View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Explore Bristol Research

Samaras, S., Mygdalis, V., & Pitas, I. (2017). Robustness in blind camera identification. In 2016 23rd International Conference on Pattern Recognition (ICPR 2016): Proceedings of a meeting held 4-8 December 2016, Cancun, Mexico. (pp. 3874-3879). Institute of Electrical and Electronics Engineers (IEEE). DOI: 10.1109/ICPR.2016.7900239

Peer reviewed version

Link to published version (if available):
10.1109/ICPR.2016.7900239

Link to publication record in Explore Bristol Research
PDF-document

This is the author accepted manuscript (AAM). The final published version (version of record) is available online via IEEE at http://ieeexplore.ieee.org/document/7900239/. Please refer to any applicable terms of use of the publisher.

University of Bristol - Explore Bristol Research

General rights

This document is made available in accordance with publisher policies. Please cite only the published version using the reference above. Full terms of use are available:
http://www.bristol.ac.uk/pure/about/ebr-terms.html

Robustness in Blind Camera Identification

Stamatis Samaras† , Vasilis Mygdalis† and Ioannis Pitas†⋆
†Department of Informatics, Aristotle University of Thessaloniki, Thessaloniki, 54124, Greece
⋆Department of Electrical and Electronic Engineering, University of Bristol, UK
Email: pitas@aiia.csd.auth.gr

***Abstract*—In this paper, we focus on studying the effects of various image operations on sensor fingerprint camera identification. It is known that artifacts in the image processing pipeline, such as pixel defects or unevenness of the responses in the CCD array as well black current noise leave telltale footprints. Nowadays, camera identification based on the analysis of these artifacts is a well established technology for linking an image to a specific camera. The sensor fingerprint is estimated from images taken from a device. A similarity measure is deployed in order to associate an image with the camera. However, when the images used in the sensor fingerprint estimation have been processed using e.g. gamma correction, contrast enhancement, histogram equalization or white balance, the properties of the detection statistic change, hence affecting fingerprint detection. In this paper we study this effect experimentally, towards quantifying the robustness of fingerprint detection in the presence of image processing operations.**

I. Introduction

Source camera identification is a well studied problem in digital forensics [1], [2] over the past decade in various domains. Most known applications are investigation, such as child pornography, image and video piracy or image authentication check (e.g. to detect malicious alterations of an image). Nowadays, digital images can be easily edited and manipulated with sophisticated tools (i.e., image processing tools) ,not only for malicious but also for artistic purposes. Since such tools are available to a cell phone such manipulations alter not only the perceived image content but also the embedded camera fingerprint. This creates a robustness challenge to standard source camera identification algorithms, such as [3], [4]. The vast majority of published work focuses on still image source identification and only a handful of papers analyze the effects of image alterations on its robustness [5], [6], [7]. The most common image alterations tackled by published work primarily focus on geometric translations such as rotation, zoom, crop and on JPEG compression. However, to the best of our knowledge, non of the published work have analyzed the alterations of telltale footprints, when the captured image have undergone image processing manipulations.

In this paper, we focus our study on image alterations that are commonly used to improve the quality content [8] (e.g. the low pass filter, contrast enhancement, histogram equalization, gamma correction and white balance). We address the robustness of source camera identification when the images taken by that camera have undergone image processing [8]. More specifically, we intend to determine the model and brand of a cell phone camera used in image acquisition in the presence of such image processing attacks. It works by first estimates the sensor fingerprint from a set of images positively known to have been taken by a particular camera. Once the fingerprint is acquired one can prove that a given image under investigation was taken by the exact same camera by using a signal detection approach. A positive match between an image and a camera fingerprint ties the image with a very high certainty to its source camera. Without loss of generality the experiments were conducted on cell phone cameras, due to their wide use in everyday life.

