Determination of stop-criterion for incremental methods constructing camera sensor fingerprint

Babak Mahdian, Adam Novozámský, and Stanislav Saic

Institute of Information Theory and Automation of ASCR,
Prague, Czech Republic
{mahdian, novozamsky, ssaic}@utia.cas.cz

Abstract. This paper aims to find the minimum sample size of the camera reference image set that is needed to build a sensor fingerprint of a high performance. Today's methods for building sensor fingerprints do rely on having a sufficient number of camera reference images. But, there is no clear answer to the question of how many camera reference images are really needed? In this paper, we will analyze and find out how to determine the minimum needed number of reference images to remove the mentioned uncertainty. We will introduce a quantitative measure (a stop-criterion) stating how many photos should be used to create a high-performance sensor fingerprint. This stop-criterion will directly reflect the confidence level that we would like to achieve. By considering that the number of digital images used to construct the camera sensor fingerprint can have a direct impact on performance of the sensor fingerprint, it is apparent that this, so far underestimated, topic is of major importance.

Keywords: Image ballistics, source camera verification, pattern noise, PRNU, fingerprint performance, laplace distribution

1 Introduction

Generally, there are two essential tasks in forensics analysis of digital images and videos: their integrity verification (genuineness analysis) and ballistics analyzes. In this paper we will deal with image (video) ballistics which does address the problem of linking digital images (videos) under investigation to the exact source imaging device that has been used to capture photos (videos) under investigation. 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.

Although past research was mainly focused on data hiding and digital watermarking approaches [1–3] to perform 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 [4]. 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 [5, 6], traces of non-consistencies in color filter array interpolation [7], traces of geometric transformations, [8], cloning [9], computer graphics generated photos [10], JPEG compression inconsistencies [11], etc. Typically, pointed out methods are based on the fact that digital image editing brings specific detectable statistical changes into the image.

In the image ballistics area, methods mainly focused on camera sensor noise and systematic artifacts that are brought into the image [12–18]. These artifacts have been used to link a digital image to its exact acquisition device.

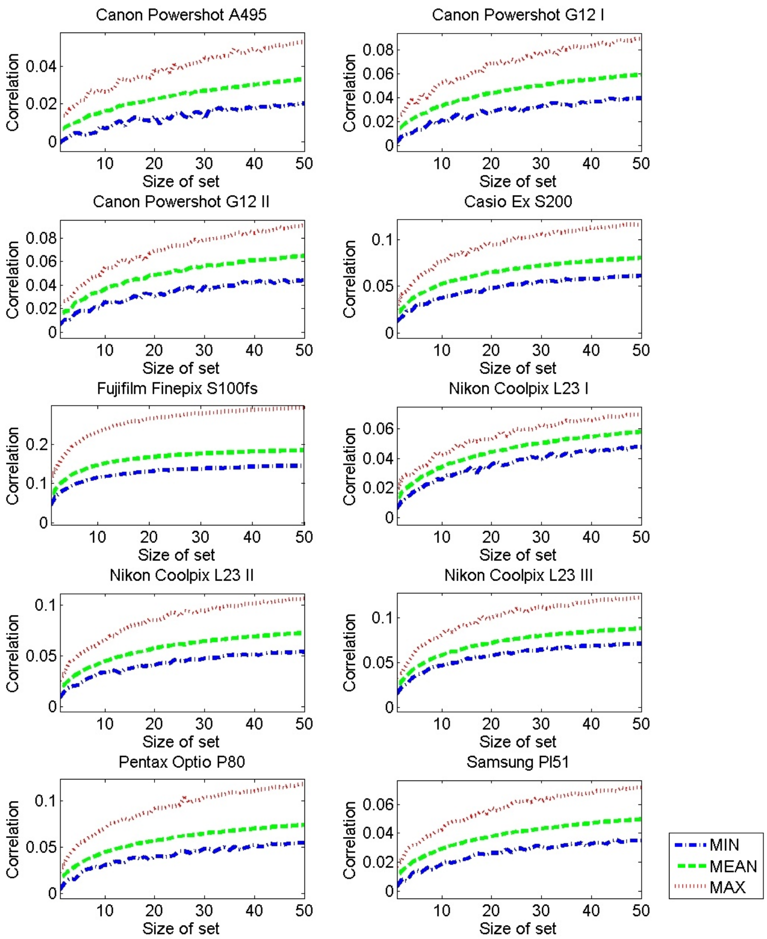

Fig. 1. Performance of camera sensor fingerprint constructed using camera reference sets of different sizes and 100 test images for each camera.

