Median Filtering Detection Using Edge Based Prediction Matrix

Chenglong Chen and Jiangqun Ni*

School of Information Science and Technology, Sun Yat-Sen University
Guangzhou 510006, P.R. China
c.chenglong@gmail.com, issjqni@mail.sysu.edu.cn

Abstract. In digital image forensics, there is an increasing need for the development of techniques to identify general content-preserving operations, such as resampling, compression, contrast enhancement and median filtering (MF). As a contribution towards this goal, we present, in this paper, a new blind forensic scheme for MF detection in images. The proposed method is based on the observation that, compared with original and linear filtered images, median filtered images exhibit distinct intrinsic traces around edges, e.g. neighborhood correlation, noise suppression and good edge preservation. Such MF intrinsic fingerprints are characterized as the Edge Based Prediction Matrix (EBPM), which contains the estimated prediction coefficients of neighborhood prediction among different edge regions in images. By incorporating the support vector machine (SVM), the MF detector is developed based on EBPM. Extensive simulations are carried out, which demonstrates the superior performance of the proposed scheme in terms of effectiveness and robustness.

Keywords: Median Filtering, Digital Image Forensics, Neighbor Prediction.

1 Introduction

In recent years, digital images have been widely used in news media, law enforcement, and military applications. With such high popularity and widespread availability of digital image editing software, we can no longer take the originality and authenticity of digital images for granted. Traditional methods for image authentication including digital signature and digital watermarking belong to active image authentication techniques. However, some pre-processing of these approaches such as signature generation and watermark embedding must have been done before the distribution of images, which would limit these approaches to specially equipped digital cameras in practical applications [1]. As a result, there is an increasing need for developing techniques to assess the authenticity of images without relying on such pre-processing.

* Corresponding author.

Y.Q. Shi, H.J. Kim, and F. Perez-Gonzalez (Eds.): IWDW 2011, LNCS 7128, pp. 361–375, 2012.

Recently blind forensic methods, which work in the absence of any watermark or signature, have become the domain of extensive research. In contrast to the active techniques, these methods operate under the premise that the only information available is the image itself with undetermined authenticity [1]. Although digital forgeries may leave no visual clues that indicate modification, they may indeed alter the underlying statistics of an image [1]. By identifying the traceable statistical artifacts left behind by manipulations imposed on images, blind forensic methods can assess the authenticity of digital images and identify image alterations without access to the source images or source device.

Image manipulations can generally be classified into malicious tampering and content-preserving manipulations. Correspondingly, the works in image forensics fall into two main categories. In the first category, numerous forensic methods focus on the detection of malicious tampering of the image content, such as copy & move and image splicing. In the second one, methods have been proposed to detect content-preserving manipulations, such as resampling [1] [2], JPEG compression [3], contrast enhancement [4] and median filtering [5] [6]. Although the content-preserving manipulations do not change the visual appearance of an image, their blind detection is still of forensic interest. First, these manipulations are usually employed as post-processing operations, which destroy the actual state of an image after previous tampering operations, thus may affect the set of forensic tools we are using and decrease the reliability of forensic algorithms. Second, certain post-processing operations may interfere with or diminish visual traces of previous tampering operations, such as the resampling operator [7]. Hence evidence obtained from image forensic analysis of such content-preserving manipulations would provide useful information to assess the authenticity of digital images.

In this paper, we focus on the detection of median filtering (MF). As most of existing forensic methods, such as resampling and CFA interpolation detection schemes [1] [2], rely on some kind of linearity assumption, blind detection of non-linear MF becomes especially challenging. Due to its non-linearity, MF can serve as an anti-forensics technique to destroy the linear constraints with image forgery operations and affect the reliability of existing forensic methods. An example is the new resampling scheme reported in [7], which applies MF to hide interpolation traces and is undetectable by Popescu and Farids resampling detector [2]. Therefore, forensic detection of MF can provide useful forensic information to identify the possible resampling operation.

Blind MF detection has already been studied by Kirchner [5] and Cao [6]. In [5], streaking artifacts, which are measured using distribution of first-order differences, are employed to detect MF in bitmap images. While for MF detection in JPEG post-compressed images, instead of streaking artifacts, the subtractive pixel adjacency matrix (SPAM) features are incorporated to analyze the conditional joint distribution of first-order differences. In [6], the probability of zero values on the first-order difference image in textured regions is adopted as MF statistical fingerprint to detect MF. The works in [5] [6] depend on, to some extent, the measurements of streaking artifacts by means of first-order differences