Source Attribution of Modern Multi-camera Smartphones

Manoranjan Mohanty[a]
Center for Forensic Science, University of Technology Sydney, Australia

Keywords: PRNU, Source Camera Verification, Camera Fingerprint, Multi-camera Smartphones.

Abstract: The PRNU (Photo Response Non-Uniformity)-based source camera attribution is a useful method for verifying if a camera has taken an image (e.g., a crime image). Although this method has matured for images taken by single-camera smartphones, its usability is yet unknown for multi-camera smartphones. A multi-camera smartphone, such as iPhone XS or Huawei P20 Pro, combines output from a number of rear cameras for providing high-quality images. In this paper, we study the effectiveness of the PRNU-based method for a multi-camera smartphone using two simple approaches: (i) multi-fingerprint verification, and (ii) mixed fingerprint verification. In the verification process, the first approach uses fingerprint from each camera whereas the second approach uses a mixed-fingerprint that is obtained by averaging the fingerprints from all cameras. The experimental result shows that the proposed approaches are useful for some camera models. For some other camera models, a more sophisticated method, however, is required.

1 INTRODUCTION

The PRNU (Photo Response Non-Uniformity) based source camera attribution is an effective method for verifying if a camera has captured an anonymous crime image (Lukáš et al., 2006) (Taspinar et al., 2017). This method is based on the PRNU noise pattern of the camera that results due to the non-uniform response of the individual pixels of the camera sensor to light intensity. Using this technique, a fingerprint of the camera is first computed from a set of images taken by the camera (physical access to the camera not required). Then this fingerprint is correlated with the estimated PRNU noise of the anonymous query image to determine if the camera has taken the image (Figure 1). This PRNU-based method has been matured for images (Lukáš et al., 2006) (Taspinar et al., 2017) (Li, 2010) (Sencar and Memon, 2013) (Lawgaly and Khelifi, 2017) (Valsesia et al., 2015) (Caldelli et al., 2010) (Dirik and Karaküçük, 2014) (Bayram et al., 2015) (Rosenfeld et al., 2010) (Goljan et al., 2010). This method has also been extended to videos (Taspinar et al., 2016) (Chen et al., 2007).

The existing PRNU methods assume that a single camera was used to capture an image. This assumption, however, no longer holds for recent multi-camera smartphones (e.g., iPhone 11 series or Huawei P30 series), which use more than one rear cameras to capture an image. Figure 2 shows an example of double camera smartphones. In a multi-camera setup, the output from all cameras can be combined (the combination method can be different for different camera models) for providing better quality images. For example, for providing bokeh effect, both iPhone and Huawei combine output from two different cameras. iPhone, however, provides optical zooming by using output from two different cameras for two different zoom level.

Our work studies the effectiveness of PRNU based verification for multi-camera smartphones by using two simple approaches: (i) multi-fingerprint verification, and (ii) mixed fingerprint verification. Both these approaches compute individual fingerprints from individual cameras. Unlike the first approach, the second approach, however, mixes the fingerprints using simple averaging operation. In the first approach, the verification is done by correlating the estimated PRNU of the query image with each computed fingerprint. In the second approach, the estimated PRNU is correlated with the mixed fingerprint. The experiment result shows that although the proposed approaches can be effective in some cases, they fail for some other camera models as camera manufacturers are now using the sophisticated image capturing techniques. Based on the study, we believe that the well established PRNU-based methods for

[a] https://orcid.org/0000-0002-0258-4586

Mohanty, M.
Source Attribution of Modern Multi-camera Smartphones.
DOI: 10.5220/0011102200003209
In *Proceedings of the 2nd International Conference on Image Processing and Vision Engineering (IMPROVE 2022)*, pages 219-225
ISBN: 978-989-758-563-0; ISSN: 2795-4943

