Forensic use of photo response non-uniformity of imaging sensors and a counter method

Ahmet Emir Dirik[*] **and Ahmet Karaküçük**

Dept. of Electrical-Electronic Engineering, Faculty of Engineering, Uludag University, Bursa, 16059 Turkey

[*]*edirik@uludag.edu.tr*

Abstract: Analogous to use of bullet scratches in forensic science, the authenticity of a digital image can be verified through the noise characteristics of an imaging sensor. In particular, photo-response non-uniformity noise (PRNU) has been used in source camera identification (SCI). However, this technique can be used maliciously to track or inculpate innocent people. To impede such tracking, PRNU noise should be suppressed significantly. Based on this motivation, we propose a counter forensic method to deceive SCI. Experimental results show that it is possible to impede PRNU-based camera identification for various imaging sensors while preserving the image quality.

OCIS codes: (100.2000) Digital image processing; (100.5010) Pattern recognition.

References and links

1. J. Lukáš, J. Fridrich, and M. Goljan, "Digital "bullet scratches" for images," in "IEEE Int. Conf. on Image Processing 2005," (IEEE, 2005), pp. III–65.
2. A. E. Dirik, H. Sencar, and N. Memon, "Digital single lens reflex camera identification from traces of sensor dust," IEEE T. Inf. Foren. Sec. **3**, 539–552 (2008).
3. A. E. Dirik, H. Sencar, and N. Memon, "Flatbed scanner identification based on dust and scratches over scanner platen," in "Proc. IEEE Int. Conf. Acoustics, Speech and Signal Process. (ICASSP'09)," (IEEE, 2009), pp. 1385–1388.
4. K. S. Choi, E. Y. Lam, and K. K. Wong, "Automatic source camera identification using the intrinsic lens radial distortion," Opt. Express **141**, 11551–11565 (2006).
5. M. Goljan and J. Fridrich, "Camera identification from cropped and scaled images," in "Proc. SPIE 6819, Security, Forensics, Steganography, and Watermarking of Multimedia Contents X," (2008), pp. 68190E1 – 68190E13.
6. K. Rosenfeld, H. T. Sencar, and N. Memon, "A study of the robustness of prnu-based camera identification," in "Proc. SPIE 7254, Media Forensics and Security," (2009), p. 72540.
7. M. Goljan, J. Fridrich, and M. Chen, "Sensor noise camera identification: countering counter-forensics," in "Proc. SPIE 7541, Media Forensics and Security II," (2010), 607, pp. 75410S1 – 75410S12.
8. M. Goljan, J. Fridrich, and M. Chen, "Defending against fingerprint-copy attack in sensor-based camera identification," IEEE Trans. Inf. Foren. Sec. **6**, 227–236 (2011).
9. T. Gloe, M. Kirchner, A. Winkler, and R. Böhme, "Can we trust digital image forensics?" in "Proc. ACM 15th Int. Conf. on Multimedia (MULTIMEDIA '07)," (ACM Press, New York, USA, 2007), pp. 78–86.
10. R. Böhme and M. Kirchner, "Counter-forensics: Attacking image forensics," in *Digital Image Forensics* , H. T. Sencar and N. Memon, eds. (Springer New York, 2013), pp. 327–366.
11. M. Chen, J. Fridrich, and M. Goljan, "Digital imaging sensor identification (further study)," in "Proc. SPIE 6505, Security, Steganography, and Watermarking of Multimedia Contents IX," (2007), pp. 65050P1–65050P13.
12. J. Lukáš, J. Fridrich, and M. Goljan, "Digital camera identification from sensor pattern noise," IEEE T. Inf. Foren. Sec. **1**, 205–214 (2006).
13. C.-T. Li, C.-Y. Chang, and Y. Li, "On the repudiability of device identification and image integrity verification using sensor pattern noise," in "Information Security and Digital Forensics," , vol. 41 of *Lecture Notes of the*

#190242 - $15.00 USD Received 10 May 2013; revised 6 Oct 2013; accepted 28 Nov 2013; published 3 Jan 2014

Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, D. Weerasinghe, ed. (Springer Berlin Heidelberg, 2010), pp. 19–25.
14. J. Lukáš, J. Fridrich, and M. Goljan, "Detecting digital image forgeries using sensor pattern noise," Proc. SPIE: Image and Video Communications and Processing **5685**, 249–260 (2005).
15. M. Goljan, "Digital camera identification from images - estimating false acceptance probability," in "Digital Watermarking," , vol. 5450 of *Lecture Notes in Computer Science*, H.-J. Kim, S. Katzenbeisser, and A. Ho, eds. (Springer Berlin Heidelberg, 2009), pp. 454–468.
16. J. Fridrich, "Sensor defects in digital image forensic," in *Digital Image Forensics,* (Springer New York, 2012), chap. 5, pp. 179–219.
17. M. Goljan, J. Fridrich, and T. Filler, "Large scale test of sensor fingerprint camera identification," in "SPIE Electronic Imaging," (International Society for Optics and Photonics, 2009), pp. 72540I–72540I.
18. J. S. Lim, *Two-Dimensional Signal and Image Processing* (Prentice Hall, 1990).
19. T. Gloe and R. Böhme, "The dresden image database for benchmarking digital image forensics," J. Digital Forensic Practice **3**, 150–159 (2010).

