Chapter 74
Digital Forensics:
State-of-the-Art and Open Problems

Ruchira Naskar
National Institute of Technology Rourkela, India

Pankaj Malviya
National Institute of Technology Rourkela, India

Rajat Subhra Chakraborty
Indian Institute of Technology Kharagpur, India

ABSTRACT

Digital forensics deal with cyber crime detection from digital multimedia data. In the present day, multimedia data such as images and videos are major sources of evidence in the courts of law worldwide. However, the immense proliferation and easy availability of low-cost or free, user-friendly and powerful image and video processing software, poses as the largest threat to today's digital world as well as the legal industry. This is due to the fact that such software allow efficient image and video editing, manipulation and synthesis, with a few mouse clicks even by a novice user. Such software also enable formation realistic of computer-generated images. In this chapter, we discuss different types of digital image forgeries and state-of-the-art digital forensic techniques to detect them. Through these discussions, we also give an idea of the challenges and open problems in the field of digital forensics.

1. INTRODUCTION

In today's cyber world digital images and videos act as the most frequently transmitted information carriers. This has been made possible by the huge proliferation of low-cost, easy-to-use and efficient consumer devices such as high-resolution digital cameras for image acquisition and availability of high-speed transmission media such as the internet. Gone are the days when image acquisition was essentially an analog process. Photography and image formation was film dependent and could only be done by experts in dark rooms. With the advancement of analog to digital (A/D) converters, every step of digital image acquisition, formation and storage, is now well within the grip of the common man.

DOI: 10.4018/978-1-5225-0983-7.ch074

However, the present day easy availability of low-cost or free image and video processing software and desktop tools, having immense number of multimedia manipulating features, pose threat to the fidelity of digital multimedia data. Common image and video processing operations such as cropping, splicing, blurring etc., can be performed at the click of a mouse by an average user using such software. This situation compels us to question the trustworthiness of the digital images and videos. Since digital images and videos act as the major electronic evidences for law enforcement across the world, as they are the most effective and efficient means to collect digital evidences from crime scenes. Hence, maintenance of their trustworthiness and reliability is a major challenge in today's digital world. It is extremely crucial to preserve such digital evidences against cyber-crime for suitable presentation in court of law. The need for investigation and maintenance of the fidelity and reliability of digital images and videos, has given rise to the field of "Digital Forensics" (Sencar & Memon (eds.), 2013; Redi et. al., 2011). In the recent years, researchers have focused on the areas of digital image authentication, tampering detection, identification of image forgery as well as investigation of image sources. In this chapter, we shall focus on the basics of digital forensics and the need for research in this direction. The chapter contents will include two major topics:

1. **Image Forgery Detection:** Analysis of whether the image is *original*, or has it undergone any form of tampering. Image forgery detection is carried out with the aim of investigating whether the image under question represents the unmodified captured scene or has it been forged to deceive the viewer.
2. **Image Source Identification:** Forensic analysis to investigate which device (or class of device) captured or formed the image under question.

Since JPEG is currently the most commonly used digital image format, and it is the default image format in almost all current digital camera, in this chapter we shall majorly focus on JPEG images.

Rest of the chapter is organized as follows. In Section 2, we discuss the necessity of digital forensics in the relation to digital media content protection; we compare and contrast various pros and cons of digital forensic methods in comparison to other existing digital content protection tools and techniques. In Section 3, we present different classes of digital image forgeries and state-of-the-art digital forensic techniques to deal with those classes. In Section 3, we also present a forensic technique to detect JPEG forgery, in detail. In Section 4, we present state-of-the-art digital forensic techniques to identify the origin of an image. Finally we conclude with a discussion on the future of digital forensics, in Section 5.

2. DIGITAL CONTENT PROTECTION AND DIGITAL FORENSICS

The last couple of decades have seen rapid growth of research interest in the fields of *Digital Content Protection* and *Digital Rights Management* (Cox et. al., 2008), due to rapid increase of cyber-crime rate. The most widely used practices in this direction encompass digital techniques such as *Watermarking* and *Steganography* (Cox et. al., 2008). In this section we discuss the major difference and benefit of digital forensic techniques, over such traditional digital content protection measures.

In *Digital Watermarking* (Shih, 2007) techniques, the data to be protected (*cover data*) undergoes some form of pre-processing such as embedding, compression (lossless or lossy) etc., which later help to detect malicious third party interventions. The *watermark* is a piece of information that is kept embedded