Empirical Evaluation of PRNU Fingerprint Variation for Mismatched Imaging Pipelines

Sharad Joshi, Pawel Korus, Member, IEEE, Nitin Khanna, Member, IEEE, Nasir Memon, Fellow, IEEE

Abstract—We assess the variability of PRNU-based camera fingerprints with mismatched imaging pipelines (e.g., different camera ISP or digital darkroom software). We show that camera fingerprints exhibit non-negligible variations in this setup, which may lead to unexpected degradation of detection statistics in real-world use-cases. We tested 13 different pipelines, including standard digital darkroom software and recent neural-networks. We observed that correlation between fingerprints from mismatched pipelines drops on average to 0.38 and the PCE detection statistic drops by over 40%. The degradation in error rates is the strongest for small patches commonly used in photo manipulation detection, and when neural networks are used for photo development. At a fixed 0.5% FPR setting, the TPR drops by 17 ppt (percentage points) for 128 px and 256 px patches.

Index Terms—image forensics, photo-response non-uniformity, PRNU, camera fingerprint, sensor pattern noise

I. INTRODUCTION

Camera fingerprints based on photo-response non-uniformity (PRNU) of the imaging sensor are one of the most reliable tools in photo forensics [1]–[3]. They have been studied in the literature for over a decade [4]–[7] and are commonly used in two main applications: (1) source attribution - which links photographs to a specific instance of a camera; and (2) photo manipulation detection - which involves a local analysis of the sensor fingerprint to identify areas of mismatch [8].

The success of PRNU fingerprints stems from their stability and robustness to various post-processing that happens in real-world applications (e.g., scaling, or lossy compression). Some of this post-processing, in particular the impact of JPEG compression or denoising, have been extensively studied [9]–[12]. However, many others remain unexplored. This may lead to inaccurate detection and under-estimated error rates.

In this work, we empirically assess the sensitivity of PRNU fingerprints to mismatched imaging pipelines. This scenario arises when test images are processed differently (e.g., using 3rd-party darkroom software like LibRAW or Lightroom) than the images used for fingerprint estimation. We believe this scenario will become increasingly more common with the progress of machine learning and the increasing adoption of deep neural networks in various stages of the imaging pipeline (e.g., demosaicing [13], denoising [14], or tone-mapping [15]) or even instead of it [16]. Moreover, modern darkrooms, e.g., Luminar, extensively advertise ML-based solutions in their image processing and enhancement routines, and such a trend is likely to increase.

In this work, we take the first step in this direction and assess the impact of imaging pipeline (ISP) variation on PRNU fingerprint analysis. We used 13 software pipelines representing popular digital darkrooms and 3 neural network architectures. We consider a scenario where each pipeline uses default settings with minimal post-processing, and neural-network is trained to reproduce images visually equivalent to a standard camera pipeline [17], [18] (see Figure 1 for example image patches and residuals for Nikon D7000).

The main observations from our work are as follows:

- Correlation between camera fingerprints obtained from exactly the same images processed by different pipelines drops on average by 62 %.
- Degradation in detection statistics is the strongest for smaller image patches (128 or 256 px windows), which will be particularly detrimental to manipulation detection.
- For large patches (1024 px), standard ISPs reveal little variation in detection statistics, but the effect remains strong for neural ISPs.
- For 128 px windows commonly used in manipulation detection, we observed an average deterioration of 41% in median PCE and of 17% in TPR at 0.5% FPR.
- Imaging pipelines based on neural networks tend to distort the camera fingerprints more - TPR dropped by 20% compared to 14% for standard pipelines.
- Even for traditional pipelines, we observed unexpected...
II. BACKGROUND AND RELATED WORK

A PRNU fingerprint of a camera characterizes the consistent bias of individual pixels in its imaging sensor [8]. The fingerprint is estimated from multiple images by carefully averaging bias of individual pixels in its imaging sensor [8].