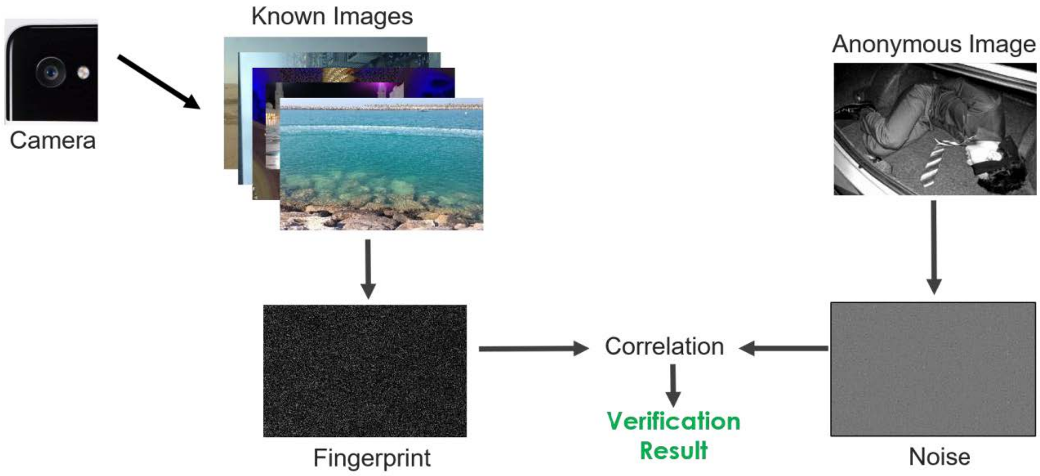

Figure 1: Camera verification using PRNU-based method.

Figure 2: Double camera smartphones.

images need to be revisited and adjusted for dealing with such sophisticated techniques (as future work).

2 MULTI-CAMERA SMARTPHONES

Smartphone manufacturers are now racing to differentiate their products from those of competitors by using multiple camera modules to provide new features, including zooming, wide-angle photography, bokeh effect in portrait mode, stellar image quality.

Zooming: Phones with the multi-camera design featuring a telephoto lens perform better at preserving fine textures and details in images with enlargement. Restricted by the thickness of a phone, the focal length of a camera sensor in a smartphone is fixed. Single-camera models make the use of cropping and resizing to offer scaled images, called digital zoom. The image quality deteriorates in the enlargement process, introducing more noise and pixelated details. To achieve a lossless zoom like in a standalone camera with variable focal length lens, designers added a dedicated telephoto module paired with a traditional camera. At the focal length of the telephoto camera, users are enabled to zoom the frame without compromising on the image quality since the camera uses a typical pipeline to process and render the image at the sensor's native resolution. With further zoom, images from the main camera and telephoto camera can be blended.

Wide-angle Photography: By adding a wide-angle lens in multi-camera setup, a new photography experience is shipped. To meet the general requirement, the lens in a single-camera smartphone is with 50mm focal length, called a standard lens. It is closest to the angle of view to the human eye, producing a natural image. Besides this versatile lens, some manufacturers integrate a wide-angle camera module to provide unnaturally zoomed-out images to satisfy amateur and professional photographers. A wide-angle lens with lower focal length and higher field of view allows users to capture more scene in one frame without stepping back. Other than standard lenses, subjects in wide-angle lenses with straight lines will appear to converge faster. This slight distortion gives images layers of depth and a sense of inclusion.

Bokeh Stimulation in Portrait Mode: To mimic the Bokeh effect that is achieved automatically in cameras with a larger sensor and wide aperture, designers incorporate the second sensor to support post processing of images. Bokeh is a photography jargon, referring to the aesthetic quality of out-of-focus blur. Because of the limited size of smartphones, the lens with narrower aperture and smaller sensors cannot generate an image with a razor-sharp subject and hazy backdrop. Therefore, traditional single-camera phones are incapable of providing a Bokeh effect.

