Computers and Electrical Engineering 000 (2017) 1–14

Contents lists available at ScienceDirect

Computers and Electrical Engineering

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

A generic passive image forgery detection scheme using local binary pattern with rich models☆

Sundus Farooq, Muhammad Haroon Yousaf*, Fawad Hussain

Department of Computer Engineering, University of Engineering and Technology Taxila, Pakistan

ARTICLE INFO

Article history:
Received 3 August 2016
Revised 4 May 2017
Accepted 6 May 2017
Available online xxx

Keywords:
Forgery
Universal forensics
Tampering detection
Steganalysis
Rich models

ABSTRACT

Image forgery detection is one of the prominent areas from research and development perspective. This research work aims to propose a scheme for the detection of multiple types of image forgeries. In this paper, a generic passive image forgery scheme is proposed using spatial rich model (SRM) in combination with textural feature i.e. local binary pattern (LBP). Moreover, different sub-model selection strategies are implemented and analyzed to investigate the performance-to-model dimensionality trade-off. Ensemble multi-class classifier is used for classifying the features into different forgery classes. The proposed scheme is evaluated on the dataset generated from IEEE IFS-TC image forensics challenge containing 10 different kinds of forgeries. The results reveal that computing LBP on noise residuals in conjunction with co-occurrence matrices using BEST-q-CLASS feature selection strategy produces a model which performs efficiently for almost any set of modifications with accuracy of 98.4%.

1. Introduction

In today's digital world, the acquisition of visual data became less-expensive and handy with rapid distribution of inexpensive and easy to use devices. With the dawn of digital cameras and powerful personal computers, the recording, storing, and sharing the visual data is done frequently. Due to which, tampering and manipulation of the visual content is no more difficult as indistinguishable photorealistic graphics are generated and widely used. This illegal practice of image manipulation called as forgery. Forgery directed the society's attention towards the digital forensics which aims at exploring the artifacts left due to altering operation and avoiding the crime caused by recovering and investigating the content found, in other words, authenticating the content in the image.

Image authentication methods fall into two categories. Active methods, which depend on image source or capturing device to detect the modification applied to the image, and passive authentication methods, which blindly detect the image altering operation applied on the image regardless to the image source. The former cannot be used when working with digital images with unknown image source whereas latter is applicable to many forensics applications. Passive authentication methods efficiently detect the forgeries applied. Now a days, there are many forgeries commonly applied to the digital images such as copying, splicing, blurring and enhancing the contrast etc. [1]. Copy-paste forgery refers to copying a region of the image and pasting it onto the same image to create a duplicate region, whereas splicing entails creating an outside

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Area Editor Dr. E. Cabal-Yepez.

* Corresponding author.
E-mail addresses: farooq.sundus12@gmail.com (S. Farooq), haroon.yousaf@uettaxila.edu.pk (M.H. Yousaf), fawad.hussain@uettaxila.edu.pk (F. Hussain).

http://dx.doi.org/10.1016/j.compeleceng.2017.05.008
0045-7906/

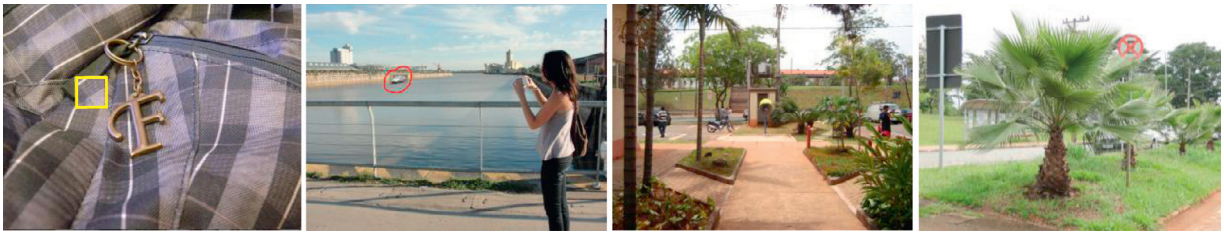

Fig. 1. Images with common types of forgeries i.e. a: Copying, b: Splicing, c: Median-Filtering and d: Gamma-Correction.

region, which is copied from another image onto the target image. Many illegal practices like crowd growing, content hiding, information adding etc. are performed using these two forgery types [2]. Additionally image enhancement involving blurring, contrast enhancement and sampling are entertained to create an imposing representation of digital images on social media [3]. On the other hand, compression although is used widely to transmit or store the media, but sometimes it becomes harmful for the processing of the digital media in term of information loss or quality trade off, thus making its detection and identification necessary [4]. Effect of different types of forgery can be perceived from Fig. 1. The highlighted area in images (a) and (b) in Fig. 1 depicts the region copied from the same and different images respectively.

