A Methodological Review on Copy-Move Forgery Detection for Image Forensics

Resmi Sekhar, Lourdes Matha College of Science and Technology, Thiruvananthapuram, India
R. S. Shaji, Noorul Islam University, Thuckalay, India

ABSTRACT

Copy-Move forgery is the very prevalent form of image tampering. The powerful image processing tools available freely helps even the naive to tamper with images. A copy-move forgery is performed by copying a region in an image and pasting it in the same image most probably after applying some form of post-processing on the region like rotation, blurring, scaling, double JPEG compression etc. This makes it difficult to develop one common technique to detect copy-move forgery. As a result a considerable number of methods have been developed in view to detect different forms of copy-move forgeries. Those techniques can be classified generally as block based techniques and key-point based techniques. This paper presents an extensive survey on the very recent methods developed for copy-move forgery detection.

Keywords: Block Based Techniques, Copy-Move Forgery, Copy-Paste Forgery, Digital Image Forensics, Image Tampering, Key-Point Based Techniques

INTRODUCTION

One of the principal aims of digital Image Forensics is image tampering detection. Tampering literally means ‘to interfere with something in order to cause damage or make unauthorized alterations’ (Redi & Dugelay, 2011). There are many instances of image tampering in History even in the nineteenth century. In those days tampering was a cumbersome work to be performed in the dark rooms of the studio. But today because of the easily available image processing tools, it is a very common practice to alter the images. Fraudulent images are seen very often in social media, press and in court rooms. As a result of this, from 2001 there was a tremendous increase in the methods developed for Image Forensics and nowadays Image Forensics has become as a routine as the application of physical forensic analysis. Generally Image Forensics techniques can be classified into two, active approaches and the passive or blind approaches (Kakar, 2012). Active approaches were used traditionally...
by employing data hiding (watermarking) or digital signatures. Requirement of specialized hardware narrows its field of application. Passive approaches or blind forensic approaches use image statistics or content of the image to verify its genuineness.

Image tampering can be done with a single image or with multiple images. Splicing (combining contents from two or more images in a single image), copy-move forgery, use of image processing operations, false captioning etc. are treated as different forgery types (Kakar, 2012). Among this, copy-move forgery is the most commonly performed one and the most studied one. It is a type of forgery in which a region from the same image is copied and pasted on the same image in order to hide something or to duplicate something. This paper aims at reviewing some of the very recent blind methods in copy-move forgery detection. The rest of the paper is organized in the following way. Under the heading copy-move forgery detection, an overview of different approaches in copy-move forgery detection is elucidated. Next Section named block based methods covers the different algorithms that basically divide the image into blocks followed by the next section of comparison of the different block based methods. Methods that extract features from image key-points are discussed in the following section preceded by a comparative study of the key-point based methods.

COPY MOVE FORGERY DETECTION

Copy Move forgery is an easy form of image tampering. Figure 1 gives an example for Copy Move attack. In copy-move forgery, a region in the image is copied and pasted in some other part of the same image. As the source and the target regions are from the same image, the image features like noise, colour, illumination condition etc. will be the same for the forged region and the rest of the image. This is the basis for all copy-move forgery detection algorithms. Some form of post-processing like rotation, scaling, blurring, noise addition, reflection, compression also are performed before the region is pasted. This makes the forgery detection more complex. So the important step in such a forgery detection technique would be extraction of features, which are invariant to the above said post-processing operations, from the image. A method that is robust to some form of post-processing may not be adequate to detect forgery with another type of post-processing. Figure 1 has been taken from the MICCF220 (Amerini, Ballan, Caldelli, & Sera, 2011) database.

Copy-Move forgery detection, CMFD, techniques can be classified into two: block based approaches and key-point based approaches (Christlein, Reiss, Jordan, Reiss, & Angelopoulou, 2012). In both the approaches some form of pre-processing will be there. In block based methods, the image will be divided into overlapping blocks of specified size and a feature vector will be computed for these blocks. Similar feature vectors are then matched to find the forged regions. In Key-point based methods, feature vectors are computed for regions with high entropy. There is no subdivision into blocks. The feature vectors are matched to find the copied blocks. The common processing steps for copy move forgery detection is given below (Christlein et al., 2012).

1. Pre-processing (convert the image to gray scale if required)
2. For Block Based methods
   a. Divide the MxN image into (M-b+1) x (N-b+1), bxb sized overlapping blocks.
   b. Compute feature vector for each block
For key-point based methods
   a. Extract key-points from the image
   b. Compute feature vector for each key-point
3. Find matching feature vectors by searching its neighbourhood. Compute shift vector for each pair of matching feature vector.
4. Remove the matching pairs whose shift vector distance is less than a predefined threshold.
5. Cluster the remaining matches.
Probabilistic Evaluation of SMS Messages as Forensic Evidence: Likelihood Ratio Based Approach with Lexical Features
www.igi-global.com/article/probabilistic-evaluation-sms-messages-forensic/72324?camid=4v1a

Social Dynamics and the Future of Technology-Driven Crime
Max Kilger (2011). *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications* (pp. 205-227).
www.igi-global.com/chapter/social-dynamics-future-technology-driven/46427?camid=4v1a