

PRNU Based Source Camera Attribution for Image Sets Anonymized with Patch-Match Algorithm

Ahmet Karaküçük¹, A. Emir Dirik^{*2}

Uludağ University, Nilüfer, Bursa, Turkey

Abstract

Patch-Match is an efficient algorithm used for structural image editing and available as a tool on popular commercial photo-editing software. The tool allows users to insert or remove objects from photos using information from similar scene content. Recently, a modified version of this algorithm was proposed as a counter-measure against Photo-Response Non-Uniformity (PRNU) based Source Camera Identification (SCI). The algorithm can provide anonymity at a great rate (97%) and impede PRNU based SCI without the need of any other information, hence leaving no-known recourse for the PRNU-based SCI. In this paper, we propose a method to identify sources of the Patch-Match-applied images by using randomized subsets of images and the traditional PRNU based SCI methods. We evaluate the proposed method on two forensics scenarios in which an adversary makes use of the Patch-Match algorithm and distorts the PRNU noise pattern in the incriminating images he took with his camera. Our results show that it is possible to link sets of Patch-Match-applied images back to their source camera even in the presence of images that come from unknown cameras. To our best knowledge, the proposed method represents the very first counter-measure against the usage of Patch-Match in the digital forensics literature.

Keywords: Patch-Match, PRNU, anonymization, source camera, identification, source camera verification, verification, digital forensics.

1. Introduction

Photo Response Non-Uniformity Noise (PRNU) was found to be very valuable in source camera identification (SCI) since its introduction into the forensics literature [1, 2, 3, 4, 5, 6]. It is used by many agencies for identifying the origin devices of digital images. Robustness of this method was also evaluated against many edge cases [7, 8] and was even experimented on topics beyond the

¹Dept. of Electrical-Electronics Engineering.

^{2*} Corresponding Author. Dept. of Computer Engineering. edirik@uludag.edu.tr

scope of image forensics [9]. Researchers have also looked to improve the handling and querying PRNU fingerprints, from compression [10, 11] to fast search algorithms [12]. However, as in many forensics & security research, counter measures against PRNU based SCI were also developed from cloning [13], to denoising [14, 15] attacks. In many of these counter measures, researchers assumed the knowledge of the underlying methodology of the PRNU fingerprint estimation and detection prior or during the attack. In contrast, image modification techniques based on image content, such as seam-carving (which alters image aspect-ratio) and re-alignment (i.e. panorama) were also considered for the purposes of anonymization as they distort the spatial synchronization of the PRNU pattern and were shown to increase the computational cost of SCI [16, 17, 18].

From the perspective of an adversary, the real advantage of such methods are their blind applicability. However, alteration of the content and form of images might not be desirable. A structural image editing algorithm called “Patch-Match”, in contrast, does not alter the form of the image and the image content is mostly preserved, which makes it a suitable tool to de-synchronize the PRNU pattern, and to use against the PRNU based SCI was first reported in 2016 [19]. Using this method, the authors efficiently redistributed the pixels of image patches to produce shuffled, but good looking images. This can be done without neither any prior evaluation of potential detection schemes nor any information related to the camera. As a result, the source cameras of patch-matched images are hardly identifiable. This notion gives any adversary the ability to become anonymous against PRNU based SCI using the Patch-Match algorithm as a low-cost, “one-click solution”.

In this paper, we evaluate a strategy that can be adopted against Patch-Match based PRNU counter-forensics attack. Since the PRNU pattern becomes very distorted after this attack, the individual Patch-match-applied images could not be linked to their PRNU fingerprints directly. However, our studies have shown that, such images can be grouped randomly into small subsets, and subsets having the majority of images from a questioned camera can be determined successfully with the proposed strategy. Specifically, we would like to answer the following questions regarding this attack:

- Can we verify the source camera device of a set of Patch-Match-applied images taken with the same camera device?
- Can we identify the source camera device of images anonymized with Patch-Match algorithm in a mixed image set comprising images taken with two different cameras?

To answer these questions, we have simulated two different scenarios and conducted experiments to evaluate the performance of the proposed approach.

Our analysis in this paper have been conducted on the dataset cited in [20, 21]. The patch-match attack implementation is the one mentioned earlier in this paper [19]. Interested readers can also access the Patch-match-applied version of the dataset used in this study here: github.com/akarakucuk/2019.PM.SCI.DATA/.

2. Photo-Response Non-Uniformity Based Source Camera Identification and Patch-Match Algorithm

In this section, we are going to introduce the PRNU based Source Camera Identification scheme and the Patch-Match algorithm very briefly. In the next section, we outline the the proposed method to identify subsets of images processed by the Patch-Match algorithm.

2.1. PRNU Based Source Camera Identification: The conventional method

In a camera sensor, photo-sites' response l to a photon intensity l_0 varies as a result of the imperfections in manufacturing process which is called as Photo-Response Non-Uniformity Noise (PRNU). These variations generates a noise pattern (PRNU fingerprint) denoted by \mathbf{F} that was proportional to the size of a sensor and serves as a attributable link to a particular imaging sensor. Extraction of PRNU fingerprint could be explained through imaging sensor output model used in [22, 6] with matrix notation: $\mathbf{L} = \mathbf{L}_0 + \mathbf{L}_0\mathbf{F} + \mathbf{\Gamma}$ where $\mathbf{\Gamma}$ represents other, mostly-random noise sources and \mathbf{L}_0 represents all intensity values apparent to the sensor for a still image. The PRNU fingerprint \mathbf{F} could be estimated from a number of wavelet noise residues $\mathbf{W}_1, \dots, \mathbf{W}_n$ [4], s.t. $\mathbf{W} = \mathbf{L} - \text{denoiser}(\mathbf{L})$, using the MLE estimator shown in [23]:

$$\hat{\mathbf{F}} = \frac{\sum_{i=1}^n \mathbf{W}_i \mathbf{L}_i}{\sum_{i=1}^n \mathbf{L}_i^2} \quad (1)$$

and in [6] and then be used to find similarity between a noise extract \mathbf{W}_i of a query image \mathbf{L}_i and MLE-estimated PRNU pattern, $\hat{\mathbf{F}}$ with peak-to-correlation energy (PCE) $\rho = \text{PCE}(\mathbf{W}_i, \mathbf{L}_i \hat{\mathbf{F}})$ which uses normalized correlation operator between the residue and the PRNU fingerprint with notable modifications [6].

2.2. PRNU De-synchronization Attack by Patch-Match

Patch-Match is an algorithm used for in-painting of images. It works by computing a dense neighborhood field of image patches with a pre-defined size, and uses information to match and replace such patches. Commercially available implementations of the method can exchange such blocks between images of multiple scenes at almost real-time. The algorithm can be forced to a single image to insert or remove contents. The PRNU de-synchronization attack implementation of it also imposes restrictions to avoid matching of a block by itself [19], and applies additional filtering to avoid significant degradation of image quality.