1.1 Motivation

When linking a digital image to an exact camera (or a video signal to camcorder), typically the following procedure is used. First, the camera sensor fingerprint is constructed [12, 13]. Second, the constructed fingerprint and image under investigation are matched (usually through a correlation measurement). This indicates if the digital image has been captured by this camera. The sensor fingerprint is constructed incrementally by using many camera reference images. Camera reference images are recommended to be of a uniformly illuminated surface. Usually, an edge-preserving denoising filter is applied on camera reference images. Residuals of digital images and their denoised versions are put together (e.g., by averaging) to construct the basic version of sensor fingerprint.

The problem is how many photos should be used to form the camera reference images so there will be a high confidence that the constructed fingerprint is of a high performance? Is the optimal size of this set 10, 50, or even 250? The topic is of major importance. The reason is that number of digital images used to construct the camera sensor fingerprint, typically, has a direct impact on performance of the sensor fingerprint. Insufficient number of reference images cause a poor performance of the fingerprint. To this end, most authors rather recommended to employ a fixed and higher number of reference images to be safe in terms of having a good performing fingerprint (in published literature we have, typically, observed recommended sizes of reference images ranging from 30 to 150).

To remove the uncertainty about the size of sets of camera reference images, we will introduce a quantitative measure determining how many photos should be used to create the sensor fingerprint to have a high performing fingerprint. In other words, we are going to search for the optimal number of reference images that will reflect our the confidence level and accuracy we want to achieve. To address the problem we will search for a stop-criterion stating that no more images are needed to be added to the set of camera reference images.

Before going on, we also explicitly define what is a fingerprint of good (high) or poor performance. A fingerprint with a good performance is such a fingerprint that enables a successful recognition of the exact source cameras when inspecting photos of various scenes, lighting conditions, etc. When a non-sufficient number of images are used to create the sensor fingerprint, the measured fingerprint is of poor performance (often random noise components dominate in there) and hence the image source verification task generate weak results. By weak results we mean lower rate of true positives. Figure 1 demonstrates performance of 10 different camera sensor fingerprints constructed by $1 \cdots 50$ reference images of uniformly illuminated surface (a white paper). The figure demonstrates obtained correlation (obtained by using Eq. 3) between 100 test images (natural images captured by same cameras) and associated camera fingerprints (minimal, maximal and mean values of obtained correlation values are shown). Apparently size of camera reference sets have a direct impact on results obtained. For the sake of completeness, we point out that false positive states for mistakenly pinpoint-

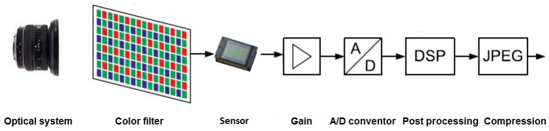

Fig. 2. A typical digital camera system.

ing the source camera. By true positive we mean correctly pinpointing a digital image to the source camera.

2 Basic Notations and Preliminaries

A typical camera consists of several different components (see Fig. 2). As pointed out in [19], the core of every digital camera is the imaging sensor. The sensor (e.g., CCD or CMOS) is consisted on small elements called pixels that collect photons and convert 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. Most commonly, Bayer color filter is used.

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.

What is important in terms 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 ballistics analysis. Typically, artifacts (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. Hence, if we are able to find kind of information brought into image by the sensor and which will remain stable and present in all images captured by that sensor and cannot be found in no image captured by any other sensor, then we can call it fingerprint of that sensor or camera. Such a camera sensor fingerprint can be employed to link digital images to particular digital cameras which captured them.

2.1 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 [19], 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 non-uniformity (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.

There has not been performed a lot of studies analyzing the PRNU noise in deeper details. Despite this, it has been shown that it has a dominant presence in the pattern noise component found in digital images. This made possible Fridrich et al. [13, 12] to employ PRNU noise to identify exact source cameras. In other words, PRNU noise is employed as the fingerprint of camera sensors. 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., [13, 12, 20, 21]). There have been published some additional papers by others authors(e.g., [14–18]) aiming to improve accuracy of results. Typically, they brought modifications to the original paper of Jessica Fridrich et al. [13, 12] based on some new theoretical or empirical findings. Nonetheless, the key concept of how to measure sensor's fingerprint has remained unchanged.

2.2 Modeling and Extracting PRNU

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

$$I_{i,j} = I^o_{i,j} + I^o_{i,j} \cdot \varGamma_{i,j} + \varUpsilon_{i,j} \tag{1}$$

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), $\varGamma_{i,j}$ denotes PRNU noise and $\varUpsilon_{i,j}$ stands for all additive or negligible noise components.

