Sensor Pattern Noise Matching Based on Reliability Map for Source Camera Identification

Riccardo Satta
European Commission - Joint Research Centre (JRC),
Institute for the Protection and Security of the Citizen, Ispra (VA), Italy

Keywords: Sensor Pattern Noise, Source Camera Identification, Digital Image Forensics, Multimedia Forensics, Reliability Map, Matching.

Abstract: Source camera identification using the residual noise pattern left by the sensor, or Sensor Pattern Noise, has received much attention by the digital image forensics community in recent years. One notable issue in this regard is that high-frequency components of an image (textures, edges) can be easily mistaken as being part of the SPN itself, due to the procedure used to extract SPN, which is based on adaptive low-pass filtering. In this paper, a method to cope with this problem is presented, which estimates a SPN *reliability map* associating a degree of reliability to each pixel, based on the amount of high-frequency content in its neighbourhood. The reliability map is then used to weight SPN pixels during matching. The technique is tested using a data set of images coming from 27 different cameras; results show a notable improvement with respect to standard, non-weighted matching.

1 INTRODUCTION

In recent years, the problem of source camera identification, i.e., to identify the camera that has been used to take a given picture, has received much attention by the digital image forensics community, due to its usefulness in a number of practical cases (e.g., on-line child abuse (Satta et al., 2013)).

Among the various techniques proposed so far for performing the task, the so-called Sensor Pattern Noise (SPN) is possibly the most mature and accurate one. The SPN is a high-frequency, low power additive noise that affects any image, left by the sensor element of the camera (Lukas et al., 2006), and is due to the unavoidable small differences in light response of each sensitive element (pixel). The SPN has two important properties: first, it is univocal of a camera sensor; second, it exhibits stability over time. As such, it can be seen as an unique fingerprint that identifies one individual device. Extraction of SPN can be performed by first de-noising an image (usually by exploiting adaptive low-pass filters), and then obtain the noise pattern by comparing the de-noised image with the original one.

In source camera identification, the task is to identify a given picture P as being taken by one camera C^* among a set of N cameras $\mathrm{C} = \{C_1, \dots, C_N\}$. A template SPN is at first created for each camera C_i by averaging the SPNs extracted from a number of images known to be taken with C_i. The SPN extracted from P is then matched against all templates and the test picture is assigned to the closest match.

One particularly notable issue that affects SPN extraction is that parts of an image that show high-frequency properties (e.g., textures, edges) can be easily mistaken as being part of the SPN itself. For this reason, template SPNs are typically created from images showing uniform background and no details (e.g. pictures of blue sky, or of a wall), which can be taken ad-hoc assuming the investigator has access to the cameras. However, test pictures can show any kind of content and may be taken in any possible environmental condition; consequently, their SPNs are usually affected by the high-frequency components problem. Ultimately, this leads to a loss of accuracy in terms of false matches.

In this paper, a method to cope with this problem is presented. Given a picture P, an SPN *reliability map* is built at first, which associates, to each pixel, an estimated degree of reliability of the corresponding SPN. In order to build the map, an edge detection algorithm is utilised to detect pixels that will most likely produce spurious SPN components, plus a dilation operation to count also neighbour pixels. The

Satta R..
Sensor Pattern Noise Matching Based on Reliability Map for Source Camera Identification.
DOI: 10.5220/0005354202220226
In *Proceedings of the 10th International Conference on Computer Vision Theory and Applications* (VISAPP-2015), pages 222-226
ISBN: 978-989-758-089-5

degree of quality of a given pixel is given by the intensity of the corresponding edge. The reliability map is then used to weight pixels during matching with templates.

The proposed technique is tested on a source camera identification scenario using a data set of images coming from 27 different cameras; results show a notable improvement with respect to standard, non-weighted matching.

The remainder of the paper is organised as follows. Section 2 first provides a brief overview of the existing body of work about source camera identification and SPN. Section 3 then describes the proposed technique. An experimental assessment of the performance of the technique is given in Section 4. Finally, Section 5 concludes the paper with some insights on future work directions.

