J. Vis. Commun. Image R. 25 (2014) 1289–1298

Contents lists available at ScienceDirect

J. Vis. Commun. Image R.

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

A passive multi-purpose scheme based on periodicity analysis of CFA artifacts for image forensics

Tang-You Chang [a,b], Shen-Chuan Tai [a,b], Guo-Shiang Lin [c,*]

[a] Institute of Computer and Communication Engineering, National Cheng Kung University, No. 1, University Road, Tainan City 701, Taiwan, ROC
[b] Department of Electrical Engineering, National Cheng Kung University, No. 1, University Road, Tainan City 701, Taiwan, ROC
[c] Department of Computer Science and Information Engineering, Da-Yeh University, No. 168, University Road, Da-Tsuen, Changhua County 515, Taiwan, ROC

ARTICLE INFO

Article history:
Received 28 January 2014
Accepted 26 April 2014
Available online 15 May 2014

Keywords:
Image forensics
PIM detection
Device class identification
Color filter array

ABSTRACT

We propose a passive multi-purpose scheme for photographic image (PIM) detection and a device class identification method. The motivation for the scheme is the periodicity phenomenon caused by color filter arrays (CFAs) and the demosaicing process. The phenomenon only occurs in the Fourier spectrum in PIMs. The proposed scheme exploits prediction error statistics, local peak detection, and a PIM classifier to analyze the phenomenon for PIM detection. We also develop a hierarchical classifier for device class identification based on the analysis of local peaks in the Fourier spectrum.

To evaluate the scheme's performance, we compile a test dataset of PIMs and PRCG (photorealistic computer graphics) images, and analyze the impact of leak peak detection, JPEG lossy compression, and cropping operations on PIM detection. The accuracy rate of the scheme on 5805 test images is 95.56%, which is higher than that of the methods proposed in Sutthiwan et al. (2009) [1] and Gallagher and Chen (2008) [2]. In addition, for device class identification, the precision rate of the proposed method is at least 93% on Canon, Sony, and Nikon images. The experiment results demonstrate the efficacy of the proposed multi-purpose scheme.

1. Introduction

In recent years, large numbers of digital images have been generated via low-cost multimedia devices, e.g., smart phones and digital cameras. Because of the nature of digital content, it has become easier to copy and manipulate such content without degrading the quality by using sophisticated digital processing tools. For instance, if a car accident is recorded by a car camcorder, the portion of the video that shows the actual accident could be replaced by copying and pasting another sub-sequence over it. In addition, some tools, such as Photoshop and 3D Max, enable non-expert users to create photorealistic computer graphics (PRCG) easily and some recent researches [3,4] focus on producing more realistic image/video. The method for generating PRCG images is described in [5]. Fig. 1(a) and (b) show a photographic image (PIM) and a PRCG image respectively. It is difficult to determine if Fig. 1(b) is a PRCG image. In real applications, content providers can easily generate PRCGs according to their requirements. Powerful tools may be utilized to produce computer generated child pornography or fake images. The potential negative impact on some applications (e.g., criminal investigations) is obvious; therefore, image/video forensics is becoming increasingly important.

Exploiting image/video forensic technology to analyze digital content can provide useful information for solving crimes. Currently, image/video forensics addresses two important issues [6]: source camera identification and forgery detection. The former identifies the source digital device (e.g., a camera, scanner, or mobile phone); and the latter tries to determine whether a digital image/video has undergone any form of manipulation or processing after capture. In this paper, we focus on source camera identification.

Source camera identification can be achieved in two ways: by digital watermarking (active or intrusive [6]) and non-watermarking (passive or non-intrusive [6]) techniques. Digital watermarking [7–9] is used to protect the copyright and authenticate the content of digital media data. The technology can be thought of an active image/video forensics approach because a specific signal (i.e., a watermark) is hidden in an image/video [6]. It is no double that digital watermarks can be embedded into images for source camera identification. For instance, the compressed-domain scheme in [8] provides dual protection for JPEG images based on informed embedding and a two-stage watermark extraction technique. The embedded watermark, which does not affect the visual quality of

* Corresponding author.
E-mail addresses: E2490668@gmail.com (T.-Y. Chang), sctai@mail.ncku.edu.tw (S.-C. Tai), khlin@mail.dyu.edu.tw (G.-S. Lin).

http://dx.doi.org/10.1016/j.jvcir.2014.04.010
1047-3203/

Fig. 1. Examples of PIMs and PRCG images: (a) PIM and (b) PRCG.

the image, can be used to verify the image's content. However, the limitation of digital watermarking technology is that digital cameras must be equipped with a special watermarking chip so that a specific signal (i.e., a watermark) can be embedded in the data. Moreover, data integrity is very important in some applications, e.g., criminal investigation. Distortions resulting from data embedding or malicious operations may not be acceptable in these applications. The reasons motivate us to develop a passive (i.e., non-watermarking) scheme that does not rely on embedded information for digital image/video forensics.

