives?



Error-Rates

intersection of curves: **Equal Error Rate**
False- **Acceptance**-Rate, i.e. False-**Positive**-Rate
False-**Rejection**-Rate, i.e. False-**Negative**-Rate

Accuracy of estimated EER/threshold

compute **confidence intervals**

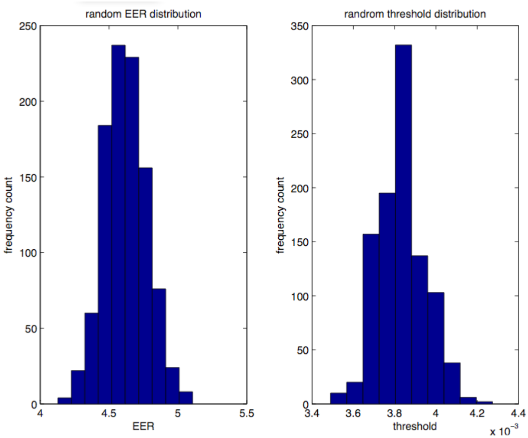
1. randomly draw n samples out of n correlation coefficients separately for matching and non-matching coefficients
2. calculate EER and threshold
3. repeat step 1 and 2 a 1000 times

Accuracy of estimated EER/threshold

compute **confidence intervals**

1. randomly draw n samples out of n correlation coefficients separately for matching and non-matching coefficients
2. calculate EER and threshold
3. repeat step 1 and 2 a 1000 times

Accuracy of estimated EER/threshold

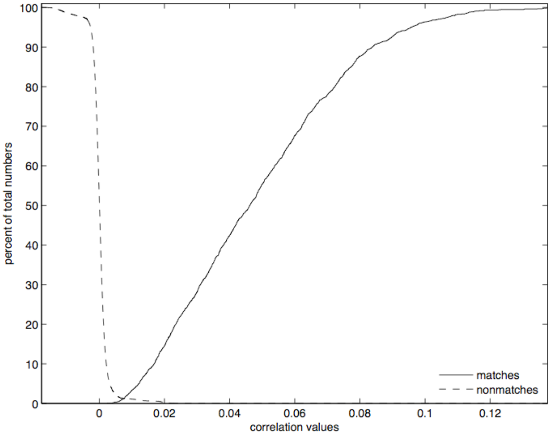


the lower and upper bound including 95% of the values represent the ”confidence-interval”

smaller confidence intervals $\Longleftrightarrow$ better accuracy

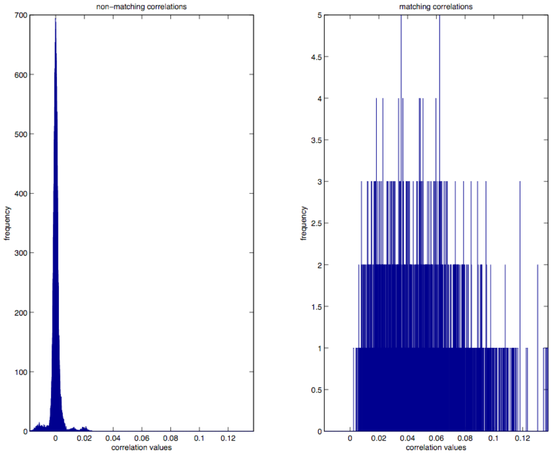
$NCC_{threshold}$ - selected image set

decrease EER and increase threshold interval by choosing images/cameras with per-camera EER of < 1



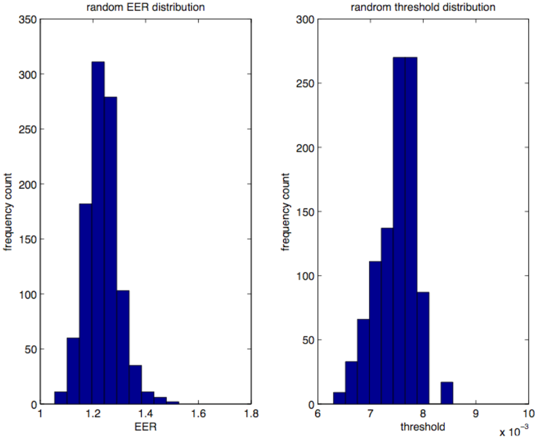
$NCC_{threshold}$ - selected image set

histograms of correlation values of images/cameras with per-camera EER of < 1



$NCC_{threshold}$ - selected image set

resulting confidence interval by choosing images/cameras with per-camera EER of < 1



$NCC_{threshold}$ - values for selected image set

EER	EER-CI	threshold	threshold-CI
1.22	1.14 -1.34	0.0075	0.0068 - 0.0079

EER: equal error rate; CI: confidence interval;

Several variants...