A standard sensor-based fingerprint identification method for camera brand and model identification is proposed by Lukas et al. [3]. The same methodology has been used in various related works [9],[1]. In July 2011 it passed the Daubert challenge [1] in the State of Alabama. That is, results of this method can be employed as evidence in court of law. By the term camera brand, we denote the camera manufacturer (e.g., Samsung or LG), and by the term model, we denote the unique product name. Fingerprint detection pinpointing the employed imaging sensor type and make is based on the telltale effects created within the proprietary image formation pipeline in cameras. Sensor fingerprints are essential artifacts due to charge couple device (CCD) sensor cell defects and minor make deviations from their standard type. That is, the fingerprint detection methodology is applicable to all digital image devices that contain CCD or CMOS sensors.

In this paper, we investigate the sensitivity of the identification performance against the aforementioned image manipulations. It is known that artifacts in the image processing pipeline, such as pixel defects or unevenness of the responses in the CCD array and black current noise leave telltale footprints. Nowadays, camera identification based on the analysis of these artifacts is a well established technology for linking an image to a specific camera. The sensor fingerprint is estimated from images taken from a device. A similarity measure is deployed in order to associate an image with the fingerprint when it exceeds a certain threshold. Moreover, the present study differs from previous camera identification methods, in terms of feature fusion.

The rest of this paper is organized as follows. Related work in source camera identification is revised in Section II. The technology behind sensor based fingerprint identification, is given in Section III. The details of the experiments and their results are provided in Section IV. In section V, we discuss future work and draw our conclusion.

[1] https://en.wikipedia.org/wiki/Daubert_standard

II. Overview of camera identification

Camera identification is a well established research area. A variety of methods have been proposed, primarily exploiting the residual artifacts and imperfections in the imaging pipeline. There are two separate camera identification methodologies according to the information source they use. The first one consists of methods which take advantage of existing sensor noise and artifacts in the CCD array [10]. The second one approaches camera identification by employing demosaicking artifacts taking place in raw image processing [11].

There have three leading studies on camera identification based on sensor noise. Geradts et al. [12] observed that large CCD arrays often contain a variety of manufacturing defects, which, in total, amount to fixed pattern noise. In addition, camera electronics generate random dark current [8]. They have observed that, while dark current has limited potential in building a forensic signature, the fixed pattern noise of the CCD array is instrumental in constructing a unique camera fingerprint. Kurosawa et al. [10] and Lukas et al.[3] also tuned their attention to the pattern noise of CCD arrays. It was found that the systematic part of the noise does not change much from image to image, it is relatively stable over camera life span and operating conditions and consists of the fixed pattern noise plus Photo Response Non Uniformity noise (PRNU) caused by the pixel non uniformities is a more persistent camera feature [13]. The PRNU can be reliably extracted by averaging the denoising residuals of several images [1] resulting in an image pattern that plays the role of a camera fingerprint. In this sense, camera identification has similarities to image watermarking [14], the difference being that the camera fingerprint is produced by the image sensors while the watermark is primarily inserted by deliberate human action.

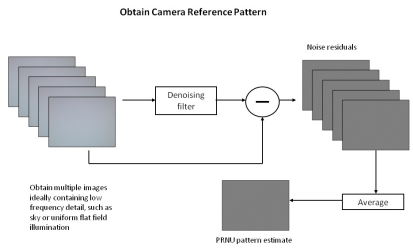
Commercial image devices use a single mosaic structured color filter array (CFA) rather than having separate filters for each color component. Camera models typically employ propriety interpolation algorithms in recreating the missing color values. The grid interpolation process, in turn, leaves footprints, such as correlation patterns between contiguous bit planes. Kharazzi et al. [4] tried to capture the differences in CFA configuration and color processing pipeline by a feature based approach. They focused on image features, such as mean value of the RGB channels, correlations between color components, differences in neighborhood probability distribution, wavelet domain statistics and image quality measures. Extensions of this work can be found in [15],[16]. Since the residuals of interpolation algorithms depend on the nature of the captured content, these algorithms were fine tuned by separately treating the smooth and non smooth image regions. In another study, Long and Huang used interpixel correlations originating from demosaicking camera fingerprinting [11]. They defined a quadratic pixel correlation model and obtained a coefficient matrix for each color band based on this model. Swaminathan et al. [17] investigated the demosaicking artifacts using an analysis by synthesis method. They divided the image into three regions based on gradient features in a local neighborhood and they estimated interpolation coefficients through Singular Value Decomposition (SVD) for each region and each color band separately. Then, they reinterpolated the sampled CFA pattern and chose the one that minimizes the difference between the estimated final image and actual image produced by the camera.