1. Introduction

Today, digital multimedia is widely used in all areas of life, such as media outlets, businesses, industries, and even courts of law as a primary way to present, process, and store information. With the advances in digital technologies, it is possible to edit and manipulate multimedia with low cost, effort, and expertise. The availability of such technologies and their ease of use risk the credibility of digital information. Thus, when digital information is used or presented, there should be some guarantee about its origin, integrity, and nature of the digital content.

Analogous to use of bullet scratches in forensic science, the authenticity of a digital image can be verified using the noise characteristics of the imaging sensor [1], physical defects [2, 3], distortions [4] in the optical path, and their effects on the digital imaging output. Unlike the shot and read-out noise, the photo-response non-uniformity (PRNU) of the imaging sensor is unique to the device and creates a noise pattern, which does not change in time [1]. PRNU is temporally constant and laterally non-uniform. Therefore, it can be considered an intrinsic fingerprint of an imaging sensor and can be used to trace back an image I to its source X when its authenticity is questioned. Studies in the literature show that PRNU-based camera identification is quite robust to image manipulations such as JPEG compression, cropping, printing [5], and downsizing [6]. Nevertheless, a PRNU pattern can be transferred from one image to another for malicious use or deception in a court case. Although there are some forensic methods [7, 8] to detect such noise transfer, they have limitations and work under certain circumstances. Furthermore, PRNU-based source camera identification has a potential to be used by an adversary for illegal identity tracking from shared images in different social networks by violating the privacy rights. Therefore, a counter method against source camera identification (SCI) is needed to protect personal privacy and to avoid mistrials in court of law [9, 10].

Previously used preventative measures against PRNU-based camera identification have shown to be surmounted [7, 8]. In [6], it is shown that reducing the image quality can degrade the PRNU noise significantly. However, PRNU-based source identification is still possible under heavy post-processing and manipulations [11]. Another counter attempt is to use a method called flat-fielding [12]. Ideally, this method has a number of physical requirements, such as capturing completely dark and uniformly lightened images having the same parameters, e.g., light sensitivity (ISO), with the targeted image. Furthermore, the color correction algorithms in various camera firmwares may also yield less accurate flat images, thus requiring the method to be applied with raw images for accurate results. Therefore, flat-fielding may not be a generic solution to remove PRNU noise and preclude SCI [9, 10, 12]. Another counter method to SCI can be realized by subtracting the PRNU fingerprint from a target image [12, 13] For a successful PRNU removal, the fingerprint should be multiplied with a specific factor, which makes the correlation between the camera fingerprint and the PRNU noise in the image near zero [12, 13].

#190242 - $15.00 USD Received 10 May 2013; revised 6 Oct 2013; accepted 28 Nov 2013; published 3 Jan 2014

One of the problems in this method is to estimate the correct multiplication factor. In addition, it is not clear whether near-zero correlation is achievable.

In this paper, we would like to answer the following question: “Can we impede the PRNU based source camera identification, without sacrificing the image quality for different camera brands or models?” To answer the question, we propose a new counter method against PRNU-based source camera identification that uses the noise-estimate of a target image and a PRNU fingerprint of the subjected camera. The proposed method does not particularly require physical access to the source device. With a set of images taken from a particular camera, it is possible to estimate the PRNU fingerprint and anonymize any image taken from the same camera. In this paper, when we use the term “anonymization” we refer to the PRNU-noise degradation process to prevent SCI.

The organization of the paper is as follows: In Section 2, we provide the notations and the preliminaries of PRNU noise and SCI. Section 3 introduces the theoretical background of the proposed counter method. The implementation of the counter method is described in Section 4. The experimental results are presented and discussed in Sections 5 and 6. Finally, Section 7 concludes the paper.

2. PRNU based source camera identification

Due to the nature of PRNU, each pixel in the imaging sensor produces slightly different reaction to the same level of light intensity. This imperfect behavior causes a temporal random noise pattern that can be considered an intrinsic fingerprint of a digital camera device. Let the PRNU pattern (fingerprint) of a digital camera X be F_x. Ignoring the gamma correction factor, the raw imaging output can be written as:

$$I_x = I_0 + (I_0 F_x + \Phi) \tag{1}$$

where I_0 is the actual optical view, and I_x is the digital output distorted with the sensor imperfections and noise. In this model, we omit the post-processing noise in the optical path due to color demosaicing, white balance, etc. In Eq. (1), Φ refers to other noise elements such as shot noise, read-out noise, dark current, and quantization distortion. The fingerprint F_x can be predicted by estimating the noise of a set of images using a wavelet-based denoising filter WDF [14]. The sensor noise estimate of a single image can be computed as:

$$N_x^{(i)} = I_x^{(i)} - \mathrm{WDF}(I_x^{(i)}) \tag{2}$$

where $N_x^{(i)}$ is the sensor noise estimate of image $I_x^{(i)}$. The fingerprint $F_x$in Eq. (1) can then be estimated with the maximum likelihood estimator as introduced in [11]:

$$\hat{F}_x = \frac{\sum_{i=1}^{M} N_x^{(i)} I_x^{(i)}}{\sum_{i=1}^{M} (I_x^{(i)})^2} \tag{3}$$

where M is the number of images used to estimate F_x. It is well known that the higher the M is, the better F_x can be estimated. However, this estimate may contain periodic signals and high spectral magnitudes that are specific to the camera brand or model class because of the color-filter-array demosaicing. To suppress these periodic traces in $\hat{F}_x$, the mean of the rows and columns of the fingerprint is set to zero [15], and Wiener filtering is applied in the frequency domain [16] after the maximum likelihood estimation. These post operations increases the uniqueness of the fingerprint estimate among the same camera brand or model class.

Similar to the identification of human fingerprints in crime scene investigations, source camera identification of a subjected image I requires a fingerprint database to measure the similarity

#190242 - $15.00 USD Received 10 May 2013; revised 6 Oct 2013; accepted 28 Nov 2013; published 3 Jan 2014

between the sensor noise estimate of I ($N = I - \mathrm{WDF}(I)$) and a fingerprint of a suspected camera. This similarity can be measured by normalized cross correlation between N and $\hat{F}_x$ as:

$$\rho(u,v;N,\hat{F}_x) = \frac{\sum_{k=1}^{K}\sum_{l=1}^{L}(N[k,l]-\overline{N})(\hat{F}_x[k+u,l+v]-\overline{\hat{F}_x})}{\|N-\overline{N}\|\|\hat{F}_x-\overline{\hat{F}_x}\|} \tag{4}$$

where $\|.\|$ is the L_2 norm. If the image I is not taken by camera X, the maximum of the correlation ratio (max(ρ)) is expected to be close to zero. If the image I is taken by camera X, then the correlation ratio should be significantly higher than zero. However, it is not possible to set a reliable detection threshold for all camera devices because of the different resolutions and sensor types. This issue has been solved using a peak-to-correlation-energy (PCE) ratio [15]. The PCE ratio is defined by:

$$\mathrm{PCE} = \frac{\rho_{\mathrm{peak}}^2}{\frac{1}{|s|-|\varepsilon|}\sum_{s\notin\varepsilon}\rho_s^2} \tag{5}$$

where, ρ is the normalized cross correlation between N and $\hat{F}_x$. ρ_{peak} is the supremum of ρ and s is the map to all entries of ρ. ε represents a small, centered region around ρ_{peak}, whereas $|s|-|\varepsilon|$ is the total number of entries outside ε. The size mismatch between N and $\hat{F}_x$ in Eq. (4), if occurs, can be compensated using zero padding to the lesser one [17]. Then, the PCE ratio is compared against a fixed threshold to decide whether the unknown image I is captured with camera X. Experimental results in [17] suggest that the decision threshold can be set to 50 or higher. For brevity, we denote the PCE as a function of I and $\hat{F}_x$, i.e., $\mathrm{PCE}(I,\hat{F}_x)$ throughout the paper. Thus, if $\mathrm{PCE}(I,\hat{F}_x) > 50$, then I is *matched with camera X*; otherwise, I is considered to be taken with another camera. Throughout the paper, these two cases will be referred to as the *matching case* and the *non-matching case*, respectively.

3. Theoretical model

In this section, we will introduce the theoretical background of our PRNU noise removal method. All operations are element-wise matrix operations. Let's consider the image model in Eq. (1) where F_xI_0 is the PRNU term and Φ_1 is the non-temporal, stationary sensor noise. For a successful PRNU-based image anonymization, the PRNU term in the output model should be zero. Let's denose the image I_x in spatial-domain with a 2D Wiener filter Ω [18]. Thus, the sensor noise can be estimated as: $N_x = I_x - \Omega(I_x)$. We assume that both PRNU (F_xI_0) and the non-temporal noise terms (Φ_1) are suppressed after applying image denosing. As a result, the noise residue N_x can be obtained as:

$$N_x = bF_xI_0 + \Phi_2 \tag{6}$$

where, $b < 1$ and $var(\Phi_2) < var(\Phi_1)$. To remove the PRNU term in N_x, let us multiply the noise residue by a constant factor ψ and subtract it from the image I_x as:

$$I_x^{'} = I_x - \psi N_x \tag{7}$$

Let us expand Eq. (7) and rewrite:

$$I_x^{'} = I_0 + (F_xI_0 + \Phi_1) - \psi(bF_xI_0 + \Phi_2) \tag{8}$$

After re-arranging the terms, we obtain:

$$I_x^{'} = I_0 + (1-\psi b)F_xI_0 + (\Phi_1 - \psi\Phi_2) \tag{9}$$

#190242 - $15.00 USD Received 10 May 2013; revised 6 Oct 2013; accepted 28 Nov 2013; published 3 Jan 2014