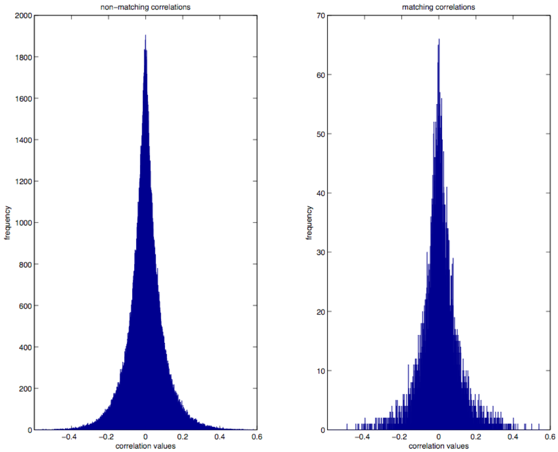
- One problem with our input data was different resolutions.
  $\Rightarrow$ Work on 512^2 pixel segments.
  - **one** segment per corner
  - **6 segments** in each corner (3 horizontal - 2 vertical) for total of 24 segments of 512^2 pixels
- **different wavelet** (db4 instead of db8)
- **different noise filter**

Several variants...

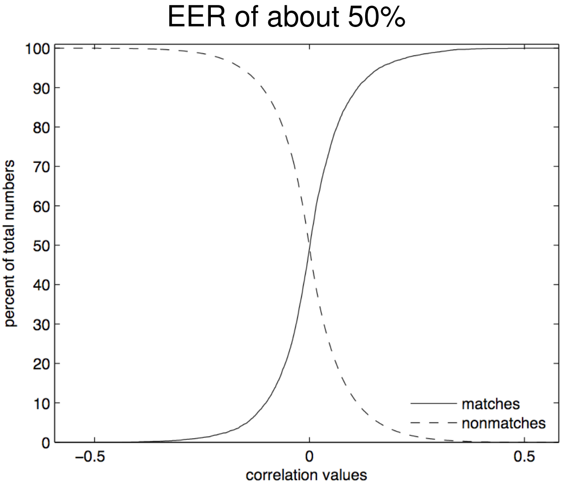
- One problem with our input data was different resolutions.
  $\Rightarrow$ Work on 512^2 pixel segments.
  - **one** segment per corner
  - **6 segments** in each corner (3 horizontal - 2 vertical) for total of 24 segments of 512^2 pixels
- **different wavelet** (db4 instead of db8)
- **different noise filter**

$NCC_{threshold}$ - using Wiener filter

histograms of correlation values by using a Wiener filter



$NCC_{threshold}$ - using Wiener filter



Discussion

- PRNU seems **practicable** for several application scenarios
- **Quality of images** to estimate the PRNU has considerable impact on the achievable error-rates
- Determining a threshold depends on **application scenario**

- Outlook
  - PRNU should be estimated **for each color channel separately**
  - consider eventual **transformations** on images before matching to fingerprint
  - e.g. [Fridrich, 2009] strongly advocates to use **Peak to Correlation Energy** measure (PCE) instead of NCC
  - (still) other **block-sizes** / **block-locations** could be considered
  - other **filters** could be used

Discussion

- PRNU seems **practicable** for several application scenarios
- **Quality of images** to estimate the PRNU has considerable impact on the achievable error-rates
- Determining a threshold depends on **application scenario**

- Outlook
  - PRNU should be estimated **for each color channel separately**
  - consider eventual **transformations** on images before matching to fingerprint
  - e.g. [Fridrich, 2009] strongly advocates to use **Peak to Correlation Energy** measure (PCE) instead of NCC
  - (still) other **block-sizes** / **block-locations** could be considered
  - other **filters** could be used

UNIVERSITÄT SALZBURG

References I

- **Fridrich, J. "Digital Image Forensic Using Sensor Noise.", IEEE Signal Processing Magazine, vol. 26, no. 2, March 2009, pp. 26-37.**
- **Goljan, M. "Digital Camera Identification from Images - Estimating False Acceptance Probability." International Workshop on Digital Watermarking, Busan, Korea, November 10-12, 2008.**
- **Gloe, T., and Böhme, R.: "The 'Dresden Image Database' for Benchmarking Digital Image Forensics". SAC'10 March 22-26, Sierre, Switzerland (2010) 1584-1590.**
- Khanna, N., Mikkilineni, A.K., Chiu, G.T.C, Allebach, J.P., and Delp, E.J.: "Forensic Classification of Imaging Sensor Types." Proc. SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents IX, vol. 6505. San Jose, CA (2007) 0U–0V.
- Gou, H., Swaminathan, A., and Wu, M.: "Robust Scanner Identification based on Noise Features," Proc. SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents IX, vol. 6505. San Jose, California (2007) 0S–0T.
- Swaminathan, A., Wu, M., and Liu, K.J.R.: "Nonintrusive Component Forensics of Visual Sensors Using Output Images." IEEE Transactions on Information Forensics and Security, vol. 2(1) (2007) 91–106.
- Popescu, A.C., and Farid, H.: "Statistical Tools for Digital Forensic," in J. Fridrich (ed.): 6th International Workshop on Information Hiding, LNCS, vol. 3200, Springer-Verlag, Berlin-Heidelberg, New York (2004) 128–147.
- Popescu, A.C., and Farid, H.: "Exposing Digital Forgeries by Detecting Traces of Resampling", IEEE Transactions on Signal Processing, vol. 53(2) (2005) 758–767.