Following the approach proposed by [13, 12], 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. The process is sped up by suppressing the scene content from the image prior to averaging. This is achieved by using a denoising filter $\mathcal{F}$ and averaging the noise residuals instead. We will denote residuals by $\hat{I}_k$ (i.e., $\hat{I}_k = I_k - \mathcal{F}(I_k)$). In other words, deterministic components of sensor noise of the camera C are computed in the following way:

$$\Gamma_{sensor} = \frac{1}{N}\sum_{k=1}^{N} \hat{I}_k = \frac{1}{N}\sum_{k=1}^{N} I_k - \mathcal{F}(I_k) \tag{2}$$

Alternatively, for example, maximum likelihood estimation (MLE) instead of simple averaging can be employed.

To reduce the false positive rate, sensor fingerprint are enhanced by Wiener filtering in the frequency domain (e.g., to reduce JPEG compression artifacts) and linear pattern removal through zero-mean operation (e.g., to remove traces of CFA interpolation) [12]. Pointed out Γ_{sensor} is the basic version of sensor fingerprint of camera. To achieve accurate results and minimize the false positive rate, it is necessary to perform additional frequency filtering, fingerprint enhancement and correction, suppressing dominant traces of camera embedded software, filtering JPEG artifacts, etc. Without such a correction, typically, a high rate of false positives is obtained (because of camera operations such as gamma correction, CFA interpolation, color enhancement, geometric deformation corrections, compression, additional embedded camera software functionalities, etc.) This part often depends on specific camera brands under investigation.

Linking of a digital image to an exact camera is carried out by performing a similarity measure of two sensor fingerprints. One is obtained from the image under investigation and second from the set of camera reference images. This can be carried out, for example, by employing a simple correlation measure. Having available two different sensor fingerprints Γ_{s_1} and Γ_{s_2}, we measure their similarity by employing a normalized correlation:

$$corr(\Gamma_{s_1}, \Gamma_{s_2}) = \frac{(\Gamma_{s_1} - \overline{\Gamma_{s_1}}) \odot (\Gamma_{s_2} - \overline{\Gamma_{s_2}})}{(\|\Gamma_{s_1} - \overline{\Gamma_{s_1}}\|) \cdot (\|\Gamma_{s_2} - \overline{\Gamma_{s_2}}\|)} \tag{3}$$

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 $\|X\| = \sqrt{X \odot X}$.

There has been carried out studies about the specific choice and effectiveness of denoising filters (e.g., [14]). It is important to note that there is no general perfect denoising filter. All of them have t heir advantages and disadvantages. Moreover, it is interesting to note that when applying the proposed PRNU estimation method on a larger set of digital images or when analyzing digital video signals consisted of thousands of individual frames, the computational time becomes a drawback of the method. It has been shown that the computational time of the method can effectively be enhanced by using GPU-accelerated version of the algorithm. For example, in [22, 23] a parallel CUDA implementation of Γ_{sensor} has been built achieving remarkable speedup in fingerprint computation (up to 5-6 times).

3 Laplacian Distributed Residuals

As pointed out in last section, for a given camera C, deterministic components of sensor noise can be estimated by averaging multiple images captured by this camera, I_k, $k = 1, \cdots, N$. The process is sped up by suppressing the scene content from the image prior to averaging by using a denoising filter $\mathcal{F}$ and averaging the noise residuals $\hat{I}_k$ instead.

Apparently samples of residuals, $\hat{I}_k$, and their corresponding averaged versions $\frac{1}{N}\sum_{k=1}^{N}\hat{I}_k$ are the key information forming the sensor fingerprint of camera, Γ_C. Let us first to find an appropriate form for the probability density function (p.d.f.) of the distribution of residual values so that they can be efficiently modeled. Figure 3 demonstrates the histogram of residuals $\frac{1}{N}\sum_{k=1}^{N}\hat{I}_k$, obtained using a typical set of reference images of sizes $N = 1, 5, 10, 15, 20, 25$.

