A Forensic Tool for Investigating Image Forgeries

Marco Fontani, Department of Information Engineering and Mathematical Sciences, University of Siena, Siena, Italy

Tiziano Bianchi, Department of Electronics and Telecommunications, Politecnico di Torino, Torino, Italy

Alessia De Rosa, National Inter-University Consortium for Telecommunications, University of Florence, Firenze, Italy

Alessandro Piva, Department of Information Engineering, University of Florence, Firenze, Italy

Mauro Barni, Department of Information Engineering and Mathematical Sciences, University of Siena, Siena, Italy

ABSTRACT

Images have always been considered a reliable source of evidence in the past. Today, the wide availability of photo editing software urges the authors to investigate the origin and the integrity of a digital image before trusting it. Although several algorithms have been developed for image integrity verification, a comprehensive tool that allows the analyst to synergically exploit these algorithms, and to reach a final decision based on their output, is still lacking. In this work the authors propose an image forensic tool trying to fill this gap. The proposed tool exploits state of the art algorithms for splicing detection, with forgery localization capabilities, and make them available to the analyst through a graphical interface. In order to help the analyst in reaching a final assessment, a decision fusion engine is employed to intelligently merge the output of different algorithms, boosting detection performance. The tool has a modular architecture, that makes it easily scalable.

Keywords: *Authenticity Assessment, Decision Fusion, Dempster-Shafer Theory of Evidence, Forgery Localization, Image Forensics, Image Forensic Analyst, Integrity Verification*

INTRODUCTION

The advent of image processing technologies easily enables modification and manipulation of digital visual data, so that we are no longer confident that what we are seeing in a photo is a true representation of what really happened: the value of photography as a record of events must be carefully evaluated. Such a need comes from different fields of application: one of the most important is the forensic scenario, in which the trustworthiness of images must be assured

DOI: 10.4018/ijdcf.2013100102

before using them as potential evidences. Image Forensics (IF) (under the umbrella of the more general Digital Forensics) is the science addressing the validation, identification, analysis, interpretation of digital images as potential evidences. One of the most interesting tasks in IF is *splicing detection*, that aims at understanding if a given photo is a composition of different shots. Several approaches for splicing detection have been proposed recently (Piva, 2013), sharing the same basic idea: creating a forgery usually requires some processing steps, and these leave some statistical footprints into the signal.

In this context, the Image Forensic Analyst (IFA from now on) is the professional that applies technological means for extracting information on image history and for assuring its credibility, after the chain of custody (COC) procedures have been applied for acquiring, transferring and storing the visual data (see Figure 1). Usually, the IFA has not any previous knowledge about the history of the images that he is considering (i.e., what device acquired them, whether a processing software has been used to edit them or not, and so on), and must produce a report about the credibility of the analysed contents. To reach this goal, the IFA today could use algorithms developed in the IF literature, but in practice several problems rise: algorithms are stand-alone, in that they focus on a specific footprint and ignore the others; they assume some prior knowledge about the kind of processing that could have been carried on the media; and, finally, they do not expose a user interface helping the IFA in setting up the analysis and interpreting the results.

As a result, several issues are still open when we consider to apply the results coming from academic research to practical cases, where the IFA needs technological instruments that facilitate him in reaching a conclusion:

- There are no tools that help the IFA to exploit the different capabilities of existing algorithms. We should consider that, in the end, the IFA is mainly concerned about image integrity (i.e. Algorithm output), and only indirectly concerned about footprint detection (i.e. Algorithm functioning);
- Usually the presence/absence of forensic fingerprints can be verified on the image as a whole, or on a selected suspected region; only few examples of tools that provide a fine-grained localization of forgery within a digital image have been proposed;
- Each tool usually considers to reveal one specific trace of tampering, but the IFA cannot know in advance which traces should be searched for. Therefore, there is need for a tool that helps in interpreting and putting together the outputs from different algorithms.

For these reasons, we believe that providing a comprehensive system for image splicing detection is an important contribution for the diffusion of image forensic technologies.

In this work we present a tool for evaluating the integrity of a digital image, by revealing whether the image is a malicious composition

Figure 1. A simplified version of the chain of custody, where the positioning of the proposed tool is highlighted