Chapter 3
An Image Region Description Method Based on Step Sector Statistics and its Application in Image Copy-Rotate/Flip-Move Forgery Detection

Likai Chen
Sun Yat-sen University, China

Wei Lu
Sun Yat-sen University, China

Jiangqun Ni
Sun Yat-sen University, China

ABSTRACT

A robust method for local image region feature description based on step sector statistics is proposed in this paper. The means and the standard deviations along the radial direction of the circle image region are extracted through the sector masks, and the rearrangement of these statistics makes this image region description method rotation-robust. The proposed description method is applied in the detection of copy-rotate-move forgery, and it can detect the exact rotation angle between the duplicate regions. With minor extension, the proposed description method can also be applied in the detection of copy-flip-move forgery. The experimental results show that the proposed description method can work well for the detection of copy-rotate/flip-move forgery.

DOI: 10.4018/978-1-4666-4006-1.ch003

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 Exchangeable 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

Figure 1. Copy-move forgery example: the original image