Digital Signal Processing 48 (2016) 285–297

Contents lists available at ScienceDirect

Digital Signal Processing

www.elsevier.com/locate/dsp

# Camera model identification based on the generalized noise model in natural images

Thanh Hai Thai [a,*], Florent Retraint [b], Rémi Cogranne [b,1]

[a] Institute of Research and Development, Duy Tan University, 182 Nguyen Van Linh, Da Nang, Viet Nam
[b] ICD, LM2S, ROSAS, UMR 6281, CNRS, Troyes University of Technology, 12 rue Marie Curie, 10010 Troyes cedex, France

ARTICLE INFO

*Article history:*
Available online 20 October 2015

*Keywords:*
Digital forensics
Camera model identification
Hypothesis testing
Natural image model
Nuisance parameters

ABSTRACT

The goal of this paper is to design a statistical test for the camera model identification problem. The approach is based on the generalized noise model that is developed by following the image processing pipeline of the digital camera. More specifically, this model is given by starting from the heteroscedastic noise model that describes the linear relation between the expectation and variance of a RAW pixel and taking into account the non-linear effect of gamma correction. The generalized noise model characterizes more accurately a natural image in TIFF or JPEG format. The present paper is similar to our previous work that was proposed for camera model identification from RAW images based on the heteroscedastic noise model. The parameters that are specified in the generalized noise model are used as camera fingerprint to identify camera models. The camera model identification problem is cast in the framework of hypothesis testing theory. In an ideal context where all model parameters are perfectly known, the Likelihood Ratio Test is presented and its statistical performances are theoretically established. In practice when the model parameters are unknown, two Generalized Likelihood Ratio Tests are designed to deal with this difficulty such that they can meet a prescribed false alarm probability while ensuring a high detection performance. Numerical results on simulated images and real natural JPEG images highlight the relevance of the proposed approach.

## 1. Introduction

Digital forensics has received a great attention from law enforcement agencies and academic researchers in the past decade. Because of dramatic advancement in computing and network technologies, the accessibility and transmission of digital images have been increased remarkably. Digital images can be easily edited, altered or falsified because of a large availability of image editing software tools. Consequently, the reliability and trustworthiness of digital images have been questioned when used as evidence in legal and security domains. Reliable forensic methods are urgently needed by law enforcement agencies to restore the trust to digital images.

### 1.1. State of the art

Generally, digital image forensics involves two key problems: image origin identification and image forgery detection (see [1] and the references therein for a detailed introduction). The problem of image origin identification aims at verifying whether a given image was acquired by a specific camera, or at determining camera models/brands as well as types of imaging mechanism (e.g. scanners, cell-phone cameras, or computer graphics). The image forgery detection aims at detecting any act of manipulation such as splicing, removal or adding in an image.

There are two approaches to address these problems. Active approach such as digital signatures [2] and digital watermarking [3] has some limitations because a dedicated information has to be embedded during the creation of an image, which increases the production cost of digital cameras, and the credibility of information embedded in the image remains questionable. Passive approach has been increasingly studied in the past decade since it does not impose any constraint and does not require any prior information. Forensic analysts have only the suspect image at their disposal and must explore useful information from that image to gather forensic evidence, trace the acquisition device and detect any act of manipulation. Passive approach is based on internal traces left by the camera in a given image. These internal traces can be provided by investigating the image acquisition pipeline; see [4,5] for an overview of the structure and processing stages of

[*] Corresponding author.
*E-mail address:* thanhhai6587@gmail.com (T.H. Thai).

[1] With the financial support from Champagne-Ardenne region, IDENT project.

http://dx.doi.org/10.1016/j.dsp.2015.10.002
1051-2004/© 2015 Elsevier Inc. All rights reserved.

a typical digital camera. Every stage from real-world scene acquisition to image storage can provide clues for forensic analysis.

In image origin identification problem, it is important to distinguish the problem of camera instance identification and the problem of camera model/brand identification. More specifically, fingerprints used for camera instance identification should capture individuality, especially cameras coming from the same model. For camera model/brand identification, it is necessary to exploit fingerprints that are shared between cameras of the same model/brand but discriminative for different camera models/brands.

In general, passive forensic methods proposed for the image origin identification problem can be divided into two fundamental categories. Methods in the first category rely on the assumption that there are differences in image processing techniques and component technologies among camera models. Lens aberration [6], Color Filter Array (CFA) pattern and interpolation algorithms [7–10], and JPEG compression [11] are considered as influential factors for camera model/brand identification. Using these factors, a forensic feature set is provided and used in a machine learning algorithm. The main challenge is that the image processing techniques remain identical or similar, and the components produced by a few manufacturers are shared among camera models. Moreover, as in all applications of machine learning, it is difficult to select an accurate feature set.