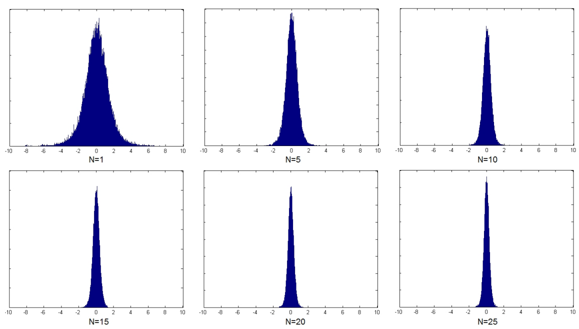

Fig. 3. Distribution of averaged residuals Γ_C constructed using a typical camera reference image set of different sizes $N = 1, 5, 10, 15, 20, 25$.

These figures demonstrate that the Laplacian p.d.f. fits the observed distribution well. Γ_C has a Laplace (μ, b) distribution if its probability density function is

$$f(\Gamma_{C_{i,j}}|\mu, b) = \frac{1}{2b}\exp\left(-\frac{|\Gamma_{C_{i,j}} - \mu|}{b}\right) \tag{4}$$

where μ is a location parameter and $b \geq 0$ is sometimes referred to as the diversity.

To estimate parameters of the Laplace distribution, maximum likelihood estimator is used. Maximum likelihood estimator of b can be obtained by:

$$\hat{b} = \frac{1}{M}\sum_{i=1}^{M}|\Gamma_{C_{i,j}} - \hat{\mu}| \tag{5}$$

Having Laplacian-distributed residuals, $\hat{I}_k$, we easily can estimate parameters the of associated p.d.f. Specifically, we focus on parameter b and will analyze its behavior during computation process of the sensor fingerprint. Figure 4 demonstrates values of b for different number camera reference images of 10 different cameras. Apparently, b follows a descending trend. Specifically, we can see that b descends as the number of camera reference images grows. It is important to note that the descending trend is steep in the beginning. On the other hand, b becomes almost stable for higher number of images.

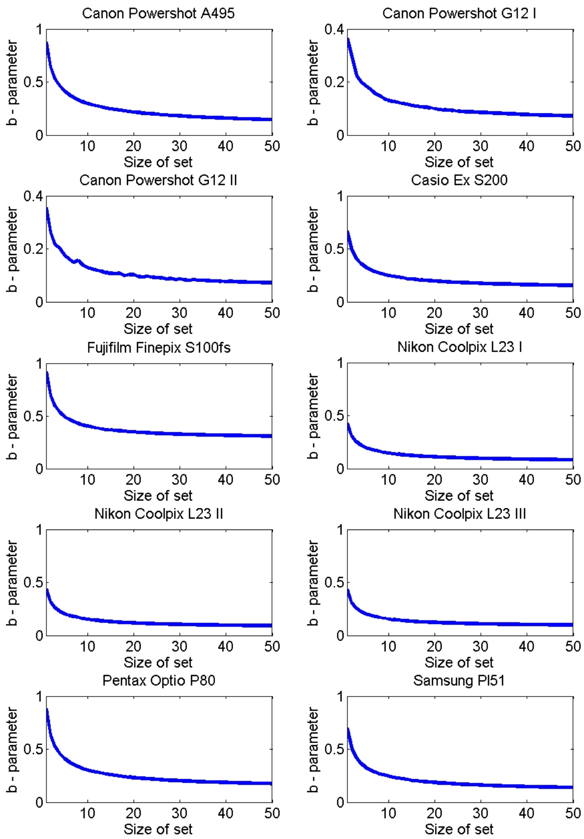

Fig. 4. Estimated parameter b for 10 different sensor fingerprints constructed using camera reference image sets of sizes $N = 1 \cdots 50$.

4 Determination of Stop-Criterion for Size of Reference Images

The uncertainty which is addressed in this paper is about the needed number of reference images, N, that is needed to construct a sensor fingerprint, Γ_{sensor}, of high performance. As pointed out previously, in literature, it is often pointed out that $N \rightarrow \infty$ brings a more accurate sensor fingerprint and suppressed Υ.

In last section we introduced the parameter b that is based on Laplace distribution modeling of residuals. Moreover, we have shown that b has a specific behavior and descends as the number of camera reference images grows. It has been shown that the descending trend of b is steep in the beginning. On the other hand, b becomes almost stable for higher number of images.

