Digital Image Authentication:
A Review

Yue Li, Nankai University, Tianjin, China

Chia-Hung Wei, Ching Yun University, Taiwan

ABSTRACT

Digital image authentication refers to all the techniques performing anti-falsification, digital image copyright protection, or access control. A large number of DIA techniques have been developed to authenticate digital images, including cryptography-based digital image authentication (CBDIA) techniques and data-hiding-based digital image authentication (DHBDIA) techniques. This paper not only provides some practical applications on image authentication, but also describes general frameworks of image watermarking and the general techniques, including robust watermarking, fragile watermarking, and semi-fragile watermarking. This paper also addresses the potential issues on future research directions, including managing the PRNU database, development of advanced PRNU-based blind authentication techniques, and search for digital fingerprints.

Keywords: *Data Hiding, Digital Fingerprints, Forensic Science, Image Authentication, Watermarking*

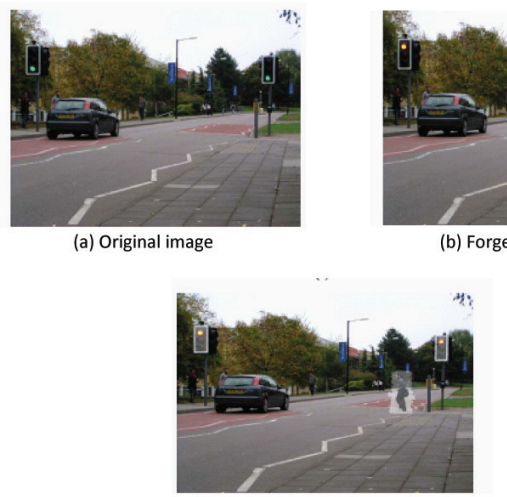
1. DIGITAL IMAGE AUTHENTICATION

Due to the fast growth of digital technology, daily activities can be easily captured and saved in digital images, and then transmitted via the Internet. Despite the convenience, digital images suffer from problems, which can be summarised by the following questions: which person/device produces the image, who are authorised to access this image when it is stored and distributed, and whether the image is modified (Rey & Dugelay, 2002). As a result, digital image authentication (DIA) techniques have been developed in order to solve those security problems (Liu & Qiu, 2002). In the research of image authentication, DIA is a generic term for all the techniques performing anti-falsification, digital image copyright protection or access control (Lu & Liao, 2001).

1) **Anti-Falsification:** Anti-falsification is one of the primary functions of DIA techniques, which aims to prove the authenticity and integrity of digital images (Li & Hong, 2008). If an image is modified, the DIA techniques for anti-falsification should be able to detect the modification and localise the modified areas. Figure 1 demonstrates the anti-falsification function by authenticating the image of a traffic scene, which may be used as evidence in the court of law. Figure 1(a) is the original image, while Figure 1(b) is a tampered version with a pedestrian embedded and the traffic lights altered. The authentication

DOI: 10.4018/jdls.2011040104

Figure 1. The anti-falsification function of DIA



(a) Original image

(b) Forged image

(c) Authenticated image

result is illustrated as Figure 1(c), with the tampered region shaded.

2) **Digital Image Copyright Protection:** Copyright protection is another important authentication function in DIA (Wolfgang & Delp, 1997). In the application of copyright protection, the DIA techniques need to either identify the ownership of images or identify the source of images. To protect the commercial value of images and to fight against piracy, DIA techniques are applied to identify the ownership of the digital images. On the other hand, the trustworthiness of the source of digital images is also an important issue when the images are used in the news and media industry (Bartolini, Tefas, Barni, & Pitas, 2001). Therefore, the DIA techniques are also used to identify the source of digital media, including scanners, digital cameras and computer graphic software. Figure 2 illustrates the two applications in copyright protection.

Figure 2(a) illustrates a computer graphic artwork where the visual signature on the upper-right corner can be easily removed or changed. Thus DIA techniques are required to ascertain the ownership of the work in the case of copyright infringement. Figure 2(b), on the other hand, illustrates a photo captured by a traffic surveillance camera, showing a car illegally parking aside the road.

3) **Access Control:** Access control is also an important authentication function for DIA. In many applications, the images involve sensitive data. When these images are stored in the database or transmitted via the Internet, they should only be accessed by the authorised users with the proper level of access rights. For example, in the system for protecting digital mammogram proposed by Li and Li (2009), the access right is divided into three levels according to the role of the users as demonstrated in Table 1. For instance, the doctor in charge of a case can access the patient's informa-