References II

Popescu, A.C., and Farid, H.: "Exposing Digital Forgeries in Color Filter Array Interpolated Images." IEEE Transactions on Signal Processing, vol. 53(10) (2005) 3948–3959.

Farid, H.: "Exposing Digital Forgeries in Scientific Images." Proc. ACM Multimedia & Security Workshop. Geneva, Switzerland (2006) 29–36.

Popescu, A.C., and Farid, H.: "Exposing Digital Forgeries by Detecting Duplicated Image Regions." Technical Report, TR2004-515. Dartmouth College, Computer Science (2004).

Lukáš, J., Fridrich, J., and Goljan, M.: "Digital Camera Identification from Sensor Pattern Noise." IEEE Transactions on Information Forensics and Security, vol. 1(2) (2006) 205– 214.

Chen, M., Fridrich, J., and Goljan, M.: "Digital Imaging Sensor Identification (Further Study)." Proc. SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents IX, vol. 6505. San Jose, California (2007) 0P–0Q.

Goljan, M., and Fridrich, J., "Camera Identification from Scaled and Cropped Images," In E. J. Delp et al. editors, Security, Forensics, Steganography, and Watermarking of Multi- media Contents X, vol. 6819 (2008) 68190E.

Chen, M., Fridrich, J., Goljan, M., and Lukáš, J.: "Determining Image Origin and Integrity Using Sensor Noise," IEEE Transactions on Information Security and Forensics, vol. 3(1) (2008) 74–90.

Lukáš, J., Fridrich, J., and Goljan, M.: "Determining Digital Image Origin Using Sensor Imperfections," Proc. SPIE, Image and Video Communications and Processing, vol. 5685, San Jose, California (2005) 249–260.

References III

- Lukáš, J., Fridrich, J., and Goljan, M.: "Detecting Digital Image Forgeries Using Sensor Pattern Noise." Proc. SPIE, Electronic Imaging, Security, Steganography, and Water- marking of Multimedia Contents VIII, vol. 6072. San Jose, California (2006) 0Y1–0Y11.
- Goljan, M., Chen, M., Fridrich, J., "Identifying Common Source Digital Camera From Image Pairs," Proc. ICIP 2007. San Antonio, Texas (2007).
- Khanna, N., Mikkilineni, A.K., Chiu, G.T.C., Allebach, J.P. and Delp, E.J.: "Scanner Identification Using Sensor Pattern Noise." Proc. SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents IX, vol. 6505. San Jose, CA (2007) 1K–1.
- Sankur, B., Celiktutan, O., and Avcibas, I.: "Blind Identification of Cell Phone Cameras." Proc. SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents IX, vol. 6505. San Jose, California (2007) 1H–1I.
- Chen, M., Fridrich, J., and Goljan, M.: "Source Digital Camcorder Identification Using CCD Photo Response Non-uniformity." Proc. SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents IX, vol. 6505. San Jose, California (2007) 1G–1H.
- Goljan, M., Fridrich, J., and Lukáš, J., "Camera Identification from Printed Images," In E. J. Delp et al. editors, Security, Forensics, Steganography, and Watermarking of Multimedia Contents X, vol. 6819 (2008) 68190I.
- Dirik, A.E., Sencar, H.T., Husrev T., Memon, N.: "Source Camera Identification Based on Sensor Dust Characteristics," Proc. IEEE Workshop on Signal Processing Applications for Public Security and Forensics, Washington, DC (2007) 1–6.
- Choi, K.S., Lam, E.Y., Wong, K.K.Y.: "Automatic source camera identification using the intrinsic lens radial distortion," Optics Express, vol. 14(24) (2006) 11551–1565.

References IV

- Bayram, S., Sencar, H.T., Memon, N., Avcibas, I. : "Source camera identification based on CFA interpolation," Proc. ICIP 2005. IEEE International Conference on Image Processing (2006) 69–72.
- Filler, T., and Fridrich, J.: "Using Sensor Pattern Noise for Camera Model Identification," Proc. ICIP'08, San Diego, California (2008) 12–15.
- Sutcu, Y.; Bayram, S.; Sencar, H.T.; Memon, N. "Improvements on Sensor Noise Based Source Camera Identification," Proc IEEE, International Conference on Multimedia and Expo, (2007) 24–27.
- Mihcak, M.K., Kozintsev, I., and Ramchandran, K. "Spatially Adaptive Statistical Modeling of Wavelet Image Coefficients and its Application to Denoising," Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing, Phoenix, AZ, vol. 6, pp. 3253?3256, March 1999.

Thank you for your attention.

Questions?