However, based on the parallax effect, phones fitted with multiple camera sensors can measure the depth of objects in a frame by using images from two slighted offset sensors. After creating a depth map, post-shot editing gives a pleasing blurred background while also keeping in-focus items clear. A specialized portrait mode was first introduced by iPhone 7 Plus, which stimulates Bokeh to attract attention to the subject in focus. Since then, most multi-camera phones feature the portrait mode. Combined with several technologies, including advanced algorithms and enhanced image signal processor (ISP), the depth estimation is accurate. Therefore, bokeh is sophisticated and as close as that in DSLR.

Enhancement of Image Quality: Image quality can be improved by extra information provided by the additional sensors in smartphones. The camera module of a single-camera phone uses an RGB sensor, which contains colour filter array (CFA) to record only one of several primary colours at each pixel. By filtering out any colours unmatched with the CFA pattern, each pixel effectively captures around 1/3 of incoming light, leading to the compromises in image quality. There are two approaches in multi-camera packs to mitigate the inevitable side-effect of RGB sensors. The ideal design is to introduce a monochrome sensor. A monochrome camera is capable of higher details and light sensitivity without colour filter array over the sensor. Information from the RGB sensor and the monochrome sensor is gleaned by Image Signal Processor (ISP) to generate a detailed final image. This combination excels in dim light, maintaining pleasing colour rendering, good details and low noise level. An alternative way is to pair a low-resolution RGB camera with a high-resolution RGB camera. Combining images from two RGB sensors would diminish a loss of resolution caused by the colour filter. Overall, images taken by multi-camera phones precede those from phones with a single camera module in most situations.

Table 1 shows different use of multi-cameras by various leading smartphones (which are considered in this paper).

Table 1: Functions of phones.

	Opt zoom	Wid ang	Bokeh	enhnc
Huawei Nova 3i			✓	
Meizu M6 Note			✓	
Moto G5s plus			✓	
iphone XS	✓		✓	
LG V30+		✓	✓	
Samsung A8		✓	✓	
Huawei P20 Pro	✓		✓	✓

When capturing an image, these smartphones can (i) use one of the cameras (e.g., when providing zooming) or (ii) mix output from multiple cameras (e.g., in image enhancement). In the next section, we propose two different methods for these two different possibilities (mixing is performed using averaging operation). However, note that the cameras can use more sophisticated techniques than what is considered in this paper. Since these techniques are propitiatory, it is difficult to know them.

3 PROPOSED METHOD

In this section, we propose two methods for performing PRNU-based verification in multi-camera smartphones. The first method, called multi-fingerprint verification, treats individual cameras of the multi-camera smartphones as different single cameras and performs camera attribution accordingly. The second method, called mixed-fingerprint verification, treats all cameras of the multi-camera smartphone as one camera and performs camera attribution by combining output from different camera sensors. These two methods are based on the insight drawn from the previous section.

3.1 Multi-fingerprint Verification

This method treats each camera of a multi-camera smartphone as a separate camera. A camera fingerprint is computed (using the PRNU-based method) for each camera from a set of known images of the camera. Each camera fingerprint is then stored separately. For verifying if the smartphone was used to take an anonymous image, the extracted noise of the image is correlated with each fingerprint. If at least one correlation result is above a threshold, the image is said to be taken by the smartphone. Otherwise, the image is considered not to be taken by the smartphone.

Figure 3 provides an overview of this method for a double camera smartphone. As shown in the figure, two camera fingerprints are computed. The first fingerprint comes from images taken by Camera 1, and the second fingerprint comes from images taken by Camera 2. For verifying if the anonymous image is taken by the smartphone, two correlations are done (in no particular order). The first correlation is done between Fingerprint 1 and the Noise, and the second correlation is done between the Fingerprint 2 and the noise. If the correlation result of either Correlation 1 or Correlation 2 is above a preset threshold, the image is said to be taken by the camera.