2 RELATED WORK

In digital image forensics, it is often feasible to associate various kinds of useful ancillary *metadata* to a digital images. Examples are Exif data, image tags, or text associated to the image (e.g., contained in the same web page), etc.

Exif metadata (that is, a set of key-value properties embedded in the image file, containing date and time of acquisition, brand and model of the device, camera settings and other information) has received much attention by the community of investigators, since it stores useful information about the device that produced the picture. From a forensic viewpoint however, the information provided by Exif metadata must be taken into account with particular care; it can be fairly easy, in fact, to modify, fake or remove it with the help of image processing software (e.g., Photoshop[1]) as well as with free tools available on the Internet (e.g., ExifTool[2]).

A great deal of research has been conducted in the field of digital camera fingerprinting in order to provide a cue which is more robust and discriminative than Exif for recognising source cameras. To this aim, researchers have exploited SPN (Kang et al., 2012; Li and Li, 2012; Lukas et al., 2006), interpolation artefacts caused by de-mosaicking filter (Cao and Kot, 2009; Long and Huang, 2006; Popescu and Farid, 2005) and JPEG compression (Sorrell, 2009), traces of dust in the sensor (Dirik et al., 2008), or lens aberrations (Choi et al., 2006; Van et al., 2007), as possible fingerprints.

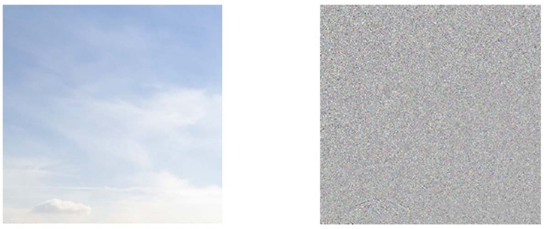

Figure 1: A portion of picture showing blue sky (left), and the corresponding extracted SPN (right).

The Sensor Pattern Noise (SPN) (also known as Photon Response Non-Uniformity - PRNU - in the literature) is the pattern of the noise left by the sensor element of the camera (Lukas et al., 2006), which is due to the unavoidable small differences in light response of each sensitive element (pixel). Differently to the other aforementioned techniques, the SPN exhibits the desired characteristics of uniqueness and stability that make it a proper fingerprint of a camera device. It is produced by the small imperfections and differences among the sensitive elements (pixels) that constitute an imaging sensor; these ultimately result in a deterministic pattern of small pixel intensity variations that appear in the image, much like a noise (Lukas et al., 2006). The SPN has been studied and tested in various forensic tasks, e.g.: source device identification (Chen et al., 2008; Fridrich, 2009; Kang et al., 2012; Li and Li, 2012; Li and Satta, 2011; Li and Satta, 2012; Lukas et al., 2006), forgery detection (Chen et al., 2008; Fridrich, 2009; Li and Li, 2012), source device linking (Fridrich, 2009), clustering of images with respect to the source camera (Caldelli et al., 2010), identification of the possible author of a photo from its social network account (Satta and Stirparo, 2014).

A common way to extract the SPN from an image P is by exploiting the additive noise model proposed by Lukas et al. (Lukas et al., 2006):

$$n_P = P - F(P) \tag{1}$$

where n_P is the noise residual and F is a denoising filter, which should ideally extract non-noise (typically low-frequency) components of P.

Usually, SPN extraction is carried out in a transformed domain (e.g., Fourier, Wavelet) as in such domains it comes easier to separate high-frequency components from the image. Most papers use Discrete Wavelet Transforms, with Daubechies 8-tap wavelet and scaling functions, as proposed in (Lukas et al., 2006). In this case, Eq. ((1)) becomes:

$$n_P = DWT(P) - F_{DWT}\big(DWT(P)\big) \tag{2}$$

[1] http://www.photoshop.com/products/photoshop

[2] http://en.wikipedia.org/wiki/ExifTool

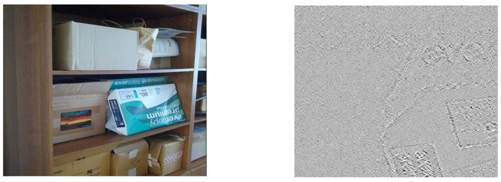

Figure 2: Example artefacts produced by high-frequency components of the image.

where $DWT(\cdot)$ denotes the Discrete Wavelet Transform, and F_{DWT} refers to a de-noising filter in the wavelet domain.

