A Novel Method for Identifying Exact Sensor Using Multiplicative Noise Component

Babak Mahdian and Stanislav Saic
Institute of Information Theory and Automation
Academy of Sciences of the Czech Republic
Prague, Czech Republic
{*mahdian,ssaic*}*@utia.cas.cz*

***Abstract*—In this paper, we analyze and analytically describe the multiplicative deterministic noise component of imaging sensors in a novel way. Specifically, we show how to use the multiplicative nature of this component to derive a method enabling its estimation. Since this noise component is unique per sensor, consequently, the derived method is applied on digital image ballistics tasks in order to pinpoint the exact device that created a specific digital photo. Moreover, we enhance the method to be resistent to optical zoom and JPEG compression.**

***Keywords*-Image forensics; image ballistics; source camera identification; Photo Response Non Uniformity; PRNU;**

I. Introduction

Generally, there are two essential tasks in forensics analysis of digital images: integrity verification (genuineness analysis) and image ballistics. In image ballistics we address the problem of linking digital images under investigation to either a group of possible source imaging devices or to one particular source imaging device which has been used to capture these photos. The latter one is the main topic of this paper.

Since image ballistics makes possible to differentiate between source cameras of the same make and model, it became especially useful in the forensic, law enforcement, insurance, and media industries. Insurance companies, for example, often need to know whether or not claim-substantiating photos were taken by the person looking for compensation. Law enforcement agencies are also tasked with finding the source camera when criminal activity is discovered in digital images (e.g. child pornography, etc).

Although past research were mainly focused on data hiding and digital watermarking approaches [1], [2], [3] to carry out digital image integrity verification and image ballistics, today there is a relatively new approach called passive one which does not need embedding any secondary data into the image. So, in contrast to active methods, the passive approach does not need any prior information about the image being analyzed. There have been methods developed to detect image splicing [4], [5], traces of non-consistencies in color filter array interpolation [6], traces of geometric transformations, [7], cloning [8], computer graphics generated photos [9], JPEG compression inconsistencies [10], etc. Typically, pointed out methods are based on the fact that digital image editing brings specific detectable statistical changes into the image.

Our aim in this paper is to uncover some important drawbacks of existing source identification methods and analytically develop a novel way to identify particular source cameras by employing their sensor properties [11], [12], [13]. Specifically, we will use the multiplicative nature of PRNU noise component present in digital images. Moreover, we also will deal with artifacts brought into the image by vignetting and JPEG. Effectiveness of proposed analytical concept will be experimentally measured and compared to state-of-the-art.

II. Fingerprints of Different Camera Components

A typical camera consists of several different components (see Fig. 1). As pointed out in [14], the core of every digital camera is the imaging sensor. The sensor (typically, CCD or CMOS) is consisted on small elements called pixels that collect photons and covert them into voltages that are subsequently sampled to a digital signal in an A/D converter. Generally, before the light from the scene which is being photographed reaches the sensor it also passes through the camera lenses, an antialiasing (blurring) filter, and then through a color filter array (CFA).

The CFA is a mosaic of tiny color filters placed over the pixel of an image sensor to capture color information. Color filters are needed because typical consumer cameras only have one sensor which cannot separate color information. The color filters filter the light by wavelength range, such that the separate filtered intensities include information about the color of light. Most commonly, Bayer color filter is used. Here, each pixel captures intensity of one of the red, green, or blue color information. This output is further interpolated (demosaicked) using color interpolation algorithms to obtain all three basic color channels for each pixel.

The resulting signal is then further processed using color correction and white balance adjustment. Additional processing includes gamma correction to adjust for the linear response of the imaging sensor, noise reduction, and filtering operations to visually enhance the final image. Finally, the digital image might be compressed stored and stored in a specific image format like JPEG.

978-0-7695-5140-1/13 $26.00 © 2013 IEEE
DOI 10.1109/ISM.2013.46

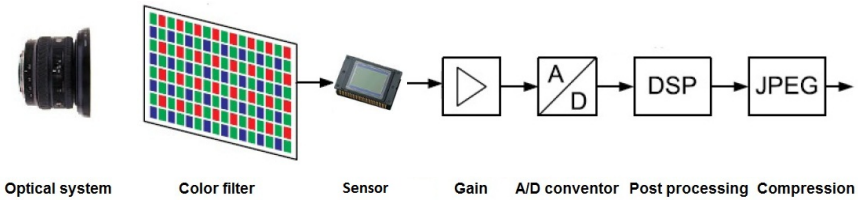

Figure 1. A typical digital camera system.

