Forensic Science International xxx (2015) e1–e6

Contents lists available at ScienceDirect

Forensic Science International

journal homepage: www.elsevier.com/locate/forsciint

Case report

Detection of manipulations on printed images to address crime scene analysis: A case study

Irene Amerini [a,*], Roberto Caldelli [a,c], Alberto Del Bimbo [a], Andrea Di Fuccia [b], Anna Paola Rizzo [b], Luigi Saravo [b]

[a] Media Integration and Communication Center, University of Florence, Florence, Italy
[b] Presidenza Consiglio dei Ministri – Scientific and Technological Department, Rome, Italy
[c] National Interuniversitary Consortium for Telecommunications – CNIT, Florence, Italy

ARTICLE INFO

Article history:
Received 22 January 2015
Received in revised form 20 March 2015
Accepted 23 March 2015
Available online xxx

Keywords:
Evidence manipulation
Image tampering detection
CADET
Image analysis

ABSTRACT

Photographic documents both in digital and in printed format plays a fundamental role in crime scene analysis. Photos are crucial to reconstruct what happened and also to freeze the fact scenario with all the different present objects and evidences. Consequently, it is immediate to comprehend the paramount importance of the assessment of the authenticity of such images, to avoid that a possible malicious counterfeiting leads to a wrong evaluation of the circumstance.

In this paper, a case study in which some printed photos, brought as documental evidences of a familiar murder, had been fraudulently modified to bias the final judgement is presented. In particular, the usage of CADET image forensic tool, to verify printed photos integrity, is introduced and discussed.

1. Introduction

Each investigation starts with the forensic analysis of the crime scene that is carried out with scientific methods, accuracy and systematic approach [1–4]. The basic goal of scientific crime scene investigation is finding out the author(s) and understanding the sequence of the facts.

In particular, one of the step in death scene investigation is to obtain detailed photographic documentation; this creates a permanent historical record of the scene and allows an examination of the mutual spatial location of the objects present within the scene itself which constitute a judicial proof as well [5]. However, the crime scene could have undergone an accidental contamination (e.g. caused by the first response) or a voluntary alteration (e.g. realized by the author), which might lead to a misinterpretation of the facts. Recently, this has happened, for instance, during the Oscar Pistorius trial in which some photographs seemed to underline that the crime scene has been altered[1].

Beside such alterations, there is a different kind of manipulation of the facts, that consists in the fraudulent modification of forensic evidences, tests report or other documents such as photos and videos taken on the crime scene that might address the judge to a wrong conclusion during the trial [6,7]. In particular, there are very disparate cases in which the authenticity of the multimedia materials brought as evidence was doubted: for example, on 2014 in West Virginia, the police was accused to have altered a video evidence in the death of a mentally ill black man[2] or, on 2008 in North Carolina, the integrity of an audio recorded during an arrest for cocaine traffic was questioned[3].

In the light of this, it can be assessed that the preliminary analysis of the genuineness of multimedia evidences has become the first step of any forensic examination. This is especially true when digital images are involved and, above all, in each circumstance in which there is uncertainty of their intrinsic authenticity. This mainly happens when the provenance of the images is unreliable and the whole acquisition procedure has not been taken under control. Furthermore, in many countries, the reliability of digital images has been questioned by courts

* Corresponding author. Tel.: +39 0552751391.
E-mail address: irene.amerini@unifi.it (I. Amerini).

[1] http://www.cbc.ca/news/world/oscar-pistorius-trial-photographs-show-police-altered-crime-scene-1.2576673.

[2] http://www.reuters.com/article/2014/08/28/us-usa-west-virginia-shooting-idUSKBN0GS2TV20140828.

[3] http://www.wral.com/news/local/story/2320627/.

http://dx.doi.org/10.1016/j.forsciint.2015.03.020
0379-0738/

Fig. 1. The mock scene (left) and the above view of the black table (right). In the mock scene the bloody handprint has been reproduced in white just to enhance the visualization during the experiments.

themselves. The Convention on Cybercrime (Budapest 2001) helped legitimize their use as evidence [8]. Now digital images are mostly accepted in courts like other evidence types (DNA, fingerprints, micro traces, etc.) and play a fundamental role in investigation scene documentation [9]. This was re-enforced in Italy with the ratification of the Budapest Convention in 2008 [10].

