Forensic Science International 279 (2017) 8–21

Contents lists available at ScienceDirect

Forensic Science International

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

Copy–move forgery detection through stationary wavelets and local binary pattern variance for forensic analysis in digital images

Toqeer Mahmood[a], Aun Irtaza[b], Zahid Mehmood[c], Muhammad Tariq Mahmood[d,*]

[a] Department of Computer Engineering, University of Engineering and Technology, Taxila 47050, Pakistan
[b] Department of Computer Science, University of Engineering and Technology, Taxila 47050, Pakistan
[c] Department of Software Engineering, University of Engineering and Technology, Taxila 47050, Pakistan
[d] School of Computer Science and Engineering, Korea University of Technology and Education, Cheonan 330-708, Republic of Korea

ARTICLE INFO

Article history:
Received 22 March 2017
Received in revised form 4 July 2017
Accepted 27 July 2017
Available online 4 August 2017

Keywords:
Digital forensic
Circular block
Image tampering
Forged region detection
Passive authentication

ABSTRACT

The most common image tampering often for malicious purposes is to copy a region of the same image and paste to hide some other region. As both regions usually have same texture properties, therefore, this artifact is invisible for the viewers, and credibility of the image becomes questionable in proof centered applications. Hence, means are required to validate the integrity of the image and identify the tampered regions. Therefore, this study presents an efficient way of copy-move forgery detection (CMFD) through local binary pattern variance (LBPV) over the low approximation components of the stationary wavelets. CMFD technique presented in this paper is applied over the circular regions to address the possible post processing operations in a better way. The proposed technique is evaluated on CoMoFoD and Kodak lossless true color image (KLTCI) datasets in the presence of translation, flipping, blurring, rotation, scaling, color reduction, brightness change and multiple forged regions in an image. The evaluation reveals the prominence of the proposed technique compared to state of the arts. Consequently, the proposed technique can reliably be applied to detect the modified regions and the benefits can be obtained in journalism, law enforcement, judiciary, and other proof critical domains.

1. Introduction

Digital media is playing an important role in our life due to the growing popularity of low-priced and high-resolution digital cameras. On the other hand, image editing tools have made it easier even for a novice to manipulate the image content without leaving any visual traces. These open and possible manipulations make the image authenticity questionable; especially when presented in the news reports, as evidence in the judicial courts, and for insurance claims. Therefore, the image forensic techniques are tuned to verify the integrity of the images.

Previously, the most common way for image content authentication that may have some legal value was through digital watermark or the digital signatures [1]. But the watermark or signature based techniques are unable to help in the situations where the embedded information is missing [2]. Therefore, recently the emphasis of research is on finding the ways to perform the image manipulation detection in an automatic way [3]. Furthermore, to elaborate the manipulations in an image it becomes necessary to establish what exactly happened in the image: if the portion of image is covered, if a region is cloned, if cloning involves the regions of multiple images, or if all these processes are combined to conceal the actual image contents [4]. Hence, the resulting techniques address the possible tampering as either copy-move forgery (CMF) [5] or image splicing [6]. A visual example of CMF and image splicing is presented in Fig. 1.

In particular, a skilled counterfeiter when creates the feigned image by cloning a region elsewhere in the same image employs various transformations and post-processing operations. The post-processing operations i.e. region rotation, region scaling, illumination changes etc. applied over the forged regions make the forgery detection even more challenging and difficult to address. The existing block-based methods (details in Section 2) either assume that the copied regions have not undergone any post-processing operations, or these techniques are unable to address a large number of post-processing operations. The block based techniques also suffer from the higher computational cost due to the high dimensional feature vectors and a number of overlapping

* Corresponding author.
E-mail addresses: toqeer.mahmood@yahoo.com (T. Mahmood), aun.irtaza@uettaxila.edu.pk (A. Irtaza), zahid.mehmood@uettaxila.edu.pk (Z. Mehmood), tariq@koreatech.ac.kr (M. Tariq Mahmood).

http://dx.doi.org/10.1016/j.forsciint.2017.07.037
0379-0738/

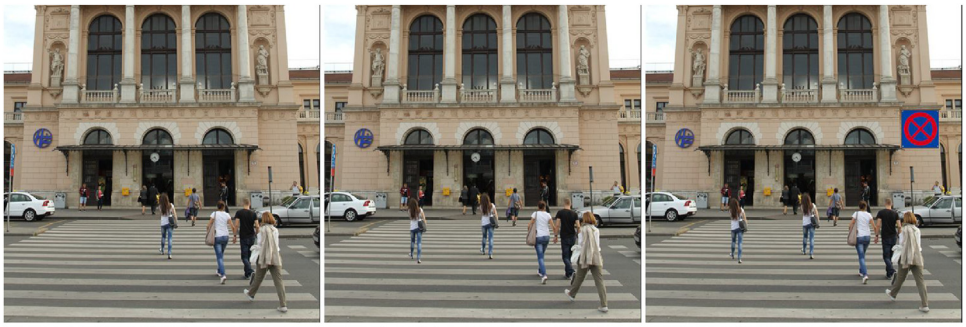

Fig. 1. A visual example of CMF and image splicing [7].

blocks. Similarly, the second main class of CMFD techniques such as keypoints-based techniques (details in Section 2) poorly perform in the presence of smooth regions [8].