What is important in sense of forensic analyzes of digital images is that different components of camera leave different kind of artifacts or fingerprints useful for integrity verification of photos or ballistic analysis. Typically, fingerprints left by CFA, post processing, and compression parts are in common for cameras of same make and model. In other words, assuming that we know their value and behavior for a particular camera make and model and based on the fact that digital image editing (e.g., photoshopping) change these values (fingerprints), they can be employed for verification of the originality of digital images .

On the other hand, each camera has its own unique sensor which consists of millions of pixels each of unique properties. Thus, if we are able to find such an information brought into image by the sensor and which will remain stable and present in all images captured by that sensor and cannot be fount in no image captured by any other sensor, then we can call it fingerprint of that sensor or camera. Such a fingerprint can be employed to link digital images to particular digital cameras which captured them.

A. Sensor as a Camera Fingerprint

Image sensors suffer from several fundamental and technology related imperfections resulting in their performance limitations and noise. As pointed out in [14], if we take a picture of an absolutely evenly lit scene, the resulting digital image will still exhibit small changes in intensity among individual pixels which is partly because of pattern noise, readout noise or shot noise.

While readout noise or shot noise are random components, the pattern noise is deterministic and remain approximately the same if multiple pictures of the same scene are taken. As a result, pattern noise can be the fingerprint of sensors which we are searching for.

Pattern Noise (PN) is consisted of two components called Fixed Pattern Noise (FPN) and photo response nonuniformity (PRNU). FPN is independent of pixel signal, it is an additive noise, and some high-end consumer cameras can suppress it. The FPN also depends on exposure and temperature.

PRNU is formed by varying pixel dimensions and inhomogeneities in silicon resulting in pixel output variations. It is a multiplicative noise. Moreover, it is not dependent on temperature and seems to be stable over time.

The values of PRNU noise increases with the signal level (it is more visible in pixels showing light scenes). In other words, in very dark areas PRNU noise is suppressed. Moreover, PRNU is not present in completely saturated areas of an image. Thus, such images should be ignored when searching for PRNU noise.

Despite the fact that there are not a lot of studies analyzing the PRNU noise in deeper details (probably due to physical limitations and no significant demand for it so far), it can be shown that it has dominant presence in the pattern noise component. This made possible for Fridrich et al. [15], [11] to employ PRNU noise to identify source cameras. In other words, PRNU noise is employed as the fingerprint of camera sensors.

III. Motivation

Generally, it can be claimed that state-of-the-art source identification methods are mostly based on methods proposed by Jessica Fridrich et al. (e.g., [15], [11], [16], [17]). There have been published some additional papers by others (e.g., [18], [19], [20], [21], [22]) aiming to improve accuracy of results. Generally, they brought modifications to the original paper of Jessica Fridrich et al. [15], [11] based on theoretical or empirical findings. Nonetheless, the key concept of how to measure sensor's fingerprint remained unchanged.

Having available a larger set of cameras of same and different models and a large set of ground-truth digital images captured by these devices, one can simply run an experiment to analyze the effectiveness and fragileness of existing methods. By performing such an experiment, it is quite easy to notice that state-of-the-art source identification methods suffer from a number of essential non–perfections. Below we discuss two important drawbacks specifically caused by optical zoom and JPEG.

1) Impact of optical zoom: When applying typical PRNU-based camera identification methods (e.g., [15], [11]) on digital images acquired by cameras enabling rich optical zoom operations, then they typically fail. Let us demonstrate the problem by carrying out a simple experiment by employing Fujifilm FinePix S100fs camera. The focal length of this camera can be changed from 28 mm to 400 mm. We captured 50 images of blue skye for each of the following focal lengths $Z \in \{28, 50, 100, 200, 400\}$ and used them

to calculate camera sensor's fingerprint using the algorithm pointed out in [11]. In other words, 5 different fingerprints of the same camera have been obtained. Moreover, we took 5 images of a natural scene for each of mentioned focal lengths to carry a basic source identification task.

