Forensic Science International 251 (2015) e9–e14

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 30 March 2015

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/© 2015 Elsevier Ireland Ltd. All rights reserved.

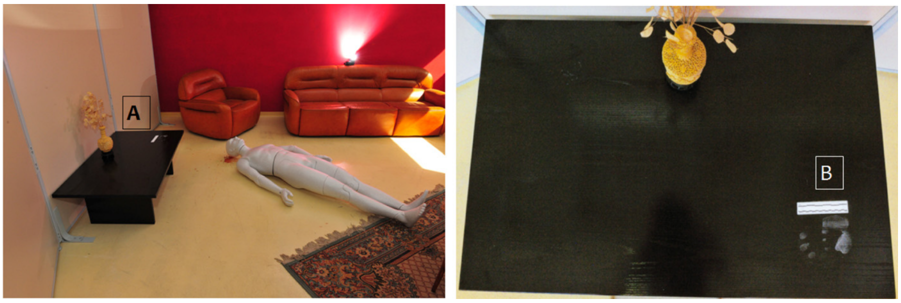


Fig. 1. The mock scene (left) and the above view of the black table (right). In the mock scene the bloody handprint has been reproduced in white just to enhance the visualization during the experiments.

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.

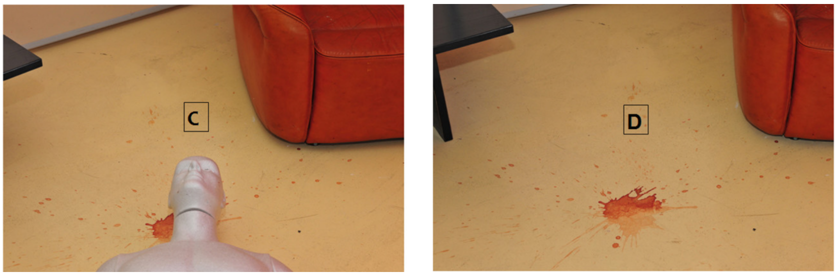


Fig. 2. The bloodstain patterns over the head of the victim with the body (C) and without (D).

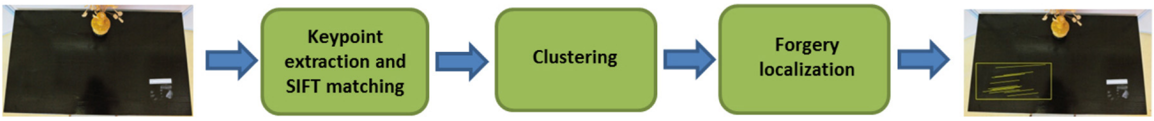


Fig. 3. Pipeline of the CADET stages.

as a result of beating, stubbing and other damages of hematic vascular system. In the area over the head of the victim (see Fig. 2), there are several spattered bloodstains caused by a hit, instead of a void area that should be present if the attacker was behind the victim at the moment of the assault. In particular a void occurs when a person or an object blocks the path of the blood. So it is possible to establish that the position of the assailant within the scene was not behind the woman because no void bloodstain patterns are found in the scene (Fig. 2). Moreover, there is no other evidence (shoeprints, footprints, etc.) that could support the hypothesis of the presence of the husband in that position during the mugging.

In light of the investigators depositions, the judge required a technical report to a forensic scientist asking for the verification of the authenticity of the pictures brought to the bar.

In such a framework, the examination of the printed pictures, presented as documentary evidences to validate the defense's thesis, becomes crucial both to ensure the reliability of the photographic evidence and to unearth a possible swindle. So the pictures have been analyzed to verify their authenticity, especially regarding Fig. 1 (right), which was basic to support the theory of the accusation against the husband. To evaluate the originality of such printed picture, a new tool, named CADET (Cloned Area DETector), has been applied to address the crime scene analysis.

The image analyst were asked to answer about the authenticity of the pictures without any knowledge about the potential repositioning of the hand in the image allowing to avoid possible bias during the analysis.

3. The image forensic tool: CADET

The image analysis was performed by the image forensic tool, named CADET, which implements a technique proposed by Amerini et al. in [24][5].

In this case, having to deal with printed images, to-be-checked photos have been firstly re-acquired and then passed to the CADET tool. In particular, such a methodology, devised to deal with digital images, has been tailored for printed image case by adjusting some settings according to [22].

The CADET tool is specific to detect copy–move attack and basically relies on SIFT (Scale Invariant Features Transform) [25] features matching; then it adopts a robust clustering, based on the J-linkage algorithm [26], to achieve forgery localization. A schema of the whole procedure is shown in Fig. 3.