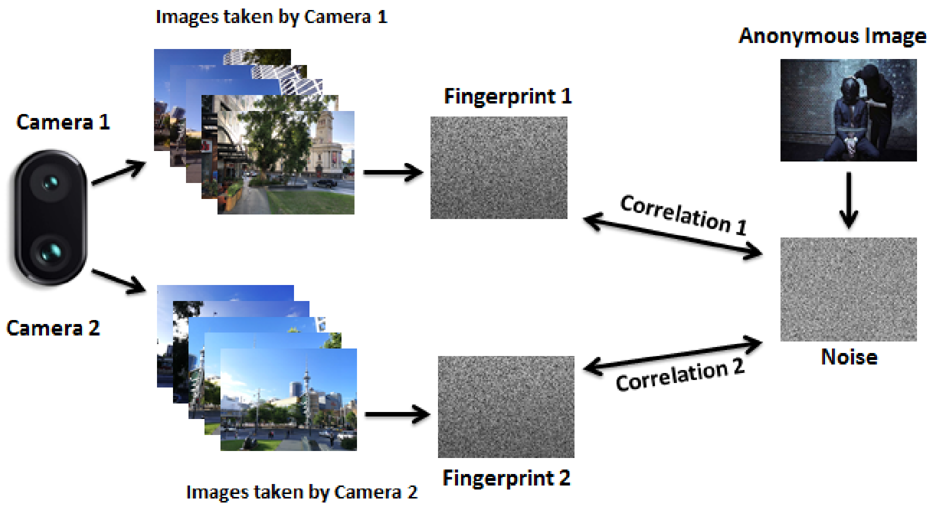

Figure 3: Multi-fingerprint verification process.

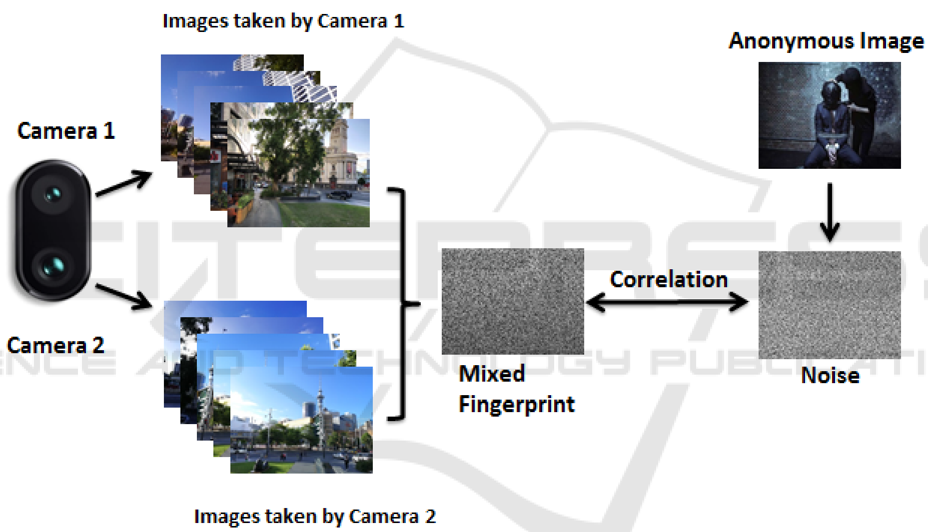

Figure 4: Mixed-fingerprint verification process.

3.2 Mixed Fingerprint Verification

Inspired by composite fingerprint proposed by Bayram et al. (Bayram et al., 2010), we proposed the mixed-fingerprint verification approach. In this approach, a camera fingerprint is computed (using the PRNU-based method) for each camera from a set of known images of the camera (similar to the previous method). Then the fingerprints are mixed using averaging operation. I.e., each i^{th} pixel of the fingerprints (which are in image form) are averaged for producing the i^{th} pixel of the mixed-fingerprint. The mixed-fingerprint is then stored for the future verification process. For verifying if the smartphone was used to take an anonymous image, the extracted noise of the image is correlated with mixed-fingerprint. If the correlation result is above a threshold, it is considered that the image has been taken by the smartphone.