Figure 2 demonstrates results of 25 test images and 5 fingerprints. First image shown in Figure 2 demonstrates results of analyzing test images with sensor fingerprint of Fujifilm FinePix S100fs obtained by photos captured with focal length of 28 mm. Five test images captured by the same focal length exhibit high correlations (in other words, source camera has been found correctly). Nonetheless, all other test images captured by the same camera but different focal lengths exhibited very low correlations (in other words, source camera has not been identified). Second image shown in Figure 2 shows result of testing test images with sensor fingerprint obtained by photos captured with focal length of 50 mm. Five test images captured by the same the focal length exhibit high correlation. Again, all other test images failed. Other images shown in Figure 2 uncovers the same problem under scenarios of using other focal lengths in Z.

We also carried out the same experiment with other cameras such as Nikon Coolpix L23, Canon PowerShot A495, Pentax Optio P80, etc. with very similar results. Apparently, this is a serious drawback as it is very difficult to create a stable fingerprint for a cameras having rich focal length. To cover all focal lengths, one should create one fingerprint per each available focal length which is very time consuming and almost impossible in real-life applications.

The question is why this problem happens? The reason behind this is, so called, vignetting which causes change of PRNU values at different zoom levels. There are several types of vignetting such as mechanical, optical, natural or pixel vignetting [23]. Some types of vignetting can be completely covered by lens settings (using special filters), but most digital cameras use built-in image processing to compensate with vignetting when converting raw sensor data to standard image formats such as JPEG or TIFF. Typically, vignetting is stronger at the non-central parts of the photo.

2) Impact of JPEG: Assume we have a digital camera producing heavily compressed JPEG images (or digital images on Internet). As it is known, highly JPEG compressed images exhibit blocking artifacts. Figure 3 provides a simple example of blocking artifact. Here, first 8 rows and 9 columns of a same photo compressed with different JPEG qualities is shown. As apparent, absolute difference between boundary pixels (pixels at 8th and 9th column) of (a) is 0. Same for (b) is 6. and for (c) is 14. These JPEG blocking artifacts can be in common within various digital images captured by different devices. In other words, this is a dangerous source of false positive results when linking a photo to a set of possible source cameras (existing source identification results are based on measuring correlation between tested image and camera). Moreover, this is a quite common problem occurred in real-life applications (for example, when inspecting Facebook photos or Youtube videos).

To understand why blocking artifacts occur, we need to understand how JPEG algorithm does work. Although JPEG file can be encoded in various ways, the most common algorithm is the following one.

Typically, the image is first converted from RGB to YCbCr, consisting of one luminance component (Y), and two chrominance components (Cb and Cr). Mostly, the resolution of the chroma components are reduced, usually by a factor of two. Then each component is split into adjacent blocks of 8×8 pixels. Block values are shifted from unsigned to signed integers. Each block of each of the Y, Cb, and Cr components undergoes a discrete cosine transform (DCT). Let $f(x, y)$ denote a pixel (x, y) of an 8×8 block. Its DCT is:

$$F(u,v) = \frac{1}{4}C(u)C(v) \sum_{x=0}^{7}\sum_{y=0}^{7} f(x,y) cos\frac{(2x+1)u\pi}{16} cos\frac{(2y+1)v\pi}{16}, \tag{1}$$

where

$$\begin{aligned} &u, v \in \{0 \cdots 7\}; \\ &C(u), C(v) = 1/\sqrt{2} \quad \text{for} \quad u, v = 0; \\ &C(u), C(v) = 1 \qquad \text{otherwise.} \end{aligned} \tag{2}$$

In the next step, all 64 $F(u, v)$ coefficients are quantized. This is done by simply dividing each component in the frequency domain by a constant for that component, and then rounding to the nearest integer.

Thus, it is apparent that it is the quantization step in conjunction with splitting the image into block 8×8 that bring into the decoded photo shown blocking artifacts.

IV. Modeling and Extracting PRNU

Let us model the image acquisition process in the following way:

$$I_{i,j} = I^o_{i,j} + I^o_{i,j} \cdot \Gamma_{i,j} + \Upsilon_{i,j} \tag{3}$$

Here, $I_{i,j}$ denotes the image pixel at position (i, j) produced by the camera, $I^o_{i,j}$ denotes the noise-free image (perfect image of the scene), $\Gamma_{i,j}$ denotes PRNU noise and $\Upsilon_{i,j}$ stands for all additive or negligible noise components.

