

Shedding Light on some Leaks in PRNU-based Source Attribution

Andrea Montibeller
andrea.montibeller@unitn.it
University of Trento
Italy

Fernando Pérez-González
fperez@gts.uvigo.es
Universidad de Vigo
Spain

Roy Alia Asiku
royalia.asiku@unitn.it
University of Trento
Italy

Giulia Boato
giulia.boato@unitn.it
University of Trento
Italy

ABSTRACT

Forensic image source attribution aims at deciding whether a query image was taken by a specific camera. While various algorithms leveraging forensic traces have been proposed, the most effective techniques rely on Photo Response Non-Uniformity (PRNU), a pattern introduced by camera sensors during the image acquisition process. In recent years, advances in image acquisition and processing technologies in modern devices have been found to impact the performance of PRNU, seemingly challenging its uniqueness. In this paper, we build upon recent discoveries of leaks in PRNU uniqueness, focusing on the dataset recently published by Iuliani et al. which has been instrumental in identifying numerous issues related to source attribution. Specifically, we analyze the effects in terms of false positive of visible watermarks applied to Xiaomi Mi 9 images, and reveal artifacts in the magnitude of the Discrete Fourier Transform of Samsung A50 images, indicative of the absence of non-unique artifacts. Furthermore, we demonstrate how several false positive cases are attributed to mislabeled devices. Finally, we show that a number of false negatives from the dataset are traceable to radially corrected images, and to images processed by third-party software that had not been previously noticed.

CCS CONCEPTS

• Computing methodologies → Image and video acquisition; Image processing.

KEYWORDS

Source Attribution, PRNU, Multimedia Forensics, Non-Unique Artifacts

ACM Reference Format:

Andrea Montibeller, Roy Alia Asiku, Fernando Pérez-González, and Giulia Boato. 2024. Shedding Light on some Leaks in PRNU-based Source Attribution. In *Proceedings of the 2024 ACM Workshop on Information Hiding and Multimedia Security (IH&MMSec '24)*, June 24–26, 2024, Baiona, Spain. ACM, New York, NY, USA, 6 pages. <https://doi.org/10.1145/3658664.3659654>



This work is licensed under a Creative Commons Attribution International 4.0 License.

IH&MMSec '24, June 24–26, 2024, Baiona, Spain
© 2024 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-0637-0/24/06.
<https://doi.org/10.1145/3658664.3659654>

1 INTRODUCTION

Forensic image source attribution [1] aims at deciding whether a query image has been taken by a specific device, and is customarily used in police investigations and presented as evidence in court proceedings [2]. To attribute a multimedia file to its device, a number of algorithms exploiting forensic traces in the camera acquisition process [3, 4], radial correction artifacts [5], dark currents [6], or camera residuals [2] have been proposed. Nevertheless, the most effective techniques for source attribution exploit the so-called Photo Response Non-Uniformity (PRNU) [1], consisting of sensitivity variations across the pixels of an image sensor due to unique imperfections or non-uniformities in the sensor's manufacturing process. The PRNU of a certain device can be estimated (using maximum likelihood principles) from a collection of images taken with it [2]. Then, the PRNU can be used as fingerprint to decide whether a test image can be attributed to a certain camera by measuring their Peak to Correlation Energy (PCE) [7].

In recent years, PRNU-aided source attribution algorithms have encountered challenges due to continuous advancements in image acquisition and processing technologies. Initially, issues affecting PRNU were related to both in-camera and out-camera processing, such as digital zoom [8], radial correction [9, 10], gamma correction [11], high dynamic range correction [12], and electronic image stabilization [13–15]. These issues necessitated reversing in-camera operations to restore the PRNU's consistency. However, recently, sources of misattribution have been ascribed to a loss of uniqueness in PRNU in modern devices, stemming from new camera acquisition processes also aided by artificial intelligence (AI) [16].

Building upon the latest discoveries regarding sources of leaks in PRNU uniqueness, our work will expand them by focusing on some of the most problematic devices featured in the dataset for source attribution published by Iuliani et al. [16], which we will refer to by the name of the creators' research group: FORLAB. It is important to emphasize that our study exclusively focuses on the FORLAB Dataset [16], which has received a lot of attention due to its richness in data and its effectiveness in pinpointing numerous issues related to source attribution. Specifically, in this paper, we will study the effects of some artifacts produced by modern devices in terms of False Positives (FP), and present some preliminary results suggesting a negative correlation between artifacts in the magnitude of the Discrete Fourier Transform (DFT) and the presence of Non-Unique Artifacts (NUA) in images of the Samsung A50. Finally, we will present evidence showing the presence in the FORLAB Dataset of

misabeled devices and a large number of images processed with third-party software, some of which were radially corrected.