Regarding F_{DWT}, the usage of an adaptive Wiener de-noising filter has been proposed in (Lukas et al., 2006); such a filter has been then adopted in various works (Chen et al., 2008; Fridrich, 2009; Kang et al., 2012; Li and Li, 2012; Li and Satta, 2012; Satta and Stirparo, 2014), and produces SPNs similar to the one shown in Fig. 1 as example. The interested reader is referred to Appendix A of (Lukas et al., 2006) for additional details on the filter.

Given a *template* SPN n_C corresponding to one known camera C, a common approach to perform a comparison (Li and Li, 2012; Li and Satta, 2012; Lukas et al., 2006; Satta and Stirparo, 2014) is to compute the Normalised Cross-Correlation (NCC), which is defined as

$$\rho(n_P, n_C) = \frac{(n_P - \bar{n}_P) \cdot (n_C - \bar{n}_C)}{\|n_P - \bar{n}_P\| \cdot \|n_C - \bar{n}_C\|} \qquad (3)$$

where $\bar{n}_P$ and $\bar{n}_C$ are the means of n_P and n_C, respectively. The value of $\rho(n_P, n_C)$ measures the likelihood that P has been taken with the camera T.

3 A RELIABILITY MAP FOR SPN

While effective, the implementation of SPN extraction using the additive noise model of Eq. (2) and Wiener filtering can produce far-from-perfect results. In particular, high-frequency components of the image (highly textured regions, edges, etc.) tend to be deemed as being part of the SPN instead. An example is provided in Fig. 2.

In this paper, we argue that those artefacts can be located in a given image by using common edge detectors (Oskoei and Hu, 2010). In particular, the power of an edge may be taken as roughly representing the likelihood that the SPN extracted in that location will be affected by artefacts. As such, it can be used as a weight of the corresponding pixels during matching.

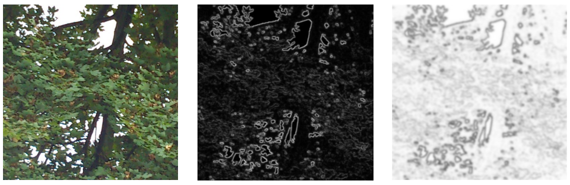

Figure 3: From left to right: steps for creating the reliability map (see the text for details).

Following the above statement, in this work a reliability map is generated from a given picture P through the following procedure (see Fig. 3):

1. An edge power image E is produced from P, by using a simple difference-based edge detector, which for each pixel calculates the maximum difference between pixels around it in 4 directions.
2. The map E is inverted so that edges (pixels with maximum edge power) will have the lowest weight, and normalised in $(0,1)$.
3. E is filtered through a 11×11 Gaussian filter with $\sigma = 15$, in order to mitigate spikes and to "distribute" the energy of edge pixels to surrounding non-edge ones, which still are likely to contain some artefacts.

Such a reliability map is then utilised as source of weights for each pixel when matching the SPN n_P extracted from P, with a given template SPN n_C corresponding to a camera C. In order to do so, in place of the Normalised Cross-Correlation of Eq. (3), a Weighted Normalised Cross-Correlation (WNCC) is used, defined as:

$$\rho_w(n_P, n_C, w_P) = \frac{w_P \cdot (n_P - \hat{n}_P) \cdot (n_C - \hat{n}_C)}{\|w_P(n_P - \hat{n}_P)\| \cdot \|w_P(n_C - \hat{n}_C)\|} \qquad (4)$$

where w_P is the vector of weights computed from P using the above mentioned procedure, and $\hat{n}_P$ and $\hat{n}_C$ are the *weighted* averages of n_P and n_C, respectively.