Now, we can find the ψ factor that makes the PRNU term zero in $I_x^{'}$ as:

$$\psi_0 = 1/b \tag{10}$$

Equations (9) and (10) show that there exists a positive ψ factor that makes the noise term of $I_x^{'}$ uncorrelated with the camera fingerprint estimate $\hat{F}_x$. $\psi \geqslant 1$ because b is smaller than 1. Although we choose to use 2D Wiener filter to remove the PRNU term, the proposed model can be extended to any denoising algorithm. Spatial-domain Wiener filter used in the anonymization is intentionally chosen to show that PRNU suppression can be achieved with different denosing filter than used in SCI [17].

The image quality degradation introduced by anonymization can be computed from ψ and Φ_2. While the PRNU term in Eq. (9) becomes zero with a carefully chosen ψ factor, the $(-\psi\Phi_2)$ term adds noise to the image and decreases the image quality. The PSNR of $I_x^{'}$ after anonymization can be estimated as follows:

$$PSNR(I_x^{'}, I_x) = 10log_{10}(255^2) - 10log_{10}(var(F_x I_0) + \psi^2 var(\Phi_2)) \tag{11}$$

The SNR of PRNU noise is approximately -50 dB or less [5]. Thus, ignoring the PRNU term, Eq. (11) can be simplified to:

$$PSNR(I_x^{'}, I_x) \approx 10log_{10}(255^2) - 10log_{10}(\psi^2 var(\Phi_2)) \tag{12}$$

Let us consider a case where $var(\Phi_2) = 0.5$ and $\psi = 3$. Then, the PSNR of the anonymized image becomes 41.60 dB. From Eq. (12), it is seen that the ψ and Φ_2 terms directly affect the PSNR. A lower variance of Φ_2 corresponds to a higher PSNR. This shows that PRNU-based image anonymization can be achieved without significantly degrading the image quality, depending on the performance of the denoising algorithm. In the following section, we will show how the ψ value is estimated using the PRNU fingerprint F_x and the peak-to-correlation-energy (PCE) ratio.

4. Image source anonymization

The main objective of image source anonymization is to remove the PRNU term in Eq. (1). As it is shown in the previous section, this objective can be realized by subtracting a sensor noise estimate, which is multiplied with a specific gain factor ψ, from a target image. It is expected that after source anonymization, the target image yields a PCE metric lower than the decision threshold. To achieve such low PCE value, we will introduce an iterative PRNU removal process using the PCE ratio to measure how well the ψ factor is estimated for the target image. We will use the term $I_x^{'}$ as an intermediate - not-yet-anonymized version of the target image I, whereas I_x^a is the ultimate anonymized image. To simplify the description of the anonymization process, let us define the PCE as a function of ψ factor for $I_x^{'}$ as:

$$f_{\text{PCE}}(\psi) = \text{PCE}(I_x^{'}(\psi), \hat{F}_x) \tag{13}$$

$I_x^{'}(\psi)$ is the output of Eq. 7. Our ultimate goal is to find the best value of ψ factor that makes $f_{\text{PCE}}(\psi)$ zero. For a generic PRNU removal method, it is notably hard to estimate ψ factor analytically. Thus, we will search for the value of ψ factor using $f_{\text{PCE}}(\psi)$ as an objective function. The exhaustive search can be formulated as:

$$\psi_o = \underset{\psi \in [1,\infty)}{\arg\min}(f_{\text{PCE}}(\psi)) \tag{14}$$

#190242 - $15.00 USD Received 10 May 2013; revised 6 Oct 2013; accepted 28 Nov 2013; published 3 Jan 2014

where ψ_o is the optimum factor of the PRNU noise estimate of image I_x. However, searching for the optimum ψ_o in Eq. (14) may not be viable. For the purpose of anonymization, a more viable approach is to impede the source camera identification by rendering a *matching case* into a *non-matching case* and finding this condition using a grid search. This process can be achieved by implementing the condition in Eq. (15).

$$f_{\mathrm{PCE}}(\psi_a) \leq \varepsilon_a \tag{15}$$

The decision threshold ε_a could be set to 50 or to a smaller metric such as the PCE metric of any known non-matching case (an image from camera Y), which is given by $\varepsilon_a \leq \mathrm{PCE}(I_y, \hat{F}_x)$. Then, the source identification method would not be able to decide whether I_x is originating from device X or device Y.

$$I_x^a = I_x - \psi_a(I_x - W(I_x)) \tag{16}$$

Therefore, instead of finding the value of optimum ψ_O, we could use a near-optimum solution ψ_a to create an anonymized image, I_x^a, as given in Eq. (16). After the anonymization, I_x^a cannot be associated with camera X any more because its source could be any other camera device. The condition in Eq. (15) can be used to compute the success rate of the anonymization (AR) for a given set of M anonymized images against any ε_a:

$$\mathrm{AR}(\varepsilon_a)= \tfrac{100}{M}\textstyle\sum_{i=1}^{M} \mathrm{S}(i;\varepsilon_a); \quad \mathrm{S}(i;\varepsilon_a) = \begin{cases} 1 \quad \text{if} \quad f_{\mathrm{PCE}}(\psi_a(i)) \leq \varepsilon_a; \quad \text{i=1,..,M} \\ 0 \qquad\qquad\qquad \text{otherwise} \end{cases} \tag{17}$$

where, $\psi_a(i)$ is the anonymization factor for i th image. If ε_a is chosen as the decision threshold (e.g., 50), then Eq. (17) gives the miss rate of source camera identification method for the anonymized image set, and could also be used against the source camera identification.