The remainder of this paper is organized as follows: in Sect.2, we present the state of the art. In Sect.3, we examine the effects of visible watermarking applied by the Xiaomi Mi 9 in terms of FPs, and those of artifacts found in some Samsung A50 images' DFT magnitudes. We will also substantiate the existence of mislabeled devices. In Sect.4, we provide evidence, up to now only partially noticed, of more than 1500 images processed by third-party software in the FORLAB Dataset, as well as radially corrected images affecting the results of [16] in terms of False Negatives (FN). Our conclusions and future work are presented in Sect.5.

2 RELATED WORKS

Image source attribution has been addressed in various ways. Source attribution algorithms typically leverage forensic traces introduced during camera acquisition [3] or image correction processes [5]. However, the most effective techniques for source attribution are those that extract and correlate residuals [2, 17] related to the camera sensor, being the PRNU [2] the most popular. Given a set of L images taken with a camera device, it is possible to estimate a residual from the l th image using:

$$\mathbf{W}_l = \mathbf{I}_l - F(\mathbf{I}_l) \quad (1)$$

where $F(\cdot)$ represents Mihcak's wavelet-based denoiser [18]. Then, $\{\mathbf{W}_l\}_{l=1}^L$ can be used to estimate the so-called camera fingerprint $\mathbf{K}$ as:

$$\mathbf{K} = \frac{\sum_{l=1}^L \mathbf{W}_l \cdot \mathbf{I}_l}{\sum_{l=1}^L \mathbf{I}_l \cdot \mathbf{I}_l} \quad (2)$$

where all products and divisions are pixelwise. The camera fingerprint $\mathbf{K}$, once estimated, can be tested against the residual of the query image $\mathbf{I}$, i.e. $\mathbf{W} = \mathbf{I} - F(\mathbf{I})$, in a binary hypothesis test aimed at verifying if $\mathbf{W}$ contains $\mathbf{K}$. We will denote the match hypothesis, where $\mathbf{W}$ contains $\mathbf{K}$, as H_1 , and the mismatch one as H_0 . To conduct this binary hypothesis test, the Peak-of-Correlation-Energy (PCE) between $\mathbf{W}$ and $\mathbf{K}$ is measured and compared against a threshold τ . The PCE is defined as follows:

$$\text{PCE}(\mathbf{K}, \mathbf{W}) = \frac{\text{sgn}(\rho(\mathbf{K}, \mathbf{W})_{\delta_{\text{peak}}}) \cdot \rho^2(\mathbf{K}, \mathbf{W})_{\delta_{\text{peak}}}}{\frac{1}{MN - |\mathcal{D}|} \sum_{\delta \in \mathcal{I} \setminus \mathcal{D}} \rho^2(\mathbf{K}, \mathbf{W}_{i+\delta_1, j+\delta_2})} \quad (3)$$

where ρ is the cross-correlation between $\mathbf{W}$ and $\mathbf{K}$ [8], and $\delta = (\delta_1, \delta_2)$ represents all possible shifts that may occur between $\mathbf{W}$ of size $M' \times N'$ and $\mathbf{K}$ of size $M \times N$, satisfying $0 \leq \delta_1 \leq M - M'$ and $0 \leq \delta_2 \leq N - N'$. Here, δ_{peak} denotes the coordinates of the peak of correlation as described in [8], $\mathcal{I}$ defines all possible pixel coordinates in the image, while $\mathcal{D}$ represents a cyclic exclusion neighborhood around the peak of correlation (typically of size 11×11 pixels) [8] to prevent contamination of cross-correlation peaks from H_1 when estimating the cross-correlation noise under H_0 [8].

The PRNU has proven to be one of the most reliable tools for solving source attribution problems; however, in recent decades, it has been challenged by the technological improvements of camera devices and their camera acquisition pipelines [16, 19]. Initially, those challenges were related to spatial transformations for correcting image geometrical distortions [8, 9, 12, 14]. Indeed, by mapping

the image pixels to their new coordinates, the PRNU underwent the same transformation, resulting in the loss of correlation between $\mathbf{W}$ and $\mathbf{K}$ and in an increase of the overall False Negative Rate (FNR).

While problems related to an increase in the overall FNR due to image spatial corrections can be addressed by undoing such processing, dealing with sources of false positives is arguably more complex. In [16], for the first time, Iuliani et al. released a large dataset of modern devices (referred to as the "FORLAB dataset") showing severe problems of misattribution. Specifically, the authors illustrated how images from different devices but of the same camera model exhibited very large PCE values when they should not.