The rationale behind passive image/video forensics is that inherent traces of a digital image resulting from the creation phase and any other subsequent process exist in the image's history. The traces are usually imperceptible to the human eye and illegal uses may not note these traces. As mentioned in [6,10–14], several characteristics of digital signal processing and recording devices can be analyzed and exploited in image/video forensics, e.g., color filter array (CFA), sensor pattern noise, JPEG quantization, blocking artifacts, and quality modification. It is expected that passive methods based on these inherent characteristics can achieve image/video forensics while the image/video quality remains unchanged. However, prior knowledge of an image is often unavailable in real applications. Therefore, we propose a passive-blind scheme for source camera identification.

Source camera identification involves PIM detection (i.e., distinguishing between PIM and PRCG images), device class identification, and identifying the specific device used to capture an image [1,2,15–19]. A number of PIM detection methods have been proposed. Sutthiwan et al. [1] developed a method based on the JPEG 2D array. The method first measures different JPEG 2D arrays in the horizontal and vertical directions. Then, some features derived from the transition probability matrices of different JPEG 2D arrays are analyzed for PIM detection. Lyu and Farid [19] proposed a PIM detection method that extracts statistical features from sub-band images after image decomposition based on quadrature mirror filters. It considers a total of 216 features for PIM detection. In [2], Gallagher and Chen presented a method for distinguishing between PIM and PRCG images. First, a high-pass filter is applied and the variance of each diagonal is estimated in the green channel. Then, the periodicity of the variance signal is analyzed in the Fourier domain for PIM detection.

Some methods have been proposed for device class identification [15–18,20–22]. The objective is to identify the model and/or manufacturer of the device that produced the image in question. In addition to color features, a set of image quality metrics are measured as features [16], which are used to develop a classifier based on the support vector machine (SVM) for device class identification. In [21], Filler et al. proposed a camera model identification method based on photo-response non-uniformity (PRNU), which is the noise that results from the manufacturing process. As PRNU is modified by in-camera processing, it can be exploited to identify the camera brand or model. Generally, device class identification can be regarded as the pre-processing stage of specific device identification. Information about the company that produced the camera used to capture the image in question can facilitate specific device identification.

A huge number of images are stored on and/or transmitted via the Internet. When the authenticity of an image is in doubt, the first step of source camera identification can determine whether or not the image was produced by a camera (i.e., PIM detection). Then, device class identification or specific device identification techniques can be applied according to the type of application, e.g., video surveillance and criminal investigation. We posit that a scheme that combines PIM detection and device class identification would improve the efficiency and accuracy of image forensics. Currently, there is a dearth of multi-purpose image forensics schemes. To fill this gap, we propose a multi-purpose passive-blind scheme for PIM detection and source class identification.

The remainder of this paper is organized as follows. In Section 2, we describe the proposed scheme. In Sections 3 and 4, we elaborate on the PIM detection and device class identification aspects of the scheme respectively; and in Section 5, we discuss the experiment results. Section 6 contains our concluding remarks.

2. System description

It is known that, except professional triple-CCD/CMOS cameras, CFA is an important component in consumer grade cameras. Fig. 2 shows some examples of CFAs. The most popular CFA, called the Bayer array, comprises three color[1] filters that sample red, green, and blue information. Because only one color is sampled in each pixel, the other two colors must be estimated to produce a three-channel color image. The demosaicing process, also called CFA interpolation, estimates the missing color information required for commercial-grade cameras. Usually, the process estimates the values of the missing pixels by interpolating the known values of the neighboring pixels in each color channel. The derived traces can then be analyzed by image forensic techniques. Note that the traces should not appear in PRCG images. In addition, most companies use different CFAs and demosaicing algorithms. Here, we present the proposed multi-purpose scheme, which is based on the analysis of CFAs and demosaicing.

The color filters in CFAs are usually organized periodically [23]. In some demosaicing algorithms (e.g., [23–25]), the estimation of the value of the new lattice based on the known values can be regarded as a filtering process in which an interpolation kernel is periodically applied to the original image. Moreover, it has been found that the variance of the prediction error of acquired pixels is higher than that of interpolated pixels [26]. Therefore, based on Fig. 2, we expect that higher variances appear at acquired pixels so that the variance of the prediction error in each color channel is a periodic signal. It is no double that the phenomenon also occurs in the Fourier domain. Fig. 3 illustrates the Fourier spectrums of variances in the prediction error in the diagonal, vertical, and horizontal directions. The first three rows of the figure were obtained from images captured by Canon, Nikon, and Sony cameras; and the last row was measured from PRCG images. There are obvious peaks in the Fourier spectrum of the PIMs, and the Fourier spectrums of the PRCG images are noisy. In addition, different CFAs and demosaicing algorithms are often used for different manufacturers. It is assumed that the pattern of local peaks resulting from CFA and demosaicing can be analyzed for source class identification.

Based on the above observations, we propose a scheme for analyzing the Fourier spectrums of the variances in the prediction

[1] For interpretation of color in Fig. 2, the reader is referred to the web version of this article.