The first step of the CADET tool performs the extraction of the image keypoints and, for each of these, a local descriptor, constituted by a vector of 128 SIFT features, is computed. SIFT features are robust to scaling, rotation and affine transformations so they are well-suited for the detection of copy-move forgeries as it has been recently demonstrated in [20], [24].

In particular, when a copy-move manipulation has occurred, the extracted SIFT keypoints of the copied region have similar description vectors to those of the original source area; according to this a matching operation among SIFT descriptors of image keypoints can be operated.

The second step of the method considers the use of a clustering algorithm to identify the duplicated regions and therefore detect if the image has been tampered with. CADET tool implements a clustering technique that works in the affine transformation domain of the matched points based on J-linkage algorithm (see [26] for details). This kind of clustering is able to separate duplicated regions that are close to each other and to identify a patch as single, when it contains keypoints with a non-uniform spatial distribution. Finally, if one geometrical transformation (or more) is detected, the system declares that the image has been altered by a copy–move attack. If an image is classified as forged, the system allows, in its third phase, to obtain an accurate localization of the duplicated regions.

4. The adopted procedure

Hereafter the forensic examination procedure used to analyze the printed images related to the case of the woman murder is presented (see Fig. 4). Given the printed image to be checked (obviously the quality and the dimension of the printed image is not under control of the analyst), the forensic analyst, first of all has acquired a digital image through a scanner at his disposal. Usually, it is preferable to take different scanning resolutions to get a range of various levels of detail of an image for different in-depth inspections and to obtain a reliable detection keeping the false alarm rate as small as possible. In particular, in the case of the present work, two resolutions (300 dpi and 600 dpi) have been selected.

[5] It is possible to download the first release of the CADET software here http://lci.micc.unifi.it/labd/2015/01/copy-move-forgery-detection-and-localization/.

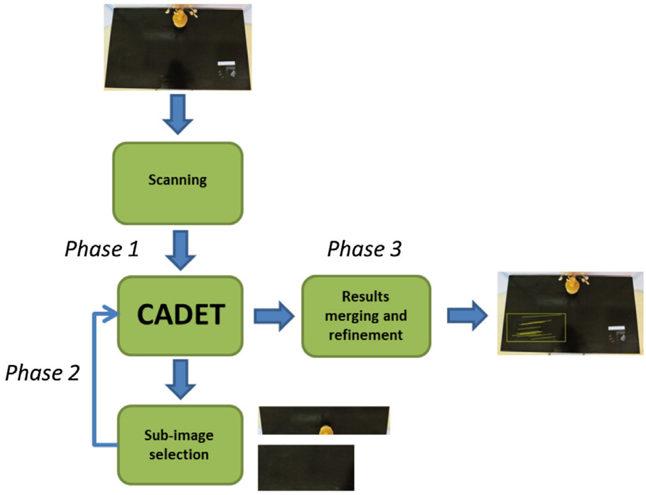
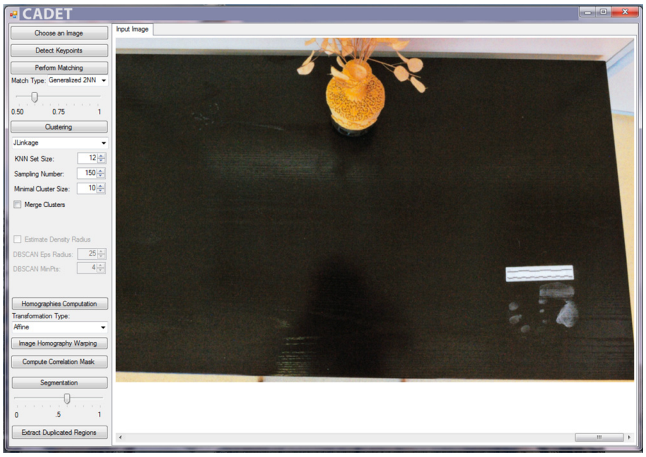


Fig. 4. The workflow of the adopted procedure.



Match Type: Generalized 2NN

0.50 0.75 1

JLinkage

KNN Set Size: 12

Sampling Number: 150

Minimal Cluster Size: 10

□ Merge Clusters

□ Estimate Density Radius

DBSCAN Eps Radius: 25

DBSCAN MinPts: 4

Transformation Type: Affine

0 .5 1

Fig. 5. The CADET tool interface.