Many passive forensic methods have been proposed during the past decade to identify the digital image forgery, and determine the authenticity of detail. A significant work is witnessed in this field specifically on copy-paste forgery detection [5]. The copy-paste tempered regions are identified and located using fuzzy block-matching algorithm based on improved Singular Value Decomposition (SVD). Block based SVD of the whole image is computed and used as features. Then the duplicated blocks are identified and matched based on their feature vectors and decision of forgery detection is made depending on the correlation coefficient threshold [6]. Discrete Cosine Transform (DCT) and Multi-support Region Order-Based Gradient Histogram (MROGH) also exhibit good detection performance when used with Blocking Artifact Grid (BAG) and Generalized-2-Nearsest Neighbor (g2NN) algorithm respectively. The Scale Invariant Feature Transform (SIFT) performed best when used to detect copy-paste forgery. The 128-dimentional SIFT features are computed. The matching key-points are located using Best Bin First (BFF) algorithm which identified the nearest neighbors with high probability and used only a limited volume of computation [7]. Later, the dimensionality of the SIFT feature vectors is reduced additionally for a low computational complexity. For this purpose, Discrete Wavelet Transform (DWT) of the image is computed initially to reduce the image into 4 sub-blocks. Features of only high detail coefficients block (LL) which comprises of only low frequency information, are described using SIFT and achieved better accuracy [8]. Further, the features from SIFT are combined with Speeded up Robust Features (SURF) followed by g2NN algorithm. Experimental results show that the proposed method achieved a very high accuracy compared with previous methods which used SIFT key points as features [9]. DCT is used with LBP and Block Posterior Probability Map (BPPM) to efficiently detect the splicing forgery [10,11]. A better practice of DCT is realized when used with DWT for achieving even more accuracy [12]. Locally and globally applied contrast enhancement is identified using image's statistical intrinsic fingerprints [13].

A method is proposed to differentiate between single and double JPEG compression based on machine learning. First, the difference JPEG 2D arrays are used to enhance the double JPEG compression artifacts. Then to model the difference 2D arrays, Markov random process is applied for utilizing the second-order statistics [14]. To detect the blurring or normally called as smoothing, a blur detection technique is proposed which uses the Haar wavelet transform by analyzing the edge characteristics. The scheme is based on the ability of Haar wavelet to discriminate different types of edges by recovering sharpness from blurred images and the fact that some edges like Dirac and A-step structures disappear when blur occurs. Experimental results proved the efficiency and effectiveness of the proposed method [15].

The above discussion reveals that the methods previously proposed are forgery specific. They are meant for the detection of popular forgeries such as copy-paste, splicing, blurring, contrast enhancement and simple tempering and other altering operations [4,6,16]. These methods perform remarkably well for the forgeries they are designed for, but failed to detect other forgeries. Furthermore they cannot be extended to identify other operations due to their methodology, and the set of certain features, on which they count for decision making. Additionally, existing methods lean towards giving a binary result and usually classify the doubtful image supposing if the image has been manipulated by a certain operation or not. To satisfy this demand, a universal forensic method [17] is proposed based on borrowed Steganalytic features [18] from steganography to detect some type of image altering operations. It is observed that Steganalytic features, when used in forensics, proved to be very useful. The basis for using steganalysis in forensics is that applying image processing operation changes many pixel values, which destroys the inherent properties of original image as in steganography. These spatial domain rich features are further used as splicing and copy-paste forgery detector giving improved performance [19,20]. On the other hand, modern steganographic methods have a tendency to insert data in the more complicated textures [21]. This is analogous to applying forgeries on the digital images, which modify or distort its texture properties. As a result, textural features can also be used to uncover steganography similar to altering operations in the case of forgeries. Local Binary Patterns are considered as the powerful textural features for revealing the embedding applied on the digital images, hence they can be used in forensics to capture textural deviations identical to embedding. As in [11], LBP is employed with DCT to detect splicing operation giving

Please cite this article as: S. Farooq et al., A generic passive image forgery detection scheme using local binary pattern with rich models, Computers and Electrical Engineering (2017), http://dx.doi.org/10.1016/j.compeleceng.2017.05.008