Following the approach proposed by [15], [11], the PRNU component is estimated in the following way. For a given camera, PRNU noise is estimated by averaging multiple images I_k, $k = 1, \cdots, N$ captured by this camera. This process is sped up by suppressing the scene content from

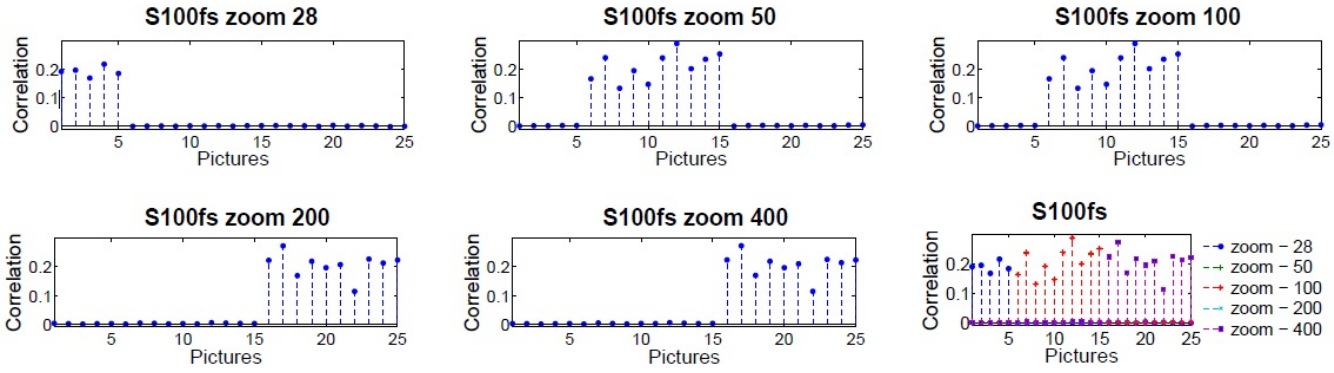

Figure 2. Problem of camera source identification caused by optical zoom. Fujifilm FinePix S100fs is a camera having different possibilities of focal lengths. Shown results demonstrate that correctness of source identification test is dependent on particular sensor reference images and corresponding focal length.

(a)

128	124	125	125	127	125	127	128	128
109	120	124	125	127	126	127	128	128
127	121	139	128	120	125	127	128	128
121	125	128	122	122	126	127	128	128
124	128	122	134	124	127	126	128	128
124	126	121	128	122	125	127	128	128
110	128	128	128	122	124	127	128	128
120	120	120	120	126	127	127	128	128

(b)

127	125	124	124	127	126	127	127	128
108	118	126	123	130	127	122	130	128
128	125	136	126	119	128	130	125	128
119	124	128	125	119	125	126	131	128
126	128	122	135	126	126	123	128	128
123	125	118	131	119	126	131	126	128
110	131	128	126	122	124	124	129	128
120	119	119	122	126	127	127	128	128

(c)

119	122	124	125	125	126	129	132	128
120	123	125	126	125	125	128	130	128
122	124	126	126	125	124	127	129	128
123	125	127	126	124	124	125	128	128
123	125	127	126	124	124	125	128	128
122	124	126	126	125	124	127	129	128
120	123	125	126	125	125	128	130	128
119	122	124	125	125	126	129	132	128

Figure 3. JPEG blocking artifact. (a) shows pixels of rows 1 to 8 and columns 1 to 9 of a RAW digital image. In (b) its JPEG 95% version is shown. In (c) JPEG 65% version of (a) is shown.

the image prior to averaging. This is achieved by using a denoising filter F and averaging the noise residuals I_k^d instead. In other words, PRNU of the camera C is computed by:

$$C_{PRNU} = \frac{1}{N}\sum_{k=1}^{N} I_k - I_k^d \tag{4}$$

Alternatively, maximum likelihood estimation (MLE) instead of simple averaging is employed.

In our work, we focus on multiplicative nature of PRNU component and analytically derive its estimation. Specifically, denoting the digital image captured by the camera by I, and the corresponding noise-free perfect image of the scene by I_0, then the fingerprint of the camera can be calculated in the following way.