In [20], Bhat et al. proposed a classifier based on SPAM features [21] to examine some of the devices in the FORLAB Dataset [16]. The intuition behind this classifier was that, since SPAM features capture dependencies between image pixels, these dependencies should be modified due to the presence of Non-Unique Artifacts (NUA), which are a source of false positives in the FORLAB Dataset [16]. The classifier proposed by Bhat et al. [20] was trained and tested on five Huawei, six Samsung, and one Redmi smartphones, classifying many of their images as affected by NUA. Unfortunately, this approach does not render any rationale for the observed FPs.

Albisani et al. [19] and Baracchi et al. [22] further investigated the discoveries made by Bhat et al. [20] on several Huawei, Xiaomi, Samsung, OnePlus, and iPhone devices in the FORLAB Dataset [16], attributing the source of false positives and NUA to bokeh images [19, 22] or to other correlation artifacts introduced during the camera acquisition process. In their paper, Albisani et al. [19] proposed a technique able to identify these NUAs by dividing the camera fingerprint $\mathbf{K}$ into non-overlapping blocks $\mathbf{K}_1, \dots, \mathbf{K}_u$ and measuring if $\text{PCE}(\mathbf{K}_i, \mathbf{K}_j) > \tau, \forall i, j$ such that $i \neq j$.

While the method proposed by Albisani et al. [19] allowed the identification of several devices affected by NUAs due to bokeh image processing, problems affecting misattribution and the overall False Positive Rates (FPR) of the Huawei P20 Pro and Samsung S9 and S9+ persisted, and were attributed to other kinds of camera processing [19]. Moreover, even after removing images affected by bokeh, many devices showed a low True Positive Rate [19], suggesting the presence of other types of camera processing.

Finally, Butora and Bas [23], in their recent work, discovered a subset of images in the FORLAB dataset that were processed out-camera by Adobe Lightroom Software. Moreover, the authors demonstrated the presence of "spikes" in the cross-correlation of residuals of images processed with Adobe Lightroom. The authors attributed these spikes, with periodicity 128×128 , to Lightroom, also demonstrating their influence in terms of false positives. To solve this problem, Butora and Bas [23] proposed a modified version of the Gram-Schmidt orthogonalization process to remove the NUAs introduced by Lightroom, thus reducing the overall FPR.

Drawing inspiration from the above-mentioned works, in the next sections we will study the effects of visible watermarking and NUAs on the Xiaomi Mi 9 and the Samsung A50. Furthermore, we will present evidence of: 1) mislabeled devices; 2) more than 1500 images processed by third-party software, the presence of which was not foreseen in the FORLAB Dataset; and 3) a substantial number of radially corrected images. These factors severely affect the results in terms of misattribution.

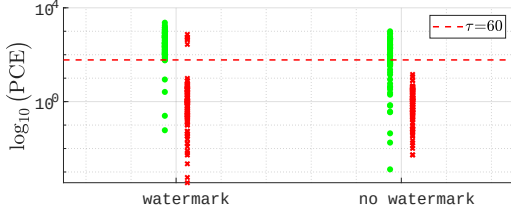


Figure 1: PCE scatter plot of the Xiaomi Mi 9 181825808@N05. The green dots corresponds to H1 samples, the red crosses to H0 samples. With “watermark” we refer to the results obtained using K' and with “no watermark” using K'' .

3 SOURCES OF FALSE POSITIVES IN THE XIAOMI MI 9 AND SAMSUNG A50

In this section, we will present some intriguing results obtained on two of the devices in the FORLAB Dataset [16] that experienced many cases of false positives: the Xiaomi Mi 9 and the Samsung A50.

3.1 Xiaomi Mi 9

Concerning the Xiaomi Mi 9, during our analysis, we noticed that many of its images embedded a visible watermark, such as the one shown in Fig. 2a. Specifically, many of the reference images used in [16] to compose K , and the test images of devices 181825808@N05, 182469844@N02, 184843762@N03, and 161942930@N04 contained the Xiaomi visible watermark.

Watermarks, in general, can contribute to misattribution [23], prompting us to delve deeper into the impact of the watermark overlaid by the Xiaomi Mi 9 in terms of FPs. Our aim was to determine whether the effects of the watermark were localized in a specific region of the image (e.g., the bottom left corner) or they were spread across the image.