As Patch-Match shuffles a given image with its most similar patches, it implicitly breaks the synchronization between the noise residue of a Patch-Match-applied image and a PRNU fingerprint of the camera that took the image, by distorting the spatial correspondence between the noise residue and the PRNU pattern.

This gives the Patch-Match based attack the advantage of blind applicability, as it requires neither an analysis nor any prior information other than the image

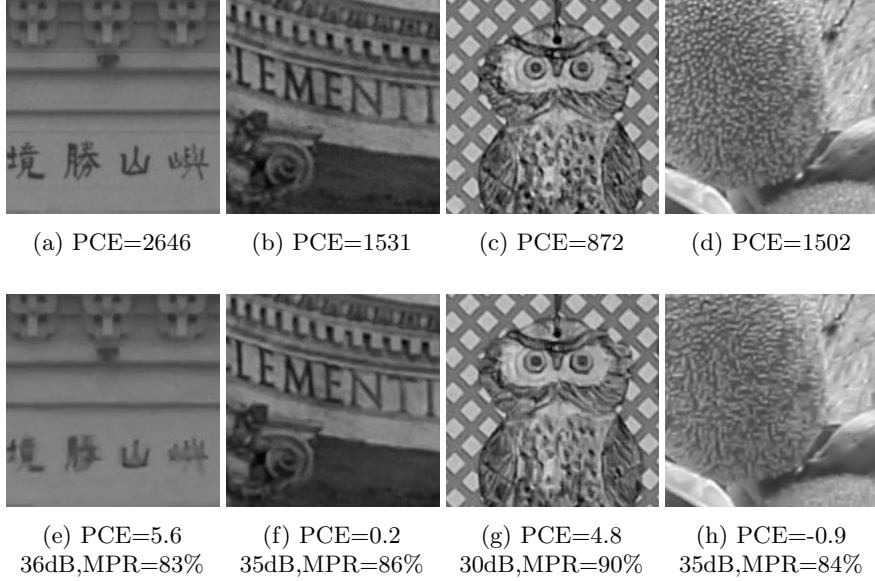


Figure 1: Example images. Images in the first row are original, whereas those in the second row are PM-images. In addition, the first column’s images are from camera A57, the second’s from D7000, the third’s from D90 and the last column’s are images from 60D. Under each PM-image, PSNR in terms of dB and MPR values are also noted. For MPR description and equation, please see Section 3 and Eq. 4. Example images are trimmed to 158×158 pixels in size, with half scale for better viewing.

it is being applied to. This advantage makes the method very versatile to the conventional PRNU based SCI approach. In Figure 1, a few examples of Patch-Match-applied images can be seen along with image quality levels in terms of PSNR.

The Patch-Match-applied images tend to become flatter, and lose some fine details (such as the thin lines and small spots) w.r.t. their original counterparts. The example images in Figure 1 show the effect of Patch-Match algorithm. Reduction in PCE value is evident, and images still have acceptable image quality. Please note that both versions are re-compressed only once and trimmed from the very same coordinates.

On the use of terminology, we would like to indicate that in the rest of the paper we use “PM” as a short-hand to refer to the Patch-Match algorithm, and “PM-images” to indicate images that have been processed with the PM algorithm. More information on the use of remaining notation will be provided in the coming sections.

3. Source Attribution of Images Anonymized with Patch-Match Algorithm

To be able to gain SCI opportunity on PM-images, we looked for weaknesses of the PM from the perspective of a forensic analyst. The PM attack exploits the redundancies (similarities) within a given image and shuffles small portions of images with other, same sized portions. The redundancies here are specific to each scene content, thus they can be assumed to be randomly distributed between different scenes.

This gives us an initial idea for identifying the sources of PM-images, by incorporating multiple PM-images, we can attribute these image combinations to their sources. Our next observation is regarding the differences between a PM-image and its source.

That is, on each image we evaluated, the ratio of pixels that stood the same was around 15% on average, and fluctuated between 55% to 8%. This indicates that it may be possible to attribute the source of PM-images to their originating camera, however it may require more than one image to do so, in other terms, we can merge the noise residues from PM-images, then check for similarities between this “merged” noise residue and the PRNU fingerprint of the analyst which is assumed to be taken from pristine images of the query camera. For all experiments, we assume that the analyst is able to estimate a PRNU fingerprint from 25 pristine images from the query camera and denote this estimate with a bold symbol \mathbf{F}_q .

The adversary, on the other hand, has applied several countermeasures against SCI: PM and meta-data removal on any incriminating image he has. Having received a storage media full of incriminating images which have unknown origin, and a query camera, the analyst’s task is seemingly simple: Finding out if any incriminating image on this disk was obtained with the query camera.

The analyst estimates the PRNU fingerprint of the query camera, \mathbf{F}_q . Using this estimate, she tries to attribute the incriminating images on a storage media with the query camera using the classical PRNU based SCI methods. As all images originating from the query camera were PM-images, this attempt fails. However, using the proposed method, she can try to see if combining subsets of these images would increase his/her chances to attribute these subsets of images to the query camera. As our results will show, using the proposed method, she will have more chances to link the image subsets with at least one PM-image from the query camera, and in some cases has 100% chance to find subsets of images which have at least one PM image from the query camera.

Briefly, we’ll consider two scenarios: Scenario #1 shows when the storage media contains only PM-images that originate from the query camera. The disk content for the Scenario #2 on the other hand, is mixed and has three types of images, with the following ratios: i) 50% of the total disk content is from PM-images of the query camera; (ii) 25% PM images that originate from the unknown camera, and lastly (iii) 25% original images from the unknown camera. Images used in the scenario #1 will be called S_α , and those used in Scenario

Algorithm 1: Pseudo-code for PRNU Subset and Fusion SCI using Small Image Sets

inputs:
 $X \leftarrow$ list of all images in the storage media;
 $K \leftarrow$ initialize the number of subsets to 100;
 $\tau \leftarrow$ initialize PRNU similarity threshold to 50 in terms of PCE;
 $n \leftarrow$ subset length;
 $q \leftarrow$ query camera label;
 $\mathbf{F}_q \leftarrow$ load the PRNU fingerprint of query camera;
 $o \leftarrow$ unknown camera's label;
 $p \leftarrow$ corresponding Case ID from q and o ;
 $S_\alpha \leftarrow$ list of PM-images from query camera (q);
 $S_\beta \leftarrow$ list of PM and non-PM-images from unknown camera (o);
 $\Phi \leftarrow \emptyset$ initialize an empty fusion set;
 $S = \{X_1, \dots, X_N\} \in \{S_\alpha \cup S_\beta\} \leftarrow$ populate image set (file paths);

iteration:
for $k := 1$ **to** K **do**
 $S_k \leftarrow$ A new subset of n randomly selected images from S within the loop according to Eq. 3;
 $\mathbf{F}_k \leftarrow \text{GenerateFingerprint}(S_k)$;
 $\rho_k \leftarrow$ PCE value between \mathbf{F}_k and \mathbf{F}_q ;
 if $\rho_k \geq \tau$ **then**
 $\Phi_p \leftarrow \Phi_p \cup \{S_k\}$, add the set of image paths into fusion set;
 return k th subset (S_k) and PCE value (ρ_k);
 end
end
if Φ_p is not empty **then**
 $\mathcal{F}_p \leftarrow \text{GenerateFingerprint}(\Phi_p)$;
 $\varrho_p \leftarrow$ PCE value of Φ_p ;
 return p th fusion set (Φ_p) and PCE value (ϱ_p);
end

#2 will be called S_Σ .