Several enhancement techniques have been proposed to reduce contamination of PRNU by the image content. Kang et al. [19] proposed a method that estimates PRNU only from the phase components of noise residuals. Lin and Li [20] proposed smoothing the Fourier spectrum of the estimated PRNU using local averaging. These two methods were based on the hypothesis that the sensor pattern noise is white noise (i.e., it has a flat frequency spectrum). On the other hand, Li [21] assume that PRNU is a weak signal, while scene details are likely to be much stronger. They proposed several models that produce weighted versions of wavelet coefficients of a noise residual. An inverse wavelet transform on the weighted coefficients provides the enhanced noise residuals.

Various denoising filters have also been evaluated in the literature. These include a context-adaptive interpolator (CAI) [5], 2-pixel approach [22], adaptive spatial (AS) filtering [23], content adaptive guided image (CAGI) filtering [24], and block-matching and 3D (BM3D) algorithm [12].

A recent method proposed usage of a convolutional neural network (CNN) to improve the estimation of noise residual extracted by traditional means [26].

The large size and random nature of sensor fingerprints combined with a computationally expensive fingerprint matching create difficulty in managing large databases. Many methods have proposed alternative representations [27]-[30] of the PRNU fingerprint. A recent method attempts to use a fused CNN-based approach that combines camera model features and PRNU to improve small-scale tampering detection [31].

III. EXPERIMENTAL RESULTS AND DISCUSSION

To assess the impact of the image processing pipeline (ISP) on PRNU fingerprints, we construct a new dataset derived from raw images from 4 cameras and 13 different ISPs. We then follow the standard fingerprint estimation procedure [8] and assess the impact on: (1) the correlation between different fingerprint estimates; (2) the distributions of PCE scores obtained with mismatched estimation and test ISPs; (3) the receiver operation statistics and relevant detection metrics (AUC and TPR at FPR=0.5%).

A. Dataset and FingerPrint Estimation

We collected raw images for 4 cameras: Nikon D7000 (N7k), Nikon D90 (N90), Canon EOS 40D (C4D) and Canon EOS 5D (C5D). The Nikon and Canon images were taken from the Raise [33] and MIT-5k [34] datasets, respectively. We collected 120 full-resolution images, out of which 60 were used for PRNU estimation and 60 for subsequent attribution experiments.

We then processed all images using 13 different ISPs. We included popular digital darkroom software (both commercial and open-source) as well as recent neural-network-based ISPs. We included 10 darkrooms: RawTherapee 5.6 (RT) [37], Corel AfterShot Pro 3 (AT) [38], LightZone 4.1.9 (LZ) [39], DCRaw 9.27 (DR) [40], LibRaw 0.17.2 (LR) [41], Affinity Photo 1.6.6 (AF) [42], Luminar 3 (LR) [43], DXO PhotoLab 2 (DX) [44], Capture One 12 (C1) [45], and Adobe Lightroom 5 (LT) [46]. The neural ISPs included a popular model for joint demosaicing and denoising (DNet) [47], the UNet (UN) [48] model, and a simple network that mimics a standard ISP (Inet) [17]. All NN models were trained to reproduce the result of a standard imaging pipeline.

To assess the most optimistic scenario, we made sure to: (1) select the same images for PRNU estimation; (2) use an automatic mode with default settings and no scaling in each ISP; (3) work on uncompressed bitmap images. In a real-world setting, these conditions are unlikely to be met.

B. Analysis of Camera Fingerprint Similarity

To compare the PRNU fingerprints, we compute the normalized correlation coefficients between all possible pairs of estimation pipelines. If necessary, we align the fingerprints by shifting one of them to the location indicated by a peak in cross-correlation (needed sometimes due to minor differences

\[
I_1 = \sum_{i=1}^{N} R_i I_i
\]

At test time, the corresponding residual of a test image is correlated with the camera fingerprint - either globally (for attribution) or locally (for manipulation detection).