5. Experimental setup and results

In this section, we compare the performance of our proposed anonymization method with two other counter attacks: flat-fielding and image denoising. Since flat-fielding requires specially captured images such as dark field and flat frames we choose to use Dresden Image Database [19] providing dark and flat frames along with other images for a variety of digital cameras.

Table 1. The camera models used in the experiments from the Dresden Image Database.

Camera	Model	Native Resolution	Device Id. (matching case)	Other Id. (non-matching case)
Sony	DSC-H50	3456×2592	Id 0	Id 1
Nikon	D200	3872×2592	Id 1	Id 0
Panasonic	DMC-FZ50	3648×2736	Id 0	Id 2

The Dresden Image Database provides necessary information to distinguish cameras of the same model by device id. For example, if a user wishes to access two images taken by two different devices of one model, such as Nikon D200, the user is provided with a list of direct links to the images acquired using a specific device in a particular model class. From this database, 3 camera models were used in the experiment for comparing the performance of flat-fielding against our proposed anonymization method.

We downloaded the natural, dark and flat images taken by three camera models, which are listed in Table 1. The images were cropped to 1024 × 1024 pixels without inducing any quality loss to speed up the process of iterative anonymization. Here, the experiment will be explained for only one camera model because we have repeated the same process for the images from the other camera models. Images from device 1 were selected to simulate the matching case.

Table 2. Grid search statistics (num. of iteration and ψ_a) per camera.

Camera	Avg. Iter.	Avg. ψ_a	Std. ψ_a
Sony	68.2	2.93	0.26
Nikon	84.4	2.83	0.34
Panasonic	80.7	3.27	0.32

To estimate the image sensor noise N_x, the noise residues of three color channels of individual images were combined with rgb to gray conversion weights as it is introduced in [17]. Then, the PRNU fingerprint $\hat{F}_x$ was computed with Eq. (3) using the noise estimates of 50 images (training set) taken from device 1. Apart from the images used in the fingerprint $\hat{F}_x$ computation, 50 additional images of the same device (test set), not used in the training, were used to benchmark the PRNU removal techniques, which include our proposed anonymization method. To simulate the "non-matching" case, each camera fingerprint is paired with 50 images captured with another device of the same model, which will be denoted by "other device".

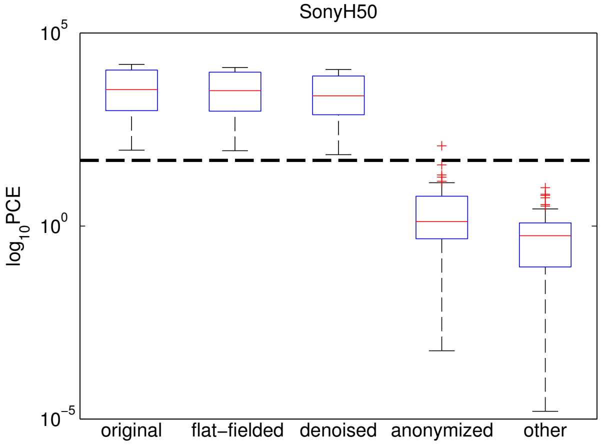

Fig. 1. Comparison of the PRNU removal methods for Sony H50. The proposed method "anonymized" 98% of the images taken with Sony H50. (Decision Threshold=50)

To create the flat-fielded versions of the test images, 25 dark and 25 light frames were first averaged for each selected device. Then, these average frames were used to perform flat-fielding on each of the test images. In addition to flat-fielding, we performed image denoising for the test images using 2D Wiener filter in the spatial domain. It is known that image denoising suppresses the PRNU noise to some extent but does not completely remove the PRNU term. This type of attack corresponds to the case where $\psi_a = 1$ in our proposed method.