III. Camera sensor identification based on PRNU

The main artifact that is being used to estimate a sensor fingerprint for each camera is the so called Photo-Response Non-Uniformity (PRNU) [13]. Each pixel value generated from either CCD or CMOS sensors slightly but consistently differs from its nominal value. This forms a specific pattern on every image taken by this camera and is known to be unique for every camera model. A camera fingerprint is generated by images known to have been taken by this camera. Once estimated, it can be tested whether it resides on an image and thus tell if it was taken using this specific camera.

The estimation method of the PRNU fingerprint can be seen in Figure 1. Analytic description of the PRNU estimation model is given bellow.

Fig. 1. Estimation of the PRNU fingerprint



Let us assume that the output image will be denoted as $\mathbf{I}$ and the image captured under the absence of any imperfections as $\mathbf{I}_0$. The following sensor output model was established in [3].

$$\mathbf{f} = \mathbf{f}_0 + \mathbf{f}_0\mathbf{K} + \mathbf{v} \tag{1}$$

where $\mathbf{K}$ is the PNRU factor (fingerprint) and $\mathbf{v}$ includes all other components, such as dark current, shot noise, read-out noise and quantization noise. The fingerprint $\mathbf{K}$ can be estimated from N images $\mathbf{f}_1, \mathbf{f}_2, \ldots, \mathbf{f}_N$ taken by the camera and $\mathbf{f}_0\mathbf{K}$ is understood element wise. The pixel intensity of the i, j-th pixel in the kth image $\mathbf{f}_k$ will be denoted $I_{ijk}, 1 \leq i \leq k_1, 1 \leq j \leq k_2$. Let $\mathbf{W}_1, \mathbf{W}_2, \ldots, \mathbf{W}_N$ be the noise residuals obtained using a denoising filter F as

$$\mathbf{W}_k = \mathbf{f}_k - F(\mathbf{f}_k), k = 1, \ldots, N \tag{2}$$

Assuming the following linearized sensor model for the residual

$$\mathbf{W}_k = \mathbf{f}_k\mathbf{K} + \mathbf{\Xi}_k, k = 1, \ldots, N \tag{3}$$

where $\mathbf{\Xi}_k$ is a $n_1 \times n_2$ matrix of independent and identically distributed (i.i.d.) Gaussian random variables with zero mean, the maximum likelihood estimation of the PNRU multiplicative factor $\mathbf{K}$ is given by :

$$\widehat{\mathbf{K}} = \frac{\sum_{k=1}^{N} \mathbf{f}_k \mathbf{W}_k}{\sum_{k=1}^{N} (\mathbf{f}_k)} \tag{4}$$

The detection of the fingerprint $\mathbf{K}$ in $\mathbf{W}$ can be formulated as a two channel hypothesis testing problem:

$$\begin{aligned} H_0(\text{non matching image}) &: \mathbf{K_1} \neq \mathbf{K_2} \\ H_1(\text{matching image}) &: \mathbf{K_1} = \mathbf{K_2}, \end{aligned} \tag{5}$$

where:

$$\begin{aligned} \widehat{\mathbf{K}}_1 &= \mathbf{K}_1 + \mathbf{\Xi}_1 \\ \mathbf{W} &= \mathbf{I}\mathbf{K}_2 + \mathbf{\Xi}_2, \end{aligned} \tag{6}$$

where the estimate of the camera fingerprint, $\widehat{\mathbf{K}}_1$, is obtained using (4), $\mathbf{W}$ is the noise residual and a Gaussian corrupting noise $\mathbf{\Xi}_{1,2} \sim \mathcal{N}(\mu, \sigma^2_{\Xi})$. A good approximation to the generalized likelihood ratio test for the aforementioned hypothesis testing problem is the normalized correlation $\rho(\widehat{\mathbf{K}}_1, \widehat{\mathbf{K}}_2; 0, 0)$ between $\widehat{\mathbf{K}}_1$ and $\widehat{\mathbf{K}}_2$:

$$\rho(\mathbf{U}, \mathbf{V}; \tau_1, \tau_2) = \frac{\sum_{i,j}(U_{i,j} - \overline{\mathbf{U}})(V_{i+\tau_1, j+\tau_2} - \overline{\mathbf{V}})}{\sqrt{\sum_{i,j}(U_{i,j} - \overline{\mathbf{U}})^2}\sqrt{\sum_{i,j}(V_{i+\tau_1, j+\tau_2} - \overline{\mathbf{V}})^2}} \tag{7}$$

where the bar stands for the sample mean, vectors $\mathbf{U}$ and $\mathbf{V}$ could be any matrices like the fingerprint estimation $\widehat{\mathbf{K}}$ and the query fingerprint $\mathbf{K}$, range of indices i, j, τ_1, τ_2 in 7 is $1 \leq i, \tau_1 \leq n_1, 1 \leq j, \tau_2 \leq n_2$.

Note that under H_0, we correlate two i.i.d. Gaussian signals since the fingerprint itself is well modeled by an i.i.d. Gaussian random variable. It can be established from the central limit theorem that in this case $\rho(\widehat{\mathbf{K}}_1, \widehat{\mathbf{K}}_2; 0, 0) \sim \mathcal{N}(0, \frac{1}{N})$. Thus, in order to set a fixed threshold for the correlation that guarantees a prescribed false alarm of fingerprint detection, it must be scaled by $\sqrt{N}$:

$$\rho(\mathbf{K}, \widehat{\mathbf{K}}; 0, 0) \rightarrow \sqrt{N}\rho(\mathbf{K}, \widehat{\mathbf{K}}; 0, 0) \tag{8}$$

A frequently used detection statistic is the Peak Correlation to Energy ratio (PCE) or signed (PCE) also referred to as the Circular Correlation Norm (CCN) defined as:

$$PCE(\mathbf{K}, \widehat{\mathbf{K}}) = \frac{\rho^2(\mathbf{K}, \widehat{\mathbf{K}}; 0, 0) \times sign(\rho(\mathbf{K}, \widehat{\mathbf{K}}; 0, 0))}{\frac{1}{n_1 n_2 - |\mathcal{N}_{max}|} \sum_{\tau_1, \tau_2 \notin \mathcal{N}_{max}} \rho^2(\mathbf{K}, \widehat{\mathbf{K}}; \tau_1, \tau_2)} \tag{9}$$

where $\mathcal{N}_{max}$ is a small neighborhood around the origin and $|\mathcal{N}_{max}|$ is the number of elements in the neighborhood. Note that the PCE can be viewed as another way to normalize the correlation - the denominator is an estimate of the correlation variance under the assumption that it has a zero mean.

The case when H_1 is rejected for an image that was captured from the original camera that is tested is called false rejection. False acceptance means accepting H_1 when the image was taken by another camera. We donote the false rejection rate FRR and the false alarm rate FAR. The FRR is obtained from experiments and depends mainly on image quality and content and the number of images used to obtain the PRNU fingerprint and their quality. Both FAR and FRR are functions of the detection threshold.

IV. Experimental results

In this section, we present the conducted experiments in order to evaluate the robustness of image processing manipulations (i.e., image filtering). To this end, we have employed a publicly available camera cell phone identification dataset. Detailed description of this dataset is found in IV-A. In subsection IV-C, we study the effect of different training set sizes employed to obtain the PRNU factor. Finally, in subsection IV-D, we evaluate the performance of state-of-the art blind camera identification methods in manipulated images.

A. Evaluation Dataset

The employed dataset is the BUSIM cell phone database [2]. This datasets consists of images captured from 16 models of different cell phone cameras. There are six brands among those 16 devices which are Motorola, Nokia, Samsung, Sony, Treo Palmone and LG. In fact, we have two Motorola models, five Nokia, three Samsung, three Sony and one of Treo Palmone and LG models. The camera models are listed in Table I,.