Despite addressing a sensor-level phenomenon, the analysis is typically performed in the RGB color space. As a result, the fingerprint is affected by various steps in the camera’s ISP, e.g., demosaicing, denoising, or tone-mapping. Some researchers have proposed exploiting knowledge of specific camera components to estimate a better fingerprint, e.g., given the color filter array, one can consider only the measured color channels [32]. Alternatively, a more recent line of work explores inversion of the ISP and estimation at the raw level [33], [34].
in how ISPs crop the raw images; see Table IV in the supplemental file).

We collected the obtained results in Table I (for Nikon D7000; the results are similar for other cameras). It can be observed that despite a conservative evaluation setting, the estimated fingerprints tend to differ considerably. The average correlation for all cross-ISP pairs is only 0.38. Some of the ISPs, e.g., DCRaw, LibRaw, and Affinity, tend to correlate better, which may indicate some common components in their functionality (e.g., use of the DCRaw routines in LibRaw [49]).

Interestingly, fingerprints from CaptureOne and RawTherapee do not correlate with any other ISPs for neither of Nikon cameras (marked in red). Based on visual comparison of image patches, it would appear both programs apply some slight geometric transformation while cropping full-frame raw images, which de-synchronizes the fingerprints. We emphasize that this happens despite explicit instructions to leave image size intact and that the problem does not occur for Canon cameras (this may be related to the format of raw images in our dataset - NEF for Nikon and DNG for Canon cameras).

C. Impact on PCE Detection Statistics

To assess the impact on fingerprint detection statistics, we measured peak-to-correlation-energy (PCE) for all possible pairs of ISPs (using different pipelines for PRNU estimation and test images). To increase the number of samples, we extract all possible non-overlapping patches from full-resolution images. This yields from 600 to 55,000 patches for patch sizes ranging from 1024 px to 128 px.

In general, using the same imaging pipeline leads to the best matching performance (see median PCE scores for Nikon D7000 in Table II). In cross-ISP matching, the PCE deteriorates on average by 61, 56, 50, and 41% for patches of 1024, 512, 256, and 128 px, respectively. Full distributions of PCE scores for 512 px patches from all cameras and selected ISPs are shown in Figure 2 (Note that the PCE distributions are shown in logarithmic scale.) Configurations with the same ISP are shown with solid lines, whereas mismatched digital darkrooms and neural ISPs are shown with dashed and dotted lines, respectively.

Overall, we see a similar trend as in fingerprint correlation (Section III-B). Apart from obvious matching failures for CaptureOne and RawTherapee for Nikon cameras, we observe various degrees of PCE deterioration. The most significant and consistent deterioration occurs for neural ISPs. In some cases, e.g., for Canon cameras in our experiments, they seemed to have incompatible fingerprints.

D. Impact on ROC Curves and Error Rates

To assess the impact of ISP mismatch on effective error rates, we generate full receiver operating characteristics (ROC curves). An example set of ROC curves for all patch sizes, all cameras, and a single PRNU estimation ISP (LibRaw) is shown in Figure 3. Analogously to previous experiments, we can see a significant variation of matching performance with the strongest deterioration for small patch sizes and for neural ISPs.

To quantitatively summarize the degradation, we show true positive rates corresponding to a fixed 0.5% false-positive rate (Table III). We focus on 128 and 256 px patches due to the much larger number of available samples. For the illustrated LibRaw and Affinity Photo ISPs, the average deterioration in TPR was 17 percentage points (13 ppt for well-synchronized standard darkroom software and 20 ppt for neural ISPs).
We experimented with 13 different pipelines representing various digital darkrooms and neural networks. The degradation was the strongest for smaller patches which are commonly used in photo manipulation detection. Specifically, for false positive rate fixed at 0.5%, an average degradation of 17 percentage points was observed for patches of size 128 px (sample size 55,000) and 256 px (sample size 13,000).