Methods in the second category aim at identifying unique characteristics or fingerprints of the acquisition camera device. Sensor Pattern Noise (SPN) is caused by imperfections during the manufacturing process and non-uniformity of photo-electronic conversion due to inhomogeneity of silicon wafers. This is the unique fingerprint which the methods are mainly based on to identify the camera unit. The reader is referred to [12] for the first version of this work and [13–15] for the enhanced version. Two main components of the SPN are the Fixed Pattern Noise (FPN) and the Photo-Response Non-Uniformity (PRNU) noise. The FPN used in [16] for camera unit identification can be compensated by subtracting a dark frame from the output image. Therefore, the FPN is not a robust fingerprint and no longer used in later works. The PRNU, which is directly exploited in [13–15], can be also used for camera model identification as proposed in [17] based on the assumption that fingerprint obtained from images in the TIFF or JPEG format contains traces of post-acquisition processes (e.g. demosaicing) that carry information about the camera model. The ability to extract this noise reliably from a given image is the main challenge in this category due to interference of non-unique operations (e.g. demosaicing and JPEG compression).

### *1.2. Main contributions of the paper*

The present paper addresses the problem of camera model identification based on passive approach. In the literature, a majority of prior works are based on machine learning methods to design a detector. The main drawback is that this framework requires an expensive training stage that comprises many images with different characteristics (e.g. image content or camera settings) from various sources to represent a real-world situation, which might be hardly available in practical forensic situations. Another drawback of all machine learning methods is that the assessment of their statistical performance still remains an open problem [18]. Within this framework, their performance is only evaluated empirically on a large image database and it is difficult to warrant a prescribed false alarm rate.

On the opposite, the approach proposed in this paper is based on hypothesis testing framework [19]. While the application of hypothesis testing is often more complex than the training of a classifier using machine learning methods, this first approach has indisputable advantages. Typically, this approach allows the design of a statistical test that is optimal with respect to a desired criterion, for instance minimizing false alarm probability and maximizing detection power and, very often permits the establishing of theoretical priorities of the optimal test, that is probabilities of false alarm and miss detection. Besides, hypothesis testing usually provides valuable insight into the problem of how each parameter impact the performance of the optimal statistical test.

However, one of the main challenges when applying the hypothesis testing framework is that it requires an accurate statistical image model so the detector can be designed with high performance. In our previous works, hypothesis testing framework has already been exploited to address the problem of camera model identification [20,21]. More specifically, the first camera model identification method [20] proposed within this framework has been targeting RAW images using heteroscedastic noise model. This noise model takes into account the contribution of Poisson noise in the RAW image acquisition process by characterizing the noise variance as a linear function of RAW pixel's expectation [25,26]. However, the RAW format is hardly available in majority of practical forensics applications and most cameras output digital directly in JPEG format. Hence, for a more practical application, we have recently proposed an approach for camera model identification using Discrete Cosine Transform (DCT) coefficients from JPEG images [21]. Those works exploited a state-of-the-art statistical model of DCT coefficients provided in [23,22] that was obtained by studying and modeling the main steps involved in the image processing pipeline of a typical digital camera [22].

It is important to note that the two main differences between the former approach proposed in [20] and the latter one in [21] is that 1) the former exploits noise statistics in the spatial domain while the latter is based on the fact that statistics of DCT coefficients change with different sensor noises combining with various in-camera processing algorithms and 2) those approaches have targeted different image formats, i.e. RAW format for the former and JPEG format for the latter.

It should be noted that, to the best of our knowledge, the problem of camera model identification from rendered natural images (not RAW) in the spatial domain has not been studied within the framework of hypothesis testing theory. The main advantage of using pixels in the spatial domain is that this information is always available regardless the file format and compression scheme. The goal of this paper is thus to study the design of an optimal detector from rendered images and using pixels in the spatial domain.

As noted above, to apply the hypothesis testing theory, it requires a model to represent the rendered image in the spatial domain. Recently, the study of noise statistics in the spatial domain of a rendered digital image has been performed in our previous research [24]. Since the heteroscedastic noise model characterizes accurately a RAW image, it is proposed to start from that model and take into account effects of post-acquisition processes to develop a so-called generalized signal-dependent noise model that has not been proposed yet in the literature. This noise model describes a non-linear relation between output pixel's expectation and variance. The generalized noise model can characterize an original rendered image accurately, see more details in [24]. Similar to [20], the present paper exploits the generalized noise model to design a statistical test within hypothesis testing framework for camera model identification from rendered images. The main contributions are the following:

- The approach is based on the generalized noise model that characterizes accurately the statistical properties of rendered digital image, after in-camera post-acquisition processes. Three parameters $(\tilde{a}, \tilde{b}, \gamma)$ that are specified in the generalized noise model are exploited as camera fingerprint for camera model identification.