Pattern Recognition Letters 39 (2014) 92–101

Contents lists available at ScienceDirect

Pattern Recognition Letters

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

# Open set source camera attribution and device linking

Filipe de O. Costa [a], Ewerton Silva [a], Michael Eckmann [b], Walter J. Scheirer [c,d], Anderson Rocha [a,*]

[a] Institute of Computing, University of Campinas (Unicamp), Av. Albert Einstein, 1251, Cidade Universitária "Zeferino Vaz", Campinas, SP CEP 13083-852, Brazil
[b] Dept. of Mathematics and Computer Science, Skidmore College, Saratoga Springs, NY 12866, USA
[c] School of Engineering and Applied Sciences, Harvard University, 29 Oxford Street, Cambridge, MA 02138, USA
[d] Dept. of Molecular and Cellular Biology, Center for Brain Science, Harvard University, 52 Oxford Street, Cambridge, MA 02138, USA

ARTICLE INFO

*Article history:*
Available online 21 September 2013

Communicated by S. Sarkar

*Keywords:*
Open set recognition
Camera attribution
Device linking
Decision boundary carving

ABSTRACT

Camera attribution approaches in digital image forensics have most often been evaluated in a closed set context, whereby all devices are known during training and testing time. However, in a real investigation, we must assume that innocuous images from unknown devices will be recovered, which we would like to remove from the pool of evidence. In pattern recognition, this corresponds to what is known as the *open set recognition problem*. This article introduces new algorithms for open set modes of image source attribution (identifying whether or not an image was captured by a specific digital camera) and device linking (identifying whether or not a pair of images was acquired from the same digital camera without the need for physical access to the device). Both algorithms rely on a new multi-region feature generation strategy, which serves as a projection space for the class of interest and emphasizes its properties, and on *decision boundary carving*, a novel method that models the decision space of a trained SVM classifier by taking advantage of a few known cameras to adjust the decision boundaries to decrease false matches from unknown classes. Experiments including thousands of unconstrained images collected from the web show a significant advantage for our approaches over the most competitive prior work.



## 1. Introduction

With the rise of digital photography, a growing number of digital images have become associated with evidentiary pools for criminal and civil proceedings. This presents an often frustrating dilemma for those charged with verifying the integrity and authenticity of such images, since they are not always generated by known devices, and can be modified with ease (Rocha et al., 2011). Moreover, with an estimated 250 million images being added to Facebook every day[1] from an enormous set of unknown sources, looking for images from a particular camera of interest becomes a significant challenge. In this article, we investigate a fundamentally new approach for the specific problems of *Image Source Attribution* and *Device Linking* in the context of open set recognition, where not all cameras are known during training time (Fig. 1).

Similar to a ballistics exam in which bullet scratches allow forensic examiners to match a bullet to a particular gun (Li, 2002), image source attribution techniques look for artifacts left in an image by the source camera such as dust on the lens, the interaction between device components and the light, factory defects, and other effects (Swaminathan et al., 2009). Sensor attribution problems span a variety of devices such as cameras (Kurosawa et al., 1999; Dirik et al., 2008; Lukáš et al., 2006; Li, 2010), printers (Chiang et al., 2009; Kee and Farid, 2008), and scanners (Khanna et al. 2007; Khanna et al., 2009). Beyond a basic examination of the EXIF headers, which contain textual information about the digital camera type and the conditions under which the photograph was taken but can be easily tampered with or destroyed (Rocha et al., 2011), a class of methods exists that identifies the brand/model of the source camera (Popescu and Farid, 2005; Kharrazi et al., 2004) by directly considering the image data. These methods generally perform an analysis of color interpolation algorithms. However, many camera brands use components by only a few factories, and the color interpolation algorithm is the same (or very similar) among different models of the same brand of cameras (Rocha et al., 2011; Swaminathan et al., 2009).

Since fine-grained categorization is of more value to the field of digital image forensics, most source attribution approaches have the objective of identifying the specific camera that took a photograph instead of just the device's brand and model. There is some previous work that analyzes device defects for image source identification (Kurosawa et al., 1999; Geradts et al., 2001), as well as artifacts caused by dust on the lens at the time the image was taken (Dirik et al., 2008). The problem with such methods is that some current camera models do not contain any obvious defects,

* Corresponding author. Tel.: +55 19 3521 5854; fax: +55 19 3521 5838.
*E-mail addresses:* filipe.costa@ic.unicamp.br (F. de O. Costa), ewerton.silva@ic.unicamp.br (E. Silva), meckmann@skidmore.edu (M. Eckmann), wscheirer@fas.harvard.edu (W.J. Scheirer), anderson.rocha@ic.unicamp.br (A. Rocha).

[1] Public disclosure to the U.S. Securities and Exchange Commission by Facebook: http://goo.gl/cAU0O.