Figure 4 provides an overview of this method for a double camera smartphone. As shown in the figure, two camera fingerprints computed from two different cameras, Camera 1 and Camera 2, are mixed. For verifying if the anonymous image is taken by the smartphone, only one correlation is done between the Mixed-Fingerprint and the Noise. If the correlation result is above a preset threshold, the image is said to be taken by the smartphone.

4 EXPERIMENTS

The experiment is performed using approximately 1300 images taken by seven multi-camera smartphones. We provide more information about the smartphones and images below.

Smartphones: The following smartphones are used in the experiment: Huawei Nova 3i, Meizu M6 Note, Moto G5s Plus, iPhoneXS, LG V30+, Samsung A8, Huawei P20 Pro.

Images: Images were taken under different environmental conditions and different shooting modes. We took seven different conditions into account: (1) Blr: instable images taken with movements of human hands, (2) Bkh: images with Bokeh effect, (3) Indrs: images taken indoors with inconsistent luminance, (4) Otdrs: images taken outdoors with inconsistent luminance, (5) NgtO: images taken at night with flashlight, (6) NgtF: images taken at night without flashlight, (7) Sky: bright sky images.

Image Format: The images from iPhoneXS and Android-based camera models were mostly JPEG images. However, non-portrait mode images from iPhoneXS were in HEIC format. Since our experiment required JPEG images, we used an online econverter for converting HEIC to JPEG.

4.1 Multi-fingerprint Verification

Fingerprint: In this approach, the fingerprint of each of the following camera sensors were generated from a set of clear sky images. The considered camera sensors are: (1) Nova: pattern noise of main camera in Huawei Nova 3i, (2) Meizu: pattern noise of main camera in Meizu M6 Not, (3) Moto: pattern noise of main camera in Moto G5s Plus; (4) iPhx1: pattern noise of wide-angle camera in iPhoneXS, (5) iPhx2: pattern noise of telephoto camera in iPhoneXS, (6) LGW: pattern noise of wide-angle camera in LG V30+, (7) LGU: pattern noise of ultra wide-angle camera in LG V30+, (8) SamS: pattern noise of wide-angle front camera of Samsung A8, (9) SamW: pattern noise of ultra wide angle front camera of Samsung A8, (10) P20x1: pattern noise when zooming is not used (no use of telephote camera), (11) P20x3: pattern noise when optical zooming is used.

Query Image: The correlation for a query image was done by matching the noise of the image with fingerprint. For finding true positive, the correlation was done between the full-resolution noise and full resolution fingerprint of the same camera model. For false positive, a cropped noise was correlated with a cropped fingerprint from a different camera. The cropping was done from 3000×2800 topmost left part of the noise and fingerprint. Note that cropping is required for finding false positive as images from different smartphones have typically different resolutions.

Table 2: True positive of the multi-fingerprint approach.

	Blr	Bkh	Indrs	Otdrs	NgtO	NgtF	Sky
Nova	20/20	0/20	20/20	20/20	1/10	0/10	20/20
Meizu	20/20	20/20	20/20	20/20	10/10	10/10	20/20
Moto	20/20	0/20	18/20	20/20	3/10	10/10	20/20
iPhx1	20/20	NaN	20/20	20/20	6/10	10/10	20/20
iPhx2	20/20	0/20	20/20	20/20	1/10	0/10	20/20
LGW	18/20	NaN	4/20	20/20	0/10	10/10	20/20
LGU	16/20	NaN	5/20	20/20	0/10	0/10	20/20
SamS	20/20	NaN	20/20	20/20	10/10	8/10	20/20
SamW	20/20	NaN	20/20	20/20	10/10	10/10	20/20
P20x1	19/20	20/20	15/20	20/20	5/10	0/10	20/20
P20x3	12/20	0/20	1/20	0/20	0/10	0/10	7/20

Results: Table 2 shows the true positive cases. The false positive rate was zero. However, the true positive is lower than expected for some camera models and image capturing conditions.