Therefore, being digital images crucial, scientific literature has researched lots of strategy to protect the forensic science community from possible malicious frauds [11], thus to establish whether an image is authentic or not [12,13], (at least, to assess, with a certain degree of probability, its authenticity) or to determine the provenance, that is its acquisition source [14–17].

Whenever an image, is presented as an evidential information to a Court, it should be followed the approach to analyze the document with a forensic methodology in order to determine if it contains traces of manipulation. Furthermore, it is important to highlight that if an alteration has been detected, it could be fundamental to understand which was the final aim of who had created such a modification.

In order to alter the original meaning of an image, diverse attacks can be put in practice. Besides common image processing that can be carried out with an editing software such as Photoshop®, two are the main kinds of manipulation that can be applied: the *splicing attack* and the *copy–move attack*. The first one consists in extracting an image portion from a photo (source image), possibly adapt it and then pasting it onto another one (destination image) in order to change its final meaning. In the second one, the image patch is taken and cloned onto the same image (source and destination coincide). Image forensics literature offers several examples of specific detectors for such manipulations [18]; some of them are based on the assumption that an image alteration implies a resampling or a double JPEG compression [19], others resort at visual local features descriptors [20,21] to detect similarities between different image areas.

However, in some investigative circumstances (e.g. the case described in this paper), instead of a digital photo only its analogue version might be available to the investigator. In this case, there will be the need to identify a possible forgery from a printed picture rather than its digital counterpart [22]. In fact, scanned documents or recaptured (by a digital camera) printed documents are still widely used in a number of different scenarios, like medical imaging, law enforcement and banking documents, forensic prints and daily consumer use.

In this paper, a case study of a murder in which some printed (fraudulently modified) photos were brought as documental evidences from the defense advisors is presented. Such images should have served to reject the theory of accusation, given by the Prosecutor, and to malevolently bias the final judgement. The adoption of an image forensic tool, named CADET (Cloned Area DETector) [22] has permitted to analyze such printed documents and to detect and localize an altered area. Consequently, the photos have been deemed as not authentic and thus defense's thesis has been dismantled. The results of such examination are presented on images of a mock scene reproduced by crime scene experts[4] according to the case, whose photos cannot be pictured being the legal proceedings still in progress.

The paper is organized as follows: in Section 2, the case under study is briefly presented, in Section 3, the characteristics of the CADET forensic tool are described, while in Section 4, the adopted procedure and the results are shown. Finally, Section 5 concludes the paper.

2. A case study

In this paper, we show a mock scene reproducing a cold case, in which some images, taken from the native crime scene, have been fraudulently manipulated by means of an editing software, with the aim to mislead the juridical conclusion.

In the case under investigation, there has been a woman found dead in her sitting room hit by a stick that had caused a severe head fracture (see Fig. 1 left). According to the police report, the woman was found by her husband, who had stained his hands with blood during the attempt to rescue her.

The defense of the injured party had brought to the bar a set of photos that depicted a bloody handprint belonging to the husband in a zone that allowed to sustain the accusation of homicide towards the husband himself (area A in Fig. 1 left and, in detail, area B in Fig. 1 right). According to such a thesis, the husband would have struck his wife several times, even when she was already lying on the floor and then would have left his bloody handprint on the black table when standing up from behind of his wife's body.

Unfortunately, the original printed pictures had been destroyed in a fire occurred in the police station, some days before. However, according to the deposition of the investigators, the bloody handprint left from the husband (area B in Fig. 1 right) was not originally there but on the left side of the table. Probably, it had been cloned from its native position on the table to that one where it appears on Fig. 1 (right) and, after that, the original handprint had been deleted by covering it with an image patch of the black table. Such an image alteration had completely changed the interpretation of the crime scenario in support of the defense's thesis.

Nevertheless, the examination of the crime scenario showed that such conclusion (i.e. the husband was the offender) was not acceptable also according to the bloodstain pattern analysis (BPA) [3], [23]. The BPA can reconstruct the facts by analyzing the presence, the shape and the morphology of a group of bloodstains

[4] Thanks to the Superior Institute of Investigative Techniques of Arma dei Carabinieri, for the support in the mock scene reconstruction.

Please cite this article in press as: I. Amerini, et al., Detection of manipulations on printed images to address crime scene analysis: A case study, Forensic Sci. Int. (2015), http://dx.doi.org/10.1016/j.forsciint.2015.03.020