INTRODUCTION

Digital images have become the main information source in our daily life. However, with the increasing availability of sophisticated photo-editing software and the widespread use of the Internet, digital image forgery has become so widespread a problem that seriously debases the credibility of photographic images as definite records of events. As a result, image forensics aiming to prevent or reveal forgery operations in digital images is receiving more and more attentions (Farid, 2009).

As active detection techniques for digital image forgery, digital signatures (Lu & Liao, 2003) and watermarking (Katzenbeisser & Petitcolas, 2001) have made great contributions. Huang and Fang (2010) exploited the Exchange-
able Image File format (EXIF) Metadata-based image watermarking in the copyright protection of digital images. However, digital signatures and watermarking are restricted to only a few fields of application because they should be embedded in the images beforehand (Kundur & Hatzinakos, 1999; Lin, Podilchuk, & Delp, 2000; Fridrich, Goljan, & Du, 2001). In contrast, passive digital image forgery detection techniques can be used in a lot of fields without such limitations, which makes it much more popular in digital image forensics (Ng, Chang, & Sun, 2004).

Among all digital image forgeries, copy-move forgery is a common one. It is a kind of manipulation in which a part of the image is copied, and then pasted onto another part of the same image in order to insert or cover some objects in the image (Bayram, Sencar, & Memon, 2009). Figure 1 and Figure 2 show an example of copy-move forgery in a news photo (“Iran test-fired long-range missiles,” 2008). Figure 1 is the original image, while Figure 2 is a fake counterpart where the third missile from the left is a duplication of another missile.

During the copy-move process, the duplicate regions may go through geometrical modifications such as rotation, scaling and/or illumination adjustment for a better visual effect. And the tampered images may also be blurred, noised, or compressed in order to hide the traces of forgery. Thus a good forgery detection algorithm should take these operations into account.

The simplest approach to detect copy-move forgery is the exhaustive search (Fridrich, Soukal, & Lukas, 2003), in which the image is compared with all its cyclic-shifted versions to look for the closest matching regions. Although this method works for copy-move forgery detection, its high computational burden prevents it from practical applications.

Block matching is proposed to reduce the computational time. In the matching procedure, an image is divided into overlapping blocks first, and then all duplicate block pairs are marked. The key lies in finding some robust representations for each image block, and then the duplicate blocks can be identified even they are not exactly the same.

Fridrich et al. (2003) proposed to represent the image blocks with quantized Discrete Cosine Transform (DCT) coefficients, and lexicographical sorting is adopted to detect the copy-move blocks. An improved DCT-based method was proposed by Huang et al. (2011) to detect
Related Content

Facial Reconstruction as a Regression Problem
Maxime Berar, Françoise Tilotta, Joan A. Glaunès, Yves Rozenholc, Michel Desvignes, Marek Bucki and Yohan Payan (2011). *Digital Forensics for the Health Sciences: Applications in Practice and Research* (pp. 68-87). www.igi-global.com/chapter/facial-reconstruction-regression-problem/52285?camid=4v1a

A Novel Progressive Secret Image Sharing Scheme Based on Arithmetic Mean
Biometrical Processing of Faces in Security and Forensics
Pawel T. Puslecki (2010). Handbook of Research on Computational Forensics, Digital Crime, and Investigation: Methods and Solutions (pp. 79-103). www.igi-global.com/chapter/biometrical-processing-faces-security-forensics/39214?camid=4v1a

Calm Before the Storm: The Challenges of Cloud Computing in Digital Forensics