To illustrate qualitative impact on tampering localization, we show an example forgery and the corresponding authentication results in Figure 4. The depicted example is a synthetic forgery created by pasting a foreign patch of 1024 px inside a full resolution image taken with Nikon 7000 and processed by each pipeline. We show both local PCE responses and tampering probabilities obtained from p-values of PCE statistics [50]. It can be clearly observed that even for conventional darkroom software, the results exhibit strong variation.

We expect that the presence of diverse imaging pipelines, and increasing adoption of computational methods inside of the cameras, will have more significant impact on PRNU analysis in the future. Negative impact of this variation is likely to be most pronounced not only in tampering localization, but also in reduced forms of PRNU used in massive-scale attribution [27–30]. Further research will be needed both to assess the problem and to design effective solution for matching against existing camera fingerprints. Some early work in this direction includes PRNU analysis in high-dynamic-range (HDR) photographs [51].
REFERENCES

[1] M. A. Arbib, Digital Image Forensics: There is More to a Picture than Meets the Eye. USA, NY, New York: Springer, 2013.

[2] A. Piva, "An overview on image forensics," ISRN Signal Processing, vol. 2013, pp. 1–22, Oct. 2012.

[3] P. Korus, "Digital image integrity—a survey of protection and verification techniques," Digital Signal Processing, vol. 71, pp. 1–26, 2017.

[4] J. Lukas, J. Fridrich, and M. Goljan, "Digital camera identification from sensor pattern noise," IEEE Transactions on Information Forensics and Security, vol. 1, no. 2, pp. 205–214, 2006.

[5] X. Kang, J. Chen, K. Lin, and P. Anjie, "A context-adaptive snp predictor for trustworthy source camera identification," EURASIP Journal on Image and Video Processing, vol. 2014, no. 1, p. 19, 2014.

[6] L.-B. Zhang, F. Peng, and M. Long, "Identifying source camera using guided image estimation and block weighted average," Journal of Visual Communication and Image Representation, vol. 48, pp. 471–479, 2017.

[7] M. Al-Ani and F. Khelifi, "On the spn estimation in image forensics: A systematic empirical evaluation," IEEE Transactions on Information Forensics and Security, vol. 12, no. 5, pp. 1067–1081, 2017.

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

[9] E. Quiring and M. Kirchner, "Fragile sensor fingerprint camera identification," in 2015 IEEE International Workshop on Information Forensics and Security (WIFS). IEEE, 2015, pp. 1–6.

[10] E. Quiring, M. Kirchner, and K. Rieck, "On the security and applicability of fragile camera fingerprints," in European Symposium on Research in Computer Security. Springer, 2019, pp. 450–470.

[11] A. Cortiana, V. Conotter, G. Boato, and F. G. De Natale, "Performance comparison of denoising filters for source camera identification," in Media Watermarking, Security, and Forensics III, vol. 7880. International Society for Optics and Photonics, 2011, p. 788007.

[12] G. Cierchio, S. Parrilli, G. Poggi, C. Sansone, and L. Verdoliva, "On the influence of denoising in prnu based forgery detection," in Proceedings of the 2nd ACM workshop on Multimedia in forensics, security and intelligence, 2010, pp. 117–122.

[13] M. Gharbi, G. Chaurasia, S. Paris, and F. Durand, "Deep joint demosaicking and denoising," ACM Transactions on Graphics, vol. 35, no. 6, pp. 1–12, nov 2016.

[14] J. Lehtinen, J. Munkberg, J. Hasselgren, S. Laine, T. Karras, M. Aittala, and T. Aila, "Noise2noise: Learning image restoration without clean data," arXiv preprint arXiv:1803.04189, 2018.

[15] G. Eilertsen, J. Kronander, G. Denes, R. Mantiuk, and J. Unger, "HDR mapping and global tonal adjustment with a database of input/output image pairs," in CVPR 2011. IEEE, 2011, pp. 97–104.