Given Eq. 3, let us divide both sides of this equation by I^o and introduce a natural logarithm operator:

$$\frac{I_{i,j}}{I^o_{i,j}} = \frac{I^o_{i,j} + I^o_{i,j}\cdot\Gamma_{i,j} + \Upsilon_{i,j}}{I^o_{i,j}}$$

$$\ln(I_{i,j}) - \ln(I^o_{i,j}) = ln(1 + \Gamma_{i,j} + \frac{\Upsilon_{i,j}}{I^o_{i,j}}) \tag{5}$$

Having derived Eq. 5 and knowing that Taylor series expansions of the logarithmic function $\ln(1+x)$ is

$$\ln(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \frac{x^5}{5}\cdots$$

we can simply derive the following:

$$\ln(I_{i,j}) - \ln(I^o_{i,j}) = \Gamma_{i,j} + \frac{\Upsilon_{i,j}}{I^o_{i,j}} + \cdots$$

For the sake of simplicity, in the rest of this paper we omit pixel indexes (i,j) in our denotations. Now, having available N digital images captured by the same camera and considering the deterministic behavior of the PRNU noise component of its sensor, Γ_{sensor}, we can derive the following:

$$\frac{1}{N}\sum_{k=1}^{N}\ln(I_k) - \ln(I^o_k) = \Gamma_{sensor} + \frac{1}{N}\sum_{k=1}^{N}\frac{\Upsilon_k}{I^o_k} + \cdots$$

Assuming that Υ is a zero-mean noise component, we can conclude that

$$\lim_{n\to\infty}\frac{1}{N}\sum_{k=1}^{N}\frac{\Upsilon_k}{I^o_k} = 0$$

Ignoring higher order terms of Taylor expansion we can state that PRNU noise component of the sensor under analysis, Γ_{sensor}, can be estimated in the following way:

$$\Gamma_{sensor} = \frac{1}{N}\sum_{k=1}^{N}\ln(I_k) - \ln(I^o_k) \tag{6}$$

So, considering Γ_{sensor} as fingerprint of the camera's sensor based on PRNU noise, using Eq. 6 we can extract it from

a set of image or even from one image. But, it is apparent that as $N \rightarrow \infty$ the more accurate estimate of Γ_{sensor} we get. As stated before, Eq. 6 we use the multiplication nature of PRNU component (recall that $ln(a) - ln(b) = ln(\frac{a}{b})$).

Now, using simple a correlation we can measure similarity of different fingerprints. For example, having available two different sensor fingerprints Γ_{s_1} and Γ_{s_1}, we measure their similarity by employing a normalized correlation:

$$corr(\Gamma_{s_1}, \Gamma_{s_2}) = \frac{(\Gamma_{s_1} - \overline{\Gamma_{s_1}}) \odot (\Gamma_{s_2} - \overline{\Gamma_{s_2}})}{(\|\Gamma_{s_1} - \overline{\Gamma_{s_1}}\|) \cdot (\|\Gamma_{s_2} - \overline{\Gamma_{s_2}}\|)} \quad (7)$$

where $\overline{X}$ denotes mean of the vector X, $\odot$ stands for dot product of vectors defined as $X \odot Y = \sum_{k=1}^{N} X(k)X(k)$ and $\|X\|$ denotes L_2 norm of X defined as $\|X\| = \sqrt{X \odot X}$.

It has been shown in [15] that a good way of approximating I^0 is by de-noising I and compute the residual of these two images:

$$I^0 \approx I - I^d \quad (8)$$

Here, I^d denotes the de-noised digital image. While some studies were carried out about the specific choice and effectiveness of de-noising filters (e.g., [18]), our experiments uncovered that although a proper de-noising filter improves results of source identification, this part usually does not play the most critical part in receiving accurate results. It might happen that in some cases (e.g., based on spatial distribution of the image) some filters work better and some worse.

As mentioned previously, digital images suffer from different kind of noise and imperfections brought into them by different components of digital camera. Some of them such as optical zoom and JPEG can cause serious problems in terms of higher false positive or lower true positive rates.

3) Resistence to optical zoom: Non-central parts of the digital image are effected the most by vignetting. In order to minimize this problem, we only consider the central part of the image. All other pixels are omitted. In our experiments, only the central part of size 320×320 pixels is considered. Cropping operation always has been carried out with respect to JPEG lattice so there was no corrupted JPEG block resulting from this operation.

