SOURCE CAMERA IDENTIFICATION USING ENHANCED SENSOR PATTERN NOISE

Chang-Tsun Li

Department of Computer Science, University of Warwick, Coventry CV4 7AL, UK
c-t.li@warwick.ac.uk

ABSTRACT

Sensor pattern noises (SPN), extracted from digital images as device fingerprints, have been proved as an effective way for digital device identification. However, the limitation of the current method of extracting the sensor pattern noise is that the SPNs extracted from images are highly contaminated by the details from the scene and as a result the misclassification rate is high unless images of large size are used. In this work we propose a novel approach for enhancing sensor pattern noises so as to improve the performance of the identifier. The hypothesis underlying our fingerprint enhancer is that the stronger a signal component is, the less trustworthy the component should be and thus should be attenuated. An enhanced fingerprint can be obtained by assigning weighting factors inversely proportional to the magnitude of the signal components.

***Index Terms*—**Source device identification, digital forensics, digital investigation, sensor pattern noise

1. INTRODUCTION

While digital imaging devices, such as digital cameras and scanners, bring unquestionable convenience of image acquisition, powerful image processing software also provides means for editing images so as to serve good and malicious purposes. To combat image manipulations for malicious purposes, researchers have proposed ways of verifying the integrity of images based on the detection of local inconsistencies of device attributes or data processing related characteristics, such as sensor pattern noise (SPN)[1-3], camera response function [4], resampling artifacts [7], color filter array (CFA) interpolation artifacts [8, 13], and JPEG compression [10, 11]. Similar device attributes and data processing related characteristics have also been exploited to identify and classify the source devices in aiding forensic investigations [2, 6, 9, 12]. While many methods [4, 7, 8, 13] require that specific assumptions be satisfied, methods based on sensor pattern noise have drawn much attention due to the relaxation of the similar assumptions. The deterministic component of pattern noise (SPN) is mainly caused by imperfections during the sensor manufacturing process and different sensitivity of pixels to light due to the inhomogeneity of silicon wafers [5]. It is because of the inconsistency and the uniqueness of manufacturing imperfections and sensitivity to light that even sensors made from the same silicon wafer would possess uncorrelated pattern noise, which can be extracted from the images produced by the devices. This property makes sensor pattern noises a robust fingerprint for identifying the origin and verifying the integrity of images.

The commonly adopted model proposed in [6] for extracting the SPN, n, from an image I is

$$n = I - F(I) \tag{1}$$

where F is a denoising function which filters out the sensor pattern noise. Although various denoising filters can be used as F, the wavelet-based denoising filter described in Appendix A of [6] has been reported as effective in producing good results. However, the key limitation of Eq. (1) is that the SPN, n, is highly contaminated by the details from the scene. For example Figure1 (a), (b) and (c) show a reference SPN of a camera, which is the average SPN of 50 images of blue sky taken by a digital camera, an image of a natural scene taken by the same camera, and the SPN extracted from that image, respectively. Figure 1(a) is what a clean SPN should look like. However, from Figure 1(c) we can see that the SPN contains strong details from the scene, which dominates the real SPN. To improve the accuracy of source device identification, the contaminated SPN need to be cleansed or enhanced. The hypothesis underlying our fingerprint enhancer is that

> The stronger a signal component in n is, the less trustworthy the component should be. An enhanced fingerprint n_e can be obtained by assigning weighting factors inversely

proportional to the magnitude of the signal components.

