



GEORG-AUGUST-UNIVERSITÄT
GÖTTINGEN

Fragile Sensor Fingerprint Camera Identification

Erwin Quiring

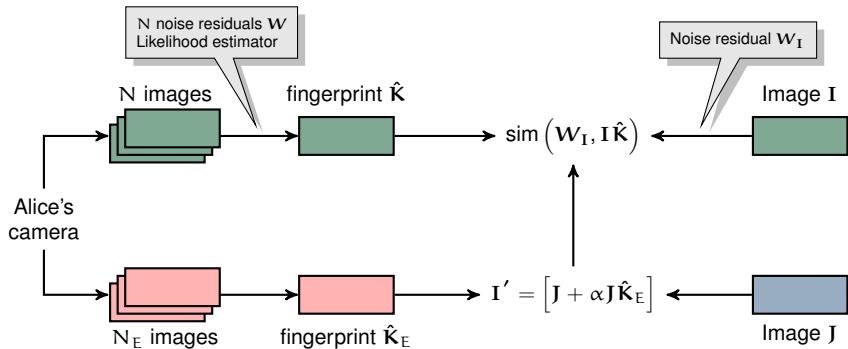
University of Göttingen

Matthias Kirchner

Binghamton University

IEEE International Workshop on Information Forensics and Security
Rome, Italy | November 19, 2015

Camera Identification with Adversaries

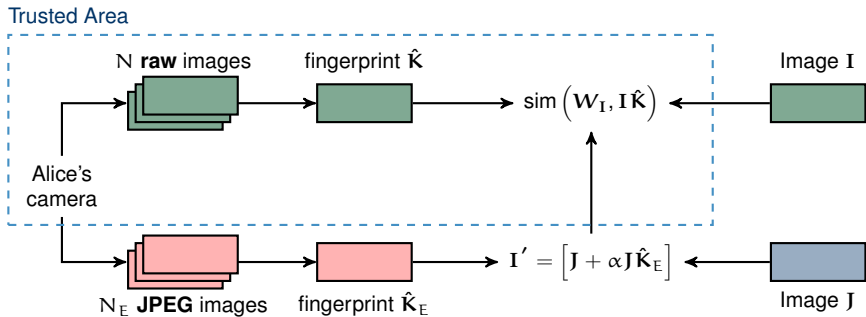


» Countermeasure: Triangle Test

- ▷ Alice may test all images ever made public by her
- ▷ Less reliable with increasing N_E

(Fridrich 2013; Goljan et al. 2011)

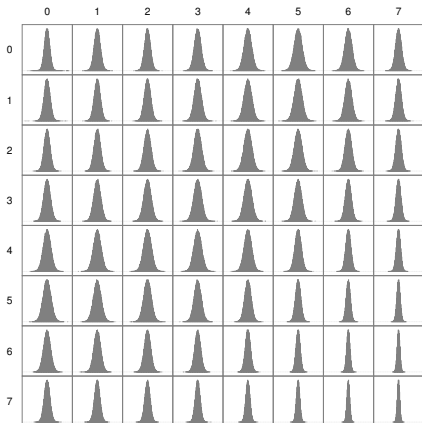
■ Scenario with Asymmetries



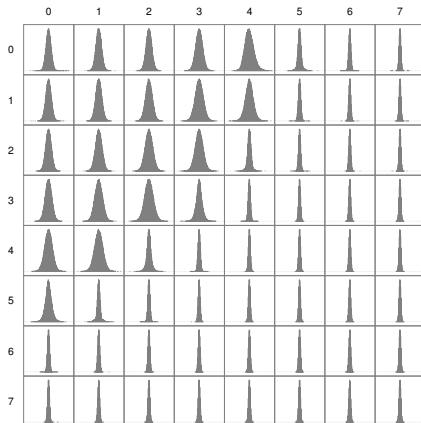
- » Alice's camera supports raw images
- » Alice has shared only JPEG images with the public
- » Eve's goal is to make an image look like Alice's raw images

