International Journal of Digital Crime and Forensics
Volume 11 • Issue 1 • January-March 2019

A Universal Image Forensics of Smoothing Filtering

Anjie Peng, School of Computer Science and Technology, Southwest University of Science and Technology, Mianyang, China & Guangdong Key Laboratories of Information Security Technology, Sun Yat-Sen University, Guangzhou China

Gao Yu, School of Computer Science and Technology, Southwest University of Science and Technology, Mianyang, China

Yadong Wu, School of Computer Science and Technology, Southwest University of Science and Technology, Mianyang, China

Qiong Zhang, School of Data and Computer Science, Sun Yat-Sen University, Guangzhou, China

Xiangui Kang, School of Data and Computer Science, Sun Yat-Sen University, Guangzhou, China

ABSTRACT

Digital image smoothing filtering operations, including the average filtering, Gaussian filtering and median filtering are always used to beautify the forged images. The detection of these smoothing operations is important in the image forensics field. In this article, the authors propose a universal detection algorithm which can simultaneously detect the average filtering, Gaussian low-pass filtering and median filtering. Firstly, the high-frequency residuals are used as being the feature extraction domain, and then the feature extraction is established on the local binary pattern (LBP) and the autoregressive model (AR). For the LBP model, the authors exploit that both of the relationships between the central pixel and its neighboring pixels and the relationships among the neighboring pixels are differentiated for the original images and smoothing filtered images. A method is further developed to reduce the high dimensionality of LBP-based features. Experimental results show that the proposed detector is effective in the smoothing forensics, and achieves better performance than the previous works, especially on the JPEG images.

KEYWORDS

Autoregressive Model, Digital Image Forensics, Local Binary Pattern, Smoothing Filtering

1. INTRODUCTION

The increase of forged images on the Internet has attracted much concern from researchers on multimedia security. When a forger creates a forged image, he often conducts smoothing filtering operations to beautify the forged image and make it look like an ordinary one. Thus, the forensics of smoothing filtering is able to provide auxiliary clues to identify the forged images. Furthermore, the smoothing filtering history of an image is an essential element for stegography (Kodovský & Fridrich, 2014; Pevný, Bas, & Fridrich, 2010) and steganalysis (Barni, Cancelli, &Esposito, 2010). Kodovský et al. pointed out thatit is not secure to embed a message into a smoothing filtered image (Kodovský

DOI: 10.4018/IJDCF.2019010102

& Fridrich, 2014). Therefore, the forensics of smoothing filtering is of particular significance in multimedia security.

There are some excellent works about the median filtering forensics (Yuan, 2011; Zhang, Li, Wang, & Shi, 2014; Chen, Ni, & Huang, 2013; Cao, Zhao, Ni, Yu, & Tian, 2010; Niu, Zhao, & Ni, 2017; Kang, Stamm, Peng, & Liu, 2012; Yang, Ren, Zhu, Huang, & Shi, 2017). Relatively, only a few universal forensic methods are devoted to detecting commonly used smoothing filtering operations, such as the average filtering, Gaussian low-pass filtering and median filtering. Yu (Yu &Chang, 2005) proposed to detect smooth regions via DCT coefficients, which was heavily dependent on high-frequency coefficients and was not robust against JPEG compression. Bayram (Bayram, Avcibas, Sankur, & Memon, 2006) employed a 188-D joint feature set composed of three types of steganalysis features to detect the smoothing operations. Their methods can achieve high detection accuracy; however, they are semi-blind and are not suitable to be used in the blind scenario. Recently, with the rapid development of computation equipment, it is preferable for the forensic task to use large dimensional feature or powerful deep learning model, such as rich model steganalysis feature with 34671-D (Qiu, Li, Luo, & Huang, 2014; Li, Luo, Qiu, & Huang, 2016) and deep learning automatically learned features (Bayar & Stamm, 2016). The rich model based feature and deep learning model really have achieved great improvements. However, the classification using large dimensional feature set and complicated learning model needs higher computation resources, larger number of images for training, longer time for training and testing, thus it is not applicable to the limited computation and storage resources (such as sensors, mobile phone). More importantly, the classification using a large dimension feature set may bear greater risk of over-fitting than that which using small dimensional feature set.

In this paper, we propose a universal smoothing filtering detector with the following goals: (1) it can simultaneously detect the commonly used smoothing filtering operations including the average filtering, Gaussian lowpass filtering and median filtering; (2) it can be robust against the commonly post operation- JPEG compression; (3) it should have a feature set with low dimension. We hope the proposed detector can satisfy the requirement of low computational resource. To this end, we firstly select high-frequency residuals elaborately to analyze the fingerprints left behind by the smoothing filtering operations, and then construct a composite feature set with small dimension for the forensic task.

2. THE PROPOSED METHOD

In this section, we first analyze the statistical differences between original images and smoothing filtered images in the high frequency residual domain. Then we employ autoregressive model and local binary patterns to extract the fingerprints left behind by the smoothing filtering operations in the residual domain. We finally introduce how to ensemble LBP and AR feature set for smoothing filtering forensics.

2.1. The High Frequency Residual

How to select an appropriate domain to analyze the fingerprints of smoothing filtering is the first critical factor for the smoothing filtering forensics. Generally, the diversity of natural image contents and post manipulations (such as the commonly used JPEG compression) always interferes with the performance of the forensic detector. The high frequency components, such as image differences or filtered residuals, contain very few image contents, so that they are always employed as being the analyzed domain to reduce the interference from image contents (Chen, Ni, & Huang, 2013; Cao, Zhao, Ni, Yu, & Tian, 2010; Kang, Stamm, Peng, & Liu, 2012, Yang, Ren, Zhu, Huang, & Shi, 2017). Inspired by our prior work (Kang, Stamm, Peng, & Liu, 2012), the median filtered residual (MFR) defined in (1) is employed as being the analyzed domain. Compared with the horizontal or vertical image differences, MFR is able to reveal the statistical information in various directions.

Methods to Identify Spammers

Tobias Eggendorfer (2009). *International Journal of Digital Crime and Forensics (pp. 55-68).*

www.igi-global.com/article/methods-identify-spammers/1599?camid=4v1a