0167-8655/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.patrec.2013.09.006

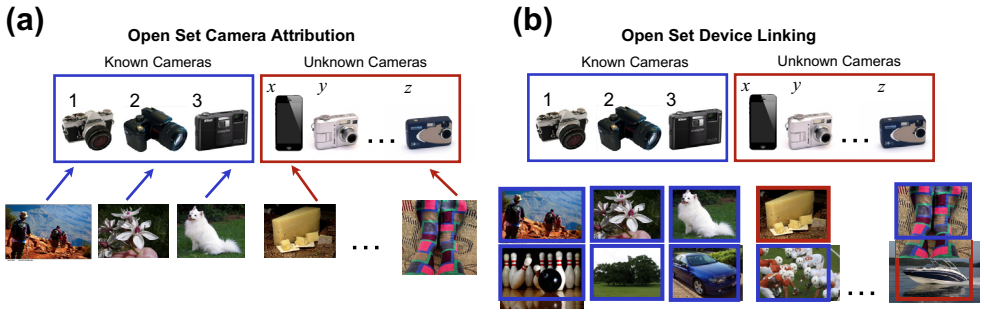


**Fig. 1.** Image source camera attribution is the process of identifying whether or not an image was captured by a specific digital camera. Device linking is the process of identifying whether or not a pair of images comes from the same digital camera – without the need for physical access to the device. While much progress has been made in both areas, the most promising recent approaches (Lukáš et al., 2006; Li, 2010; Goljan and Fridrich, 2007) restrict evaluation to a closed set scenario, where all cameras are known during training and testing. For instance, closed set camera attribution considers only images from known cameras during training and testing (blue cases in (a)), while closed set device linking considers matched and non-matched pairs of images from known cameras (blue cases in (b)). A more realistic scenario for real world investigations is open set evaluation, where during testing (the operational scenario) we must consider images from unknown cameras. For camera attribution, images from unknown cameras should be rejected to avoid false attribution (*e.g.* the red arrow cases in (a)). Similarly, pairs of images containing images from unknown cameras should also be rejected to avoid false linking (*e.g.* the red/blue and blue/red pairs on the right of (b)). (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

while others eliminate defective pixels by post-processing their images on-board. Further, some artifacts are strictly temporal by nature and can be easily destroyed (*e.g.*, the lens may be cleaned or switched). In response, forensic experts have given special attention to methods based on sensor pattern noise (SPN) because they can identify specific instances of the same camera model by using the deterministic component of SPN (Lukáš et al., 2006; Li, 2010). This component is a robust fingerprint for identifying source cameras and verifying the integrity of images because it is the result of factors such as the variable sensitivity of each sensor element to light, the inhomogeneity of silicon wafers, and the uniqueness of manufacturing imperfections that even sensors of the same model possess (Rocha et al., 2011; Swaminathan et al., 2009; Lukáš et al., 2006).

SPN is also useful for cases in which all a forensic examiner has is a set of photographs and the question is to determine whether or not the photographs were taken by the same camera. This challenge is known in the literature as device linking. With device linking methods, we can attest that a set of images was taken by a specific camera by comparing each image to another image that we know belongs to the specific camera – without needing physical access to it. This is a practical problem with potentially important implications in the age of social media. With the possibility of different photo albums spread across sites (Flickr, Facebook, Picasa, etc.), useful evidence can be isolated if an investigator knows that certain suspect images came from the same device, even if she only has access to the public images, and not the camera itself. Solutions to this problem also apply to the scenario of discovering whether or not illegal photos posted on the Internet were generated by a known stolen camera (when an investigator is in possession of a collection of reference images). Further, the commercial space has also expressed interest in the device linking problem: a premium service is already available for public and private investigators[2].

Nearly all of the prior work in image source attribution and device linking was evaluated in a closed set scenario, in which one assumes that an image under investigation was generated by one of $n$ known cameras available during training. However, it is possible that the image may have been generated by an unknown device not available during training (*i.e.*, in the set of suspect devices under investigation). Therefore, it is essential to model attribution problems as *Open Set* scenarios (Fig. 1), which resemble a realistic situation where we only have partial knowledge of the world we are modeling. In this case, we need a classification model for the few available classes (cameras under investigation), while trying to take the large unknown set of unavailable cameras into consideration.

In this article we describe a new feature generation approach for open set classification, as well as a new method for adjusting the decision boundary of an SVM classifier, based on the available knowledge of the world during training, called *decision boundary carving* (de Oliveira Costa et al., 2012). For image source attribution in an open set scenario, we obtain better results compared to state-of-the-art approaches for a very large dataset composed of 13, 210 images from 400 different cameras, including "in the wild" images from 375 cameras taken from public Flickr albums. Similarly, we achieve higher accuracies for the device linking problem in an open set scenario for a dataset composed of 25,000 pairs images sampled from the same set used for attribution. Our approach can be used by investigators to analyze images with different resolutions and acquisition circumstances, with good classification results across all conditions. In addition, the classification methods we propose are general enough to also be useful in a diverse set of classification problems outside of the realm of forensics.

Our contributions in this article, which is an extension of our recent conference paper (de Oliveira Costa et al., 2012), can be summarized as follows:

1. A review of the recent literature on camera attribution problems in the context of realistic open set recognition scenarios.
2. A new feature generation approach that addresses the open set classification problem in digital image forensics by serving as a projection space for the class of interest.
3. Algorithms for image source attribution and device linking incorporating decision boundary carving – a new approach for modeling the decision space of a trained SVM.
4. Large scale open set experimentation incorporating thousands of unconstrained images from the web, including an assessment of statistical significance for all algorithms considered.

## 2. Related work

To expand upon what we have touched on above, the problem of matching an image to the device that captured it is known in the forensics literature as *image source attribution* (Rocha et al., 2011). There are several features one can rely on for tackling this

[2] Quintel Intelligence: http://goo.gl/0pRN9.