Information Sciences 321 (2015) 250–262

Contents lists available at ScienceDirect

Information Sciences

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

Detection of copy–move image forgery using histogram of orientated gradients

Jen-Chun Lee [a], Chien-Ping Chang [b], Wei-Kuei Chen [b,*]

[a] Department of Electrical Engineering, Chinese Naval Academy, Taiwan
[b] Department of Computer Science and Information Engineering, Chien Hsin University of Science and Technology, Jhongli 320, Taiwan

ARTICLE INFO

Article history:
Received 23 March 2014
Received in revised form 12 February 2015
Accepted 8 March 2015
Available online 14 March 2015

Keywords:
Copy–move forgery
Digital image forensics
Histogram orientated gradients
Duplicated region detection

ABSTRACT

The increasing popularity of digital media and media editing software has led to widespread tampering of multimedia files for malicious purposes. The most common form of tampering associated with digital images is copy–move forgery, in which a portion of an image is duplicated and substituted in a different location. Thus, law enforcement and forensics experts require reliable and efficient means of detecting copy–move forgery. This paper proposes a blind forensics approach to the detection of copy–move forgery. The input image is segmented into overlapping blocks, whereupon a histogram of orientated gradients is applied to each block. Statistical features are extracted and reduced to facilitate the measurement of similarity. Finally, feature vectors are lexicographically sorted, and duplicated image blocks are detected by identifying similar block pairs after post-processing. Experiment results demonstrate that the proposed method is able to detect multiple examples of copy–move forgery and precisely locate the duplicated regions, even when dealing with images distorted by translation involving small rotations, blurring, adjustment of brightness, and color reduction. We are currently working to improve detection in regions with rotation and scaling adjustment over large areas.

1. Introduction

News sources depend on digital images to represent the truth of their stories; however, digital image processing tools (e.g. Photoshop) have made it extremely easy to tamper with digital images, often for malicious reasons. Various methods have been developed to counter tampering and forgery in order to ensure the authenticity of images [2,10]. Current forgery detection methods can be categorized as active [9,22,24] and passive (blind) [8,19]. Most active methods are based on digital signatures and watermarking; however, this requires that data be preprocessed, which can be troublesome [11]. Passive methods are used to analyze images without using a priori information (such as embedded watermarks or signatures), such that a blind decision must be made regarding whether images have been tampered with. Most passive techniques are based on supervised learning through the extraction of specific features to differentiate the original image from tampered versions. The practicality and wide applicability of passive methods have made them a popular topic of research.

Copy–move is the most common form of digital image forgery, in which a portion of an image is copied and pasted into another portion of the same image to conceal something or duplicate elements. The wide availability of image processing

* Corresponding author. Tel./fax: +886 34581196.
E-mail address: wkchen@uch.edu.tw (W.-K. Chen).

http://dx.doi.org/10.1016/j.ins.2015.03.009
0020-0255/

software has made it easy to perform copy–move operations. The region altered by copy–move forgery is often almost imperceptible by the human eye; therefore, detecting evidence of these actions is an important issue in image forensics. This paper presents a robust algorithm for the detection of copy–move forgery based on the histogram of orientated gradients (HOG) [7]. The performance of the proposed method is compared with existing methods with regard to detection accuracy and computational complexity.

The remainder of the paper is organized as follows. Section 2 introduces related research and background on the topic of forgery detection. HOG is outlined in Section 3 and the proposed method is detailed in Section 4. In Section 5, we present the results of experiments designed to evaluate the performance of the proposed method in detection accuracy and computational complexity. Conclusions are presented in Section 6.