The question is what is the relation between b and the performance of the sensor fingerprint and how can we employ b to predict the future performance level of the fingerprint in terms of true positives? Here, we will use a differential operator to quantify the behavior of b. In other words, having $\Gamma_C = \frac{1}{N}\sum_{k=1}^{N}\hat{I}_k$, we will measure the rate at which the value of the b changes with respect to change of k:

$$\Delta b_k = b_{k+1} - b_k \tag{6}$$

To create a stop-criterion, we collected 25 different cameras and for each of them created a camera reference image sets of 50 images and a test image sets of 100. We constructed 50 sensor fingerprints Γ_C by using $1 \cdots 50$ reference images per camera. Reference photos have been selected randomly. Having 50 different sensor fingerprints constructed using a different size of reference image sets, we carried out an image ballistics test using Eq. 3 that calculated the true positive rate for all test images. A global threshold has been employed for the classification part of this part. At the same time we also measured Eq. 6 for all camera fingerprints (to remove local outliers, a low-pass filter always have always been applied on Δb). Having available 50 different true positive rates as well as 50 values of b for each camera sensor fingerprint, we analyzed their relation and empirically gained an optimal b for different rates of true positives. Efficiency that can be obtained by using b as the stop-criterion is shown the next section. In this study, we selected the false positive rate to be 0.1 percent. For the sake of simplicity, for the parameter searching and experimental part, there only have been chosen cameras that are distinguishable using the basic version of sensor fingerprint enhanced by Wiener filtering in the frequency domain (e.g., to reduce JPEG compression artifacts) and linear pattern removal through zero-mean operation as recommended in [12].

Figure 5 demonstrates a portion of results of our analysis. Specifically, shown is performance of fingerprint constructed by sets of reference images of sizes $N = 1 \cdots 50$. Also shown is the associated and estimated b.

5 Experimental Results

Table 1 demonstrates efficiency of using Δb for 10 test camera sensor fingerprints. These cameras have not been used in the process of determination of optimal Δb. We have selected our true positive rate to be 99.99 percent with having false positive rate of 0.01 percent. Considering these desired true and false positive rates we have computed the optimal Δb. As mentioned in last section, this stop-criterion has been calculated using a 25 different cameras and associated sets of

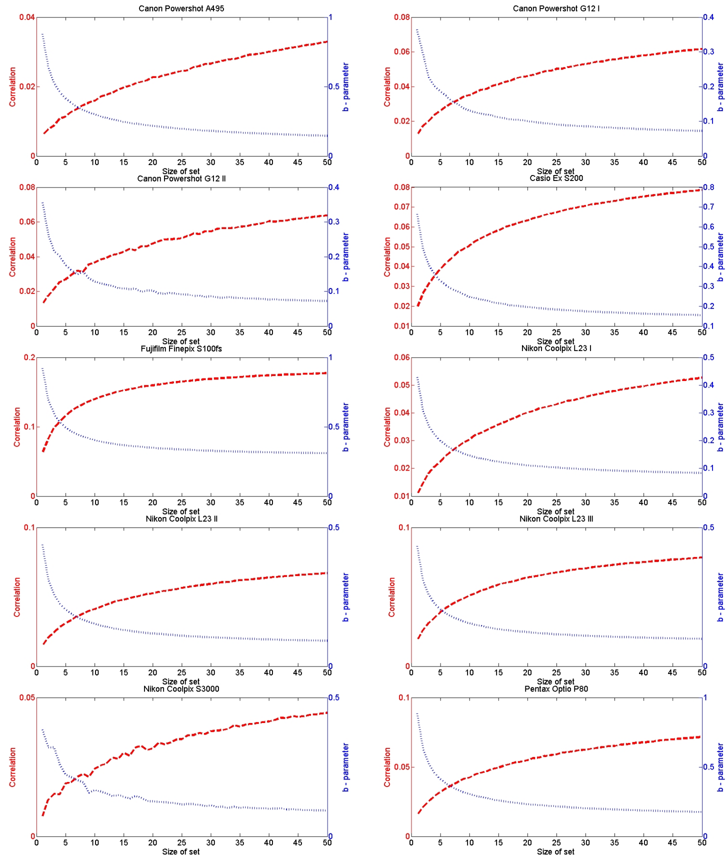

Fig. 5. Shown is performance of fingerprint constructed by sets of reference images of sizes $N = 1 \cdots 50$. Also shown is the associated and estimated b.

reference images of sizes $N = 1 \cdots 50$. In our case, optimal Δb was 0.0050. For each test camera, Table 1 shows gained true positive rate and associated size of camera reference image set (shown in square brackets). In this experiment, we gained 0 percent false positive rate.

Table 1 demonstrates gained true positive rates for 100 test images per camera. Moreover, size of camera reference images used to construct the camera sensor fingerprint is shown either. For the sake of completeness, we also show different values of Δb and associated results obtained.

6 Discussion and Conclusion

In this paper we addressed the problem of uncertainty of how many reference images should be used to construct a high performance camera sensor fingerprint.