[16] M. Al-Ani, F. Khelifi, A. Lawgaly, and A. Bouridane, "A novel image filtering approach for sensor fingerprint estimation in source camera identification," in 2015 12th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS). IEEE, 2015, pp. 1–5.

[17] A. J. Cooper, "Improved photo response non-uniformity (prnu) based source camera identification," Forensic science international, vol. 226, no. 1, pp. 132–141, 2013.

[18] H. Zeng and X. Kang, "Fast source camera identification using content adaptive guided image filter," Journal of forensic sciences, vol. 61, no. 2, pp. 520–526, 2016.

[19] K. Dabov, A. Foi, V. Katkovnik, and V. Egiazarian, “Image denoising by sparse 3-d transform-domain collaborative filtering,” IEEE Transactions on image processing, vol. 16, no. 8, pp. 2080–2095, 2007.

[20] E. Kirchner and C. Johnson, “Spn-cnn: Boosting sensor-based source camera attribution with deep learning,” arXiv preprint arXiv:2002.02927, 2020.

[21] S. Bayram, H. T. Sencar, and N. Memon, “Sensor fingerprint identification through composite fingerprints and group testing,” IEEE Transactions on information forensics and security, vol. 10, no. 3, pp. 597–612, 2014.

[22] D. Valsesia, G. Coluccia, T. Bianchi, and E. Magli, "Compressed fingerprint matching and camera identification via random projections," IEEE Transactions on Information Forensics and Security, vol. 10, no. 7, pp. 1472–1485, 2015.

[23] L. Bondi, P. Bestagini, F. Perez-Gonzalez, and S. Tubaro, "Improving prnu compression through preprocessing, quantization, and coding," IEEE Transactions on Information Forensics and Security, vol. 14, no. 3, pp. 608–620, 2018.

[24] S. Taspinar, H. T. Sencar, S. Bayram, and N. Memon, "Fast camera fingerprint matching in very large databases," in 2017 IEEE International Conference on Image Processing (ICIP). IEEE, 2017, pp. 4088–4092.

[25] A. G. Poyraz, A. E. Drik, A. Kara吐c整体, and N. Memon, “Fusion of camera model and source device specific forensic methods for improved tamper detection,” arXiv preprint arXiv:2002.10123, 2020.

[26] C.-T. Li and Y. Li, "Color-decoupled photo response non-uniformity for digital image forensics," IEEE Transactions on Circuits and Systems for Video Technology, vol. 22, no. 2, pp. 260–271, 2011.

[27] A. Mehrish, A. V. Subramanyam, and S. Emmanuel, "Sensor pattern noise estimation using probabilistically estimated raw values," IEEE Signal Processing Letters, vol. 23, no. 3, pp. 693–697, 2016.

[28] ——, “Robust prnu estimation from probabilistic raw measurements,” Signal Processing: Image Communication, vol. 66, pp. 30–41, 2018.

[29] D.-T. Dang-Nguyen, C. Pasquini, V. Conotter, and G. Boato, “Raise: A raw images dataset for digital image forensics,” in Proceedings of the 6th ACM Multimedia Systems Conference. ACM, 2015, pp. 219–224.

[30] V. Bychkovsky, S. Paris, E. Chan, and F. Durand, “Learning photographic global tonal adjustment with a database of input/output image pairs,” in CVPR 2011. IEEE, 2011, pp. 97–104.

[31] Rawtherapee. Accessed: May, 2019. [Online]. Available: https://rawtherapee.com

[32] Affershoto pro 3 raw photo editor. Accessed: May, 2019. [Online]. Available: https://www.affershopto.com/en/

[33] Lightzone. Accessed: May, 2019. [Online]. Available: https://lightzoneproject.org

[34] Dcraw: Decoding raw digital photos in linux. Accessed: May, 2019. [Online]. Available: https://www.dechifro.org/dcraw

[35] Libraw. Accessed: May, 2019. [Online]. Available: https://www.libraw.org

[36] Infinity photo. Accessed: May, 2019. [Online]. Available: https://infinity.serif.com/en-us/

