Chapter 7
A Survey of Digital Forensic Techniques for Digital Libraries

Yue Li
Nankai University, China

ABSTRACT

Today, many digital forensic techniques for digital images are developed to serve the purpose of the origin identification and integrity verification for security reasons. Generally speaking, these methods can be divided into two classes, the methods based on the extracted features, which are usually the high frequency noise inside the investigating images and the methods based on the contents of the images. Different techniques may be developed specially against different forging attacks, while be vulnerable to other malicious manipulations on the images. This paper reviews the most popular techniques in order to help the user to understand the techniques and find the most proper methods for variety forensic purpose in different situations.

1. INTRODUCTION

Nowadays, the widely applied digital imaging devices bring great convince to the people in daily life. At any time, people can capture scenes around them by the portable cameras or the built-in camera in the mobile; the government can achieve 24-hour surveillance by the widely installed CCTV; the journalists can records the 1/24-second-motions by the professional camera. However, the security of the captured digital images remains unprotected and such problem needs urgently investigation by the research and the engineer (Chen, Fridrich, Goljan, & Lukas, 2008). The malicious user can easily forge an image with modified contents or replace the output images of the camera with a fake one. These operations are defined as attacks in the study of security of multimedia and protection of digital libraries while the user who operated these attackers are defined as attackers. Practically, these attacks may be operated for different purposes. For example, the attacker may fake an origin marks in the image to announce an illegal copyright of the digital multimedia products, or the attacker may modify the contents inside an image or a video,

DOI: 10.4018/978-1-4666-2928-8.ch007

which is used as evident in court. It is obvious that these attacks will cause tremendous loss in practical if no proper protections are implied, and therefore, many security techniques have been developed to fight against these attacks.

Digital watermarking are traditionally developed to protect the digital multimedia products (Rey & Dugelay, 2006; Liu & Qiu, 2002; Lu & Liao, 2001; Li & Hong, 2008; Wolfgang & Delp, 1997). The term of digital watermarking, which is similar to the real watermarking implanting a mark in the secret paper documents or bank notes, refers to an operation embedding an imperceptible mark into the digital multimedia products to authorise the integrity and origin of the images. The user, who needs to authorise the products, extracts and investigates the integrity of the embedded watermark. If the watermark is broken or destroyed, then the product is deemed as forged. Digital watermarking techniques may be developed to achieve advance functions. For example, some techniques can localise which area is modified by the attacker (Liu & Qiu, 2002; Lu & Liao, 2001; Wolfgang & Delp, 1997) whereas other techniques can survival after the attack and can be further used to reconstruct the images (Rey & Dugelay, 2004; Liu & Qiu, 2002; Lu & Liao, 2001).

Despite of the advantages in theory and effectiveness in practices, digital watermarking are not widely applied in the implementation due to some disadvantages,

1. Firstly, digital watermarking is a class of intrusive security techniques that modify the contents inside the images. Although this modification is imperceptible and the embedded images preserve high visual qualities, the contents inside the embedded images are altered more or less due to the modification (Swaminathan, Wu, & Liu, 2007; Cox, Doerr, & Furon, 2006). Digital watermarking techniques are inappropriate in the applications where identical images are requested. For example, the images submit to court as evident cannot be watermarked in most situations due to the laws, which request the images must be original without any modification.
2. Multiple watermarking methods cannot be applied on the same multimedia products. According to the research, one watermarking techniques may be only limited attacks (Cox, Miller, Bloom, Fridrich, & Kalker, 2007). For example, the watermarking techniques developed in spatial domain and based on block dependency are always fragile to localise the modified area but cannot survive under the (Rey & Dugelay, 2002; Liu & Qiu, 2002; Lu & Liao, 2001; Li & Hong, 2008; Wolfgang & Delp, 1997; Swaminathan, Wu, & Liu, 2007; Cox, Doerr, & Furon, 2006; Cox, Miller, Bloom, Fridrich, & Kalker, 2007). While the techniques in transform domain are normally robust and able to be clearly identified after the attack but unable to point out the modified regions. In contrast, the attackers normally applies many attacking techniques in one attack. For example, the attacker may modifies the contents of the multimedia products while destroy the origin marks left in the images. If fragile watermarking techniques are applied to localise the tampered area, the origin marks will not be protected. When the robust watermarking is applied to implant the marks into the image and robust the attacks, the robustness make the localisation function fails. Although several works are done (Osborne, Abbott, Sorell, & Rogers, 2004; Li, 2010) aiming to employ different watermarking techniques at the same time, the employed techniques are normally owning similar function, such as robust or fragile, but unable to serve the two purposes at the same time.
3. Due to the aforementioned two disadvantages, in the implementation of digital watermarking, the user must first determine