TABLE I
Models of cameras tested

LG 5600	Samsung D500
Motorola V3	Samsung D600
Motorola V500	Samsung E720
Nokia 5140	Sony K700
Nokia 6230	Sony K700
Nokia 6600	Sony K750
Nokia 6600	Sony P910
Nokia 7270	Treo Palmone

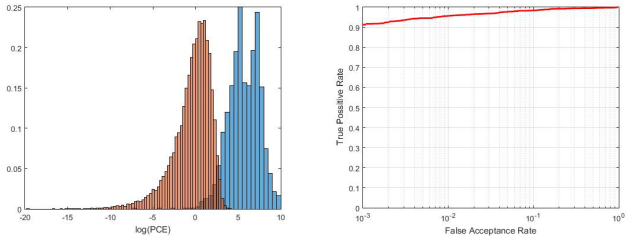
The dataset consists of 200 images with each device, a total of 3200 images, with a maximum resolution of 640×480 at daylight, auto-focus mode and in JPEG format. The images were typical shots varying from nature scenes to closeup of people. We have separated 100 of them in two groups so as to have a training and a testing set. For every experiment a different set is created, with the exception of same type studies, such as feature fusion (Figures 2 and 3), where the aim is to examine the effect of a different approach on the same data. The split of 1600 images used for training and testing happens each time independently making sure that there are no duplicate images in both training and testing set.

B. Feature fusion

In our first set of experiments, we compare two late fusion models for camera identification. The camera identification

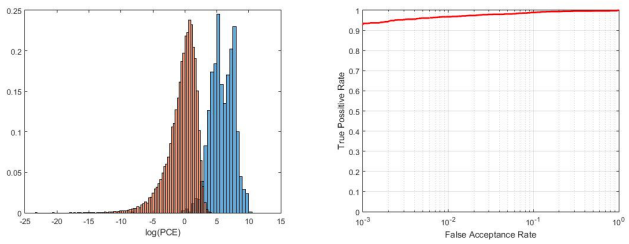
method proposed in Lukas et. al [3] suggests the use of pixel luminosities in the RBG channel, followed by a late fusion approach. That is, we follow the denoinsing and the averaging of the fingerprints with RGB to grayscale transform and work with their grayscale versions to compute the PCEs for H_0 and H_1. The results of this method are presented on Figure 2 where we have the histograms of the logarithm of the PCE values on the left and their ROC curves on the right. Its clear from the ROC that the camera identification works fine with this method and we can find a threshold t where the overall accuracy will be higher than 95% with relatively small FAR rate.

Fig. 2. Camera identification with RGB to grayscale late feature fusion



Furthermore, we explore a different feature fusion method, which we have found that improves the accuracy of the classifier. That is, after the denoising and the averaging of the fingerprints, we concatenate each color channel one after the other to create a vector of size 1440×640. This vector is thereby employed to compute the PCE for H_0 and H_1. The results of this late fusion method are shown on Figure 3.

Fig. 3. Camera identification with concatenated color channels late feature fusion



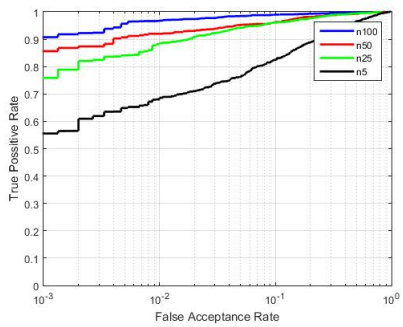
C. Number of images used to obtain PRNU factor

In our second set of experiments, we study the effect of different number of images used to obtain the PRNU factor. In order to generate the reference pattern, we employ the denoised training set. To this end, we employed the same Wavelet-based denoising filter by Mihkac et al. [18], that Lucas et al.[3] proposed in their initial presentation of the sensor fingerprint method. The PRNU pattern estimate is found by averaging the noise residuals of the training set. Once the reference pattern has been determined, it can be used to identify whether the camera used to generate the reference pattern was also used to capture a given query image. The noise residual of the query image is obtained and correlated with the reference PRNU pattern of each of the known cameras. If the correlation is greater than a given threshold t, the query image is classified to camera class with the most similar PRNU pattern. Otherwise, it is considered that the image was taken from another camera.