4 EXPERIMENTAL EVALUATION

In this Section, the proposed technique is tested in a source camera classification task. The data set used for the tests is described in Sect. 4.1. Experiment set-up and results are presented and commented in Sect. 4.2.

4.1 Data Set

The data set is composed of images coming from 27 different smart-phones of different brands and mod-

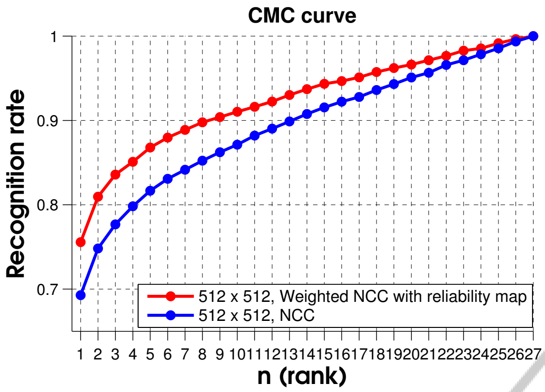

Figure 4: Cumulative Matching Characteristics curve attained by the proposed reliability map-based method, compared with standard SPN matching, using a window of size 512×512.

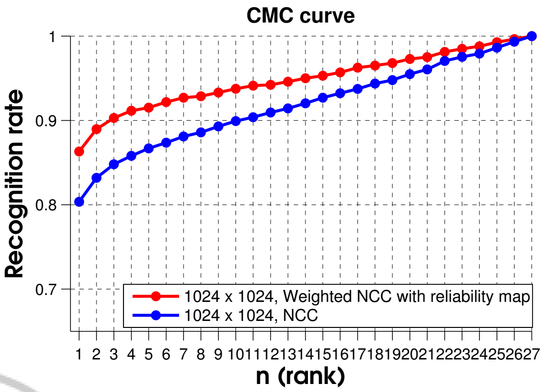

Figure 5: Cumulative Matching Characteristics curve attained by the proposed reliability map-based method, compared with standard SPN matching, using a window of size 1024×1024.

els (see Table 1). Specifically, for each device 10 pictures showing a clean white wall have been captured as templates, and 100 pictures showing various indoor and outdoor environments have been captured as probe/test images. In total, the data set contains 2970 images (2700 test images and 270 template images). All pictures have been taken with the maximum resolution and JPEG quality allowed by the device.

4.2 Experimental Set-up and Results

Experiments have been carried out to replicate a camera identification scenario, as follows. First for each device, a template SPN has been created, by extracting the SPN from the 10 template images provided by the data set, and averaging them. Then, an SPN and a reliability map has been extracted from each of the test images, and matched with templates using Eq. (4). Templates have been ranked with respect to the similarity to the test. The SPN has been extracted from a window of 512×512 and 1024×1024 pixels, positioned in the centre of the image (where the SPN typically exhibits a better quality (Li and Satta, 2011; Li and Satta, 2012)).

Table 1: Devices used to build the benchmark data set.

Brand	Model	Nr of. devices
Apple	IPhone 4	5
Apple	IPhone 4S	2
Blackberry	Bold 9900	2
Blackberry	Torch 9800	1
HTC	One X	3
HTC	7 Mozart	1
Motorola	Milestone 2 Motoblur	1
Samsung	Galaxy Ace	1
Samsung	Galaxy Nexus	3
Samsung	Galaxy Nexus S	1
Samsung	Galaxy Nexus S3	1
Samsung	Galaxy Nexus S4	1
Simvalley	SPX-5	1
Sony	Xperia S	3
Sony	Xperia Sola	1

Results are shown in Fig. 4 and Fig. 5, respectively for a window of 512×512 and 1024×1024 pixels, and expressed in terms of Cumulative Matching Characteristics (CMC) curve. The CMC is a commonly used way of measuring identification performance, which expresses the cumulative probability of having the true class (device) within the first *n* ranks. In both cases, the performance of the proposed reliability map-based method is higher than the one attained using standard, non-weighted matching.