The first phase in the procedure has been to evaluate the entire reacquired image by means of the CADET tool (in Fig. 5 the CADET interface is pictured), to point out possible areas involved in a copy-move manipulation. When suspected areas have been identified, an in-depth analysis onto such detected-as-suspicious regions has been made (*Phase 2*). Each of these regions has been inspected separately, with the CADET tool again, and, if necessary, this has been performed at different scale levels. For each of these zones a preliminary decision about their authenticity has been achieved and, finally, the results of each single area have been combined together to reach a unique outcome on the whole image.

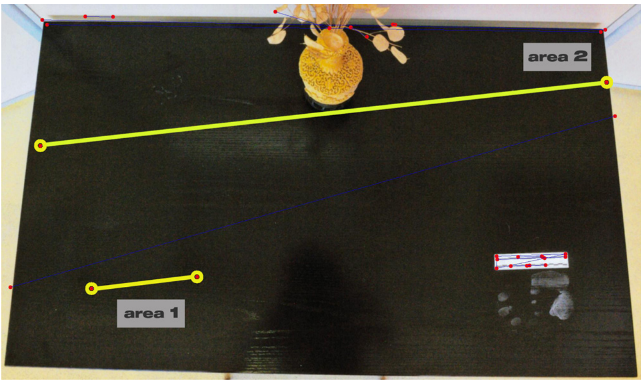


Fig. 6. Output of Phase 1. Two possible tampered areas have been detected: AREA 1 in the bottom-left part of the image and AREA 2 at the top of it. Therefore, both were cropped and passed forward to the successive Phase 2 (For interpretation of the references to color in text, the reader is referred to the web version of this article).

A final refinement (*Phase 3*) has been carried out to enhance the readability of the obtained upshot.

4.1. Experimental steps

The support of the image under observation, representing the black table with the bloody handprint, is a photo on a glossy paper with a dimension of 18 cm × 13 cm.

The scanner used by the forensic analyst to acquire the given photo is the DellMFP3115cn scanner with two different resolutions: 300 dpi and 600 dpi. The images have been stored in TIFF uncompressed format and the dimensions of the acquired images were 2028 × 1188 pixels and 4171 × 2232 pixels, respectively. Then, both the digitized images have been analyzed by the CADET tool; two suspicious regions have been detected and labelled as AREA 1 and AREA 2 (see Fig. 6). Each region contains one keypoints match (yellow straight line) indicating a possible copy-move manipulation in the area.

It is possible to exclude the others matches (blue lines linking a couple of red dots), which are recognizable within the image, as clue of tampering, due to their positions in the image (they are mostly on the border and out of the black table). The procedure has proceeded to the second step (*Phase 2*) in which the two areas, AREA 1 and AREA 2, are investigated separately in detail. First of all the two regions have been selected and cropped separately. The new images have been stored in TIFF format, with a size of 844 × 404 pixels in the case of AREA 1 and 1920 × 416 pixels for AREA 2.

The studies at different scanning resolutions and image dimensions have seen that there can be some possible matching errors which may affect the result. To solve this problem the proposed method uses a procedure able to select good matches (inliers) from the others (outliers) inside the region named AREA 1.

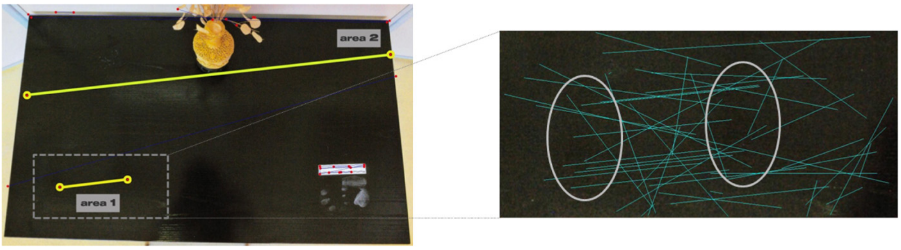


Fig. 7. Output of Phase 2: output of the CADET tool regarding AREA 1 (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article).

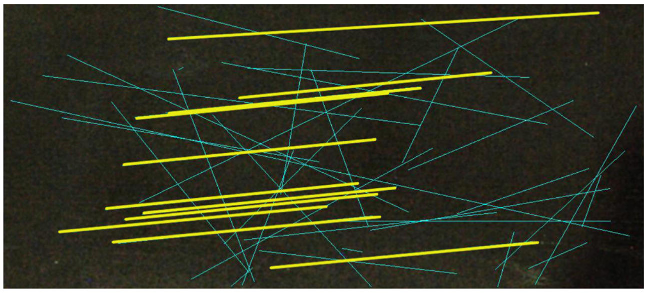


Fig. 8. Output of Phase 2: highlighting of connections between source and destination areas. A sub-group of matches (inliers) satisfying the same geometric transformation is highlighted (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article).