In order to measure the similarity between the fingerprint and the image query, we employ PCE metric. The PCE is a more stable test statistic than correlation as it is independent of the image size and has other advantages. We introduced on how PCE is obtained on (9) and we used $\mathcal{N}_{max}$ to be a square region 11×11 around the peak where the maximum of the normalized correlation exists. For each camera fingerprint we evaluate PCE under H_1 for the remaining matching images of the test set which will provide the data needed for estimating the FRR. Similarly we evaluate PCE under H_0 for all the non-matching images of the test set to obtain the FAR. The PCE histograms for each hypothesis differ greatly in size. For H_1 we have a total of 1600 PCE values, while all the non matching cases of H_0 produce 24000 PCE scores. Those numbers stand for every experiment that follows.

The sensor fingerprint is estimated with real content images rather than flat fields. Previous works propose flat fields for better results. To generate the reference pattern, a set of flat field images are first created by capturing between 20 and 50 images of a uniformly lit surface using a known camera. For example, out of focus images of a bright cloudy sky can be used. However, experiments show that real content images can perform as good as long as there are enough of them to draw a better estimate. We have tested the performance for different training set size that range from $n = 5$ to $n = 100$ images. The collective ROC curves for each set are depicted in Figure 4.

Fig. 4. Different number of training image sets and their ROC curves



As can be seen, when real content images are employed instead of flat fields, values of $n = 20$ or $n = 50$ are not enough to provide a good estimation of the PRNU factor. Instead, values of $n = 100$ should be employed. When the content of the images is not flat field then a greater number of images is required to achieve better results and higher accuracies.

D. Camera classification under image manipulations

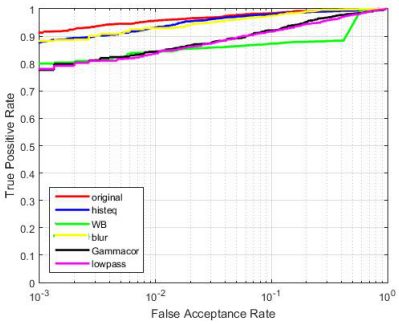
Finally, we study the effects of image manipulations in camera classification. There are instances where the images

presented to a camera identifier are manipulated with malicious or innocent intent. We have subjected our images under the effects of low pass filter, contrast enhancement, histogram equalization, gamma correction and white balance. Note that we have not gone too far with the manipulations and every attack is a subtle one (3×3 filters, small gamma correction factors, etc.). We aim to produce results that can relate to real life scenarios where either the attacker has a malicious intent and wants to counterfeit an original photo or he simply puts every image he captures under a desired filter for improving the content of his image.

Some cases of manipulations such as histogram equalization and white balance are applied with the same effect on all images. While, the cases of low pass Gaussian and blur filter as well as gamma correction have varying parameters on all images. Such as 3×3 and 5×5 filters changing randomly for blur and low pass Gaussian, and gamma correction factor varying from $\gamma \in [1.5, 3]$.

We have conducted two classification experiments according to the aforementioned scenarios. In the first experiment, we have put both the training set and the testing set under the effect of the same manipulations. That is, we employed $n = 100$ training images for each camera. This is the scenario were we assume that all images might be subject of prior manipulation, e.g., low-pass filter. The results for every filter are presented collectively with their ROC curves on Figure 5.

Fig. 5. ROC curve of the "innocent" image manipulations scenario, i.e., both the training set and the testing set are under the effect of the same manipulations.



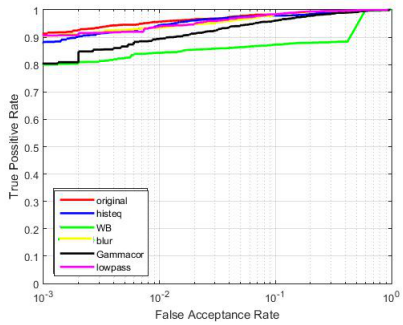
In our second scenario, the training set is not manipulated with any filter. However, we assume that only the test set have gone under image processing manipulations. This is the scenario that relates to the malicious intent. The collective results of this scenario are shown on Figure 6.

