Chapter 3
An Overview on Passive Image Forensics Technology for Automatic Computer Forgery

Jie Zhao
School of Computer and Information Engineering, Tianjin Chengjian University, Tianjin, China

Qiuzi Wang
School of Electronic Information Engineering, Tianjin University, Tianjin, China

Jichang Guo
School of Electronic Information Engineering, Tianjin University, Tianjin, China

Lin Gao
College of Software, Nankai University, Tianjin, China & School of Computer and Information Engineering, Tianjin ChengJian University, Tianjin, China

Fusheng Yang
School of Computer and Information Engineering, Tianjin Chengjian University, Tianjin, China

ABSTRACT

Currently, with the popularity of sophisticated image editing tools like Photoshop, it is becoming very difficult to discriminate between an authentic image and its manipulated version, which poses a serious social problem of debasing the credibility of photographic images as definite records of events. Passive image forgery detection technology, as one main branch of image forensics, has been regarded as the promising research interest due to its versatility and universality. Automatic computer forgery employs computer intelligent algorithms to forge an image in an automatic way, which is rather more complex than copy-move forgery since the source of duplicated region could be non-continuous. In this paper, the authors provide a comprehensive overview of the state-of-the-art passive detection methods for automatic computer forgery.

DOI: 10.4018/978-1-7998-3025-2.ch003

1. INTRODUCTION

During the past decade, digital image forensics has attracted great research interests since the prevalence of sophisticated image editing softwares have caused a large number of digital forgery image without obvious traces, which poses a serious social problem of debasing the credibility of photographic images as definite records of events. Currently, image forensics techniques can be broadly classified into two categories: active forensics and passive forensics. Active forensics represented by digital watermark requires prior knowledge about the original image, the drawback of which is that an imperceptible digital code must be inserted at the time of recording. In contrast, passive forensics aims at identifying the authenticity of an image without any prior knowledge which works by assuming that even though the doctored images do not reveal any visual artifacts, the underlying statistics of these images would be distinct from the original ones. Owing to its incomparable advantage, passive forensics has been regarded as the promising research interest in the field of image forensics.

Currently, a large number of passive techniques have been proposed for the exposure of image forgeries, which include source device identification (Chen, 2008), copy-move forgery (Yu, 2016; Silva, 2015), image splicing (Fan, 2015; Zhao, 2015), double JPEG compression (Taimori, 2015), lighting inconsistency (Johnson, 2007), resampling (Wei, 2010), etc. Note that almost all the above-mentioned methods are developed for artificial processing images. In other words, counterfeit images are produced by forgers using professional image editing software such as Photoshop, which is time-consuming and inconvenient to make a doctored image with no obvious traces. Conversely, it is more efficient and convenient to employ automatic intelligent algorithms to forge an image that reduces the complexity of image processing to a certain extent. Up to present, however, little study has been done on passive forensics approaches for this kind of fake images.

In this paper, the authors attempt to provide a complete and comprehensive overview of the state-of-the-art passive detection algorithms for automatic computer forgery. The rest of this survey is organized as follows. Section 2 briefly introduces automatic computer forgery techniques, particularly exemplar-based inpainting and seam carving. Section 3 focuses on the review of existing passive forensics methods for automatic computer forgery with their advantages and disadvantages. Finally, discussion and conclusion are presented in section 4.

2. REVIEW OF AUTOMATIC COMPUTER FORGERY TECHNIQUES

The automatic computer forgery techniques denoted in this paper refer to image inpainting and seam carving, both of which can achieve object removal. In this section, these two kinds of forgery techniques will be briefly introduced.

2.1. Image Inpainting

Image inpainting is an intelligent image processing algorithm to fill in undesired portions using the information from the remaining area of the image in an automatic way, which is playing a significant role in contents correction and image restoration in recent years. The original purpose of image inpainting is used to restore the loss information in old photographs, remove image scratches, and conceal errors in videos. However, it could also be a forgery manipulation, which is exploited to remove image semantic