■ Sensor Fingerprint DCT Distribution

\hat{K}_A from uncompressed images



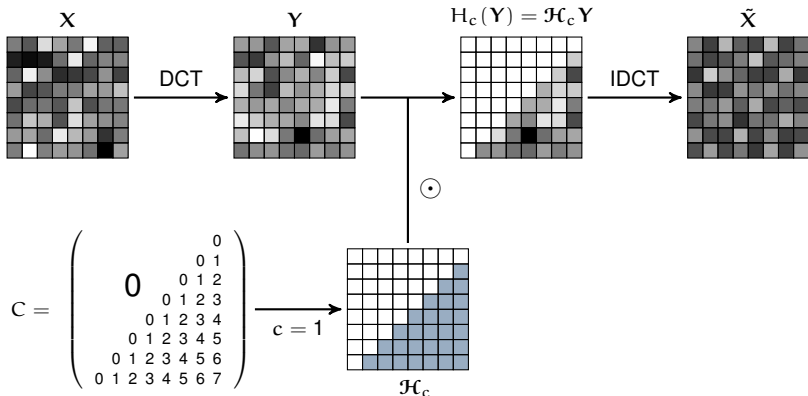
\hat{K}_E from JPEG90 images



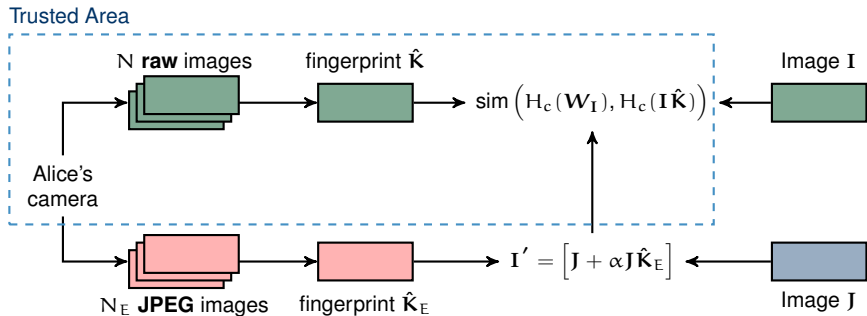
Each fingerprint was estimated from the same 25 flat field images taken by a Nikon D200

■ Fragile Sensor Noise Fingerprint

- » Fingerprint from high-frequency sub-bands only
- » Fingerprint part that is *fragile* to lossy JPEG compression
- » Sub-band selective highpass filter $H_c(\cdot)$:



Revised Scenario



- » Alice can always provide the full fingerprint
- » Eve's estimate lacks accurate high-frequency information
- » Presence of fragile fingerprint indicates authenticity of image
- » Low-frequency fingerprint is orthogonal to fragile fingerprint

■ Setup

- » 6390 uncompressed images from two image databases:

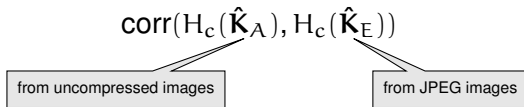
Image Database	Camera model	Camera 0	Camera 1
Dresden (Gloe and Böhme 2010)	Nikon D70	175	188
	Nikon D70s	175	174
	Nikon D200	360	370
RAISE (Dang-Nguyen et al. 2015)	Nikon D7000	4948	—

+ 25 flat field images from each Dresden Database camera

- » Fingerprint Estimation
 - ▷ Noise residuals obtained from Wavelet denoising filter (Mıhçak et al. 1999)
 - ▷ Likelihood Estimator
 - ▷ Post-processing: Zero-meaning & Wiener filtering
- » Similarity criterion: Peak-to-Correlation Energy (PCE)

■ Fragile Fingerprint Estimation (1/2)

» Quality of fingerprint estimation:



» Dresden Image Database:

N_E	JPEG	c					
		full	1	2	3	4	5
150	100	0.3720	0.3484	0.3245	0.2850	0.2302	0.1607
	95	0.2522	0.0870	0.0561	0.0337	0.0160	0.0100
	90	0.1865	0.0294	0.0157	0.0058	0.0009	0.0029
	85	0.1449	0.0109	0.0029	-0.0007	-0.0022	0.0012
	80	0.1174	0.0027	-0.0014	-0.0031	-0.0027	-0.0000
	75	0.0977	-0.0012	-0.0029	-0.0030	-0.0026	-0.0005
	70	0.0851	-0.0029	-0.0037	-0.0036	-0.0030	-0.0011

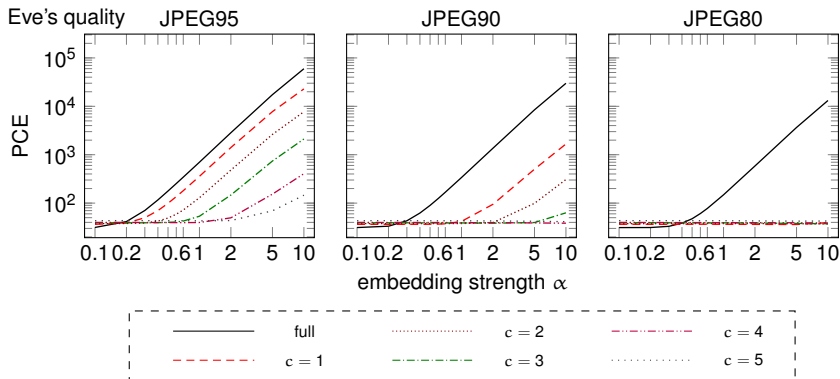
■ Fragile Fingerprint Estimation (2/2)

» RAISE Image Database:

N_E	JPEG	c					
		full	1	2	3	4	5
2000	100	0.6128	0.6002	0.5565	0.4838	0.3828	0.2627
	95	0.5291	0.3752	0.2645	0.1600	0.0800	0.0524
	90	0.4381	0.1513	0.0762	0.0357	0.0169	0.0177
	85	0.3758	0.0506	0.0154	0.0055	0.0023	0.0046
	80	0.3347	0.0172	0.0009	-0.0014	-0.0008	0.0028
	75	0.3035	0.0055	-0.0041	-0.0034	-0.0007	0.0016
	70	0.2837	0.0015	-0.0053	-0.0042	-0.0015	0.0007
4648	100	0.6414	0.6322	0.5924	0.5250	0.4302	0.3123
	95	0.5704	0.4536	0.3464	0.2235	0.1173	0.0773
	90	0.4798	0.2047	0.1087	0.0520	0.0243	0.0253
	85	0.4167	0.0705	0.0231	0.0084	0.0028	0.0078
	80	0.3756	0.0249	0.0024	-0.0019	-0.0013	0.0037
	75	0.3445	0.0085	-0.0049	-0.0042	-0.0000	0.0027
	70	0.3254	0.0036	-0.0063	-0.0059	-0.0008	0.0017

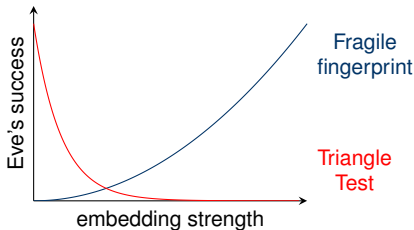
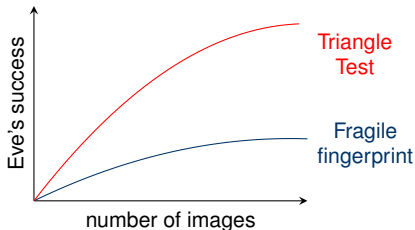
Fingerprint-Copy Attack

» Dresden Image Database ($N_E = 150$):



■ Conclusion

- » Context: Fingerprint-copy attack
 - ▷ Eve frames her victim Alice with a high-quality forgery
 - ▷ Eve plants a fake fingerprint from JPEG images on raw image
- » Alice's countermeasures:
 - ▷ Fragile sensor fingerprint
 - ▷ Triangle Test (Goljan et al. 2011)



■ Future Work

- » Linkage to adversary-aware signal processing
(Barni and Pérez-González 2013)
 - ▷ Alice and Eve have access to training data of different quality
 - ▷ Similarity to hypothesis testing problem in adversarial environment

- » Side channel strategies for DCT coefficient selection

- » Theoretical analysis of high-frequency information in JPEG images
 - ▷ When is Eve able to recover the fingerprint?
 - ▷ Effect of quantization on the fingerprint?

■ References I

- Barni, Mauro and Fernando Pérez-González (2013). “Coping With the Enemy: Advances in Adversary-Aware Signal Processing”. In: *IEEE International Conference on Acoustics, Speech, and Signal Processing*, pp. 8682–8686. DOI: 10.1109/ICASSP.2013.6639361.
- Dang-Nguyen, Duc-Tien, Cecilia Pasquini, Valentina Conotter, and Giulia Boato (2015). “RAISE: a Raw Images Dataset for Digital Image Forensics”. In: *6th ACM Multimedia Systems Conference*, pp. 219–224. DOI: 10.1145/2713168.2713194.
- Fridrich, Jessica (2013). “Sensor Defects in Digital Image Forensic”. In: *Digital Image Forensics: There is More to a Picture Than Meets the Eye*. Ed. by Husrev Taha Sencar and Nasir Memon. Springer, pp. 179–218. DOI: 10.1007/978-1-4614-0757-7_6.
- Gloe, Thomas and Rainer Böhme (2010). “The Dresden Image Database for Benchmarking Digital Image Forensics”. In: *Journal of Digital Forensic Practice* 3.2–4, pp. 150–159. DOI: 10.1080/15567281.2010.531500.
- Goljan, Miroslav, Jessica Fridrich, and Mo Chen (2011). “Defending against Fingerprint-Copy Attack in Sensor-Based Camera Identification”. In: *IEEE Transactions on Information Forensics and Security* 6.1, pp. 227–236. DOI: 10.1109/TIFS.2010.2099220.
- Mihçak, M. Kivanç, Igor Kozintsev, and Kannan Ramchandran (1999). “Spatially Adaptive Statistical Modeling of Wavelet Image Coefficients and its Application to Denoising”. In: *IEEE International Conference on Acoustics, Speech, and Signal Processing*. Vol. 6, pp. 3253–3256. DOI: 10.1109/ICASSP.1999.757535.