As can be seen, prior image manipulation of the training set does not affect the performance of camera de-identification. In all cases, the most effective filter for camera de-identification is the White Balance filter as well as the low pass and blur filters but this is mainly because of the 5×5 filters which are known to leave a visual impact on the image.

E. Camera classification under JPEG compression

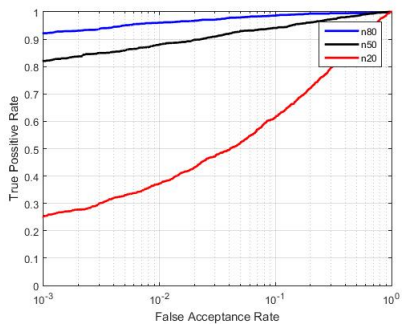
Cell phone images can be highly compressed, hence the effect of compression is studied. JPEG compression is an important factor in determining the robustness of fingerprint, since performance of fingerprint extraction algorithm degrades due to compression. We have subjected our images under the effects of JPEG compression with varying quality factors. The quality factor of the JPEG algorithm is instrumental in the accuracy of the camera identification algorithm. We have produced results with three different values of quality, $q = 20, 50, 80$. Quality factor values close to 100 mean almost no effect to the original image. The same factor is applied throughout all images.

Fig. 6. ROC curve of the "malicious" image manipulations scenario, i.e., only the test set have gone under image processing manipulations.



Once again, two classification experiments are conducted. First, both the training and testing set are under the effects of JPEG compression. The collective results of this scenario for three different quality factor values are presented on Figure 7.

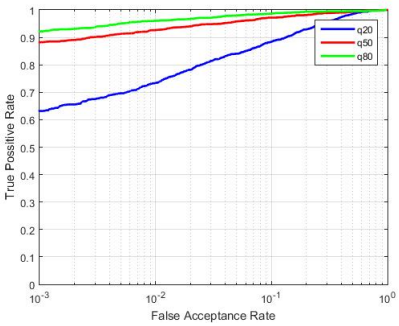
Fig. 7. ROC of JPEG compression on both sets



In the second scenario, the training set does not go under JPEG compression, having only the training set under the alteration. The results of this experiment are shown on Figure 8.

It can be seen that JPEG compression can affect the identification algorithm especially when the quality factor is low and the compression algorithm is used on both the images that were used for the camera fingerprint estimation as well as the query image. However, we should also note that when JPEG compression quality factor $q = 20$ is employed, the resulting image is visibly altered.

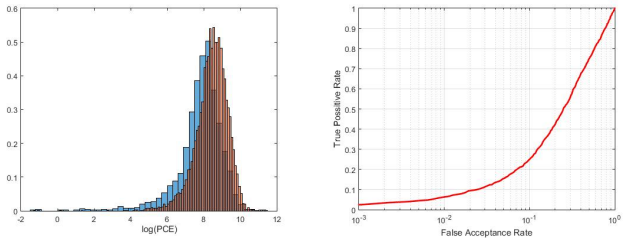
Fig. 8. ROC of JPEG compression on both sets



F. Camera de-identification by fingerprint removal

Finally, we investigate the scenario where the malicious user intents to employ the PRNU factor from a set of images of his own camera, and employ post-processing to remove it. In this scenario, we have created a training set of $n = 100$ real life images and estimated the PRNU factor for every camera model. Afterwards, the estimated PRNU factor is subtracted from the test set. Experimental results are shown in Figure 9. As can be seen, effective camera de-identification can be obtained, which should be alarming to forensics investigators.

Fig. 9. Camera identification with fingerprint removed from testing images



V. Conclusion

In this paper, we have presented a detailed study on camera identification, on images manipulated by standard image processing application. Experimental results have shown that the camera identification is still possible when specific filtering applications have been applied. However, legal authorities should be alarmed when advanced PRNU related manipulations have been applied, which is not visible to the human eye. Future work could include further evaluation in larger datasets, as well as more detailed experimental analysis.