In this section, for the purpose of simplicity, we are going to denote a “pseudo-operator” denoted with $\text{GenerateFingerprint}(S)$ to describe a PRNU fingerprint generation function. This function accepts any list of images S , s.t. $S = \{\text{image1.png}, \text{image2.png}, \dots\}$, and it is essentially a wrapper for the process of PRNU fingerprint estimation, as shown in Eq. 1 thus produces a PRNU fingerprint estimate from any given set of image list S , such that $\mathbf{F}_S = \text{GenerateFingerprint}(S)$. Whenever we want to specify a specific type of images, we add a subscript next to the set, e.g. S_α .

The subscripts denote the origin of the image set, where α represents the PM-images from the query camera (with camera PRNU fingerprint known to the analyst), β represents both PM and pristine images from unknown cameras

(whose PRNU fingerprints are unknown to the analyst). If, however, both two collections are used, the subscript Σ is used. Similarly, whenever we say, “PCE of S ” we refer to a PRNU similarity value in terms of PCE, between a PRNU fingerprint generated from a set S , and the query camera PRNU fingerprint \mathbf{F}_q the analyst has,

$$\text{“PCE of } S\text{”} = \text{PCE}(\mathbf{F}_q, \mathbf{F}_S), \quad (2)$$

and S is any set of images.

The Algorithm 1 shows the procedure we used for PRNU subset SCI. More information about the scenarios will be given in Section 4.

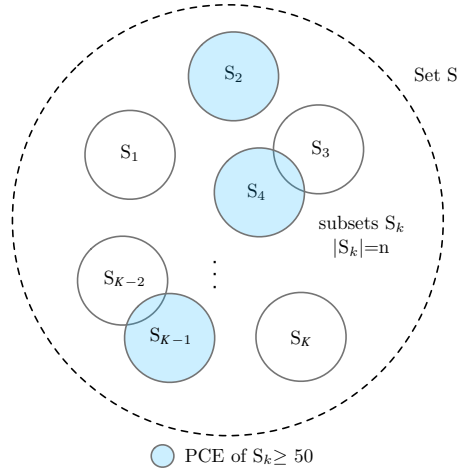


Figure 2: Image subsets

One approach for the attribution subsets of PM-images to their source cameras would be to generate PRNU fingerprints for all possible combinations in a given image dataset (N images), which would consist of $K = 2^N - 1$ fingerprints. Assuming there were $N = 30$ images, a total of 1.07×10^9 fingerprints would be needed. On the other hand, if we were to reduce the number of combinations, K number can be selected sparsely, e.g. from subsets with length of 5 samples to 20 samples with 5 increments, then the number of fingerprints would reduce to one fifth of the previous amount, which would be still far from practical. We therefore limited the number of fingerprints to 100 in each experiment, by limiting the number of subsets to 100 for each 4 subset size in all scenarios we will present.

In Figure 2, a diagram outlining the usage of subsets is given. As shown in the figure, each subset S_k is populated by randomly sampling the whole set S with the subset size, n . These subsets are allowed to overlap, however each one is unique. Such that, there are $K = 100$ subsets, each having cardinality n , where $n = 5, 10, 15, 20$, and any subset is chosen to not be identical with any other subset, which can be formally stated for each n value, as:

$$S_i \neq S_j \Rightarrow |S_i \cap S_j| < n \quad (3)$$

where S_i and S_j are any two subset populated within the loop in the algorithm, with $|S_i| = |S_j| = n$. If the PCE of any subset is found over the threshold τ , for example the PCE of i th subset $S_i > \tau$, the content (list of image paths) of the subset is then added to the p th fusion set, Φ_p . When the loop ends, the PCE of Φ_p is used to calculate the PRNU similarity of the fusion set populated within the loop. τ is set to 50 along this paper as the PRNU similarity threshold in terms of PCE as discussed as the lower end in [6]

4. Experimental Setup & Results

In this section we describe the environment of our experiments for the proposed approach to source camera attribution of PM-image subsets, starting with the creation of the PM database in Section 4.1, then we explore two main scenarios an analyst may face for SCI on PM-image sets. The first one (in Section 4.2) is the homogeneous scenario, where the PM-images are captured only from the known “query camera”, which can be presumed as the easiest scenario for any SCI task. Followed by the second scenario in Section 4.3, the heterogeneous scenario, in which the analyst has to find a link between incriminating images from a query camera within a set of images including images from an unknown camera, denoted as “unknown camera”.

4.1. Creating a PM-image dataset

In this study, the dataset we used is based on the Realistic Tampering dataset in [20, 21], which consists of pristine images along with their manipulated version for four different cameras, each having 55 pristine images with single resolution, which is 1920×1080 pixels without meta-data fields.

From these pristine images, we randomly selected a list (file names) of 25 images to estimate the camera PRNU fingerprint. The list of the remaining 30 images were reserved for tests.

The PM implementation we targeted produces only gray-scale images and trims each image by 7 pixels from each side (the trim size is the size of patch window size minus one, where the patch window size is 8×8). It is possible to overcome the gray-scale limitation, but we preferred to execute the method as it was in the original paper. As the size and color differences between images might influence our study, we produced two versions for each image: a) PM version, b) non-PM version. Naming convention for these versions are as the follows; “out-pm-before-file.ext” for the non-PM version, and “out-pm-after-file.ext” for the PM version. The interested readers can find links to the dataset in: github.com/akarakucuk/2019_PM_SCI_DATA/.

The non-PM images were generated by applying the very same crop settings and color conversion. These images were then used to generate the query camera’s PRNU fingerprint estimate, \mathbf{F}_q using the selected list mentioned earlier.

This way, we have a PM version for each non-PM image, which are both saved once without compression, and allowed us to be able to compare and evaluate the manipulation caused by PM in terms of the manipulated pixel’s rate (MPR) and the image quality (PSNR). Some example images are given in Figure 1.