Observing that the reference images used in [16] to compose K for device 181825808@N05 include a substantial number of both watermarked and non-watermarked images, we created two fingerprints for this device: K' , composed of images from 181825808@N05 exhibiting the Xiaomi’s visible watermark, and K'' , composed of images without it. Subsequently, we tested the match hypothesis (H1) against the test images of 181825808@N05, and the mismatch hypothesis (H0) against both the test and reference images of 184843762@N03 and 161942930@N04 (the rationale behind excluding device 182469844@N02 is provided in SubSect. 3.1.1).

As illustrated in Fig. 1, the use of K'' affords a significant reduction in terms of false positives compared to K' when the H_1 acceptance PCE threshold is set to 60, a value adopted by many other state-of-the-art methods [16, 19, 20, 23]. Indeed, K' yielded high PCE values (see Eq. (3)) for H_0 when tested against other watermarked images.

To understand if the effect of the Xiaomi visible watermark was localized in a specific region of the images or if it was spread, we produced a PCE-map by dividing K' and the test image residual W into $m \times n$ non-overlapping blocks of size 128×128 and estimating the PCE between each block $K'(u, v)$ and the corresponding $W(u, v)$,

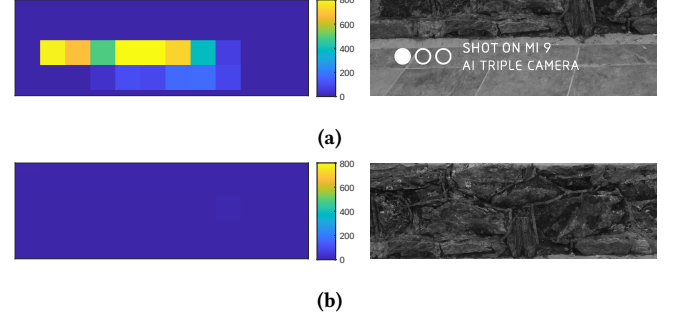


Figure 2: Left: Crop of the PCE map obtained using the camera fingerprint K_w of 181825808@N05, composed of watermarked images, and tested against the image 184843762@N03_48863111582_ccb6c5318f_o.jpg of device 184843762@N03. Right: Corresponding image area containing the visible watermark. Panel (a): crops [1 : 1500, 3500 : 4000]; Panel (b): crops [1 : 1500, 2900 : 3400].



Figure 3: PCE scatter plot of all Xiaomi Mi 9 devices. [16] are the results obtained by Iuliani et al.; “no watermark” correspond to cropping out the watermark; “no watermark-no mislabeled” correspond to the previous case accounting also for the mislabeled devices. Green dots: H1 samples, red crosses: H0 samples.

using:

$$\text{PCE}(K'_{(u,v)}, W_{(u,v)}), \forall (u, v) \in [1, m] \times [1, n], \quad (4)$$

In Fig.2, we show two crops of the produced PCE-map, paired with the corresponding image crops (i.e., the area where the watermark was overlaid and the one right above it). As evident in Fig.2, the impact of the watermark is confined to the bottom left corner and does not affect other regions of the images. As a consequence, we found that this effect could be nearly entirely neutralized by cropping out the visible watermark. This approach is highly convenient as it obviates the need to compose the camera fingerprint exclusively with non-watermarked images.

3.1.1 Mislabeled devices. Following the discoveries regarding the visible watermark of the Xiaomi Mi 9, we decided to extend the experiment depicted in Fig. 1 to include all the devices of this model. However, this time, we centered-cropped a region of size $(M-600) \times (N-600)$ pixels ($M \times N$ is the original image size) from both K and W to exclude the possibility of either containing the visible watermark. Here, the value of 600 was determined empirically using images of size 4000×3000 pixels.



Figure 4: (a) reference image 182469844@N02_48233052237_7ec4f16d37_o.jpg from Xiaomi Mi9 182469844@N02, and (b) reference image 181825808@N05_48081100761_bbbbb363de_o.jpg from Xiaomi Mi9 181825808@N05.

We present the results obtained for all Xiaomi Mi 9 devices in Fig. 3. While using K obtained from images without the Xiaomi visible watermark reduces FPs, this improvement is not evident when all the Xiaomi Mi9 devices in the FORLAB dataset are considered (see center plot in Fig. 3).

Upon further analysis of images from Xiaomi Mi 9 devices, we observed that some devices producing false positive results, despite being labeled as distinct, systematically appear to belong to the same user, so much so that they are likely mislabeled. We provide an example of these images in Fig. 4. After taking care of this by integrating every pair of mislabeled devices into one, the issues with false positives with the Xiaomi Mi 9 practically disappear, as seen in the rightmost scatter-plot of Fig. 3 “no watermark, no mislabeled”.

