Chapter 6
Multimedia Forensic Techniques for Acquisition Device Identification and Digital Image Authentication

Roberto Caldell
University of Florence, Italy

Irene Amerini
University of Florence, Italy

Francesco Picchioni
University of Florence, Italy

Alessia De Rosa
University of Florence, Italy

Francesca Uccheddu
University of Florence, Italy

ABSTRACT

Multimedia forensics can be defined as the science that tries, by only analysing a particular digital asset, to give an assessment on such a content and to extract information that can be useful to address and support an investigation linked to the scene represented in that specific digital document. The basic idea behind multimedia forensics relies on the observation that both the acquisition process and any post-processing operation leave a distinctive imprint on the data, as a sort of digital fingerprint. The analysis of such a fingerprint may permit to determine image/video origin and to establish digital content authenticity.

DOI: 10.4018/978-1-60566-836-9.ch006

INTRODUCTION

Digital crime, together with constantly emerging software technologies, is growing at a rate that far surpasses defensive measures. Sometimes a digital image or a video may be found to be incontrovertible evidence of a crime or of a malevolent action. By looking at a digital content as a digital clue, Multimedia Forensic technologies are introducing a novel methodology for supporting clue analysis and providing an aid for making a decision on a crime. Multimedia forensic researcher community aimed so far at assisting human investigators by giving instruments for the authentication and the analysis of such clues. To better comprehend such issues let firstly introduce some application scenarios. Let's imagine a situation in which the action itself of creating a digital content (e.g. a photograph) implies an illegal action related to the content represented in the data (e.g. child pornography). In such a case, tracing the acquisition device that took that digital asset, can lead the judge to blame the owner of the "guilty" device for that action. Forensic techniques can help in establishing the origin/source of a digital media, making the "incriminated" digital content a valid, silent witness in the court. A similar approach can be used in a different circumstance, in which a forensic analysis can help the investigator to distinguish between an original multimedia content and an illegal copy of it. Different types of acquisition devices can be involved in this scenario, from digital cameras, scanners, cell-phones, PDAs and camcorders till photorealistic images or videos created with graphic rendering software. In this context, the possibility of identifying how that digital document was created may allow to detect illegal copy (e.g. digital cinema video recaptured by a camcorder). A more insidious digital crime is the one that attempts to bias the public opinion through the publication of tampered data. Motivations can spread from joking (e.g. unconvincing loving couple), to changing the context of a situation in which very important people are involved, or to exaggerating/debasing the gravity of a disaster image. Image forensic techniques can give a support in recognizing if, how and possibly where the picture has been forged.

Forensic tools work without any added information, the only features that can be evaluated are the ones intrinsically tied to the digital content. The basic idea behind multimedia forensic analysis relies on the observation that both the acquisition process and any post-processing operation leave a distinctive imprint on the data, as a sort of digital fingerprint. The estimation of such fingerprints really suggests how to evaluate the digital clue, turning it into an actual evidence.

It is the aim of this chapter to present the principles and the motivations of digital forensics (i.e. concerning images and videos), and to describe the main approaches proposed so far for facing the two basic questions: a) what is the source of a digital content? b) is such a digital content authentic or not? The chapter will be organized as it follows. The first section will introduce the reader to the basics of multimedia forensics; the different approaches for obtaining information from a digital content will be presented, as well as the diverse type of digital data that can be usually analyzed; then, the possible application scenarios that can benefit from forensic techniques will be described and an overview over the intrinsic digital fingerprints will be presented. The second and the third sections will be devoted to the analysis of the principal techniques exploited respectively for identifying the acquisition device of digital images and videos, and for assessing the authenticity of digital images. Future trends will be suggested and some conclusions will be provided in the last sections. Bibliographic references will complete the chapter.