We would like to highlight that, out of the images we mentioned we would use for evaluations of PM-images, there were a few images (1 for A57, 3 for D90), which were still identifiable by the PRNU based SCI. At a first glance, inclusion of these images in our evaluations might be more realistic. However, such images should be simply filtered-out by running individual images through the conventional PRNU based SCI or by running the proposed algorithm by setting n to 1. Including these images can be problematic in certain scenarios, for example in Scenario #2 in the Section 4.3, the PRNU similarity of subsets dominated by non-matching images could also be lifted over the decision threshold, which could in turn produce a lower performance. By the same token, should we choose to include them in our evaluations in Scenario #1, Section 4.2, it could have served as make-up to our proposed methods’ advantage and produce higher performance. Therefore, we opted not to make use of these PM-images when the performance of the proposed method was evaluated anytime \mathbf{F}_q corresponds to these cameras. Please note that these 4 individual images are included if the camera PRNU fingerprint estimate \mathbf{F}_q was not either A57 or D90.

Readers are referred to Table 1 and its accompanying figure, Fig. 3 to have an understanding regarding the initial state of the dataset. The referred table and the figure show the values of initial PCE, PSNR and Manipulated-Pixel-Rate (MPR) between the PM and the non-PM image versions. The latter shows the percentage of changed pixels of each image pair, and calculated simply by,

$$\text{MPR} [\%] = 100 \times \frac{1}{R \times C} \sum_{r=1}^R \sum_{c=1}^C \text{sign}(|\mathbf{L}(r, c) - \mathbf{L}_{pm}(r, c)|) \quad (4)$$

while ignoring signum function $\text{sign}()$ at value 0. Here, \mathbf{L} denotes the non-PM version, \mathbf{L}_{pm} denotes the PM version of an image. R and C are the width and height values in pixels. Also in the table are the camera labels that were used to name the cameras. The values given in Table 1 are median values, and they show the manipulation efficiency of the PM, when compared to non-PM values in terms of PCE. For all cameras and images, the observed PCE values were found very low, with high PSNR and MPR rates.

4.2. *Scenario #1: Performance on Homogeneous Image Subsets*

In this scenario, we evaluate the performance on a case where the storage media contains PM-images from only the query camera, which represents the most hygienic scenario an analyst can face in any circumstance. Please recall that these 100 image subsets were populated randomly, each including 5 to 20 (n) image to reasonably increase the recall rate of the images as mentioned in Section 3.

Table 1: Properties of the Patch-Match Image Data-set. MPR stands for Manipulated Pixel Rate, which is the percentage of pixels that have changed after application of Patch-Match. The metrics shown in the table are median values.

Camera		Number of Images	PCE		PSNR [dB]	MPR [%]
Make	Label		non-PM	PM		
Sony	A57	29	1963	1.05	38	85
Nikon	D7000	30	888	2.92	36	78
Nikon	D90	27	1231	0.14	33	86
Canon	60D	30	1289	1.91	34	86

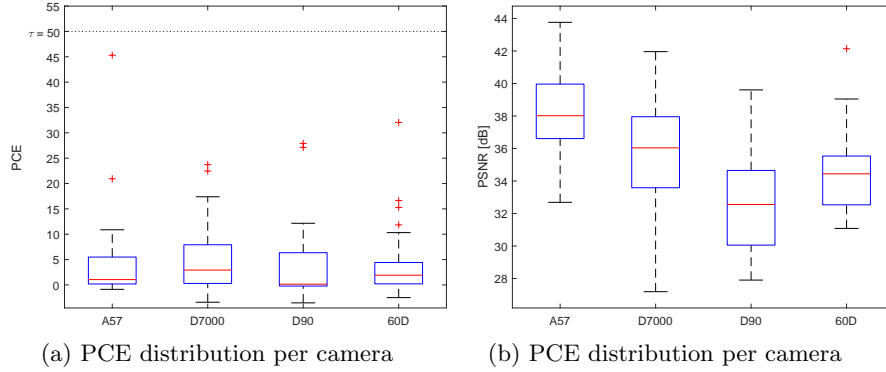


Figure 3: Distributions of PRNU similarity and the image quality of each image in the PM database per camera. In the left the PRNU similarity in terms of PCE and in the right, the image quality metric, PSNR in terms of dB were given.

The PCE values are given in Table 2 and indicate a few cases where the set attribution approach may fail. Specifically, the D90 has an unexpected result, where the performance gets worse with elevated n values. One possible explanation could be based on the initial median values of PM-images for this camera (Table 1) which is, 0.14 for PCE. This is an eighth of its closest performer, A57 camera in the same test, which was 1.05. The distribution of the values is also similar in terms of both PCE and PSNR distribution for this particular camera, as it can be seen in Fig. 3. This indicates that the majority of images from D90 are more heavily affected by PM, the performance of D90, with only one subset with $n=5$ was above the PCE threshold. We’ll compare this and other results more closely through the coming table, Table 3.

Table 3 shows the results from the fusion set, broken down by each camera label and subset size (n) the test was conducted on. The fusion sets were populated by setting S_β constantly to \emptyset in Algorithm 1, in order to be in line with the Scenario #1. In Table 3, $|\Phi_p|$ denotes the total number of images i.e. cardinality, of each fusion set and their PCE values, s.t. PCE of Φ_p . PCE values here represent the PRNU similarity when all images in each fusion set were incorporated. The “Recall” value were also given in this table, which shows

Table 2: Scenario #1, Median and Average PCE values of PM-image subsets, with the exception of $n=1^*$ which does not from a subset and provided only as a reference. Values above the detection threshold are emphasized in bold characters.

Camera	Median PCE					Maximum PCE				
Label	$n=1^*$	$n=5$	$n=10$	$n=15$	$n=20$	$n=1^*$	$n=5$	$n=10$	$n=15$	$n=20$
A57	1.1	14.3	36.0	51.6	77.0	45.3	82.7	80.6	94.1	109.3
D7000	2.9	11.5	18.2	36.0	45.9	23.7	48.1	63.2	71.9	83.9
D90	0.1	3.7	7.4	9.7	12.6	27.9	55.7	43.8	35.9	27.9
60D	1.9	13.1	22.3	33.3	47.2	32.1	54.2	52.5	80.6	79.9

the recall rate of PM-images that belong to the labeled device populated into the fusion set, formally given by:

$$\text{Recall } [\%] = 100 \times \frac{|\Phi_p|}{|S_\alpha|}. \quad (5)$$

There are missing fusion sets, denoted with “—” in the table. For example on D7000, there was no fusion set for $n=5$, meaning none of the PM-image subsets for this camera with this subset size were reached over PCE value threshold τ . In addition, D90 also indicates that there is only one subset of PM-images brought together a combined PRNU noise pattern that matched with the camera’s PRNU fingerprint estimate. The results from the remaining sets ($n=10$ to $n=20$) through this scenario confirm this one-off situation as none of them provided similar rates.

