Computers and Electrical Engineering 000 (2017) 1–11

Contents lists available at ScienceDirect

Computers and Electrical Engineering

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

Forgery detection in digital images via discrete wavelet and discrete cosine transforms[☆]

Khizar Hayat[a,b,*], Tanzeela Qazi[a]

[a] COMSATS Institute of Information Technology, University Road, Abbottabad 22060, Pakistan
[b] Computer Science Section (DMPS), College of Arts and Sciences, University of Nizwa, Sultanate of Oman

ARTICLE INFO

Article history:
Received 5 January 2016
Revised 13 March 2017
Accepted 14 March 2017
Available online xxx

Keywords:
Image tampering
Image forgery
Discrete Wavelet Transform(DWT)
Discrete Cosine Transform (DCT)
Image forgery detection

ABSTRACT

When an image is forged through some sophisticated software editing tool, with imperceptibility being the goal, the idea is not to leave any observable trace that may help to distinguish the forged image from the original one–at least with a naked eye. We believe that no matter which type of forgery is employed, there ought to be imperfections in the tampered image that may eventually prove its fakery. Even, forging an image with noble intentions, needs a reasonable amount of care. With this in perspective, we present a forgery detection method that depends on the discrete wavelet transform (DWT) as well as the discrete cosine transform (DCT) for feature reduction. The DCT is applied to the individual blocks obtained after dividing the DWTed image. The blocks are then compared on the basis of correlation coefficients. A mask-based tampering method is also developed as part of the experiments in order to test the detection method. The method shows interesting results when compared to two methods from the literature.

1. Introduction

In today's digital world, many different tools are used for the manipulation of images. In most cases, the altered image may not have any apparent clues regarding the original, especially if the latter is not easily accessible. Due to these sophisticated image editing software tools, the authenticity of a given image is always questionable and may give rise to many issues. No longer can the authenticity and integrity be guaranteed. The main problem is that it undermines the credibility of digital image as photographic evidence. Another important issue concerning digital fakery is the relative ease to use the tools and graphics algorithms, leading to serious vulnerabilities, that cast doubt on the integrity of digital images [1,2]. These problems bring into the fore the need to develop such tools and techniques that can easily discriminate the natural images from the tampered or synthetically generated images.

Digital image forensics is a field that analyzes images of a particular scenario, in order to establish the credibility and authenticity (or otherwise), through a variety of means. It is fast becoming a popular field because of its potential applications in many domains like intelligence, sports, legal services, news reporting, medical imaging and insurance claim investigations [1,2]. With the ever increasing reliance on digital media, the need to ensure its authenticity and trustworthiness is of vital importance. The creation and manipulation of digital images, with no obvious tampering, is becoming easier and easier with

[☆] Reviews processed and recommended for publication to the Editor-in-Chief by Guest Editor Dr. E. Cabal-Yepez.
[*] Corresponding author.
E-mail address: khizar.hayat@unizwa.edu.om (K. Hayat).

http://dx.doi.org/10.1016/j.compeleceng.2017.03.013
0045-7906/© 2017 Elsevier Ltd. All rights reserved.

each passing day. Unfortunately, the counter efforts are undermined by the lacking of techniques to ascertain the origin or potential integrity of digital images. Research in digital image forensic needs to be aggressive and based on solid reasoning in order to uncover the actual facts while keeping pace with the development of image editing tools.

In this paper we present a forgery detection method that is applicable in the case of copy/move forgery. The proposed transform domain technique relies on both the discrete wavelet transform (DWT) and the discrete cosine transform (DCT). The purpose is to reduce the features by first applying DWT to get the approximate sub-band. This is followed by dividing the latter to fixed sized square blocks and then applying DCT to each block separately, in order to reduce the features further. After lexicographically sorting the reduced set of features, correlation coefficients are used to judge the similarity of blocks.

The rest of the paper is arranged as follows. Section 2 presents a concise survey of the related literature. This is followed by the presentation of the proposed method in Section 3. The simulation results are illustrated in Section 4 in somewhat detail. Section 5 concludes the paper.

2. Related work

In early 1840's, Hippolyte Bayrad created the first known fake image in which he was shown committing suicide[1]. About two decades later, another fake image was created in which the head of Lincoln (US President) was shown on the body of John Calhoun, a Southern politician [3]. In the subsequent years, there had been a steady growth in the population of such tampered images. With the advent of color photography and subsequent coming of digital age, on the fly tampering was just a *fait accompli*. Today many advanced software and editing tools are available that can rather seamlessly forge images through a variety of techniques . Due to such forgeries, photography has lost its innocence.

Image forgeries can be classified as [2]:

- Copy/move forgery,
- Image splicing and
- Image retouching.

The techniques from each of these categories can be implemented additionally via a) active or b, passive approaches [4]. The active approaches are mostly concerned with the data hiding techniques, such as digital watermarking/copyrighting, wherein prior information is considered essential and integral to the process. The passive approaches do not require any prior information about the original image . The passive blind techniques, where the analyzer has just the final product at his/her disposal, provide a solution to identify image alterations without relying on the insertion of an extrinsic data or digital signatures for image authentication.

Forgery detection methods are broadly categorized as visual and statistical methods. Visual methods are based on the visual clues and sometimes require no hardware or software tools. It only detects, intelligently, the inconsistencies and light information of an image. In contrast, the statistical methods analyze pixel values of image and are hence more robust and convincing. The passive blind forgery detection scheme, outlined in [5], is based on content adaptive quantization table estimation. This technique is used for the detection of different types of forgeries, i.e. copy/move, splicing and synthetics. The accuracy rate is claimed to be high as compared to other techniques. It is claimed to be robust against the JPEG compression. For a detailed account of the methods on forgery detection, the readers can consult our earlier work on the subject [6]. Several surveys and feature analysis studies are available on copy/move forgery detection [7,8]. Many copy/move forgery detection techniques, proposed in the literature, exhibit good results but at the cost of relatively high computational time . Most of the copy/move forgery detection rely on block-wise comparison and the risk is that, “Similar but Genuine Objects (SGO)” may be treated as copied objects, as explained in [9]. Ideally, in a given image, all SGOs must be accounted for while subjecting it to copy/move forgery detection.

The copy/move forgery detection technique of [10] is based on the DCT. The DCT coefficients of each block are selected to represent specific blocks. This is followed by lexicographic sorting of the four features of each block in order to check the similarity measure on the basis of a threshold value. The method is claimed to be robust against copy/move forgery. The downside is that it also detects wrong similar blocks and is sensitive to the addition noise or blurring. In [11], the authors detect copy/move forgery with the quantized DCT coefficients based block matching. The limitations of their technique include false identification of a few copied areas and low reliability with small copied images. The method in [12] divides the image into overlapping blocks and computes the DCT coefficients. By using the signs of the DCT coefficients, binary feature vectors are created. The latter are matched using the coefficient of correlation. A related method [13] employs principal component analysis (PCA) for feature reduction. In [14], the authors propose to treat the overlapping blocks to Local Binary Pattern (LBP) before applying the DCT and subsequent lexicographic sorting. Invariance to affine transformation, especially the scale, is an important aspect of copy/move forgery detection [15]. The method in [16] employs scale invariant feature transform (SIFT) in combination to DCT. The method outlined in [17] attempts to use statistical moments, computed from DCT quantized coefficients; for scale invariance, perhaps.

[1] http://www.fourandsix.com/photo-tampering-history/?currentPage=8