4) Resistence to JPEG: There have been attempts to use different type of state-of-the-art wavelet de-noising algorithms with a good edge-preserving behavior. As obvious, the spatial distribution of the image can have a strong impact on final de-noising result so employment of a specific de-nosing filter must be in accordance with digital image's distribution. It is not possible to use 1 general filter for all types of contents. When digital images are corrupted by JPEG significantly, most of de-noising algorithms either leave traces of JPEG blocking artifacts in I^0 or they bring their own artifact into the image. Thus, one effective way how to overcome this problem is to run the denoising method separately in each block depending on particular compression blocking size (e.g., 8×8 pixels for most of JPEG files). Apparently, when following this approach, there is a need to employ a de-nosing filter (kernel) with smaller support. In our experiments we used a simple median filter of size 2×2.

Working with each compression block separately gives us a better resistence to blocking artifacts which. Also Equation 7 is applied separately on each compression block. In other words, instead of obtaining one correlation value, we obtain 1600 correlation values for a digital image of size 320×320 pixels and compression blocks of 8×8 pixels (typical JPEG). Resulting correlation value is obtained by computing the median.

V. Experiments

When applying the proposed method to photos captured by a cameras enabling rich optical zoom options the benefits of the proposed method becomes apparent. In most cases where [11] fails to correctly identify the source camera, the proposed method enables that. Moreover, when digital images effected by a stronger JPEG are analyzed, the method proposed in [11] produces a higher amount of false positives. In other cases, results of both methods are very comparable.

For the sake of completeness, we point out that false positive states for mistakenly pinpointing the source camera. By true positive we mean correctly pinpointing the source camera.

To visualize the benefit of the proposed method, we selected 3 particular cameras. One Fujifilm FinePix S100FS having available lens focal lengths of 28-400mm. This camera has been chosen in order to demonstrate impact of rich optical zoom. Also, two different pieces of Canon PowerShot G12 have been employed. Two different pieces of a same camera are helpful in analyzing false-positives as they are equipped by a same embedded software and demosaicking and JPEG algorithm.

In Figure 4 experimental results are shown. Figure 4(a) is based on a camera fingerprint created by using 30 digital images captured by Fujifilm FinePix S100FS with focal length 50mm. Camera fingerprints used in Figures 4(b),(c), and (d) are created by 30 photos captured by Fujifilm FinePix S100FS with focal lengths 100mm, 200mm, and 400mm, respectively. Camera fingerprints used in Figures 4(e), (f) are created by using photos captured by two different cameras Canon PowerShot G12 (each fingerprint is based on 30 photos captured by one of these cameras).

All Figures 4(a)..4(f) show two plots. Plots shown in first row are obtained by employing the method pointed out in [11]. Plots in seconds row demonstrate results obtained by the method proposed in this paper. Always, y-axes shows the resulting correlation value and x-axes denotes index of the digital image being tested. In all figures, indexes 1-20 belong to photos captured by Fujifilm FinePix S100FS with the focal length 50mm, indexes 21-40 belong different to photos captured by Fujifilm FinePix S100FS with the focal length

100mm, indexes 41-60 belong to photos captured by same camera but with focal length 200mm, and indexes 61-80 belong to photos captured by Fujifilm FinePix S100FS, but focal length 400mm has been used. Indexes 81-100 belong to photos captured by first Canon PowerShot G12. Indexes 81-100 belong to photos captured by second Canon PowerShot G12.

For example, as it is apparent from Figures 4(a), the proposed method has much higher true-positive rate and is invariant in respect to focal length. It correctly differentiates all photos captured by Fujifilm FinePix S100FS from those others captured by two devices of Canon PowerShot G12.

VI. Conclusions

In this paper, we have shown how to employ the multiplicative nature of the PRNU component to derive a novel method to estimate it. The derived method also has been successfully applied on a digital image ballistics experiment in order to pinpoint the exact device that created a specific digital photo. Moreover, the method has been enhanced to be resistent to optical zoom and JPEG compression

VII. Acknowledgments

This work has been supported by the Ministry of the interior of the Czech Republic under Project no. MV CR, VG20102013064 and the Czech Science Foundation under Project no. GACR 13-28462S.

References

[1] H. T. Sencar, M. Ramkumar, and A. N. Akansu, *Data Hiding Fundamentals and Applications: Content Security in Digital Multimedia*. Orlando, FL, USA: Academic Press, Inc., 2004.