It is evident in this table that the proposed method has reached complete recall with $n=15$ on all the three cameras, however, in D90, only 18% of the PM-images were covered with a PCE value of 55.7 on $n=5$. In this table, it is also evident that the increased cardinality values meet with decrease in PRNU similarity in terms of PCE. The most notable is D7000, where the PRNU similarity drops from 83.2 to 67.3 when the fusion set reached from about half of the PM-images to all of such images. Similar tendencies are evident for different cameras as well. The exception is also the camera D7000, where none of the 100 subsets with cardinality 5 ($n=5$) did not reach or exceed the PCE threshold. This may indicate a need to increase the number of randomly selected subsets.

On a different note, the PRNU similarity of the PM-images from non-matching devices were also observed to see if such subsets can reach or exceed the threshold. As expected, there was none. The results regarding the non-matching and matching camera PM-images for a few example cameras were plotted in Fig. 4. More details regarding the results from the non-matching cases were omitted as they all give the same outcome.

4.3. *Scenario #2: Performance on Heterogeneous Image Sets from Camera Pairs*

In this scenario, to evaluate the performance of the proposed method when images from an unknown origin are also present along with PM-images of the

Table 3: Scenario #1: Details of fusion sets. “—” represents cases without an outcome. PCE column represents PCE of Φ_p .

Camera Label	n	Fusion Set		Recall	
		$ \Phi_p $	PCE	Value	[%]
A57	5	22	100.2	22/29	76
	10	29	100.0	29/29	100
	15	29	100.0	29/29	100
	20	29	100.0	29/29	100
D7000	5	—	—	—	—
	10	16	83.2	16/30	53
	15	30	67.3	30/30	100
	20	30	67.3	30/30	100
D90	5	5	55.7	5/27	18
	10	—	—	—	—
	15	—	—	—	—
	20	—	—	—	—
60D	5	9	82.8	9/30	30
	10	24	81.7	24/30	80
	15	30	68.7	30/30	100
	20	30	68.7	30/30	100

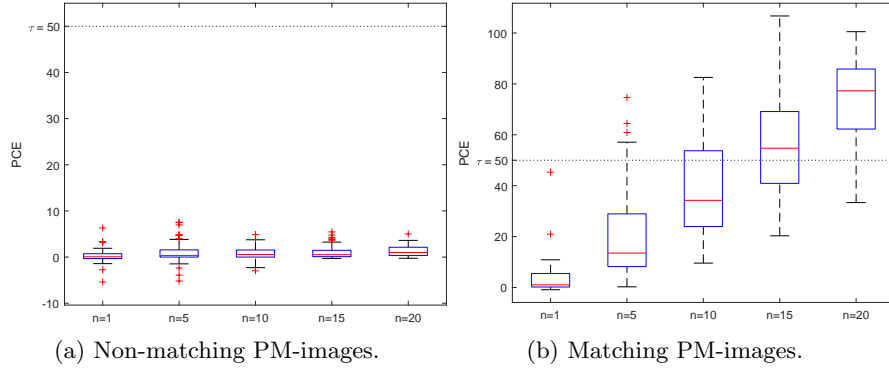


Figure 4: In (a) non-matching case (PM-image subsets from Canon 60D and PRNU fingerprint from Sony A57) and in (b), matching case (PM-image subsets from Sony A57 and PRNU fingerprint from Sony A57). The PRNU similarity values of these subsets were obtained against \mathbf{F}_q of Sony A57. In both figures, boxes on the far left are for the subset size of $n=1^*$ and only given to serve as a reference PCE distribution for per-image statistics.

query camera in the storage media.

To do so, we’d like to start by elaborating the concept of Case IDs. A Case ID simply refers to a specific pair of source cameras as shown in Table 4. For example, the Case ID 1 represents a pair when the storage media has images from both camera A57 and D7000. When all images (59) from these two

Table 4: Scenario #2: Properties of Cases. The right-most column represents PCE value when all images from both cameras are combined. $|S_\alpha|$ and $|S_\beta|$ represents number of images in the PM-image set from the query camera and mixed type of images (PM-image + original) from the unknown camera listed in each row.

Case ID	Camera Labels				PCE of S_Σ
	Query	Unknown	$ S_\alpha $	$ S_\beta $	
1	A57	D7000	29	30	32.5
2	A57	D90	29	30	30.7
3	A57	60D	29	30	78.3
4	D7000	A57	30	30	25.6
5	D7000	D90	30	30	57.0
6	D7000	60D	30	30	23.2
7	D90	A57	27	30	12.1
8	D90	D7000	27	30	6.2
9	D90	60D	27	30	4.3
10	60D	A57	30	30	45.9
11	60D	D7000	30	30	26.0
12	60D	D90	30	30	40.1

cameras, which we denote by S_Σ , were merged, the PRNU similarity is found as 32.5 as listed on the first row under the PCE column, s.t. PCE of S_Σ for Case 1, in the same table. Please recall, S_Σ term denotes a collection of images from two different cameras. The analyst is assumed to have knowledge of the PRNU fingerprint he gathered from a separate set of 25 pristine images only from the query camera. Also recall that the storage media the analyst received only has PM-images from the same query camera, whereas the images from the unknown camera has 50% chances of being a PM-image, to be avoid of any form of bias. In Table 4, initial PRNU similarities observed in terms of PCE of the listed cameras were also given.

To remind the readers about the PRNU Subset and Fusion SCI algorithm, we would like to refer once again to Algorithm 1. In the algorithm, p represents a descriptor for camera pairs, which is an integer ranging from 1 to 12 with subset sizes n starting from 5 to 20, with 5 image increments. Same number of random subsets ($K=100$) for each length per each pair were selected, as indicated in the algorithm with subscript k . Thus, the range of these values are $p=1, 2, \dots, 12$, $n=5, 10, 15, 20$ and $k=1, 2, \dots, 100$, as indicated in Table 4. Please also note that the total number of images ($|S_\Sigma| = |S_\alpha \cup S_\beta|$) vary slightly on different pairs.

The initial state of the PRNU similarities observed from the table indicates that in two cases (Case 3 and 5), the analyst might find it especially hard to distinguish images from both cameras if they were naively combined and could end up with 50% probability of mislabeling images from the unknown camera. The proposed method, on the hand, can achieve up to 100% precision on 6 different cases as shown in Table 6.

For each case listed in the Table 4, PRNU noise from 100 randomly populated

Table 5: Scenario #2, PRNU values above the detection threshold are emphasized in bold characters, with the exception of $n=1^*$ which does not constitute a subset and provided only as reference. Please note that the maximum values in the $n=1^*$ column are the same as Scenario #1. Values above the detection threshold are emphasized in bold characters.