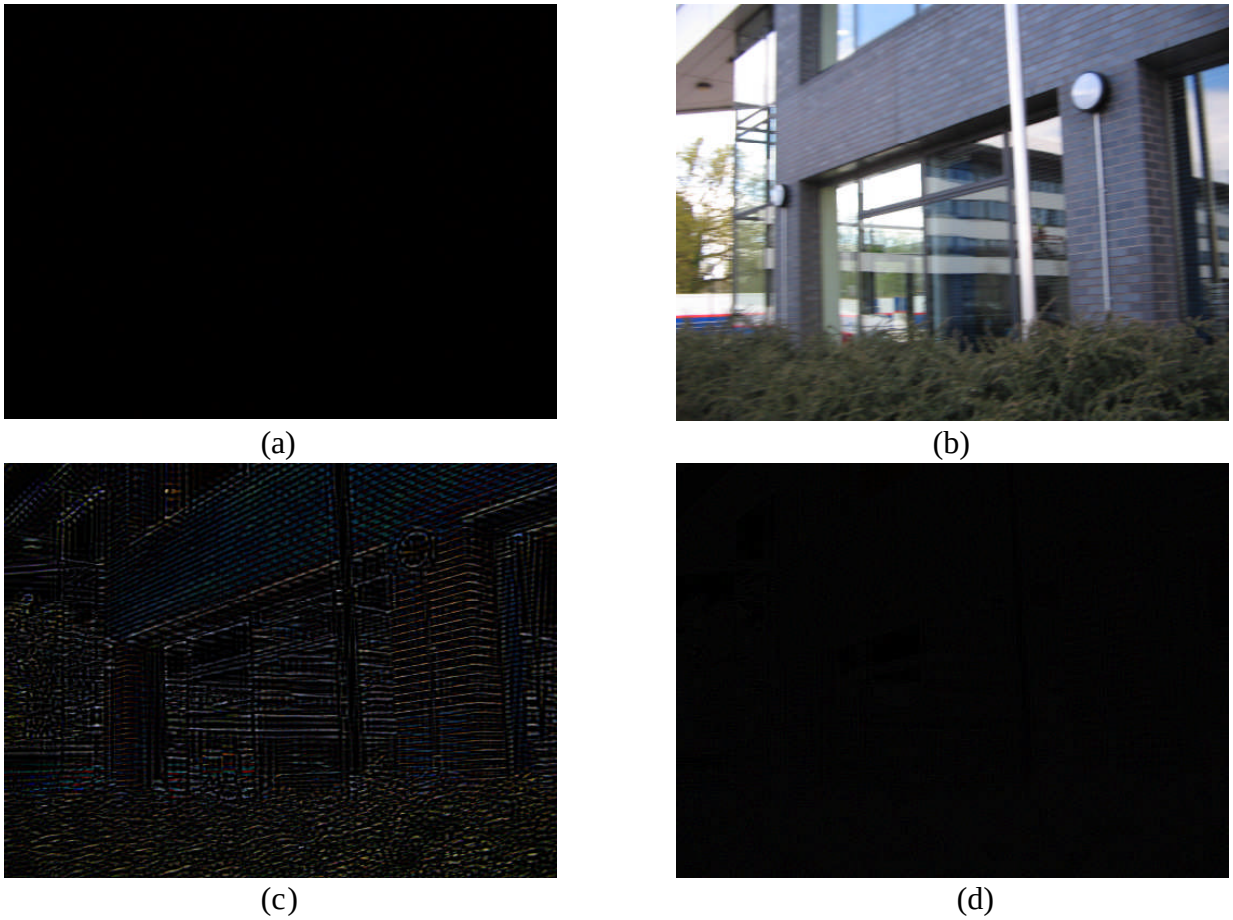

Figure 1. (a) A clean fingerprint taken from blue sky images, (b) An image of natural scene, (c) The SPN extracted from Figure 1(b) contaminated by the details from the scene. (d) The enhanced version of Figure 1(c) using Eq. (2).

2. PROPOSED SENSOR PATTERN NOISE ENHANCER

In this work, we use Eq. (1) in conjunction with the wavelet-based denoising filter described in Appendix A of [6] to extract contaminated SPNs and use Eq. (2) as *camera fingerprint enhancer* to realize the afore-mentioned hypothesis.

$$n_e(i,j)=\begin{cases} e^{-0.5\frac{n^2(i,j)}{\alpha^2}} & ,\text{if } 0\le n(i,j) \\ -e^{-0.5\frac{n^2(i,j)}{\alpha^2}} & ,\text{otherwise} \end{cases} \quad (2)$$

where $n(i,j)$ and $n_e(i,j)$ are the (i,j)th component of n and n_e, respectively. Figure 2(a) illustrates how n is transformed into n_e. We can see that α of Eq. (2) determines the rate n is attenuated and is to be specified by the user. There are various ways of realizing the same hypothesis. Four more models are given in Eq. (3) – (6).

$$n_e(i,j)=\begin{cases} 1-\frac{n(i,j)}{\alpha} & ,\text{if } 0\le n(i,j)\le\alpha \\ -1-\frac{n(i,j)}{\alpha} & ,\text{if } -\alpha\le n(i,j)<0 \\ 0 & ,\text{otherwise} \end{cases} \quad (3)$$

$$n_e(i,j)=\begin{cases} 1-e^{-n(i,j)} & ,\text{if } 0\le n(i,j)\le\alpha \\ (1-e^{-\alpha})\cdot e^{\alpha-n(i,j)} & ,\text{if } n(i,j)>\alpha \\ -1+e^{n(i,j)} & ,\text{if } -\alpha\le n(i,j)<0 \\ (-1+e^{-\alpha})\cdot e^{\alpha+n(i,j)} & ,\text{if } n(i,j)<-\alpha \end{cases} \quad (4)$$