[2] M. Arnold, M. Schmucker, and S. D. Wolthusen, *Techniques and Applications of Digital Watermarking and Content Protection*. Norwood, MA, USA: Artech House, Inc., 2003.

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

[4] T.-T. Ng and M.-P. Tsui, "Camera response function signature for digital forensics - part i: Theory and data selection," in *IEEE Workshop on Information Forensics and Security*, Dec. 2009, pp. 156–160.

[5] Z. Lint, R. Wang, X. Tang, and H.-Y. Shum, "Detecting doctored images using camera response normality and consistency," in *CVPR '05: Proceedings of the 2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05) - Volume 1*. Washington, DC, USA: IEEE Computer Society, 2005, pp. 1087–1092.

[6] A. Popescu and H. Farid, "Exposing digital forgeries in color filter array interpolated images," *IEEE Transactions on Signal Processing*, vol. 53, no. 10, pp. 3948–3959, 2005. [Online]. Available: www.cs.dartmouth.edu/farid/publications/sp05a.html

[7] B. Mahdian and S. Saic, "Blind authentication using periodic properties of interpolation," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 3, pp. 529–538, September 2008.

[8] ——, "Detection of copy–move forgery using a method based on blur moment invariants," *Forensic science international*, vol. 171, no. 2–3, pp. 180–189, 2007.

[9] A. E. Dirik, S. Bayram, H. T. Sencar, and N. Memon, "New features to identify computer generated images," in *IEEE International Conference on Image Processing, ICIP '07*, vol. 4, 2007, pp. 433 – 436.

[10] J. Fridrich and T. Pevny, "Detection of double–compression for applications in steganography," *IEEE Transactions on Information Security and Forensics*, vol. 3, no. 2, pp. 247–258, June 2008.

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

[12] T. Filler, J. Fridrich, and M. Goljan, "Using sensor pattern noise for camera model identification," in *Proceedings IEEE, International Conference on Image Processing, ICIP 2008*, San Diego, CA, October 12–15, 2008, pp. 1296–1299. [Online]. Available: http://dde.binghamton.edu/filler/

[13] Y. Sutcu, S. Bayram, H. T. Sencar, and N. Memon, "Improvements on sensor noise based source camera identification." in *ICME*. IEEE, 2007, pp. 24–27.

[14] J. Lukas, J. Fridrich, and M. Goljan, "Detecting digital image forgeries using sensor pattern noise," in *In Proceedings of the SPIE*. West, 2006, p. 2006.

[15] ——, "Digital camera identification from sensor pattern noise," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 2, pp. 205–214, June 2006.

[16] M. Chen, J. Fridrich, M. Goljan, and J. Luk, "Source digital camcorder identification using sensor photo-response nonuniformity," in *Proc. of SPIE Electronic Imaging, Photonics West*, 2007.

[17] M. Chen, J. Fridrich, and M. Goljan, "Digital imaging sensor identification (further study," in *In Security, Steganography, and Watermarking of Multimedia Contents IX. Edited by Delp, Edward J., III; Wong, Ping Wah. Proceedings of the SPIE, Volume 6505*, 2007.

[18] I. Amerini, R. Caldelli, V. Cappellini, F. Picchioni, and A. Piva, "Analysis of denoising filters for photo response non uniformity noise extraction in source camera identification," in *Proceedings of the 16th international conference on Digital Signal Processing*, ser. DSP'09. Piscataway, NJ, USA: IEEE Press, 2009, pp. 511–517. [Online]. Available: http://dl.acm.org/citation.cfm?id=1700307.1700392

[19] E. J. Alles, Z. J. M. H. Geradts, and C. J. Veenman, "Source camera identification for heavily jpeg compressed low resolution still images," *Journal of Forensic Sciences*, vol. 54, no. 3, pp. 628–638, 2009. [Online]. Available: http://www.science.uva.nl/research/publications/2009/AllesJFS2009