Acknowledgment

The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement number 316564 (IMPART) and grant agreement number 287674 (3DTVS).

References

[1] T. M. Goljan and J. Fridrich, "Large scale test of sensor fingerprint camera identification," *Electronic Imaging, Media Forensics and Security (SPIE)*, vol. 12.

[2] O. Çeliktutan, B. Sankur, and I. Avcibas, "Blind identification of source cell-phone model," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 3, pp. 553–566, 2008.

[3] J. F. J. Lucas and M. Goljan, "Digital camera identification from sensor noise," *IEEE Transactions on Information Security and Forensics*, vol. 1, no. 2, pp. 205–214, 2006.

[4] M. Kharrazi, H. T. Sencar, and N. Memon, "Blind source camera identification," in *Image Processing, 2004. ICIP'04. 2004 International Conference on*, vol. 1. IEEE, 2004, pp. 709–712.

[5] M. Goljan and J. Fridrich, "Camera identification from scaled and cropped images," *Security, Forensics, Steganography, and Watermarking of Multimedia Contents X*, vol. 6819, p. 68190E, 2008.

[6] M. Goljan, J. Fridrich, and M. Chen, "Defending against fingerprint-copy attack in sensor-based camera identification," *Information Forensics and Security, IEEE Transactions on*, vol. 6, no. 1, pp. 227–236, 2011.

[7] M. Goljan and J. Fridrich, "Sensor fingerprint digests for fast camera identification from geometrically distorted images," in *IS&T/SPIE Electronic Imaging*. International Society for Optics and Photonics, 2013, pp. 86 650B–86 650B.

[8] I. Pitas, *Digital image processing algorithms and applications*. John Wiley & Sons, 2000.

[9] M. C. M. Goljan and P. Comesana, "Effect of compression on sensor-fingerprint based camera identification," *IS&T, Electronic Imaging, Media Watermarking Security, and Forensics*, 2016.

[10] K. Kurosawa, K. Kuroki, and N. Saitoh, "Ccd fingerprint method-identification of a video camera from videotaped images," in *Image Processing, 1999. ICIP 99. Proceedings. 1999 International Conference on*, vol. 3. IEEE, 1999, pp. 537–540.

[11] Y. Long and Y. Huang, "Image based source camera identification using demosaicking," in *2006 IEEE Workshop on Multimedia Signal Processing*, 2006.

[12] Z. J. Geradts, J. Bijhold, M. Kieft, K. Kurosawa, K. Kuroki, and N. Saitoh, "Methods for identification of images acquired with digital cameras," in *Enabling Technologies for Law Enforcement*. International Society for Optics and Photonics, 2001, pp. 505–512.

[13] M. Chen, J. Fridrich, M. Goljan, and J. Lukáš, "Source digital camcorder identification using sensor photo response non-uniformity," in *Electronic Imaging 2007*. International Society for Optics and Photonics, 2007, pp. 65 051G–65 051G.

[14] N. Nikolaidis and I. Pitas, "Robust image watermarking in the spatial domain," *Signal processing*, vol. 66, no. 3, pp. 385–403, 1998.

[15] S. Bayram, İ. Avcıbaş, B. Sankur, and N. Memon, "Image manipulation detection," *Journal of Electronic Imaging*, vol. 15, no. 4, pp. 041 102–041 102, 2006.

[16] S. Bayram, H. T. Sencar, N. Memon, and I. Avcibas, "Improvements on source camera-model identification based on cfa interpolation," *Proc. of WG*, vol. 11, pp. 24–27, 2006.

[17] A. Swaminathan, M. Wu, and K. Liu, "Nonintrusive component forensics of visual sensors using output images," *Information Forensics and Security, IEEE Transactions on*, vol. 2, no. 1, pp. 91–106, 2007.

[18] K. I. Mihcak M.K. and R. K., "Spatially adaptive statistical modeling of wavelet image coefficients and its application to denoising," *IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASPP)*, vol. 6.