To address the limitations of the block-based and keypoints-based techniques, in this paper, LBPV is adapted for the CMFD over the low approximation components of the stationary wavelets. The proposed technique is evaluated in the presence of various post-processing operations i.e. translation, flipping, blurring, rotation, scaling, color reduction, brightness change and multiple forged regions. The rotation invariant LBPV is able to estimate the principal orientations of the image regions to effectively compute the region matching.

For CMFD in smooth regions, LBPV is applied over the smoothed version of the images obtained through the translation invariant stationary wavelet transform. The key benefits of our technique are:

- Reduced size feature vectors for block representation that lowers the computational time for forgery detection.
- Unveiling multiple copy–move forgeries in images.
- Robustness against translation, flipping, blurring, rotation, scaling, color reduction, brightness change and JPEG compression.

The rest of the paper is structured as follows: Section 2 presents the related work regarding CMFD. Section 3 presents the details of the proposed technique and describes the way we adapted LBPV for detection of forgeries. Experimental results are presented in Section 4. Finally, the conclusions are drawn in Section 5.

2. Related work

In copy–move forgeries, image regions are cloned to conceal some important content in the pictured image. As copied regions are apparently identical with compatible components (i.e. color and noise) therefore it becomes a challenging task to differentiate the tampered regions from authentic regions. To address the copy-move forgeries the focus of research is on two broad categories of techniques i.e. block based forgery detection, and keypoints-based forgery detection.

2.1. Block-based forgery detection techniques

Block-based region matching is frequently used for copy-move forgery detection (CMFD). These techniques generate the representation of image blocks through low-level features and compare blocks using metric or non-metric norms to detect the forgeries. In the literature, the first landmark technique for CMFD is proposed by Fridrich et al. [9], by utilizing a block matching approach based on the coefficients of discrete cosine transform (DCT). Popescu and Farid [10] suggested a solution using principal component analysis (PCA) for image block representation. The technique is demonstrated in the presence of additive noise and compression. Mahdian and Saic [11], proposed a solution employing 24 blur invariant moments extracted from each square block and for each RGB color channel. Therefore, a feature vector of length 72 represents each image block, which is reduced by applying PCA. Ryu et al. [12] proposed a solution using rotation invariant Zernike moments to identify the copy-move forgeries. Huang et al. [13], and Cao et al. [14], tried to improve the detection capability of the algorithm proposed in Ref. [9] with reduced feature vector representation and proposed a new feature comparison technique. Zhao and Guo [15] proposed a solution through DCT and singular value decomposition (SVD) for detecting image forgeries. The algorithm is effective against noise and blurring but fails when images are even slightly flipped or rotated.

Bayram et al. [16], proposed Fourier–Mellin transform (FMT) for CMFD. The technique detects the tampered regions with slight rotation and scaling. Liu et al. [17], proposed a CMFD solution by decomposing an image using Gaussian pyramid and Hu moments invariant extracted from the circular blocks. However, the technique is only sensitive to objects with obvious geometry. Bravo-Solorio and Nandi [18] proposed a technique based on log-polar coordinates for CMFD. The authors produced a descriptor by Log-polar mapping of overlapping square blocks. Lynch et al. [19], proposed an efficient expanding block technique based on direct block comparison. Li et al. [20] obtained features from circular blocks using uniform local binary patterns (LBP) which is rotation invariant. The technique is robust to blurring, noise, compression, flipping, and rotation. However, this technique failed to detect forged regions rotated with arbitrary angles. Li et al. [21], extracted the feature vectors from circular blocks using polar harmonic transform (PHT) for detecting image forgeries. Mahmood et al. [22], addressed the CMFD through KPCA features extracted from DCT coefficients. The algorithm effectively identified the duplicated segments under post-processing operations like compression, noise, and blurring.

2.2. Keypoints-based forgery detection techniques

Keypoints-based techniques are also employed in the field of forgery detection. The focus of these techniques is to identify and select the high entropy regions of the image. Two steps are usually followed in these techniques: the first is the localization of the interest points and in second step local descriptors are built against these interest points. Lowe [23] proposed scale invariant feature transform (SIFT), a keypoints-based technique for matching the features between a pair of images. Huang et al. [24] utilized SIFT keypoints and computed the local statistical descriptors for detecting the duplicated regions within the image. Later on, Pan