Case ID	Median PCE					Maximum PCE				
	$n=1^*$	$n=5$	$n=10$	$n=15$	$n=20$	$n=1^*$	$n=5$	$n=10$	$n=15$	$n=20$
1	0.2	2.1	5.1	5.6	11.2	45.3	41.8	52.7	33.9	39.7
2	0.1	1.5	6.0	7.8	11.0	45.3	65.1	37	41.3	44.6
3	0.5	6.0	14.8	19.8	23.8	45.3	47.7	59.3	66.5	74.6
4	0.1	3.2	5.5	6.6	10.5	23.7	36.6	32.7	49.5	39.2
5	0.6	5.3	11.9	14.1	19.5	23.7	35.5	58.2	63.4	54.3
6	0.3	2.7	3.8	6.8	6.2	23.7	24.9	33.7	37.6	50.2
7	0.2	0.9	2.6	4.4	4.4	27.9	19.5	27.3	21.1	24.2
8	0.0	0.8	1.5	2.1	3.5	27.9	34.4	19.4	19.7	33.3
9	0.0	0.3	0.7	2.0	2.4	27.9	34.7	30.2	31	21.6
10	1.0	4.2	7.3	11.8	15.3	32.1	39.3	45.3	43.6	57.2
11	0.7	2.4	3.9	7.0	9.1	32.1	25.4	32.6	27.1	35.6
12	0.2	2.6	6.8	10.0	13.6	32.1	31.2	44	39.1	45.6

subsets, each having the subset sizes of $n = 5, 10, 15, 20$ number of images were used to estimate a PRNU fingerprint and correlated with the query PRNU fingerprint \mathbf{F}_q . The median and maximum PCE values from these subsets were shown in Table 5.

In Table 5, values from all subsets are given and values over the threshold are emphasized in bold characters. This table shows the PRNU similarity of the incorporated subsets in terms of PCE values. In many cases, the subsets did not reach or exceed the threshold, but any subset having a PCE value over the threshold were incorporated for each n and p which forms the fusion set Φ_p , and all images in this set were then used to re-calculate the final PCE of Φ_p . The results and the number of images in the fusion set along with the Precision rates for each case are shown in Table 6. Precision value shows the ratio of PM-images from the query camera in the fusion set, and in terms of percentage, can be formally given as:

$$\text{Precision}[\%] = 100 \times \frac{|\Phi_p \cap S_\alpha|}{|\Phi_p|} \quad (6)$$

In Table 6, there are only two cases, Case 3 and 5 that produced a fusion set for plural number of subset sizes, namely, for $n=10, 15$ and 20. This calls for a further elimination for these fusion sets, which can be done by finding the intersection of fusion sets for all available n values. This produces $|\Phi_{p=3}| = 18$ which has 14 PM-image from the query camera, and improves the precision to 78%, which is higher than all individual fusion sets, which have a maximum precision of 69%. Another such case is Case 5, where the precision, with this type of elimination yields with 4/6 and 67%, which was the maximum value in

Table 6: Scenario #2: Details of the fusion sets. Cases without an outcome are represented with “-” mark.

Case ID	n	Fusion Set		Precision	
		$ \Phi_p $	PCE	Value	[%]
1	10	10	52.7	9/10	90
2	5	5	65.1	5/5	100
3	10	26	92.1	18/26	69
	15	46	92.4	26/46	57
	20	47	90.2	26/47	55
4	-	-	-	-	-
5	10	10	58.2	4/10	40
	15	24	77.9	16/24	67
	20	33	64.5	17/33	52
6	20	20	50.2	14/20	70
7	-	-	-	-	-
8	-	-	-	-	-
9	-	-	-	-	-
10	20	32	63.3	18/33	59
11	-	-	-	-	-
12	-	-	-	-	-

this case when $n=15$ in the same table. This type of elimination can find its use for highly critical tasks.

In Table 7, a summary showing the overall performance of the algorithm for this scenario is given, broken down for each n values. Here, the column labeled as “C” indicates the cases where the algorithm produced any subset having a PRNU similarity over the threshold in terms of PCE value. Values indicated under column “Average Φ ” shows the average length of fusion sets for available cases.

There are three metrics, namely, “T.Precision”, “T. Recall” and “Selection”. The last metric shows the representation rate of images in fusion sets, which is calculated by dividing the total number of images in the fusion sets to the total number of images in the represented cases, which can be written by using $\sum_{p \in C}$ operator which is used to restrict the results to cases having a fusion set, as:

$$\text{Selection } [\%] = 100 \times \frac{\sum_{p \in C} |\Phi_p|}{\sum_{p \in C} |\mathcal{S}_\Sigma|} \quad (7)$$

The other values in the Table 7, “T.Precision” and “T.Recall” denotes for Total Precision and Total Recall and indicates how well the proposed method worked in terms of accuracy and sensitivity. These were also calculated by summing over $p \in C$, given by:

Table 7: Scenario #2: Performance of PRNU based SCI w.r.t. each subset length n .

n	Cases	T.Precision		T.Recall		Selection		Average of $ \Phi $
	C	Value	[%]	Value	[%]	Value	[%]	
5	2	5/5	100	5/29	17	5/59	8	5
10	1,3,5	31/46	67	31/88	35	46/178	26	15
15	3,5	42/70	60	42/59	71	70/119	59	35
20	3,5,6,10	76/132	58	76/119	64	132/239	55	33

Table 8: Scenario #1: The T. Recall rates of fusion sets w.r.t. the subset length (n) and the number of subsets (K). The columns under percentage symbol are the average recall rates Eq. 8, and the columns under C denote the number of query cameras producing a fusion set.

K	$n = 5$				$n = 10$				$n = 15$				$n = 20$			
	$ \Phi_p $	[%]	C		$ \Phi_p $	[%]	C		$ \Phi_p $	[%]	C		$ \Phi_p $	[%]	C	
10	5	17	1		15	52	1		20	66	3		29	99	3	
20	7	22	2		25	86	1		26	87	3		30	100	3	
30	9	29	2		29	100	1		26	88	3		30	100	3	
40	9	29	2		20	66	2		28	96	3		30	100	3	
50	9	29	2		20	66	2		29	99	3		30	100	3	
60	12	41	2		19	63	3		29	99	3		30	100	3	
70	14	47	2		20	67	3		29	99	3		30	100	3	
80	14	47	2		22	74	3		29	99	3		30	100	3	
90	14	47	2		22	74	3		30	100	3		30	100	3	
100	12	42	3		23	78	3		30	100	3		30	100	3	

$$\text{Total Recall}[\%] = 100 \times \frac{\sum_{p \in C} |\Phi_p \cap S_\alpha|}{\sum_{p \in C} |S_\alpha|} \quad (8)$$

$$\text{Total Precision} [\%] = 100 \times \frac{\sum_{p \in C} |\Phi_p \cap S_\alpha|}{\sum_{p \in C} |\Phi_p|}. \quad (9)$$

The results in Table 7 shows that the most cases were reported with the subset size $n=20$, however it also had the lowest Total Precision value. The best Total Precision was reported when the subset size was the smallest, $n=5$, which was expected. Because, by allowing more images in the subsets (with PCE value over the τ), the chances of including images of unknown origin also increase. This may indicate that increasing the number of subsets K for smaller subsets would be a beneficial trade-off for the analyst. The influence of the number of subsets (K parameter in the Algorithm 1) will be discussed in the next section.