#190242 - $15.00 USD Received 10 May 2013; revised 6 Oct 2013; accepted 28 Nov 2013; published 3 Jan 2014

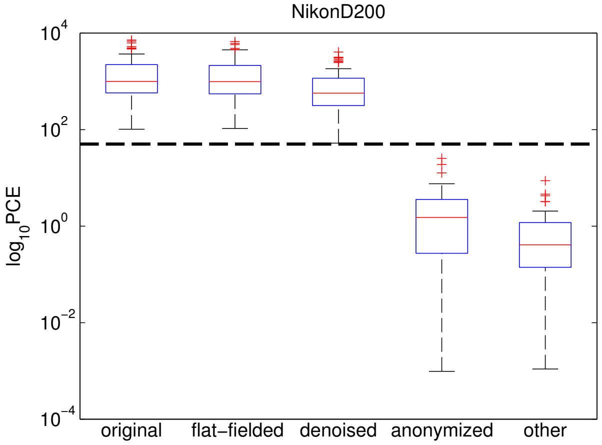

Fig. 2. Comparison of the PRNU removal methods for Nikon D200. The proposed method "anonymized" all of the images taken with Nikon D200. (Decision Threshold=50)

5.1. *Method parameters*

The proposed method was applied to estimate the ψ_a coefficient for each image, which reduces the PCE value below the decision threshold. Then, ψ_a was used in the anonymization process as shown in Eq. 16. To estimate the ψ_a value, a grid search algorithm was performed by focusing on the grid minimum iteratively until the absolute change for the PCE is lower than 0.1% and the corresponding PCE is below the decision threshold (50). This process was repeated for all images in the test set. To evaluate the convergence property of the proposed method, the average number of iterations and ψ_a values were measured for Sony, Nikon, and Panasonic cameras. These statistics are shown in Table 2. It is seen from the experimental data that the proposed method takes approximately 70-80 iterations, and the typical ψ_a values are approximately around 3.0.

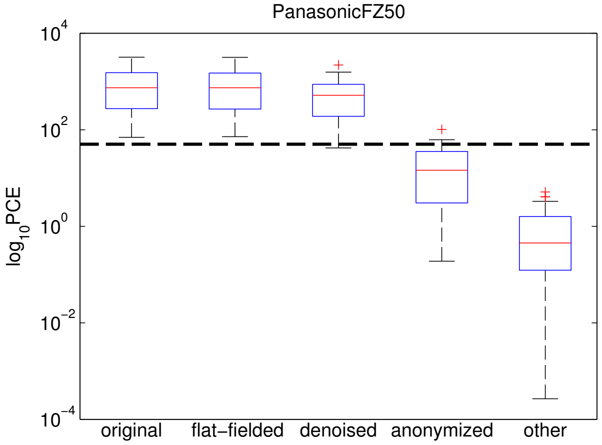

Fig. 3. Comparison of the PRNU removal methods for Panasonic FZ50. The proposed method "anonymized" 84.4% of the images taken with Panasonic FZ50. (Decision Threshold=50)

#190242 - $15.00 USD Received 10 May 2013; revised 6 Oct 2013; accepted 28 Nov 2013; published 3 Jan 2014

5.2. Benchmarking

For benchmark, we created 3 attacked versions of each test image: (i) flat-fielded version, (ii) denoised version, and (iii) anonymized version. For three counter methods, all attacked images were saved in JPEG format with 100% quality factor. Recall that we use the term “anonymized” solely for the images created with the proposed PRNU removal method. The performance of all counter methods were compared based on the PCE measurements of the attacked images. To obtain the PCE distributions for the matching (device 1) and non-matching (device 2) cases, the PCE values were computed for the images taken with device 1 and device 2. It should be noted that device 1 and device 2 have the same model and brand.

Table 3. Average PCE values (Decision threshold = **50**)

	Original	Flat-fielded	Denoised	Anonymized	Other Camera
Sony	**5621.94**	4843.05	3938.12	**6.29**	0.33
Nikon	**1852.25**	1747.09	1007.26	**2.88**	0.33
Panasonic	**978.33**	966.02	641.81	**22.50**	0.66
Average	**2880.90**	2572.30	1904.50	**10.14**	0.43

To test the performance of the proposed method, all test images were anonymized using the fingerprint estimate $\hat{F}_x$ obtained from the training set. To simulate a more realistic scenario and a fair evaluation, we allow adversary/forensic expert to have a different PRNU fingerprint estimate than used in the anonymization step. It is more realistic because the adversary may create different fingerprint estimates especially if he/she can have access to the source device or different image sets of the same camera. Therefore, for each camera, a second PRNU fingerprint was estimated using 50 new images not used in training and test steps. For brevity, this new fingerprint estimate will be denoted by F-50. In the benchmark, the PCE values of the attacked images for three counter methods were computed using the same F-50.

