Chapter 44
An Image Forgery Detection Approach Based on Camera's Intrinsic Noise Properties

Shikha Gautam
GLA University, Mathura, India

Anand Singh Jalal
Institute of Engineering and Technology, GLA University, Mathura, India

ABSTRACT

Digital images are found everywhere from cell phones to the pages of online news sites. With the rapid growth of the Internet and the popularity of digital image capturing devices, images have become major source of information. Now-a-days fudge of images has become easy due to powerful advanced photo-editing software and high-resolution cameras. In this article, the authors present a method for detecting forgery, which is detected by estimating camera's intrinsic noise properties. Differences in noise parameters of the image are used as evidence of Image tampering. The method works in two steps. In the first step, the given image is classified as forge or non-forge. In the second step, the forged region in the image is detected. Results show that the proposed method outperforms the previous methods and shows a detection accuracy of 85.76%.

1. INTRODUCTION

In the past decade, digital images have evolved to become an essential part of our life from entertainment to mass media, from medical diagnosis to criminal justice, and even in national security. However, the increasing sophistication of advanced photo-editing software (e.g. Adobe Photoshop, Corel Draw etc.), help the people to forge images easily.

These editing methods result in manipulated images with no obvious traces of these operations. For the detection of these manipulations, the techniques are widely known as image forgery detection techniques (Birajdar & Mankar, 2013). Image forgery detection deals with detection of the presence of

DOI: 10.4018/978-1-7998-2466-4.ch044

manipulation in an image. Two kinds of detection techniques are possible: Active forgery detection and passive forgery detection. At the time of the birth of digital image forensics, active forgery detection methods such as digital watermarking and signature served as major solutions to protect the integrity of digital images. However, active methods require an authentication code to be embedded with the image.

In passive detection methods, the only information available with the method is just the image (Birajdar & Mankar, 2013). The detection is performed with the help of statistical properties derived from the image. The main purpose of all forgery detection algorithms is to classify the images into one of two clusters: either forged or non-forged. Based on this classification, the forged region can further be located in the image. The objective of the proposed article is also to locate manipulated/forged region in the image. In this paper, noise is used as a statistical feature for the detection of forgery. Noise properties are used as a clue for detection of forgery. Noise in the images is the variation in the intensity of the image pixels either due to image processing steps or due to image generation processes or may be due to transmission process. These variations are generally uniform across the whole image. This helps as a tool for detection of forgery in image.

Previous approaches to detect forgery utilize the statistical properties of the image such as the properties and parameters associated with the devices which capture the image; the brightness, contrast and intensity features, inconsistencies/irregularities introduced because of manipulation of the image can also be used for detecting presence of manipulation in the image (Popescu & Farid, 2004). These features tend to be same throughout the image if the complete image is original one whereas if parts of the image are manipulated, these features may get inconsistent. These inconsistencies can be looked for in an image, for detecting the presence of forgery.

A method based on resampling is introduced by Popescu and Farid (2005) to detect forgery in images where some resize, rotate operations have been performed. Method proposed by Johnson and Farid (2005) is capable of detecting manipulations in image composites, i.e. the images which are consisting of parts from different images. In an image, the lighting direction in various parts of the image is consistent whereas if it is an image composite, the lighting directions in different parts of image will not match. Therefore, this inconsistency in lighting direction is a trace for detecting forgery in an image.

Aberration based forgery detection technique was introduced in the literature by Johnson and Farid (2006). When an image gets tampered, this aberration can be found to be inconsistent in the parts of the image, thus pointing out forgery in the image. An analysis of DCT coefficients for detecting DQ effects followed by modeling doctored DCT blocks is used for detecting forgery in JPEG images by (He, Lin, Wang, & Tang, 2006). Another interesting technique was proposed by Li, Yuan, and Yu (2008). The DCT block artifact grid (BAG) can be extracted from the JPEG image and the positions where grids are not matched shows the presence of forgery. The work Proposed by Yuan (2011) detects the median filtering (MF) manipulation, which is being done to hide the traces of tempering. A manipulated part in the image can be detected as a JPEG ghost.

A method proposed by Rocha, Scheirer, Boult, and Goldenstein (2011) detects forged regions in a JPEG image, the hypothesis being the forge region is singly compressed whereas the rest parts of the image is doubly compressed (also called as single compression forgery (SCF) hypothesis), A new probability based model based on DCT coefficients of singly compressed and doubly compressed region in the JPEG image are derived. On the basis of such model, the probability of each block being forged is measured.

Method by Bianchi and Piva (2012) automatically measures the likelihood map indicating the probability for each 8x8 DCT block of being doubly compressed. The method detects the double compressed