Sparked by the presence of those mislabeled devices, we conducted a further investigation and identified two more instances. The first pair consists of Motorola Moto E5 devices 135691873@N07 and 186736404@N02, both displaying photos of trains and belonging to Flickr users with almost identical usernames (e.g., “hatcher-hugo” and “Hugo the Hatcher”). The second pair is from Sony DSRX0 devices 64372926@N02 and 149550392@N07, for which we identified the same user’s face in both Flickr profiles¹. The results demonstrating improvements when accounting for these mislabeled devices for Motorola Moto E5 and Sony DSRX0 are shown in Fig. 5. However, it is evident how other sources of NUA are still present in DSC-RX0 as many of its samples are still classified as FPs.

3.2 Samsung A50

Next, we present some preliminary results obtained on Samsung A50 devices. The Samsung A50 was previously studied by Bhat et al. [20] as one of the devices in which a considerable number of images presented NUA.

Initially, we investigated if a plausible cause of the NUA in Samsung A50 devices, as discovered by Albisani et al. [19] and Baracchi et al. [22] for other smartphones, was the *bokeh*, which is an image

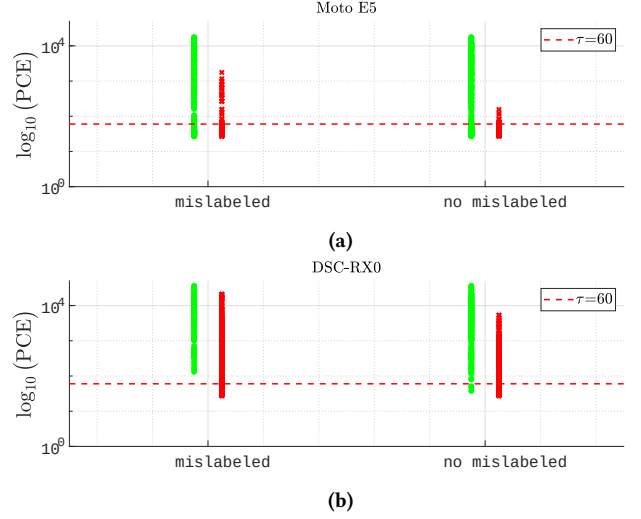


Figure 5: PCE scatter plot of all Moto E5 devices (a), and all DSC-RX0 devices (b). “Mislabeled” and “no mislabeled” corresponds to respectively considering the presence and absence of mislabeled devices.

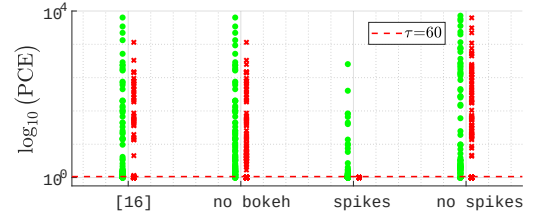


Figure 6: PCE scatter plot of all Samsung A50 devices. [16] are the results obtained by Iuliani et al. “no bokeh”: the camera fingerprint of 75853935@N07 is built by excluding any bokeh images; “spikes”: only images whose DFT magnitudes show the spikes of Fig. 7 are used; “no spikes”: only images not showing any spikes are used.

processing where the background is blurred to enhance foreground objects (often exploiting a dual-camera system). In the FORLAB Dataset [16], three Samsung A50 devices are available, of which, by checking for the presence of depth maps and embedded images [22] in the image metadata, only device 75853935@N07 contains six images with bokeh. Remarkably, those six images were found among those used to compose the camera fingerprint for this device.

Knowing that images with bokeh can be a source of FPs [19, 22], we removed them from those used to compose the camera fingerprint of 75853935@N07. However, as we show in Fig. 6, and as anticipated by Albisani et al. [19], removing the bokeh images from the estimation of the camera fingerprint of Samsung devices did not reduce the number of FPs; instead, it increased them.

