B2 Forgery Detection From Printed Images: A Tool in Crime Scene Analysis

Luigi Saravo, PhD, Dalmonte Street, Rome 00123, ITALY; Irene Amerini, PhD, Viale Morgagni 65, Firenze 50134, ITALY; Roberto Caldelli, PhD; Alberto Del Bimbo, Viale Morgagni 65, Florence 50134, ITALY; Andrea Di Fuccia, Via Tor Di Quinto 121, Rome 00121, ITALY; and Annapaola Rizzo, MD, Via Battistini, Rome 00100, ITALY*

After attending this presentation, attendees will understand the risk of image manipulation and the tools for forgery detection.

This presentation will impact the forensic science community by focusing on the importance of forensic tools in image authenticity.

The preliminary analysis of the genuineness of a photo is the first step of any forensic examination that involves images, in cases where there is not a certainty of its intrinsic authenticity.

Digital cameras have largely replaced film-based devices. Until recently, in some countries, only images made from film negatives were considered fully reliable in court. There was widespread prejudicial thought regarding a digital image which, according to some people, could not ever be considered legal proof, because of its "inconsistent digital nature."

Great efforts have been made by the forensic science community in this field and now different approaches have been unveiled to discover and declare possible malicious frauds in order to establish whether an image is authentic or not or, at least, to assess a certain degree of probability of its "pureness."

In this day and age, it's an easy practice to manipulate digital images by using powerful photo-editing tools. In order to alter the original meaning of the image, copy-move forgery is the one of the most common ways of manipulating the contents. With this technique, a portion of the image is copied and pasted once or times elsewhere into the same image to hide something or change the real meaning of it.

Whenever a digital image (or a printed image) will be presented as evidence in a court, criteria should be followed to analyze the document with a forensic approach to determine if it contains traces of manipulation.

Image forensics literature offers several examples of detectors for such manipulation. Among them, the most recent and effective are those based on Zernike moments and those based on Scale Invariant Feature Transform (SIFT). In particular, the capability of SIFT to discover correspondences among similar visual contents allows the forensic analysis to detect even very accurate and realistic copy-move forgeries.

In some situations, however, instead of a digital document, only its analog version may be available. It is interesting to ask whether it is possible to identify tampering from a printed picture rather than its digital counterpart.

Scanned documents or recaptured printed documents by a digital camera are widely used in a number of different scenarios, from medical imaging and law enforcement to banking and daily consumer use.

In this presentation, the problem of identifying copy-move forgery from a printed picture is investigated. The copy-move manipulation is detected by proving the presence of copy-move patches in the scanned image by using the Copy-Move Forgery Detection (CMFD) method; previous methodology has been adapted in a version tailored for printed image case (e.g., choice of the minimum number of matched keypoints, size of the input image, etc.).

A real case of murder is presented where an image of a crime scene, submitted as printed documentary evidence, had been modified by the defense advisors to reject the theory of accusation given by the prosecutor.

The goal of this presentation is to experimentally investigate the requirement set under which reliable copy-move forgery detection is possible on printed images in such a way that the forgery test is the very first step of an appropriate operational checklist manual.

Forgery Detection, Copy-Move Tampering, Crime Scene Investigation

 ** Presenting Author*