5 CONCLUSIONS

In this work, a novel method for matching SPNs by weighting the importance of each pixel based on a reliability map, has been presented. The rationale followed to build the reliability map comes from the empirical observation that high frequency components of an image, such as textured regions, might be mistakenly taken as SPN during the extraction process.

Results obtained in a benchmark corpus made up of 2970 pictures proved that the proposed technique provides a robust performance improvement in a source camera identification task. Future work includes trying more advanced ways of assessing the reliability of pixels, e.g. by analysing the spectrum in the frequency domain. Also, the proposed technique can likely be used to increase the performance in other tasks involving SPN fingerprints, e.g., one-to-one source camera verification and clustering.

REFERENCES

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

Cao, H. and Kot, A. C. (2009). Accurate detection of demosaicing regularity for digital image forensics. *IEEE Transactions on Information Forensics and Security*, 4(4):899–910.

Chen, M., Fridrich, J., Goljan, M., and Lukas, J. (2008). Determining image origin and integrity using sensor noise. *IEEE Transactions on Information Forensics and Security*, 3(1):74–90.

Choi, K. S., Lam, E. Y., and Wong, K. K. Y. (2006). Automatic source camera identification using the intrinsic lens radial distortion. *Optics Express*, 14(24):11551–11565.

Dirik, A. E., Sencar, H. T., and Memon, N. (2008). Digital single lens reflex camera identification from traces of sensor dust. *IEEE Transactions on Information Forensics and Security*, 3(3):539–552.

Fridrich, J. (2009). Digital image forensic using sensor noise. *IEEE Signal Processing Magazine*, 26(2):26–37.

Kang, X., Li, Y., Qu, Z., and Huang, J. (2012). Enhancing source camera identification performance with a camera reference phase sensor pattern noise. *IEEE Transactions on Information Forensics and Security*, 7(2):393–402.

Li, C.-T. and Li, Y. (2012). Color-decoupled photo response non-uniformity for digital image forensics. *IEEE Transactions on Circuits and Systems for Video Technology*, 22(2):260–271.

Li, C.-T. and Satta, R. (2011). On the location-dependent quality of the sensor pattern noise and its implication in multimedia forensics. In *Proceedings of the 4th International Conference on Imaging for Crime Detection and Prevention 2011 (ICDP 2011)*, page 37.

Li, C.-T. and Satta, R. (2012). Empirical investigation into the correlation between vignetting effect and the quality of sensor pattern noise. *IET Computer Vision*, 6:560–566(6).

Long, Y. and Huang, Y. (2006). Image based source camera identification using demosaicking. In *2006 IEEE 8th Workshop on Multimedia Signal Processing*, pages 419–424.

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

Oskoei, M. A. and Hu, H. (2010). A survey on edge detection methods. Technical Report CES-506, University of Essex, UK.

Popescu, A. and Farid, H. (2005). Exposing digital forgeries in color filter array interpolated images. *IEEE Transactions on Signal Processing*, 53(10):3948–3959.

Satta, R., Galbally, J., and Beslay, L. (2013). State-of-the-art review: Video analytics for fight against on-line child abuse. Technical Report JRC85864, European Commission - Joint Research Centre.

Satta, R. and Stirparo, P. (2014). On the usage of sensor pattern noise for picture-to-identity linking through social network accounts. In *Proceeding of the International Conference on Computer Vision Theory and Applications Lisbon (VISAPP), Portugal*.

Sorrell, M. J. (2009). Digital camera source identification through jpeg quantisation. In Li, C.-T., editor, *Multimedia forensics and security*. Information Science Reference.

Van, L. T., Emmanuel, S., and Kankanhalli, M. (2007). Identifying source cell phone using chromatic aberration. In *2007 IEEE International Conference on Multimedia and Expo*, pages 883–886.