Intrigued by these results, we checked if any artifact [23] could be observed in the Fourier domain for the reference images used to compose the fingerprints of the three Samsung A50 devices 75853935@N07, 34501321@N07, and 25052376@N00. We noted

¹See <https://flickr.com/photos/149550392@N07/42263537284/> and <https://flickr.com/photos/64372926@N02/26927758377/>

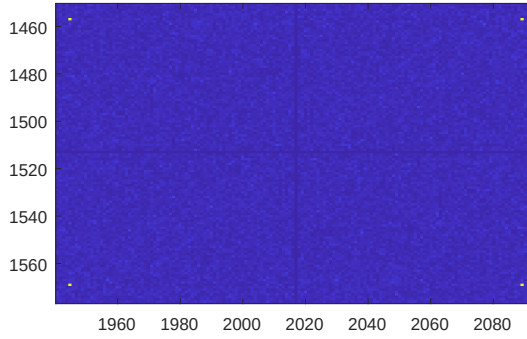


Figure 7: Example of spikes visible in the DFT Magnitude of some Samsung A50 images.

that some of these images showed “spikes”, similar to those observed by Butora et al. [23], as seen in Fig. 7. However, the spikes for the Samsung A50 are mostly visible only for low frequencies and have a periodicity of 27×27 in the DFT domain. Moreover, while the “spikes” detected by Butora et al. [23] served as a source of FPs, those of the Samsung A50 seem to indicate images that are less affected by NUAs. In fact, as illustrated in Fig. 6, when we use only images containing spikes in the DFT magnitude to compose $\mathbf{K}$, the number of false positives in the Samsung A50 is significantly reduced.

These preliminary results suggest a possible correlation between sources of NUA and the absence of spikes in some of the images of the Samsung A50. For these reasons, in a future work, we will verify if the same properties observed for the Samsung A50 generalize to other challenging Samsung devices [19]. Moreover, we will be particularly interested in understanding the nature of the Samsung spikes and proposing a way to automatically detect them.²

4 IMAGE PROCESSING AS SOURCE OF FALSE NEGATIVES

During a more in-depth analysis of the image metadata of the FORLAB Dataset [16], we verified that more than 1596 images contained traces of processing software, which had been previously noticed only at a much lower volume [23], and whose presence was excluded by the authors of the FORLAB Dataset [16]. Specifically, 49% of the 1596 detected images were processed by the app Photos, 25% using the Picasa software, 4% by the app VSCO, 8% using Photoshop, 11% with Lightroom, and 3% using an open-source editing software called Shotwell.³

While image processing applied using one of the above-mentioned editing software can be a source of NUAs [23], it can also be a source of false negatives [9, 10]. Following [9], we used their adaptive method for source attribution of radially corrected images to verify if, among the 1596 processed images, as well as the rest of the dataset, there were any radially corrected images wrongly classified as false negatives.

We employed the “Dir, Cub” variant in [9], which divides $\mathbf{K}$ and $\mathbf{W}$ into a sequence of concentric annuli and iteratively estimates the

²The complete list of Samsung A50 Bokeh images as well as those showing spikes in the DFT magnitude is provided at <https://github.com/AMontiB/PRNULeaks>

³We provide the complete list at <https://github.com/AMontiB/PRNULeaks>

Devices	STPR	NDR	% ND images postprocessed	Tot. Processed Images
iphone xs max	0.37	0.10	15	61
oneplus a6013	0.61	0.25	0	-
sm-a102u	0.22	0.13	0	-
sm-a205u	0.13	0.15	0	-
mar-lx1a	0.58	0.2	0	70
ane-lx1	0.68	0.33	0	3
sne-lx1	0.58	0.7	0	-
vtr-l09	0.67	0.11	3	71
pot-lx1	0.82	0.1	0	-
vog-l29	0.09	0.53	0	-
ele-l29	0.11	0.59	0	-
moto e5 play	0.65	0.20	0	-
ilce-6600	0.05	0.37	0	-
ilce-7s	0.33	0.19	0	-
dsc-rx0	0.2	0.79	0	-
dsc-rx100m7	0.33	0.41	0	70
ilce-6400	0.24	0.48	0	-
canon g7 x mark ii	0.32	0.60	0	-
v-lux (typ 114)	0.4	0.74	45	140
e-m1x	0.33	0.84	0	-
tg-6	0.22	0.69	56	110
x-t30	0.03	0.69	32	104
nikon z 50	0.03	0.43	0	-
coolpix a1000	0.16	0.58	100	2

Table 1: Standard True Positive Rates and New Discovery Rates for models in the dataset. Column “% ND images post-processed” contains the percentage of newly discovered post-processed images, and “Tot. Processed Images” indicates the total number of processed images per-device.

local radial correction parameters α to maximize the final PCE and effectively restore the correlation between $\mathbf{K}$ and $\mathbf{W}$. Specifically, for a given annulus, the algorithm seeks α such that the radial transformation $T_\alpha(r) = r(1 + \alpha r^2)$ applied on $\mathbf{K}$ maximizes the overall PCE.

