Digital Investigation 12 (2015) 66–76

Contents lists available at ScienceDirect

Digital Investigation

journal homepage: www.elsevier.com/locate/diin

Adaptive photo-response non-uniformity noise removal against image source attribution

Ahmet Karaküçük, Ahmet Emir Dirik*

Dept. of Electrical-Electronic Engineering, Faculty of Engineering, Uludağ University, Bursa, 16059, Turkey

ARTICLE INFO

Article history:
Received 8 September 2014
Received in revised form 6 January 2015
Accepted 25 January 2015
Available online 17 February 2015

Keywords:
PRNU
Source camera attribution
Sensor noise
Counter forensics
Privacy
Anonymization

ABSTRACT

The main objective of image source anonymization is to protect the identity of the photographer against any attempts to identify the source camera device through PRNU noise analysis. One way of impeding image source attribution is to suppress the PRNU noise as much as possible. In this paper, we introduce an improvement on the existing adaptive photo-response non-uniformity (PRNU) denoising method against source camera identification. We evaluate the performance of the proposed method with substantial experimental analysis. We also provide anonymization benchmarks with other source anonymization techniques. The benchmarks' results show that the proposed method outperforms the adaptive PRNU denoising methods for various cameras including compact and smartphone in terms of speed and image quality. The experimental analysis also shows that it is possible to impede source camera identification by PRNU noise suppression even under extreme attack conditions.

Introduction

Multimedia forensics is a field of forensic science where the materials created by various types of digital systems are investigated, which is usually required during or after the discovery of electronic material from the criminal activities. Various questions regarding the discovered digital material should be answered to determine whether the material is an admissible evidence before the court of law or not. The authenticity (the truthfulness of the origin), the integrity (was the content tampered?) and the time of creation (when this material was recorded?) are just a few questions asked during a digital investigation (Sencar and Memon, 2012). Yet, the digital materials are easily copied, erased, tampered, encrypted, faked, and even be synthesized using the simplest computer software. Therefore it is very challenging for an expert to give answers to the critical questions regarding digital materials.

In this paper, we specifically focus on countering Photo-Response Non-Uniformity (PRNU) based source camera identification (SCI) (Lukáš et al., 2006; Fridrich, 2012) of digital images. PRNU based SCI is based on the exploitation of the non-temporal noise characteristics of the digital imaging sensor, thereby forming a statistically identifiable pattern of the sensor noise in the output image (Lukáš et al., 2006; Fridrich, 2012), which is called sensor or camera PRNU fingerprint. PRNU characteristics of digital imaging sensors found many uses in digital forensics; from image (Lukáš et al., 2005) to video applications (Hyun et al., 2013), from tamper-detection to crop-detection, all being enabled by PRNU's resilience to various image manipulation techniques, such as compression and geometric manipulation. Therefore PRNU noise pattern can be considered as an intrinsic sensor identifier.

Given the fact that the imaging sensors of most consumer-level digital cameras are not replaceable, it can be assumed that a specific PRNU pattern can be linked to

* Corresponding author. Tel.: +90 224 2940 655; fax: +90 224 2941 903.
E-mail address: edirik@uludag.edu.tr (A.E. Dirik).

http://dx.doi.org/10.1016/j.diin.2015.01.017
1742-2876/© 2015 Elsevier Ltd. All rights reserved.

one camera with a specific serial number, i.e. the PRNU based SCI is capable of identifying origin device of an image, around many devices of the same model (Goljan et al., 2009). Therefore, PRNU noise can be used to pinpoint the camera device which could be undesirable for some users, such as photographers and activists who want to protect their privacy and preserve their anonymity while sharing or spreading images (Böhme and Kirchner, 2013). Such practices of PRNU noise can be nullified by counter-forensics techniques, such as *flat-fielding* (Gloe et al., 2007; Böhme and Kirchner, 2013), *seam-carving* (Bayram et al., 2013; Dirik et al., 2014), *adaptive fingerprint removal* (Lukáš et al., 2006; Li et al., 2010), or *adaptive PRNU denoising* (Dirik and Karaküçük, 2014). Among these methods, flat-fielding requires specifically captured images, called “flat-fields” to capture the PRNU of imaging sensors and it is sensitive to JPEG compression (Dirik and Karaküçük, 2014). Seam-carving (Avidan and Shamir, 2007) impedes SCI by destroying pixel-to-pixel synchronization but also changes the aspect ratio of the image, which may not be desirable for some cases (Bayram et al., 2013). Adaptive fingerprint removal is also indicated as an effective method to remove the PRNU of images in (Lukáš et al., 2006), and this claim was investigated in (Li et al., 2010). However, the robustness of this method has not been evaluated in a setting where an adversary or an analyst is able to obtain high quality and different fingerprints, i.e. using new and large number of images. It has been shown in (Rosenfeld and Sencar, 2009) that single or multiple image denoising operations can really suppress the PRNU fingerprint in an image with significant image quality degradation. On the other hand image denoising even it is applied multiple times cannot completely remove the PRNU fingerprint from the image; thus it is not effective to deceive SCI.