Table 4. Anonymization rates

	Flat-fielded	Denoised	Anonymized
Sony	0.0%	0.0%	**98.0%**
Nikon	0.0%	0.0%	**100.0%**
Panasonic	0.0%	2.2%	**84.4%**
Average	0.0%	0.68%	**94.4%**

Box plots of the computed PCE values for three counter methods (flat-fielding, denoising, and the proposed method) are depicted in Figs. 1, 2, and 3 for Sony, Nikon, and Panasonic cameras, respectively. The PCE distributions for the matching and non-matching cases are also provided in the figures for better comparison. The dashed lines in the figures represent the decision threshold of source camera identification ($\varepsilon_a = 50$). For clarity, the decision threshold is provided in the figure captions. For each box in the figures, the red line is the median of the PCE distribution. The box shape is limited with the 25th and 75th percentiles. The outliers are also shown with red plus signs. Each box is labeled according to its origin (device 1 as “original” and device 2 as “other”) and the applied PRNU removal method (denoising, flat-fielding, anonymization). The mean values of the PCE distributions are also provided in Table 3. The PCE box plots in Figs. 1-3 and mean values in Table 3 show that the proposed method

#190242 - $15.00 USD Received 10 May 2013; revised 6 Oct 2013; accepted 28 Nov 2013; published 3 Jan 2014

outperforms flat-fielding and denoising for three cameras. The experimental results also show that flat-fielding and denoising may not be effective to remove the PRNU fingerprint when they are applied to JPEG images. The success of the anonymization of three counter methods are given in Table 4. The average anonymization rate (AR) of the proposed method is 94.4%. For flat-fielding and denoising methods AR were measured 0.0% and 0.68%, respectively. Although the Wiener image denoising is a special case of our proposed method where $\psi = 1$, it does not suppress the PRNU noise.

Table 5. PSNR [dB] after anonymization

	Flat-fielded		Denoised		Anonymized	
	Avg.	Std.	Avg.	Std.	Avg.	Std.
Sony	49.76	0.51	44.24	4.15	**36.93**	**3.17**
Nikon	53.79	2.08	48.42	3.40	**41.68**	**3.22**
Panasonic	51.47	1.61	44.51	3.32	**36.68**	**3.01**
Average	47.88	1.39	45.76	3.63	**38.39**	**3.13**

One of the key parameters of our anonymization method is the image quality. Intuitively, the successive lossy operations applied to a target image can suppress the PRNU noise component. However, a significant quality loss after such operations cannot be tolerated. In the benchmark, we also compared the PSNR of the attacked images for three counter methods. The average PSNR of the anonymized images was measured as 38.39 dB with standard deviation 3.13 dB. The PSNR results for three counter methods are given in Table 5.

Table 6. Average correlation cofficients (F-50, Decision Threshold=**0.0100**)

	Original	Flatfielded	Denoised	Anonymized	Other Camera
Sony	**0.0717**	0.0652	0.0596	**0.0016**	0.0009
Nikon	**0.0407**	0.0395	0.0298	**0.0013**	0.0008
Panasonic	**0.0300**	0.0298	0.0242	**0.0039**	0.0008
Average	**0.0481**	0.0454	0.0383	**0.0022**	0.0008

Although, the objective function of the proposed method is set to minimize the PCE ratio to deceive SCI, it would be interesting to compare the counter methods in terms of correlation coefficient (ρ_{peak}). The motivation behind this comparison is that the adversary can use different correlation detectors to find a link between the test image and the subjected camera device. Therefore, we repeated the experiments measuring the correlation coefficient between the attacked images and the camera fingerprints (F-50) for all counter methods and the cameras. The correlation results are shown in Table 6. We can infer from the results that the use of the correlation coefficient does not bring any improvement to source camera identification on anonymized images.

5.3. *Further evaluation of the proposed method*

In the previous experiments, we have shown that the proposed method outperforms other counter methods in terms of the PCE ratio, and the correlation coefficient. Recall that in the benchmarks, adversary was allowed to acquire a unique fingerprint (F-50) with 50 new images not used in the training and the test steps. Recall also the camera fingerprint estimate $\hat{F}_x$ used in the objective function were generated using 50 images in the training set. This experimental

#190242 - $15.00 USD Received 10 May 2013; revised 6 Oct 2013; accepted 28 Nov 2013; published 3 Jan 2014

setting balances the quality of fingerprint estimates used in the anonymization step and final PCE computation by the adversary. On the other hand, the adversary may have more than 50 images taken from the same camera and obtain a better fingerprint than F-50. In that case, can the adversary identify the source of the anonymized image? To answer this question, we will allow the adversary to estimate a second fingerprint using 100 images taken by the same camera which are not used in the training and test step. We will denote this fingerprint by F-100 for brevity. Furthermore, to better evaluate the performance of the proposed method, we extend the camera database including smart phones (Nexus 4, Samsung S3 Mini), DSLR (Canon EOS 1100D), and compact cameras. A complete list of camera devices used in this Section is shown in Table 7.

Table 7. The camera models used in the experiment.

Camera	Model	Native Resolution
BenQ	AE100	4320×3240
Casio	QV-R200	4320×3240
LG	Nexus 4	3264×2448
Olympus	D-745	4288×3216
Samsung	S3 Mini	2560×1920
Canon	EOS1100D	4272×2848

All images were captured using “automatic mode” from various natural scenes, and saved using the native resolution with the highest image quality available for each camera model in JPEG format. Natural scenes were captured from various times of day, and various environments. We also avoid taking overexposed or underexposed images, and cropped all images to 1024×1024 pixels.

Table 8. The average number of iterations of grid search and the statistics of ψ_a per camera.

