Chapter 8
Semi-Fragile Image Watermarking, Authentication and Localization Techniques for Law Enforcement Applications

Xi Zhao
University of Surrey, UK

Anthony TS Ho
University of Surrey, UK

ABSTRACT

With the tremendous growth and use of digital cameras and video devices, the need to verify the collected digital content for law enforcement applications such as crime scene investigations and traffic violations, becomes paramount if they are to be used as evidence in courts. Semi-fragile watermarking has become increasingly important within the past few years as it can be used to verify the content of images by accurately localising the tampered area and tolerating some non-malicious manipulations. There have been a number of different transforms used for semi-fragile image watermarking. In this chapter, we present two novel transforms for semi-fragile watermarking, using the Slant transform (SLT) as a block-based algorithm and the wavelet-based contourlet transform (WBCT) as a non-block based algorithm. The proposed SLT is compared with existing DCT and PST semi-fragile watermarking schemes. Experimental results using standard test images and simulated law enforcement images indicate that the SLT is more accurate for copy and paste attacks with non-malicious manipulations, such as additive Gaussian noise. For the proposed WBCT method, watermarking embedding is performed by modulating the parent-children relationship in the contourlet domain. Again, experimental results using the same test images have demonstrated that our proposed WBCT method achieves good performances in localising the tampered regions, even when the image has been subjected to non-malicious manipulations such as JPEG/JPEG2000 compressions, Gaussian noise, Gaussian filtering, and contrast stretching. The average miss detection rate is found to be approximately 1% while maintaining an average false alarm rate below 6.5%.

DOI: 10.4018/978-1-60566-836-9.ch008

1.0 INTRODUCTION

Nowadays, with the advent of the Internet, the usage, application and communication of multimedia content such as audio, image and video data are increasingly intertwined into people's daily lives. With the growing popularity and affordability of image editing software such as Adobe Photoshop and Corel Paint Shop, even the most novice of users are able to modify the content of images to a perceptually high standard, and with relative ease. Consequently, for some practical applications such as remote sensing, legal defending, news reporting, and crime scene investigation, it is particularly important for verification or authentication of the integrity of the digital media content (Ho, 2007).

For crime scene investigation and traffic enforcement scenarios, images captured at the scene can potentially be used as evidence in the court of law. The role of a scene of crime officer (SoCOs) is to capture, as much as possible, the left-over evidence at the crime scene by taking photographs and collecting any exhibits found. After the collection of evidence, there is no other way of examining the crime scene as a whole, apart from analysing the collected exhibits and photographs taken. Crime scene photography can typically be defined according to three different kinds of photographs: "general" shots are those images that capture the whole scene, "mid-range" shots tend to hone in on a specific region of the scene, and finally "close up" shots are those that capture the details of a particular piece of evidence. Moveable exhibits are often taken back to a studio to be photographed from multiple angles (Vrusias et al., 2001). In order to maintain the integrity of the images, not only it is essential to verify that the photographic evidence remains unchanged and authentic, but any manipulated regions should also be localised to help identify which parts of the image cannot be trusted. With the tremendous growth and usage of digital cameras and video devices, the requirement to verify the digital content is paramount, especially if it is to be used as evidence in court.

Cryptography and digital watermarking are two commonly used technologies for image authentication (Haouzia and Noumeir, 2007). Cryptography can, for example, be utilised for message authentication by generating and embedding a digital signature into a message, in an effort to prevent the sending of forged messages (Menezes et al., 1996). In addition, according to Friedman (1996), digital signatures can be embedded into images by applying cryptography if the signature is metadata. In all cases, the use of cryptography is constrained by the fact that it can be lost easily during the image format conversion process, which subsequently invalidates the authentication process. Digital watermarking has attracted much attention in the past decade, particularly for copyright protection purposes for digital images (Cox et al., 2008). However, in the past few years, digital watermarking has been applied to authenticate and localise tampered regions within images (Ho, 2007). "Fragile" and "semi-fragile" digital watermarking techniques are often utilised for image content authentication. Fragile watermarking is aptly named because of its sensitivity to any form of attack whilst semi-fragile watermarking is more robust against attack, and can be used to verify tampered content within images for both malicious and non-malicious manipulations (Lin et al., 2007; Ho et al., 2004; Monzoy-Villuendas et al., 2007; Lin et al., 2005). Semi-fragile watermarking can be defined according to two methodologies: "block" and "non-block" based. The Pinned Sine Transform (PST) (Zhu et al., 2007), Discrete Cosine Transform (DCT) (Barni et al., 1998; Cox et al., 1997) and Slant Transform (SLT) (Zhao et al., 2007) can be categorised as "block-based" methods, whereas the Discrete Wavelet Transform (DWT) (Kundur et al., 1998; Wang and Lin, 2004; Tsai and Lin, 2007) can be classified as a "non-block" based method. In this chapter, we will introduce two novel semi-fragile watermarking schemes for image authentication and localisation, based on "block"