Table 9: Scenario #2: The T. Precision rates of fusion sets w.r.t. the subset length (n) and the number of subsets (K). n and K values without an outcome are represented with “-” mark. The columns under percentage symbol are the average precision rates in Eq. 9, and the columns under C denote the number of cases producing a fusion set.

K	$n = 5$			$n = 10$			$n = 15$			$n = 20$		
	$ \Phi_p $	[%]	C	$ \Phi_p $	[%]	C	$ \Phi_p $	[%]	C	$ \Phi_p $	[%]	C
10	-	-	-	10	40	1	15	73	1	34	59	1
20	-	-	-	10	63	3	15	70	2	41	59	1
30	-	-	-	13	66	3	15	70	2	37	55	2
40	-	-	-	13	66	3	15	70	2	37	55	2
50	-	-	-	13	66	3	26	61	2	30	58	4
60	-	-	-	13	66	3	26	61	2	30	58	4
70	-	-	-	13	66	3	30	60	2	33	58	4
80	-	-	-	13	66	3	33	61	2	33	58	4
90	5	100	1	15	67	3	35	60	2	33	58	4
100	5	100	1	15	67	3	35	60	2	33	58	4

5. Conclusion

In this paper, we proposed the first SCI method for images processed with Patch-Match (PM) algorithm. The PM algorithm was originally developed as an image in-painting algorithm, but recently, its use as an attack method against PRNU based SCI was successfully demonstrated. Due to its nature, the algorithm changes many pixels (up to 86%), which breaks the synchronization of the PRNU noise pattern in images, thus making PRNU based SCI almost obsolete (on 97% of images we have tested) in identifying individual images through the use of PRNU based SCI method.

We propose to identify such images using a fixed number of small subsets, and by using the conventional PRNU similarity metric as a guide to reach to a bigger set, which we call a “fusion set”. The proposed method is evaluated briefly in two scenarios. In the first scenario, the proposed method was tested in a homogeneous setting, where the analyst worked to give an answer if all the incriminating images he received were coming from a suspected, query camera. In this setting, the proposed method is shown to have up to 100% chance of finding the images on 3 out of 4 source cameras tested.

In second scenario, the analyst was given a more difficult task, because half of the images the analyst received are coming from an unknown source. In this scenario the proposed method increased the likelihood of correct source identification as well, however there exists quite a few cases (6 out of 12) where there were no conclusion.

As mentioned earlier, to specify an upper bound in computing time we had limited the number of small subsets (K) to 100 for all the analysis in this study. Nevertheless, we would like to discuss the influence of K on the analysis in both scenarios using the results we have, in Tables 8 and 9. In both tables, the results were summarized in terms of K , the number of small subsets and n , the number

of images in the subsets. Regardless of the scenario, increasing the number of K improves the SCI of more cases and query cameras, however the performance rates remain stable.

We believe the experiments and dataset released along with this study will help to advance the digital forensics related SCI research in the era of software-enriched images.

In our future studies, we plan to work on identifying traces of Patch-Match on PM-images and evaluate the proposed method outlined in this paper for manipulations with similar nature, such as image in-painting.

6. Acknowledgements

The authors want to thank Matthias Kirchner for allowing us to use the Patch-Match code for PRNU de-synchronization. We would also like to thank Pawel Korus for allowing us to re-produce a version Realistic Tampering Database for the purposes of Patch-Match related SCI research.

References

- [1] J. Lukáš, J. Fridrich, M. Goljan, Determining digital image origin using sensor imperfections, in: A. Said, J. G. Apostolopoulos (Eds.), *Proceedings of SPIE*, Vol. 5685, SPIE, 2005, p. 249. doi:10.1117/12.587105.
URL <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1530329><https://proceedings.spiedigitallibrary.org/proceeding.aspx?doi=10.1117/12.587105><http://proceedings.spiedigitallibrary.org/proceeding.aspx?doi=10.1117/12.587105>
- [2] J. Lukáš, J. Fridrich, M. Goljan, Detecting digital image forgeries using sensor pattern noise, in: E. J. Delp III, P. W. Wong (Eds.), *Proceedings of SPIE: Image and Video Communications and Processing*, Vol. 5685, 2006, p. 60720Y. doi:10.1117/12.640109.
URL <http://proceedings.spiedigitallibrary.org/proceeding.aspx?articleid=1319409><https://doi.org/10.1117/12.640109><http://proceedings.spiedigitallibrary.org/proceeding.aspx?doi=10.1117/12.640109>
- [3] J. Lukáš, J. Fridrich, M. Goljan, Detecting digital image forgeries using sensor pattern noise, in: *Proc.SPIE*, Vol. 6072, 2006, pp. 6072 – 6072 – 11. doi:10.1117/12.640109.
URL <https://doi.org/10.1117/12.640109>
- [4] J. Lukáš, J. Fridrich, M. Goljan, Digital Camera Identification From Sensor Pattern Noise, *IEEE Transactions on Information Forensics and Security* 1 (2) (2006) 205–214. doi:10.1109/TIFS.2006.873602.
URL http://ieeexplore.ieee.org/xpls/abs/_all.jsp?arnumber=1634362<http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1634362><http://ieeexplore.ieee.org/document/1634362/>