Table 1. Sown is performance (%) of sensor fingerprints based on different values of Δb. Shown is also associated number of reference images used to construct the sensor fingerprint (shown in square brackets).

Δb	0.0400	0.0300	0.0200	0.0100	0.0050	0.0040	0.0030
canon-powershot-g12-III	73 [3]	84 [4]	99 [6]	100 [9]	100 [14]	100 [16]	100 [19]
canon-powershot-g12-IV	75 [2]	97 [4]	100 [7]	100 [10]	100 [11]	100 [13]	100 [22]
fujifilm-finepix-s100fs-II	100 [4]	100 [5]	100 [6]	100 [10]	100 [14]	100 [21]	100 [25]
nikon-coolpix-l23-IV	81 [3]	93 [5]	97 [6]	100 [8]	100 [11]	100 [15]	100 [19]
nikon-coolpix-l23-V	100 [4]	100 [5]	100 [5]	100 [7]	100 [11]	100 [17]	100 [24]
nikon-coolpix-l23-VI	100 [3]	100 [4]	100 [6]	100 [7]	100 [12]	100 [14]	100 [21]
pentax-optio-p80-II	97 [4]	100 [5]	100 [7]	100 [11]	100 [18]	100 [22]	100 [27]
iphone-3GS	18 [5]	28 [6]	28 [7]	62 [12]	94 [20]	100 [27]	100 [35]
iphone-4s-I	86 [4]	98 [5]	100 [6]	100 [10]	100 [15]	100 [20]	100 [23]
iphone-4s-II	95 [4]	100 [6]	100 [8]	100 [9]	100 [12]	100 [21]	100 [28]

Typically, papers dealing with construction of sensor fingerprints proposed to incrementally use about 40 - 50 images of a uniformly illuminated surfaces. Some others simply recommended to use as much as possible.

In last sections, we have introduced a quantitative measure stating how many photos should be used. We searched for an the minimal number of camera reference images that will directly reflect the confidence and accuracy level we want to achieve. To address the problem, we introduced a stop-criterion that can determine if more images are needed to be added to the set of reference images to get the desired true positive rate.

It also has been shown that a small number of reference images available for construction a sensor fingerprint is not always a limiting factor for constructing a well performing fingerprint. It should be noted that employing camera reference image sets of N when $N \to \infty$ does not necessarily convert to a perfect sensor fingerprint. By a perfect sensor fingerprint we mean a signal that only and only consists of deterministic noise components unique for each sensor. Digital images captured by today's consumer cameras and smartphones suffer from a set of systematic and non-systematic imperfections and enhancements (sensor noise, gamma correction, CFA interpolation, color enhancement, geometric deformation corrections, and a number of additional embedded camera software functionalities) that bring a number of correlated and uncorrelated artifacts into digital images which cannot be overcome using N, $N \to \infty$, number of camera reference image.

Acknowledgments. This work has been supported by 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: Aca-

demic 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. B. Mahdian and S. Saic, "A bibliography on blind methods for identifying image forgery," *Image Commun.*, vol. 25, no. 6, pp. 389–399, 2010.
5. 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.
6. 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.
7. 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
8. 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.
9. ——, "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.
10. 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.
11. 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.
12. 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.
13. J. Lukas, J. Fridrich, and M. Goljan, "Digital camera identification from sensor pattern noise," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 2, pp. 205–214, June 2006.
14. 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
15. 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
16. 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.

17. Y. Li and C.-T. Li, "Decomposed photo response non-uniformity for digital forensic analysis," in *e-Forensics*, 2009, pp. 166–172.
18. Y. Hu, C. Jian, and C.-T. Li, "Using improved imaging sensor pattern noise for source camera identification," in *ICME*, 2010, pp. 1481–1486.
19. 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.
20. 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.
21. 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.
22. D. Williams, V. Codreanu, P. Yang, B. Liu, F. Dong, B. Yasar, B. Mahdian, A. Chiarini, X. Zhao, and J. Roerdink, "Evaluation of autoparallelization toolkits for commodity graphics hardware," in *10th International Conference on Parallel Processing and Applied Mathematics*. Warsaw, Poland: Springer, 2013, to appear.
23. D. Williams, V. Codreanu, J. B. Roerdink, P. Yang, B. Liu, F. Dong, and A. Chiarini, "Accelerating colonic polyp detection using commodity graphics hardware," in *Proceedings of the International Conference on Computer Medical Applications*, Sousse, Tunisia, 2013, pp. 1–6.