J. Vis. Commun. Image R. 31 (2015) 320–334

Contents lists available at ScienceDirect

J. Vis. Commun. Image R.

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

Copy-move image forgery detection based on Gabor magnitude [☆]

Jen-Chun Lee

Department of Electrical Engineering, Chinese Naval Academy, Kaohsiung 813, Taiwan

ARTICLE INFO

Article history:
Received 10 December 2014
Accepted 9 July 2015
Available online 15 July 2015

Keywords:
Digital image forensics
Image splicing
Copy-move forgery
Image retouching
Histogram of orientation Gabor magnitude
Gabor filter
Duplicate region detection
Lexicographical order

ABSTRACT

With advancement of media editing software, even people who are not image processing experts can easily alter digital images. Various methods of digital image forgery exist, such as image splicing, copy-move forgery, and image retouching. The most common method of tampering with a digital image is copy-move forgery, in which a part of an image is duplicated and used to substitute another part of the same image at a different location. In this paper, we present an efficient and robust method to detect such artifacts. First, the tampered image is segmented into overlapping fixed-size blocks, and the Gabor filter is applied to each block. Thus, the image of Gabor magnitude represents each block. Secondly, statistical features are extracted from the histogram of orientated Gabor magnitude (HOGM) of overlapping blocks, and reduced features are generated for similarity measurement. Finally, feature vectors are sorted lexicographically, and duplicated image blocks are identified by finding similarity block pairs after suitable post-processing. To enhance the algorithm's robustness, a few parameters are proposed for removing the wrong similar blocks. Experiment results demonstrate the ability of the proposed method to detect multiple examples of copy-move forgery and precisely locate the duplicated regions, even when dealing with images distorted by slight rotation and scaling, JPEG compression, blurring, and brightness adjustment.

1. Introduction

Nowadays, with the popularity of digital media cameras, digital media is playing an important role in our life. However, digital images can be manipulated and altered easily without leaving visible clues using digital image tools (e.g., Photoshop and 3D Max). This poses a serious social problem of the extent of trust that can be placed in the authenticity of digital content, especially when presented as evidence in a courtroom, for claiming insurance, and in the scientific world. According to some statistics [1], many journal-accepted manuscripts contain figures with inappropriate and fraudulent manipulations. Various methods have been developed to counter tampering and forgery for ensuring image authenticity [2].

Two approaches to ratifying the authenticity of a digital image can be categorized as active [3–5] and passive (blind) [6,7]. The active approach does not use actual digital content. Instead it focuses on implementing certain measures as the content is being created to confirm its authenticity afterward. Digital watermarking is the most popular approach in this category. Unlike the active approach, digital image forensics (also called passive image forensics) is a form of image analysis for finding out the condition of an image without the need for a priori information (such as embedded watermarks or signatures) and make a blind decision about whether the image has been tampered with. Most passive techniques are based on supervised learning through the extraction of specific features to distinguish the original images from tampered ones. The practicality and wide applicability of passive methods make them a popular research field. Copy-move forgery is one of the most commonly used forgery techniques that employ typical image processing tools (e.g., Photoshop and CorelDRAW). In copy-move forgery, a part of the image is copied and pasted in another part of the same image to conceal an object or to duplicate certain image elements. However, the task of detecting instances of forgery can be made significantly more difficult by post-processing on tampered images. Counterfeiters can use retouching tools, JPEG compression, or brightness to further alter forged images. To enhance the effects of image combination, the copied area can also be slightly rotated, scaled, or blurred to conceal the forgery. Thus, the effectiveness of copy-move forgery detection depends on the ability to detect regions of image duplication without being affected by post-processing operations, such as rotation, scaling, or JPEG compression. An example of copy-move forgery is shown in Fig. 1. The original image (Fig. 1(a)) has one bird, whereas the forged image (Fig. 1(b)) was manipulated using the cloning tool

[☆] This paper has been recommended for acceptance by Prof. M.T. Sun.

http://dx.doi.org/10.1016/j.jvcir.2015.07.007
1047-3203/© 2015 Elsevier Inc. All rights reserved.