$$n_e(i,j)=\begin{cases} \frac{n(i,j)}{\alpha} & ,\text{if } 0\le n(i,j)\le\alpha \\ e^{-0.5\frac{(n(i,j)-\alpha)^2}{\alpha^2}} & ,\text{if } n(i,j)>\alpha \\ \frac{n(i,j)}{\alpha} & ,\text{if } -\alpha\le n(i,j)<0 \\ -e^{-0.5\frac{(n(i,j)+\alpha)^2}{\alpha^2}} & ,\text{if } n(i,j)<-\alpha \end{cases} \quad (5)$$

$$n_e(i,j)=\begin{cases} \frac{n(i,j)}{\alpha} & ,\text{if } 0\le n(i,j)\le\alpha \\ e^{\alpha-n(i,j)} & ,\text{if } n(i,j)>\alpha \\ \frac{n(i,j)}{\alpha} & ,\text{if } -\alpha\le n(i,j)<0 \\ -e^{\alpha+n(i,j)} & ,\text{if } n(i,j)<-\alpha \end{cases} \quad (6)$$

These four models can also be better presented graphically as demonstrated in Figure 2(b) to (e). Eq. (2) and (3) allow the magnitude of n_e (i.e., $|n_e|$) to *decrease* monotonically with respect to the magnitude of n. Eq. (4) – (6) allow the magnitude of n_e to *grow* monotonically in accordance with the magnitude of n if $|n| \le \alpha$ (a threshold to be decided by the user) and to *decrease* monotonically and rapidly with respect to $|n|$ if $|n| > \alpha$. The five enhancing models can be applied in either spatial domain or frequency domain.

3. EXPERIMENTS

We have carried out a sequence of identification experiments to validate our hypothesis and Eq. (2) – (6) and observed that the optimal value of α for all models is 7. We also observed that the model of Eq. (2) performed better than other models. Figure 1(d) shows the enhanced version of Figure 1(c) after the model of Eq. (2), with α = 7, is applied. We can see that the influential details from the scene, that are prominent in Figure 1(c), have been significantly removed. To demonstrate the performance of the proposed sensor pattern noise enhancer (Eq. (2)), we have carried out identification tests on 600 photos of 1536 × 2048 pixels taken by six cameras, each responsible for 100. The six cameras are Canon IXUS 850IS, Canon PowerShot A400, Canon IXY Digital 500, FujiFilm A602, FujiFilm FinePix A902 and Olympus FE210. All of the photos are JPG compressed at quality level around 97%. Instead of testing the enhancer on the full-sized images only, we also test it on image block of 8 different sizes cropped from the centre of the full-sized images. Table 1 lists the identification rates with and without applying the proposed enhancing model of Eq. (2) to the sensor pattern noises extracted with Eq. (1). We can see that, without enhancing, the identification rate can only reach 99% when the photo size is as big as 1024 × 2048 pixels. On the other hand, after enhancing the sensor pattern noises, an identification rate greater than 99% can be reached at 256 × 512 pixels, which is 8 times smaller than the size at which the same identification rate can be achieved without enhancing the sensor pattern noises.

4. CONCLUSIONS

In this work we have pointed out the sensor pattern noise, as the fingerprint for identifying source imaging devices, extracted with the commonly used model of Eq. (1) proposed in [6] can be contaminated by the details from the scene. To circumvent this limitation we envisaged the hypothesis that *the stronger a component of the sensor pattern noise is, the less trustworthy the component should be* and proposed 5 enhancing models for realising the hypothesis. The hypothesis is tested by assigning greater weighting to the smaller components. Experiments have confirmed the soundness of our hypothesis and high identification rate can be achieved with photos 8 times as small as the size at which the same accuracy can be achieved without enhancing the sensor pattern noise.

5. ACKWONLEDGEMENT

This work has led to a pending UK patent (Application Number 0902406.5). The author would like to thank Forensic Pathways Ltd, UK, for its support of this work.

6. REFERENCES

[1] R. Caldelli, I. Amerini, F. Picchioni and A. De Rosa and F. Uccheddu, "Multimedia Forensic Techniques for Acquisition Device Identification and Digital Image Authentication," in *Handbook of Research on Computational Forensics, Digital Crime and Investigation: Methods and Solutions*, C.-T. Li (Ed.), Hershey, PA: Information Science Reference (IGI Global), Nov. 2009.

[2] R. Caldelli, I. Amerini and F. Picchioni, "Distinguishing between Camera and Scanned Images by Means of Frequency Analysis," *International Journal of Digital Crime and Forensics*, vol. 2, no. 1, Jan – March 2010.

[3] M. Chen, J. Fridrich, M. Goljan, and J. Lukáš, "Determining Image Origin and Integrity Using Sensor Noise," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 1, pp. 74-90, March 2008.

