Chapter 9
Decomposed PRNU Library for Forensics on Photos

Yue Li
Nankai University, China

ABSTRACT

Today, the digital forensic techniques for digital images are developed with the origin identification and integrity verification functions for security reasons. Methods based on photo-response-non-uniform (PRNU) are widely studied and proved to be effective to serve the forensic purposes. However, due to the interpolation noise, caused by the colour filtering and interpolation function the accuracy of the PRNU-based forensic method has been degraded. Meanwhile, the tremendous physical storage requirement and computation consumption limit the applications of PRNU-based method. Therefore, an innovative DPRNU-based forensic method has been proposed in order to solve the above problems. In the method, the artificial component and physical component are separated according to the colour filtering array (CFA) and the PRNU are only extracted from the physical component in order to remove the interference caused by the interpolation noise, which increases the accuracy of the camera identification and integrity verification. Meanwhile, due to the separation, the DPRNU are only 1/3 of the size of the traditional PRNU, which saves considerable physical storage in setting up the digital library and faster the comparison speed between the fingerprints.

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. The security problem can be summarized as which person/device produces the image and whether the image is modified. As a result, the digital forensic techniques for digital images are developed with the origin identification and integrity verification functions in order to solve the aforementioned problems.
Generally speaking, the forensic techniques extract a fingerprint, which is a digital feature left by the digital imaging device, and compared it to the reference fingerprints representing a set of imaging devices in the database (Dirik, Sencar, & Memon, 2008; Fridrich, 2009; Caldelli, Amerini, Picchioni, De Rosa, & Uccheddu, 2009; Cao & Kot, 2010). Depending on the comparing result, the forensic techniques can identify the origin and verify the integrity of the digital images (Lukas, Fridrich, & Goljan, 2006a; Lukas, Fridrich, & Goljan, 2006b). The framework of forensic techniques is illustrated in Figure 1. The scheme first extracts the digital fingerprint $S_I$ of image $I$, and then $S_I$ is compared to fingerprint $S_D$ in the fingerprint database. To identify the origin of the image, the fingerprint database contains the reference fingerprints of a variety of imaging devices. If a correlation between a reference fingerprint and $S_I$ is maximal among all correlations and greater than a predefined threshold, then the corresponding device is identified as the source device of the image under investigation. To verify content integrity, the fingerprint database consists of fingerprints on different areas of the reference image. If a reference fingerprint on a special area results in a correlation lower than the threshold, then this area is identified as a forged area.

Due to the necessity of the reference fingerprint, setting up a digital library, which stores the majority reference fingerprints of the digital devices and connect to internet/intranet, is essential to serve the forensic purposes. With the aids of the digital fingerprint library, the user can identify the source cameras by comparing the fingerprints of the camera under investigation and the fingerprint stored in the library and representing sample cameras (Lukas, Fridrich, & Goljan, 2006a; Lukas, Fridrich, & Goljan, 2006b). Meanwhile, the user can investigate the integrity of the photo using the fingerprints. Compared to the sample fingerprint in the library, if the investigated fingerprint is partially broken or entirely destroyed, then the corresponding photo can be verified as tampered in the corresponding area or entirely faked due to the destroyed fingerprint (Chen, Fridrich, Lukas, & Goljan, 2008; Chen, Fridrich, Goljan, & Lukas, 2007a). As a result, the digital library of the fingerprint can greatly benefit the user in the forensic application. However, in setting up such digital library, the user may face the serious problem in the physical storage requirement and tremendous time consuming in the computation. In the next section, a most representative and widely applied forensic method based on PRNU (Chen, Fridrich, Lukas, & Goljan, 2008; Chen, Fridrich, Goljan, & Lukas, 2008; Chen, Fridrich, Goljan, & Lukas, 2007b; Li, 2009a; Li, 2009b) is reviewed and the corresponding limitations in setting up a library on this method is discussed.

**Figure 1. A general framework of NDHBDIA techniques**