Chapter 10
Copy-Move Forgery Detection Using DyWT

Choudhary Shyam Prakash
Indian Institute of Technology, Department of Computer Science and Engineering, Dhanbad, India

Sushila Maheshkar
Indian Institute of Technology, Department of Computer Science and Engineering, Dhanbad, India

ABSTRACT

In this paper, we proposed a passive method for copy-move region duplication detection using dyadic wavelet transform (DyWT). DyWT is better than discrete wavelet transform (DWT) for data analysis as it is shift invariant. Initially we decompose the input image into approximation (LL1) and detail (HH1) sub-bands. Then LL1 and HH1 sub-bands are divided into overlapping sub blocks and find the similarity between the blocks. In LL1 sub-band the copied and moved blocks have high similarity rate than the HH1 sub-band, this is just because, there is noise inconsistency in the moved blocks. Then we sort the LL1 sub-band blocks pair based on high similarity and in HH1 blocks are sorted based on high dissimilarity. Then we apply threshold to get the copied moved blocks. Here we also applied some post processing operations to check the robustness of our method and we get the satisfactory results to validate the copy move forgery detection.

INTRODUCTION

Digital imaging is a well-known term these days and it has an important role in journalism, courtroom witnesses, medical, scientific publications, digital forensics etc. There are many advantages of this technology and it can be used for misleading and hiding the real fact. This is because, in present scenario manipulation of image is easy task with perfection that forgery cannot be detected by naked eyes. Figure 1 is a famous example of copy move forgery in which a portion of the image is copied and pasted over another region. This photo is published by the national news agency Bernana, Malaysia, in which the supporters of Prime Minister Najib Tun Razak was soon being called out on Facebook as a fake. In this photo a portion of crowd had been copied to the other region to appear the crowd larger. Finally, Bernana admitted the mistake and withdrawn the photo and take appropriate action against the forgers.

DOI: 10.4018/978-1-7998-3025-2.ch010

Figure 1. An example of copy move forgery

Forged image can be created by image tampering, splicing or cloning. Integrity of the image is lost and sometimes forged image looks so real and it cannot be detected, hence the authenticity of the image is also lost. The security concern of digital content has arisen a long time ago and different techniques are developed to validate the integrity of digital images. These techniques are basically divided into two approach: Active and Passive. In active approach, some kind of signature, such as watermark or fingerprints, is embedded into a digital image and authenticity of the image can be achieved by authenticating the true signature and the retrieved signature from the input image (Rey & Dugelay, 2002; Zhang, Cheng, Qiu et al., 2008a). There is a limitation of active approach, as the digital cameras and video recorder available in the market are not capable of embedding the extrinsic fingerprints.

Due to the limitation of the active approach we need the passive approach (Zhang, Cheng, Qiu et al., 2008b; Mahdian & Saic, 2008; Farid, 2009; Mahdian & Saic, 2009; Swaminathan, Wu & Liu, 2008; Lin, Tjoa, Zhao et al, 2009) to validate the originality of digital images. In this approach, we deal with intrinsic fingerprints of image such as sensor noise of the capturing device. The challenges in blind technique is to reduce the false positive rates, making the system fully automated, localization of forgery, detecting forgery of any type image format (compressed or uncompressed), increasing the reliability and robustness.

In this paper, we propose a passive method for copy move image duplication detection using dyadic wavelet transform (DyWT). These days, copy move is one of the most frequently used technique for image tampering. In copy move forgery, one or more part of the image is copied and pasted in the same image to conceal the originality of the image. There is many software available (e.g. Photoshop) to do such kind of tampering in such a way that it cannot be detected by naked eyes.