[4] Y. F. Hsu and S. F. Chang, "Image Splicing Detection Using Camera Response Function Consistency and Automatic Segmentation," *Proc. IEEE International Conference on Multimedia and Expo*, Beijin, China, 2 - 5 July 2007.

[5] J. R. Janesick, *Scientific Charge-Coupled Devices*, Bellingham, WA: SPIE, vol. PM83, 2001.

[6] J. Lukáš, 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.

[7] A.C. Popescu and H. Farid, "Exposing Digital Forgeries by Detecting Traces of Resampling." *IEEE Transactions on Signal Processing*, vol. 53, no. 2, pp. 758–767, 2005.
[8] A.C. 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.
[9] B. Sankur, O. Celiktutan, I. Avcibas, "Blind Identification of Cell Phone Cameras," *Proc. SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents IX*, vol. 6505, January 29–February 1, San Jose, CA, pp. 1H–1I, 2007.
[10] M. J. Sorell, "Digital Camera Source Identification through JPEG Quantisation," in *Multimedia Forensics and Security*, C.-T. Li (Ed.), Hershey, PA: Information Science Reference (IGI Global), 2008.
[11] M. J. Sorell, "Conditions for Effective Detection and Identification of Primary Quantisation of Re-Quantized JPEG Images," *International Journal of Digital Crime and Forensics*, vol. 1, no. 2, pp.13-27, April - June 2009.
[12] Y. Sutcu, S. Batram, H. T. Sencar and N. Memon, "Improvements on Sensor Noise based Source camera Identification," in *Proceeding of IEEE International Conference on Multimedia and Expo*, pp. 24 – 27, Beijin, China, 2 - 5 July 2007.
[13] A. Swaminathan, M. Wu and K. J. R. Liu, "Nonintrusive Component Forensics of Visual Sensors Using Output Images," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 1, pp. 91 – 106, March 2007.

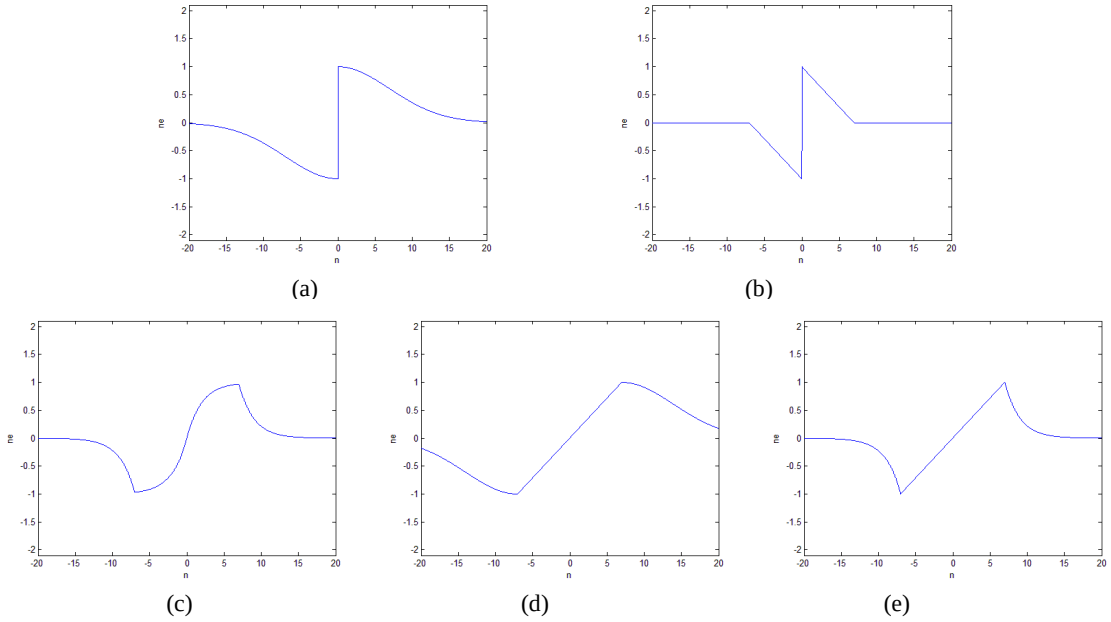

Figure 2. Five models for digital fingerprint enhancement. (a) –(e) correspond to Eq. (2) – (6), respectively.

Table 1. Identification rates with and without enhancing the sensor pattern noise with the enhancer of Eq. (2) with $\alpha = 7$.

	Identification rate (%) at different photo sizes								
	128 ×128	128 × 256	256 × 256	256 × 512	512 × 512	512 ×1024	1024×1024	1024×2048	1536 ×2048
without enhancing	31.67	42.17	48.50	62.50	73.33	86.17	97.33	**99.5**	99.83
with enhancing	86.67	94.33	97.67	**99.17**	99.33	99.50	100	100	100