For Huawei Nova 3i, Meizu M6 Note, and Moto G5s Plus, the main camera is responsible for capturing the image. Thus, only one fingerprint is used in the multi-fingerprint verification. In most cases, the single fingerprint has high correlations with images taken by the phone. But for indoor and night images and images with Bokeh-effect, the multi-fingerprint approach performs variably among the models. For example, for Huawei Nova 3i and the Nova, the night-time images give poor result, whereas for Meizu M6, the result is satisfactory.

For iPhoneXS, LG V30+, Samsung A8, and Huawei P20 Pro that possess two fingerprints, the proposed multi-fingerprint approach performs well in most cases. In some cases, including images taken with Bokeh effect and images taken indoors or at night, the approach, however, under performs.

4.2 Mixed-fingerprint Verification

In the experiments, we considered four smartphone models: iPhoneXS, LG V30+, Samsung A8 and Huawei P20 Pro. Only these models allowed us to take images from multiple cameras.

Fingerprint: Fingerprints from different cameras were mixed as described below.

(1) iPhx_Mix: mixed noise pattern extracted from 10 clear sky images taken by 12 MP wide-angle rear camera and 10 clear sky images taken by 12MP telephoto rear camera, (2) Sam_Mix: mixed noise pattern extracted from 10 clear sky images taken by 16MP front camera and 10 clear sky images taken by 8MP front camera, (3) LG_Mix: mixed noise pattern ex-

tracted from 10 clear sky images taken by 16MP wide-angel rear camera and 10 clear sky images taken by 13MP ultra wide-angel rear camera, (4) P20_Mix: mixed noise pattern extracted from 10 clear sky images without zooming and 10 clear sky images scaled by three.

Query Images: The test images are the same as those used in the multi-fingerprint verification. There are still seven types of images: blurred, indoors, outdoors, night(on), night(off), sky and Bokeh. But each type has two sets of images taken by two different cameras respectively.

Table 3: True positive of the mixed fingerprint approach.

	iPhx	Sam	LG	P20
Set1				
blurred1	20/20	14/20	18/20	18/20
indoors1	20/20	8/20	4/20	15/20
night(off)1	1/10	3/10	0/10	1/10
night(on)1	10/10	0/10	0/10	0/10
outdoors1	20/20	20/20	20/20	20/20
sky1	20/20	20/20	20/20	20/20
bokeh1	NaN	NaN	NaN	19/20
Set2				
blurred2	17/20	20/20	9/20	12/20
indoors2	18/20	20/20	5/20	0/20
night(off)2	0/10	8/10	0/10	0/10
night(on)2	1/10	10/10	0/10	0/10
outdoors2	20/20	20/20	20/20	0/20
sky2	20/20	20/20	20/20	7/20
bokeh2	20/20	NaN	NaN	0/20

Results: Table 3 shows the true positive cases. The false positive rate was zero. As shown in the table, for some camera models, the true positive of mixed fingerprint approach was a bit lower than the multi-fingerprint approach. This is due to the fact that the correlation result (such as the Peak to Correlation or PCE score) of a query image with a fingerprint of any particular camera model can be lower in mixed fingerprint approach than the multi-fingerprint approach as (i) the resolution of the fingerprint in mixed-fingerprint approach can be lower than the multi-fingerprint approach, and (ii) the quality of the fingerprint in mixed-fingerprint approach can be inferior than the multi-fingerprint approach (Bayram et al., 2010). However, the mixed-fingerprint approach requires less computation and storage (close to *n* times less for *n*-camera smartphone) than the multi-fingerprint approach.

As shown in Table 2 and Table 3, both multi-fingerprint and mixed-fingerprint approach provide significantly lower true positive than the single-camera smartphones (for single camera the rate is close to 99%). We believe such a lower true positive rate is resulting as smartphone manufacturer are using sophisticated image fusion methods. For example, Huawei P20 Pro is combining sensor output from a 40MP sensor with the sensor output from a 20MP sensor. Although the actual combining method is hard to know, this can be different than the simple averaging method considered in this paper.