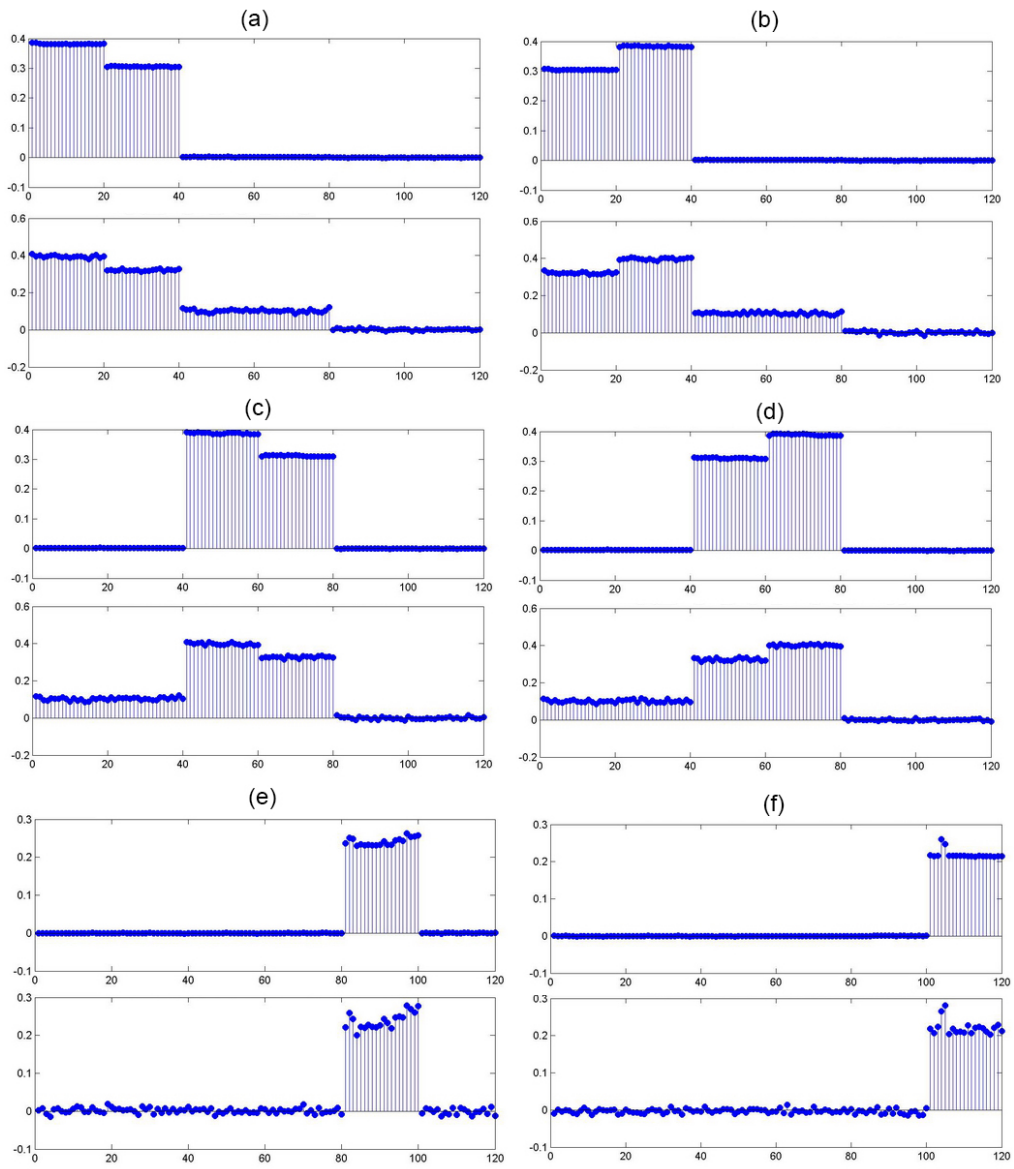

Figure 4. Source identification. One Fujifilm FinePix S100FS and two different Canon PowerShot G12 were used to generate results.

[20] C. J. Yongjian Hu, Binghua Yu, "Source camera identification using large components of sensor pattern noise," in *Computer Science and its Applications, 2009. CSA '09. 2nd International Conference on*, Jeju Island, Korea, 2009.

[21] Y. Li and C.-T. Li, "Decomposed photo response non-uniformity for digital forensic analysis," in *e-Forensics*, 2009, pp. 166–172.

[22] Y. Hu, C. Jian, and C.-T. Li, "Using improved imaging sensor pattern noise for source camera identification," in *ICME*, 2010, pp. 1481–1486.

[23] D. B. Goldman and J.-H. Chen, "Vignette and exposure calibration and compensation," in *The 10th IEEE International Conference on Computer Vision*, Oct. 2005, pp. 899–906.