[37] Skyllum luminar. Accessed: May, 2019. [Online]. Available: https://skyllum.com/luminar

[38] Dxomark. Accessed: May, 2019. [Online]. Available: https://www.dxomark.com/

[39] Capture one. Accessed: May, 2019. [Online]. Available: https://www.captureone.com/en

[40] Lightroom. Accessed: May, 2019. [Online]. Available: https://lightroom.adobe.com

[41] M. Gharbi, G. Chaurasia, S. Paris, and F. Durand, "Deep joint demosaicking and denoising," ACM Transactions on Graphics (TOG), vol. 35, no. 6, pp. 1–12, 2016.

[42] O. Ronneberger, P. Fischer, and T. Brox, "U-net: Convolutional networks for biomedical image segmentation," in International Conference on Medical image computing and computer-assisted intervention. Springer, 2015, pp. 234–241.

[43] Dcraw. Accessed: Jan., 2020. [Online]. Available: https://en.wikipedia.org/wiki/Dcraw

[44] M. Goljan, "Digital camera identification from images—estimating false acceptance probability," in International workshop on digital watermarking. Springer, 2008, pp. 454–468.

[45] M. Darvi, M. Goljan, and D. Harvish, "Camera identification from hdr images," in Proceedings of the ACM Workshop on Information Hiding and Multimedia Security, 2019, pp. 69–76.
## SUPPLEMENTARY MATERIAL

### TABLE III
**DIMENSIONS OF PROCESSED IMAGES OBTAINED USING ALL PIPELINES IN OUR DATASET**

| Camera | Unprocessed Image Dimensions | Camera | Processed Image Dimensions |
|-------|------------------------------|-------|----------------------------|
| Nikon | 6880 x 4593 | Canon EOS 5D | 2920 x 1884 |
| Canon EOS 5D | 5600 x 3733 | Nikon | 6880 x 4593 |
| Nikon | 6880 x 4593 | Canon EOS 5D | 2920 x 1884 |
| Canon EOS 5D | 5600 x 3733 | Nikon | 6880 x 4593 |

### TABLE IV
**CORRELATION COEFFICIENTS OBTAINED BY MATCHING CROSS-PIPELINE PRNUs USING IMAGES ACQUIRED BY NIKON D90, CANON EOS 40D, AND CANON EOS 5D**

| Camera | Unprocessed Image Dimensions | Camera | Processed Image Dimensions |
|-------|------------------------------|-------|----------------------------|
| Nikon | 6880 x 4593 | Canon EOS 5D | 2920 x 1884 |
| Canon EOS 5D | 5600 x 3733 | Nikon | 6880 x 4593 |
| Nikon | 6880 x 4593 | Canon EOS 5D | 2920 x 1884 |
| Canon EOS 5D | 5600 x 3733 | Nikon | 6880 x 4593 |

### TABLE V
**MEDIAN PCE VALUES FOR CROSS-PIPELINE ATTRIBUTION OF NON-OVERLAPPING PATCHES FROM CANON EOS 40D**

| Camera | Unprocessed Image Dimensions | Camera | Processed Image Dimensions |
|-------|------------------------------|-------|----------------------------|
| Nikon | 6880 x 4593 | Canon EOS 5D | 2920 x 1884 |
| Canon EOS 5D | 5600 x 3733 | Nikon | 6880 x 4593 |
| Nikon | 6880 x 4593 | Canon EOS 5D | 2920 x 1884 |
| Canon EOS 5D | 5600 x 3733 | Nikon | 6880 x 4593 |

---

Note: The tables and discussions of supplementary material cover the detailed analysis of camera pipeline performance, specifically focusing on Nikon D90, Canon EOS 40D, and Canon EOS 5D. The tables provide dimensions of processed images, correlation coefficients obtained by matching cross-pipeline PRNUs, and median PCE values for cross-pipeline attribution of non-overlapping patches from Canon EOS 40D.