So the inliers, which provide a correct estimation of the model, are highlighted by the CADET tool returning an image, which specifies both the inlier and outlier points. In fact, it is possible to see in Fig. 7 (the output of CADET tool) and, in particular in the enhanced detail in Fig. 8, that some matches exhibit the same geometrical transformation (yellow parallel lines) with respect to other random matches. This is an indication that a possible tampering, according to such specific geometric transformation, could have happened. On the contrary, the same kind of analysis has been conducted on AREA 2 without evidencing any kind of manipulation. For sake of conciseness, the results related to the case of AREA 2 are not reported because discarded by the system.

So the experimental results, carried out at sub-region level, have confirmed that a copy-move forgery was performed in the area named AREA 1. The final result, after a refinement phase performed by discarding the outliers, is showed on the full image in Fig. 9. AREA 1 has been refined by eliminating all the inconsistent matches that do not satisfy a possible geometric transformation between the source and the destination patch. Details concerning the refinement process can be found in [21].

Finally, it seems plausible to assert that a part of AREA 1 was copied and then pasted in the same region in order to cover something. However, it is not possible to determine the direction of such cloning operation, it is not understandable if the right part of AREA 1 has been copy-moved on the left part or vice versa. It is also worthy to point out that such information was not so relevant in the circumstance under investigation in which just the detection of a possible image manipulation and the localization of the involved area were sufficient to give value to the deposition of the investigators that the handprint was originally in another zone (the left side) of the black table.

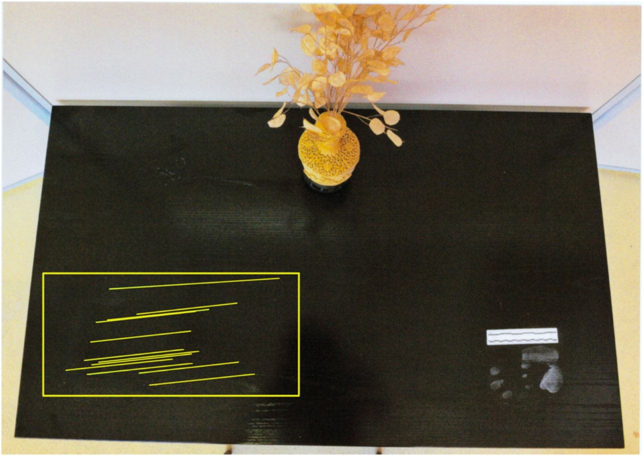


Fig. 9. Output of Phase 3: final refined outcome of the CADET tool. A copy-move forgery has been detected within the image zone denominated AREA 1.

5. Conclusions

The analytical results, obtained by means of the CADET tool, have allowed discovering an image falsification and, in particular, a copy-move manipulation inside the image representing the black table (Fig. 9). It is possible to assert that something on the table was covered by resorting at such kind of attack. Furthermore, such a result has helped to confirm the deposition of the investigators, that the bloody handprint left from the husband was originally on the left side of the table. The tool has demonstrated that the image had been falsified and to deduce that in AREA 1 the original bloody handprint was maliciously covered and then moved in a different position. Consequently, the printed images were counterfeit to support different (false) accusatory hypothesis, but the results of the image forensic analysis have comforted investigative theory that indirectly sustained the absence of the husband in that precise position.

Finally, it can be assessed that the analysis of the authenticity of the image (digital and/or printed) brought as documental evidences is fundamental especially in preliminary examination and can crucially address the successive considerations in the crime scene observation. This becomes basic nowadays that is easily possible, through the use of image editing softwares, voluntarily erase unwanted details in order to fraudulently manipulate an image.

In conclusion, the results of this paper show that image forensic tools, such as the CADET, are important to give support to the police investigation. Nowadays, each investigation requires high quality standards through the implementation of strict procedures for the verification of the integrity of each exhibit. This is particularly true when the image source is not trusted; in these cases, it might be crucial also to combine other techniques, belonging to the image forensic scientific literature. It is desirable that a specific protocol for forensic cold case analysis combining the output of image forensic science tools and intelligence examination of printed/digital images should be drawn before long.

Acknowledgments

This work was partially supported by the SECURE! Project, funded by the POR CreO FESR (D15C12008690007) 2007–2013 programme of the Tuscany Region (Italy) .