Camera	Avg. Iter.	Avg. ψ_a	Std. ψ_a
BenQ	69.8	3.74	0.85
Casio	70.4	3.78	0.46
LG	68.1	2.96	0.28
Olympus	69.8	3.34	0.17
Samsung	68.6	3.03	0.27
Canon	66.5	2.78	0.48

200 images were taken from each camera device. Randomly selected 50 images (training set) were used to estimate the PRNU fingerprint of the target camera for anonymization. The proposed method was then applied on 50 images (test set) not used in the training step by performing the grid search. The fingerprint estimates F-50 (from 50 images) and F-100 (from 100 images) were created from the rest of the 100 images. The average number of iterations of the grid search and the statistics of the estimated ψ_a factors are shown in Table 8. It is seen from the table that the average iteration for the new camera database were measured between 66-71. The average PSNR of the anonymized images for 6 cameras is 33.36 dB with 2.07 dB standard deviation. The PCE of the anonymized images and the corresponding anonymization rates are summarized in Table 9 and 10. The use of F-100 instead of F-50 increased the average

PCE around 45%. This is intuitive because F-100 was estimated from 100 images while F-50 was created using 50 images. On the other hand the average anonymization rate for 6 cameras decreased from 99.3% to 99.0 %. This result shows that the anonymized images cannot be identified even if the adversary uses a better camera fingerprint estimate e.g. F-100 for SCI. This is mostly because we do not use the camera fingerprint estimate $\hat{F}_x$ directly in the anonymization (see Eq. 16). Instead we use $\hat{F}_x$ to measure the detectability of the anonymized image by computing the PCE at each iteration.

Table 9. PCE Values and Anonymization Rates (F-50)

	Original	Anonymized	AR
BenQ	678.97	9.53	98%
Casio	357.67	6.93	98%
LG	2796.09	1.55	100%
Olympus	1608.62	1.23	100%
Samsung	1975.54	2.49	100%
Canon	102.17	3.39	100%
Average	**1253.17**	**4.18**	**99.3%**

Table 10. PCE Values and Anonymization Rates (F-100)

	Original	Anonymized	AR
BenQ	1076.53	15.13	96%
Casio	575.59	11.76	98%
LG	3969.39	2.11	100%
Olympus	2229.69	1.29	100%
Samsung	2875.23	2.78	100%
Canon	208.27	4.54	100%
Average	**1822.45**	**6.26**	**99.0%**

6. Discussion

The experimental results show that the proposed method outperforms flat-fielding and denoising methods for 9 cameras including DSLR, smart phone, and compact cameras. The average PSNR of the proposed anonymization method is around 34 dB. It is worth noting that it is possible to set a second threshold for a desired PSNR level in the anonymization process.

It is intuitive that better fingerprint estimate may lead to better identification. Keeping this in mind, the user can increase the strength of his/her privacy utilizing higher number of images during the fingerprint estimation phase. Nevertheless, it is shown in the further evaluation section that the anonymized images cannot be identified successfully even if the adversary has similar (F-50) or "better" quality fingerprint estimates (F-100) compared to the user's one. However, the analyst in a real-world setting like a court case can try much higher number of images (N>100) to identify the source camera. Therefore, we conducted an additional experiment on anonymized images for N=250, 350, 450, and 550 with Nexus 4. In none of these cases, were the source of the anonymized images identified. The corresponding average PCE ratios were measured as: 2.9, 3.3, 3.6, and 4.1, respectively. It is seen from the results that all of

#190242 - $15.00 USD Received 10 May 2013; revised 6 Oct 2013; accepted 28 Nov 2013; published 3 Jan 2014

the average PCE values are much lower than the decision threshold 50. This additional analysis also supports the robustness of the proposed method to high quality fingerprint attacks

7. Conclusion

In this paper, we introduce a novel image source anonymization method against PRNU-based source camera identification. Using theoretical and experimental analysis, it is shown that the image source anonymization is feasible for various digital camera sensors. The proposed method does not require any physical access to the source camera device. Instead, a set of images taken from the camera is enough to provide an initial fingerprint to impede the camera identification. The experimental results show that the proposed counter method does not sacrifice the image quality while degrading the PRNU noise. Performed benchmark results indicate that on all of the cameras used in the experiments, the proposed anonymization method is superior to flat-fielding and image denoising. Furthermore, the investigations show that the anonymity of the source camera is kept confidential even if an adversary uses a better-estimated fingerprint to identify the source camera. Performed experiments on 9 cameras including DSLR, compact, and smart phones indicate that illegal individual tracking using PRNU fingerprints can be prevented by the proposed anonymization method. Moreover, we believe that the presented results and issues addressed in this work will help developing better source-camera identification schemes.

Acknowledgments

This work was supported by The Scientific and Technological Research Council of Turkey (TÜBİTAK) under Project 113E092.

#190242 - $15.00 USD Received 10 May 2013; revised 6 Oct 2013; accepted 28 Nov 2013; published 3 Jan 2014