Following [9], we first measure the Standard True Positive Rate (STPR) for each camera model. The STPR represents the fraction of images that are correctly matched using the standard PCE (3) without any radial transformation inversion. Subsequently, using the “Dir, Cub” variant, we calculate the new discovery rate (NDR), which indicates the fraction of STPR false negatives that can be positively matched after applying the radial transformation inversion [9].

The thresholds used for measuring the STPR and the NDR are set individually for each camera model (e.g., Huawei P20, Samsung A50, etc.) at FPR=0.01, using images of different devices of the same model for H_0 . This decision is made to account for systematic biases, as e.g. observed in the case of the Nokia PureView 808 [9, 16].

Table 1 summarizes the results obtained on the entire dataset, highlighting cases where the NDR exceeds 0.1 (this is a conservative threshold aimed at dismissing false discoveries).

The results presented in Table 1 demonstrate that, similar to compact cameras [24], modern devices still implement in-camera

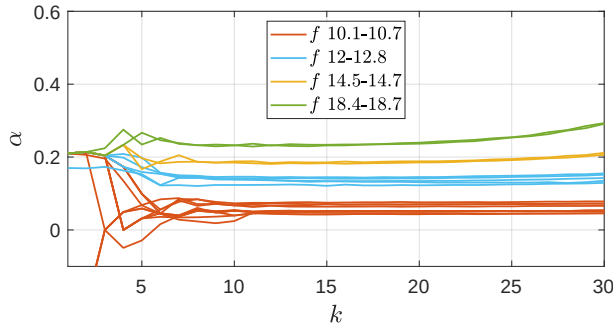


Figure 8: Radial correction parameters α as a function of annulus index k for images taken with the “Canon Powershot G7 X Mark ii”. The “Dir, Cub” variant of [9] is used to invert the radial correction. f refers to the focal length ranges.

radial corrections. By considering this aspect, significant improvements can be achieved in terms of False Negatives compared to the results presented by Iuliani et al. [16]. The presence of radial-corrected images was also confirmed in some devices containing processed images. Furthermore, the presence of radial corrections is supported by the results depicted in Fig.8, where we illustrate the radial correction inversion parameter α of certain images from the devices listed in Table 1.

In Fig. 8, we observe the behavior of the local radial correction parameter α for several images taken with different values of focal length f of the camera “Canon Powershot G7 X Mark ii”. Interestingly, Fig. 8 aligns with expectations [24], being mostly constant except for small annuli indices k (counting outward from the center). These small k values correspond to regions closer to the image geometric center where the Signal-to-Noise Ratio is generally smaller due to the smaller number of pixels [9]. Additionally, we notice how the correlation between the focal length values and those of α , already observed in compact cameras [24], also holds in modern cameras, ruling out that a fixed radial correction is applied systematically.

5 CONCLUSIONS AND FUTURE WORK

The continuous advancement in image acquisition devices, including smartphones and cameras, presents new challenges for source attribution algorithms [16]. Our study investigates the sources of false positives (FP) in several devices of a new and challenging dataset published by Iuliani et al., revealing that improper labeling contributes to some cases, while visible watermarks account for others. Additionally, for the Samsung A50, preliminary findings suggest that bokeh images are not the primary source of FPs. Quite strikingly, the presence of spikes in the DFT magnitude seems to correlate with the absence of those NUAs that generate FPs. Furthermore, we have found that a number of false negatives can be justified (and thus corrected) by the application of radial correction, while others are due to image processing by third-party software.

Based on our findings, future research will focus on modeling the artifacts observed in the DFT magnitude of Samsung A50 devices, understanding their statistical nature, and exploring their presence in other Samsung devices.