- [5] M. Goljan, M. Chen, J. Fridrich, Identifying Common Source Digital Camera from Image Pairs, in: 2007 IEEE International Conference on Image Processing, no. 1, IEEE, 2007, pp. VI – 125–VI – 128. doi:10.1109/ICIP.2007.4379537.
URL <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4379537><http://ieeexplore.ieee.org/document/4379537/>
- [6] M. Goljan, J. Fridrich, T. Filler, Large scale test of sensor fingerprint camera identification, in: E. J. Delp III, J. Dittmann, N. D. Memon, P. W. Wong (Eds.), Proceedings of SPIE, no. 607, International Society for Optics and Photonics, SPIE, 2009, p. 72540I. doi:10.1117/12.805701.
URL <http://proceedings.spiedigitallibrary.org/data/Conferences/SPIEP/17750/72540I{ }1.pdf><https://proceedings.spiedigitallibrary.org/proceeding.aspx?doi=10.1117/12.805701><http://proceedings.spiedigitallibrary.org/proceeding.aspx?doi=10.1117/12.805701>
- [7] M. Goljan, J. Fridrich, Sensor-fingerprint based identification of images corrected for lens distortion, in: Media Watermarking, Security, and Forensics 2012, Vol. 8303, International Society for Optics and Photonics, 2012, p. 83030H.
URL <https://doi.org/10.1117/12.909659>
- [8] T. Gloe, S. Pfennig, M. Kirchner, Unexpected artefacts in PRNU-based camera identification, in: Proceedings of the on Multimedia and security - MM&Sec '12, MM&Sec '12, ACM Press, New York, New York, USA, 2012, p. 109. doi:10.1145/2361407.2361426.
URL <http://doi.acm.org/10.1145/2361407.2361426><http://dl.acm.org/citation.cfm?doid=2361407.2361426>
- [9] D. Valsesia, G. Coluccia, T. Bianchi, E. Magli, User authentication via prnu-based physical unclonable functions, Trans. Info. For. Sec. 12 (8) (2017) 1941–1956. doi:10.1109/TIFS.2017.2697402.
- [10] M. Goljan, J. Fridrich, Sensor fingerprint digests for fast camera identification from geometrically distorted images, in: A. M. Alattar, N. D. Memon, C. D. Heitzenrater (Eds.), Proc. SPIE 8665, Media Watermarking, Security, and Forensics 2013, 86650B (22 March 2013), Vol. 8665, 2013, p. 86650B. doi:10.1117/12.2003234.
URL <http://ws2.binghamton.edu/fridrich/Research/fingerprint-resynchronization{ }v2.pdf><http://proceedings.spiedigitallibrary.org/proceeding.aspx?doi=10.1117/12.2003234>
- [11] S. Bayram, H. T. Sencar, N. Memon, Efficient Sensor Fingerprint Matching Through Fingerprint Binarization, IEEE Transactions on Information Forensics and Security 7 (4) (2012) 1404–1413. doi:10.1109/TIFS.2012.2192272.
URL <http://ieeexplore.ieee.org/document/6175945/>

- [12] S. Taspinar, H. T. Sencar, S. Bayram, N. Memon, Fast camera fingerprint matching in very large databases, in: Proceedings - International Conference on Image Processing, ICIP, Vol. 2017-Septe, IEEE, 2018, pp. 4088–4092. doi:10.1109/ICIP.2017.8297051.
URL <http://ieeexplore.ieee.org/document/8297051/>
- [13] M. Goljan, J. Fridrich, M. Chen, Defending Against Fingerprint-Copy Attack in Sensor-Based Camera Identification, IEEE Transactions on Information Forensics and Security 6 (1) (2011) 227–236. doi:10.1109/TIFS.2010.2099220.
URL <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5667057><http://ieeexplore.ieee.org/document/5667057/>
- [14] A. E. Dirik, A. Karaküçük, Forensic use of photo response non-uniformity of imaging sensors and a counter method, Optics Express 22 (1) (2014) 470. doi:10.1364/OE.22.000470.
URL <https://www.osapublishing.org/oe/abstract.cfm?uri=oe-22-1-470>
- [15] A. Karaküçük, A. E. Dirik, Adaptive photo-response non-uniformity noise removal against image source attribution, Digital Investigation 12 (2015) 66–76. doi:10.1016/j.diin.2015.01.017.
URL <http://dx.doi.org/10.1016/j.diin.2015.01.017><https://linkinghub.elsevier.com/retrieve/pii/S1742287615000183>
- [16] A. E. Dirik, H. T. Sencar, N. Memon, Analysis of Seam-Carving-Based Anonymization of Images Against PRNU Noise Pattern-Based Source Attribution, IEEE Transactions on Information Forensics and Security 9 (12) (2014) 2277–2290. doi:10.1109/TIFS.2014.2361200.
URL http://ieeexplore.ieee.org/xpls/abs/_all.jsp?arnumber=6914598<http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6914598>
- [17] A. Karaküçük, A. E. Dirik, H. T. Sencar, N. D. Memon, Recent advances in counter PRNU based source attribution and beyond, in: A. M. Alattar, N. D. Memon, C. D. Heitzenrater (Eds.), Proceedings of SPIE - The International Society for Optical Engineering, Vol. 9409, 2015, p. 94090N. doi:10.1117/12.2182458.
URL <http://proceedings.spiedigitallibrary.org/proceeding.aspx?doi=10.1117/12.2182458>
- [18] S. Taspinar, M. Mohanty, N. Memon, PRNU-Based Camera Attribution from Multiple Seam-Carved Images, IEEE Transactions on Information Forensics and Security 12 (12) (2017) 3065–3080. doi:10.1109/TIFS.2017.2737961.
URL <http://ieeexplore.ieee.org/document/8006244/>
- [19] J. Entrieri, M. Kirchner, Patch-Based Desynchronization of Digital Camera Sensor Fingerprints, in: Electronic Imaging, Media

- Watermarking, Security, and Forensics, Vol. 2016, 2016, pp. 1–9. doi:10.2352/ISSN.2470-1173.2016.8.MWSF-087.
 URL <http://www.ingentaconnect.com/content/10.2352/ISSN.2470-1173.2016.8.MWSF-087><http://ws.binghamton.edu/kirchner/papers/2016{ }EI{ }PM.pdf>
- [20] P. Korus, J. Huang, Multi-Scale Analysis Strategies in PRNU-Based Tampering Localization, IEEE Transactions on Information Forensics and Security 12 (4) (2017) 809–824. doi:10.1109/TIFS.2016.2636089.
- [21] P. Korus, J. Huang, Evaluation of random field models in multi-modal unsupervised tampering localization, in: 2016 IEEE International Workshop on Information Forensics and Security (WIFS), 2016, pp. 1–6. doi:10.1109/WIFS.2016.7823898.
- [22] M. Chen, J. Fridrich, M. Goljan, Digital imaging sensor identification (further study), in: A. J. e. a. Woods (Ed.), Proc. SPIE 6505, Security, Steganography, and Watermarking of Multimedia Contents IX, 2007, p. 65050P. doi:10.1117/12.703370.
 URL <http://spiedigitallibrary.org/proceeding.aspx?doi=10.1117/12.703370><http://proceedings.spiedigitallibrary.org/proceeding.aspx?doi=10.1117/12.703370>
- [23] M. Chen, J. Fridrich, M. Goljan, J. Lukáš, Source digital camcorder identification using sensor photo response non-uniformity, in: Electronic Imaging, Media Watermarking, Security, and Forensics, Vol. 6505, 2007, p. 65051G. doi:10.1117/12.696519.
 URL <http://dx.doi.org/10.1117/12.696519><http://proceedings.spiedigitallibrary.org/proceeding.aspx?doi=10.1117/12.696519>