Recently, Dirik and Karaküçük proposed an adaptive PRNU denoising (APD) method in (Dirik and Karaküçük, 2014) for image source anonymization. APD method iteratively estimates the power of the PRNU noise of a given image applying adaptive image denoising to suppress the PRNU noise. Provided benchmarks in (Dirik and Karaküçük, 2014) indicate that APD method outperforms both *single denoising* and *flat-fielding*. However, APD method (i) requires relatively large number of iterations and (ii) yields moderate quality images (30–40 dB). To overcome these issues, in this paper, we propose an improved method using adaptive wavelet denoising by extending the previous APD method. To dissolve the naming ambiguity, previous APD method will be recalled as APD-1, whereas the proposed method will be recalled as APD-2.

It is known that the sensor noise estimated in wavelet domain includes less amount of content and significant amount of PRNU noise compared to the spatial domain denoising. As a result, we achieve better convergence property and higher image quality in terms of PSNR and structural-similarity-metric (SSIM) (Wang et al., 2004). In a more realistic setting, APD algorithm can be applied right after the image acquisition for the anonymization of the photographer. Therefore, fast convergence property is essential for practical uses of APD. The robustness of the proposed method to realistic high quality fingerprint attacks was also evaluated experimentally. The PRNU removal performance of the proposed technique was investigated with experimental analysis and compared with the existing counter forensic techniques of Li et al. (2010) and Dirik and Karaküçük (2014).

Although lossy image compression such as JPEG is known to “suppress” the PRNU signal in digital images, source camera identification on lossy compressed images is still feasible (Lukáš et al., 2006). However, suppressed PRNU signal may compromise the applicability of APD methods. Keeping this in mind, it's intuitive to question their ability to impede the SCI under such circumstances. Since most of the digital images on various sharing platforms are compressed with JPEG, it is realistic to assume that the application of the anonymization methods must be evaluated in this setting. Therefore the performance of APD methods on images that has undergone various levels of lossy compression were also evaluated experimentally using the most prominent JPEG encoding. The results show that both APD-1 and APD-2 methods perform well, in terms of the rate of anonymization; while the proposed method APD-2 performs better in terms of image quality w.r.t. the original image output.

We can summarize the main contributions of the paper as follows: 1) Better evaluation of Li et al.'s method in a more realistic setting such that the adversary has access to the camera and utilizes a better camera fingerprint for SCI. To our best knowledge such evaluation has not been reported before in the literature. 2) Benchmarking of the anonymization methods of Li et al., APD-1, and APD-2 in terms of speed, image quality, and performance of the anonymization. 3) Investigation of the effect of JPEG compression to the adaptive PRNU denoising algorithms (Li et al., APD-1, and APD-2): The provided benchmarks evaluate the anonymization algorithms with various quality JPEG image inputs. 4) Robustness evaluation of the APD methods to “extreme” identification attacks using near perfect camera fingerprint F-1000* generated by 1000 images. In general, the number of images used in camera fingerprint estimation is selected around 50 or 100 in the literature. 5) Improvements on Dirik et al.'s (APD-1) method: Using wavelet based denoising, 4 dB image quality improvement is achieved for anonymized images.

The outline of the paper is as follows: Section 2 introduces PRNU based source camera identification briefly. In Section 3, details of the existing counter forensics methods (Li et al. and APD-1) are provided. Proposed source anonymization method (APD-2) is presented in Section 3. Experimental setup and results are given in Section 4. Robustness and performance analysis are also presented in Section 4. Section 5 discusses the experimental results and Section 6 concludes the paper.

PRNU based camera identification

Due to imperfections during the manufacturing process of imaging sensor arrays, reaction of each sensor varies slightly against the same amount of light. This characteristic is known as PRNU and formulated as multiplicative noise. The imaging output model can be represented in vectorized form with element-wise multiplication as (Chen et al., 2008):