REFERENCES

- [1] J. Lukáš, J. Fridrich, and M. Goljan, “Detecting digital image forgeries using sensor pattern noise,” in *Security, steganography, and watermarking of multimedia contents VIII*, vol. 6072, pp. 362–372, SPIE, 2006.
- [2] M. Chen, J. Fridrich, M. Goljan, and J. Lukáš, “Determining image origin and integrity using sensor noise,” *IEEE Transactions on information forensics and security*, vol. 3, no. 1, pp. 74–90, 2008.
- [3] A. Piva, “An overview on image forensics,” *International Scholarly Research Notices*, vol. 2013, 2013.
- [4] M. Kharrazi, H. T. Sencar, and N. Memon, “Blind source camera identification,” in *2004 International Conference on Image Processing, 2004. ICIP’04.*, IEEE, 2004.
- [5] K. S. Choi, E. Y. Lam, and K. K. Wong, “Source camera identification using footprints from lens aberration,” in *SPIE*, vol. 6069, pp. 172–179, 2006.
- [6] K. Kurosawa, K. Kuroki, and N. Saitoh, “Ccd fingerprint method-identification of a video camera from videotaped images,” in *Proceedings 1999 International Conference on Image Processing (ICIP)*, vol. 3, pp. 537–540, IEEE, 1999.
- [7] X. Kang, Y. Li, Z. Qu, and J. Huang, “Enhancing source camera identification performance with a camera reference phase sensor pattern noise,” *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 393–402, 2012.
- [8] M. Goljan and J. Fridrich, “Camera identification from cropped and scaled images,” in *Security, Forensics, Steganography, and Watermarking of Multimedia Contents X*, vol. 6819, pp. 154–166, SPIE, 2008.
- [9] A. Montibeller and F. Pérez-González, “An adaptive method for camera attribution under complex radial distortion corrections,” *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 385–400, 2024.
- [10] A. Montibeller and F. Pérez-González, “Exploiting prnu and linear patterns in forensic camera attribution under complex lens distortion correction,” in *ICASSP 2023-2023 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 1–5, IEEE, 2023.
- [11] S. Fernández-Mendiña, F. Pérez-González, and M. Masciopinto, “Source camera attribution via prnu emphasis: Towards a generalized multiplicative model,” *Signal Processing: Image Communication*, vol. 114, p. 116944, 2023.
- [12] M. Darvish Morshedi Hosseini and M. Goljan, “Camera identification from hdr images,” in *Proceedings of the ACM Workshop on Information Hiding and Multimedia Security*, pp. 69–76, 2019.
- [13] A. Montibeller, C. Pasquini, G. Boato, S. Dell’Anna, and F. Pérez-González, “Gpu-accelerated sift-aided source identification of stabilized videos,” in *2022 IEEE International Conference on Image Processing (ICIP)*, pp. 2616–2620, IEEE, 2022.
- [14] S. Mandelli, F. Argenti, P. Bestagini, M. Iuliani, A. Piva, and S. Tubaro, “A modified fourier-mellin approach for source device identification on stabilized videos,” in *2020 IEEE International Conference on Image Processing (ICIP)*, pp. 1266–1270, IEEE, 2020.
- [15] S. Mandelli, P. Bestagini, S. Tubaro, D. Cozzolino, and L. Verdoliva, “Blind detection and localization of video temporal splicing exploiting sensor-based fingerprints,” in *2018 26th European Signal Processing Conference (EUSIPCO)*, pp. 1362–1366, IEEE, 2018.
- [16] M. Iuliani, M. Fontani, and A. Piva, “A leak in prnu based source identification—questioning fingerprint uniqueness,” *IEEE Access*, vol. 9, pp. 52455–52463, 2021.
- [17] D. Cozzolino and L. Verdoliva, “Noiseprint: A cnn-based camera model fingerprint,” *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 144–159, 2019.
- [18] M. K. Mihcak, I. Kozintsev, K. Ramchandran, and P. Moulin, “Low-complexity image denoising based on statistical modeling of wavelet coefficients,” *IEEE Signal Processing Letters (SPL)*, vol. 6, pp. 300–303, 1999.
- [19] C. Albisani, M. Iuliani, and A. Piva, “Checking prnu usability on modern devices,” in *ICASSP 2021-2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 2535–2539, IEEE, 2021.
- [20] N. N. Bhat and T. Bianchi, “Investigating inconsistencies in prnu-based camera identification,” in *2022 IEEE International Conference on Image Processing (ICIP)*, pp. 851–855, IEEE, 2022.
- [21] T. Pevný, P. Bas, and J. Fridrich, “Steganalysis by subtractive pixel adjacency matrix,” in *Proceedings of the 11th ACM workshop on Multimedia and security*, pp. 75–84, 2009.
- [22] D. Baracchi, M. Iuliani, A. G. Nencini, and A. Piva, “Facing image source attribution on iphone x,” in *Digital Forensics and Watermarking: 19th International Workshop, IWDW 2020, Melbourne, VIC, Australia, November 25–27, 2020, Revised Selected Papers 19*, pp. 196–207, Springer, 2021.
- [23] J. Butora and P. Bas, “The adobe hidden feature and its impact on sensor attribution,” *arXiv preprint arXiv:2401.01366*, 2023.
- [24] M. Goljan and J. Fridrich, “Sensor-fingerprint based identification of images corrected for lens distortion,” in *Media Watermarking, Security, and Forensics 2012*, vol. 8303, pp. 132–144, Spie, 2012.