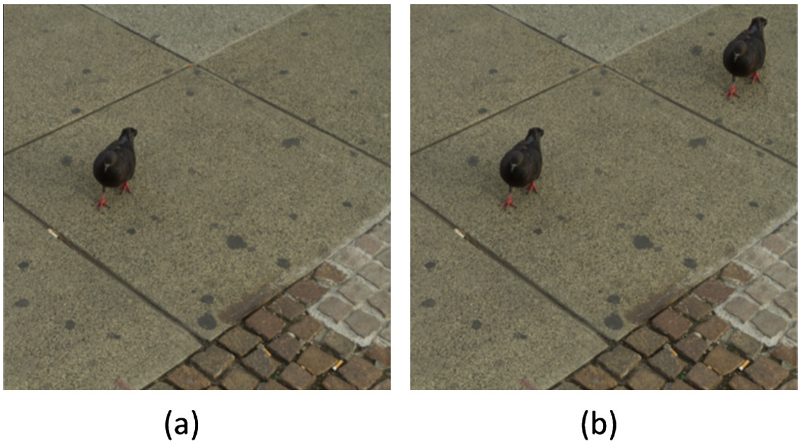

Fig. 1. Example of copy-move forgery (a) original image and (b) tampered image.

in Photoshop to show more than one bird by duplicating the bird present in the original image.

In this paper, we propose a scheme for detecting instances of copy-move forgery and authenticating images based on the Gabor transform [8]. The image is first converted into a gray-scale image and divided into overlapping fixed-size blocks. The proposed method, histogram of orientated Gabor magnitude (HOGM) descriptor, is then applied to each block for the extraction of local features and reduced the dimension of feature vectors to facilitate the measurement of similarity. Finally, each feature vector is lexicographically sorted, and regions of image forgery are detected through the identification of similar block pairs. A flow-chart of the proposed forgery detection method is shown in Fig. 2. In addition, we conducted rigorous experiments using images modified using highly convincing techniques to demonstrate the robustness of the proposed method in dealing with multiple copy-move forgeries. Compared with other methods, the main advantages of our method can be summarized as follows:

1. The histogram of orientated Gabor magnitude (HOGM) is proposed for the extraction of features from images that are suspected of forgery. Experiment results demonstrate the effectiveness of the proposed algorithm in detecting and precisely locating multiple instances of copy-move forgery within a single image. In addition, HOGM descriptors are well-suited for use in the analysis of image textures.
2. To reduce the probability of false matches, we developed a noise detector for the removal of false blocks.
3. The proposed technique is able to precisely locate regions of duplication without being affected by common post-processing techniques, such as image rotation, scaling, JPEG compression, blurring, and brightness adjustment. In most cases, the proposed method achieves better performance than other well-known approaches. In addition, the proposed method is even effective in dealing with images of high resolution.
4. Compared to most existing copy-move forgery detection techniques, the proposed method has a lower feature vector, which reduces computational complexity. Thus, this study makes a valuable contribution to the field of multimedia forensics.

The remainder of the paper is organized as follows. In Section 2, the related research about the past works is introduced, and Section 3 describes the Gabor filter. Section 4 gives the proposed method for detecting copy-move forgery. In Section 5, we present the results of experiments designed to evaluate the performance of the proposed method in terms of detection accuracy and computational complexity. The conclusions of this study are presented in Section 6.

2. Related research

Recently, many methods have been proposed to detect various forms of copy-move image forgeries. However, most methods used in the detection of image forgery can be categorized as either block-based methods or keypoint-based methods. The first such method was proposed by Fridrich et al. [6] by using a block matching detection scheme based on the discrete cosine transform (DCT). Popescu and Farid [9] proposed a copy-move forgery detection method that is different in the representation overlapping image blocks by using principal component analysis (PCA) instead of DCT. Luo et al. [10] divided blocks into four sub-blocks, which were evaluated according to the averages of the red, blue, and green color values. This method proved robust to some attacks such as JPEG compression, Gaussian blurring, and additive noise. Kang and Wei [11] applied singular value decomposition (SVD) to each image block to yield a representation with reduced dimensions, the feature matrix of which was then sorted lexicographically according to singular values. This approach achieved robust against noise distortion. Bayram et al. [12] applied the Fourier Mellin transform (FMT) and 1-D projection of log-polar values in a robust

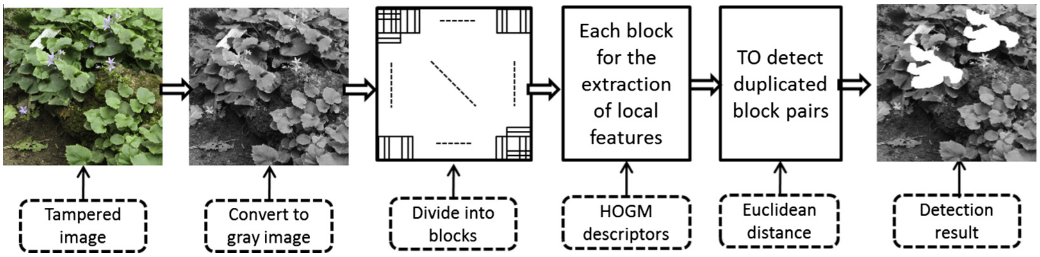

Fig. 2. The flow-chart of detection algorithm.