Other possible reasons for lower performance are various sophisticated approaches used by cameras for providing bokeh effect and dealing with low light. For example, Moto G5s Plus comes with a low-light mode where smart software is designed to control the amount of noise and other adjustments to pop the subjects. The Huawei Nova 3i is packed with AI-powered photography features to simulate details for night shooting.

5 CONCLUSION

This paper studied the effectiveness of the PRNU-based method for a multi-camera smartphone, which uses more than one rear camera to capture an image. Based on the insights drawn from a survey for multi-camera smartphones, two PRNU-based methods: : (i) multi-fingerprint verification, and (ii) mixed fingerprint verification, were explored. The first method mimicked the case when one camera is predominately used for capturing an image (e.g., for zoomed images), whereas the second method mimicked the case when output from multiple cameras are combined in some way for capturing the image. The experimental result showed that although the proposed methods worked well for some smartphones models, they were not sufficient for some other smartphone models. A further investigation revealed that such a low-performance rate is due to the fact that some models are using a more sophisticated image capturing techniques. Future work needs to focus on such sophisticated techniques and come up with a more effective and general PRNU-based method.

ACKNOWLEDGEMENTS

This work is supported by UTS MaPs Start-Up Funding 263025.0226628.

REFERENCES

Bayram, S., Sencar, H. T., and Memon, N. (2010). Efficient techniques for sensor fingerprint matching in large image and video databases. *SPIE Media Forensics and Security II*, 7541:754109–754109–8.

Bayram, S., Sencar, H. T., and Memon, N. (2015). Sensor fingerprint identification through composite fingerprints and group testing. *IEEE Transactions on Information Forensics and Security*, 10(3):597–612.

Caldelli, R., Amerini, I., Picchioni, F., and Innocenti, M. (2010). Fast image clustering of unknown source images. In *IEEE International Workshop on Information Forensics and Security*, pages 1–5.

Chen, M., Fridrich, J., Goljan, M., and Lukas, J. (2007). Source digital camcorder identification using sensor photo response non-uniformity. In *SPIE Electronic Imaging*, pages 1G–1H.

Dirik, A. E. and Karaküçük, A. (2014). Forensic use of photo response non-uniformity of imaging sensors and a counter method. *Optics Express*, 22(1):470–482.

Goljan, M., Fridrich, J., and Filler, T. (2010). Managing a large database of camera fingerprints.

Lawgaly, A. and Khelifi, F. (2017). Sensor pattern noise estimation based on improved locally adaptive DCT filtering and weighted averaging for source camera identification and verification. *IEEE Transactions on Information Forensics and Security*, 12(2):392–404.

Li, C. T. (2010). Source camera identification using enhanced sensor pattern noise. *IEEE Transactions on Information Forensics and Security*, 5(2):280–287.

Lukáš, J., Fridrich, J., and Goljan, M. (2006). Digital camera identification from sensor pattern noise. *IEEE Transactions on Information Forensics and Security*, 1(2):205–214.

Rosenfeld, K., Sencar, T., and Memon, N. (2010). A study of the robustness of PRNU-based camera identification. In *SPIE Conference on Media Forensics and Security*, pages 90–93.

Sencar, H. T. and Memon, N. (2013). *Digital image forensics: There is more to a picture than meets the eye*. Springer, New York, USA.

Taspinar, S., Mohanty, M., and Memon, N. (2016). Source camera attribution using stabilized video. In *IEEE International Workshop on Information Forensics and Security (WIFS)*, pages 1–6.

Taspinar, S., Mohanty, M., and Memon, N. (2017). PRNU-based camera attribution from multiple seam-carved images. *IEEE Transactions on Information Forensics and Security*, 12:3065–3080.

Valsesia, D., Coluccia, G., Bianchi, T., and Magli, E. (2015). Compressed fingerprint matching and camera identification via random projections. *IEEE Transactions on Information Forensics and Security*, 10(7):1472–1485.