References

[1] Technical Working Group on Crime Scene Investigation, Crime Scene Investigation: A Guide for Law Enforcement Training, U.S. Dept. of Justice, Office of Justice Programs, National Institute of Justice, Washington DC, 2004.

[2] D. Curtotti, L. Saravo, 2013 Manuale delle investigazioni sulla scena del crimine, 1(3) 3(2), Giappichelli ed.

[3] S.H. James, J.J. Nordby, S. Bell, Forensic Science: An Introduction to Scientific and Investigative Techniques, fourth ed., CRC Press, 2014.

[4] O. Ribaux, A. Baylon, E. Lock, O. Delémont, C. Roux, C. Zingg, P. Margot, Intelligence-led crime scene processing. Part II: intelligence and crime scene examination, Forensic Sci. Int. 199 (1–3) (2010) 63–71.

[5] D.R. Redsicker, G. Gordner, S.H. James, A.C. Laws, A.D. Redsicker, The Practical Methodology of Forensic Photography, second ed., CRC Press, 2000.

[6] E.M. Robinson, Legal issues related to photographs and digital images, in: Introduction to Crime Scene Photography, Elsevier, 2012.

[7] G. Baio, F. Corradi, Handling manipulated evidence, Forensic Sci. Int. 169 (2) (2006) 181–187.

[8] Council of Europe, Convention on Cybercrime, ETS 185, Budapest, 2001.

[9] E. Casey, Digital evidence and computer crime, in: Forensic Science, Computers, and the Internet, third ed., Academic Press, 2011.

[10] Gazzetta Ufficiale n. 80, Supplemento ordinario n. 79, 2008

[11] M.C. Stamm, M. Wu, K.J.R. Liu, Information forensics: an overview of the first decade, IEEE Access 1 (2013) 167–200.

[12] S. Lyu, H. Farid, How realistic is photorealistic? IEEE Trans. Signal Process. 53 (2) (2005) 845–850.

[13] E. Kee, J. O'Brien, H. Farid, Exposing photo manipulation with inconsistent shadows, ACM Trans. Graph. 32 (4) (2013) 1–12.

[14] J. Fridrich, Digital image forensic using sensor noise, IEEE Signal Process. Mag. 26 (2) (2009) 26–37.

[15] J. Fridrich, Sensor defects in digital image forensics, in: H.T. Sencar, N. Memon (Eds.), Digital Image Forensics: There is More to a Picture Than Meets the Eye, Springer, 2012.

[16] I. Amerini, R. Caldelli, P. Crescenzi, A. Del Mastio, A. Marino, Blind image clustering based on the normalized cuts criterion for camera identification, Signal Process. Image Commun. 29 (8) (2014) 831–843.

[17] F. Gisolf, P. Barens, E. Snel, A. Malgoezar, M. Vos, A. Mieremet, Z. Geradts, Common source identification of images in large databases, Forensic Sci. Int. 244 (2014) 222–230.

[18] O.M. Al-Qershi, B.E. Khoo, Passive detection of copy-move forgery in digital images: state-of-the-art, Forensic Sci. Int. 231 (1) (2013) 284–295.

[19] T. Bianchi, A. Piva, Image forgery localization via block-grained analysis of JPEG artifacts, IEEE Trans. Inf. Forensics Secur. 7 (3) (2012) 1003–1017.

[20] X. Pan, S. Lyu, Region duplication detection using image feature matching, IEEE Trans. Inf. Forensics Secur. 5 (4) (2010) 857–867.

[21] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, G. Serra, A SIFT-based forensic method for copy–move attack detection and transformation recovery, IEEE Trans. Inf. Forensics Secur. 6 (3) (2011) 1099–1110.

[22] I. Amerini, R. Caldelli, A. Del Bimbo, A. Di Fuccia, L. Saravo, A.P. Rizzo, Copy-move forgery detection from printed images, in: Proc. SPIE Electronic Imaging, 90280Y, 2014.

[23] S. James, P. Kish, P. Sutton, Principles of Bloodstain Pattern Analysis: Theory and Practice (Practical Aspects of Criminal & Forensic Investigations), CRC Press, Boca Raton, FL, 2005.

[24] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, L. Del Tongo, G. Serra, Copy-move forgery detection and localization by means of robust clustering with J-linkage, Signal Process. Image Commun. 28 (6) (2013) 659–669.

[25] D.G. Lowe, Distinctive image features from scale-invariant keypoints, Int. J. Comput. Vis. 60 (2) (2004) 91–110.

[26] R. Toldo, A. Fusiello, Robust multiple structures estimation with J-linkage, in: Proc. of ECCV, 2008.