2. Related work

Most methods used in the detection of copy–move forgery can be categorized as either block-based methods or keypoint-based methods. The first such method was proposed by Fridrich et al. [8], using a block matching detection scheme based on discrete cosine transform (DCT). Popescu and Farid [20] proposed a copy–move forgery detection method, which differs in its representation of overlapping image blocks using principal component analysis (PCA) instead of DCT. Luo et al. [18] divided blocks into four sub-blocks, which were evaluated according to the average red, blue and green color values. This method proved robust to attacks, such as JPEG compression, Gaussian blurring, and additive noise. Kang et al. [12] applied singular value decomposition (SVD) to each image block in order to yield a representation of the image with reduced dimensions, a feature matrix of which was then lexicographically sorted according to singular values. This approach proved robust against noise distortion. Bayram et al. [3] applied a Fourier Mellin transform (FMT) and 1-D projection of log-polar values in a robust scheme for the detection of image forgeries. Mahdian et al. [13] exploited blur invariant moments to detect duplicated regions, which provided robustness against post-processing such as blur degradation, additional noise, and arbitrary changes in contrast. Li et al. [16] extracted features from circular blocks using rotation invariant uniform local binary patterns (LBP). Li et al. adopted the Polar Harmonic Transform (PHT) to describe the contents of circular blocks [17]. Lynch et al. [15] proposed an efficient expanding block algorithm based on direct block comparison rather than indirect comparisons based on block features. Zhao et al. [25] applied DCT and SVD in the detection of image forgeries. Nearly all of these methods are based on a large number of blocks and the feature vectors extracted from the blocks are large, which results in high computational complexity due to the fact that multiple-index sorting is required to enable lexicographical sorting of all of the blocks.

Local interest points (e.g. SIFT and SURF) have been widely used for image retrieval and object recognition, due to their robustness in dealing with numerous geometrical transformations (such as rotation and scaling) and occlusions. Recently, researchers have attempted to apply these types of features in digital forensics. Keypoint-based methods differ from block-based methods in their reliance on the identification and selection of regions of high-entropy within an image (i.e. "keypoints"). Some approaches involve the extraction of points of interest using a scale-invariant feature transform (SIFT) [1,21,23], capable of detecting and describing clusters of points belonging to cloned areas. For example, Pan and Lyu [21] estimated the transform between matched SIFT keypoints and searched all pixels within the duplicated regions after discounting the estimated transforms. Amerini et al. [1] developed a SIFT-based method for the detection of copy–move attacks and transformation recovery. Costanzo et al. [4] proposed three novel forensic detectors with the ability to remove global or local keypoints, based on anomalies in the distribution of keypoints following manipulation. SIFT keypoints guarantee geometric invariance; therefore, these methods can be used for the detection of rotated duplication. However, SIFT-based schemes are still limited in their detection performance due to the fact that it is only possible to extract keypoints from specific locations in an image. In addition, these methods are susceptible to a number of post-processing operations, such as blurring and flipping. Shivakumar et al. [23] proposed a method for the detection of copy–move forgery based on speeded up robust features (SURF), which makes it possible to detect duplicated regions of various sizes. This approach enables the detection of copy–move forgery with a minimum number of false matches when dealing with images of high resolution. Chen et al. [5] recently employed Harris corner interest points for the extraction of image keypoints as well as step sector statistics for the representation of small circle image regions around each Harris point using a feature vector. Unfortunately, most keypoint-based methods are applicable to the detection of keypoints in an image. However, some keypoints of duplicate regions cannot be identified using keypoint based algorithms and copied regions with little textural structure may be missed entirely [7]. Clearly, both methods have their strengths and weaknesses. We must consider differences in computational cost and performance in order to differentiate between block-based and keypoint-based methods.

Most forgery detection methods are evaluated against simple forgeries that human viewers have no trouble identifying in low resolution images. This paper focused on the performance of detection methods dealing with realistic forgeries at higher resolutions.

The histogram of oriented gradients is a powerful tool for the purpose of detection [8]. This paper proposes a block-based framework, which employs HOG descriptors to extract features that can be used as evidence to demonstrate copy–move manipulation. We conducted rigorous experiments using images modified using highly convincing techniques in order to demonstrate the robustness of the proposed method in dealing with multiple copy–move forgeries. The proposed technique is able to precisely locate duplicated regions without being affected by common post-processing attacks, such as image translation, small rotation, blurring, adjustment of brightness, and color reduction.