B7 Establishing Criteria for the Authentication of Digital Imagery

Scott Anderson, MS, 2268 Marginella Dr, Reston, VA 20191; Catalin Grigoras, PhD, 1020 15th St, Ste 8I, Denver, CO 80202; and Jeffrey M. Smith, MS, 2857 S Steele St, Denver, CO 80210*

After attending this presentation, attendees will understand an analytical approach to determine if a digital image contains traces of manipulation, combining different manipulation-detecting techniques relevant to image authentication. The cognitive outline will help attendees evaluate their findings when making decisions concerning the authenticity of digital image files.

This presentation will impact the forensic science community by strengthening the criteria needed for authenticating digital images.

Digital photography has replaced film-based photography as the prominent means of acquiring images. The ability to create digital images has been integrated into cameras, cell phones, scanners, and other devices. Due to the widespread availability of image processing tools, it has become increasingly simple to modify digital image content with no perceivable indications of alteration to the naked human eye alone. When digital images are central in an investigation or produced as evidence, it may be important to verify the image files' authenticity and/or integrity. Opening, processing, and resaving a photo utilizing image processing software will create modifications in an image file. In addition, applying anti-forensic techniques to obfuscate manipulation leaves detectable traces. While there exists a wide range of manipulation detection techniques, the simple fact is that an individual with the proper tools, knowledge, and skill can create forgeries that can elude detection by any one of these techniques. However, while certain manipulation techniques can elude one or more analyses, it is difficult to elude them all.

This presentation proposes a robust authentication framework that incorporates strong manipulation detecting techniques, collectively focusing on as many unique aspects of the digital image file as possible to diminish the possibility that traces of manipulation go undetected by image analysts. Analyses of the digital file concentrate on the binary data that comprises the information about the file container, including the file format, HEX data, EXIF, MAC stamps, and file marker analysis to help uncover clear signs and traces of a digital image file's history. Global image analysis techniques examine the information that represents the overall configuration of the image content where modifications can alter the random distribution of pixel values in original images and introduce mathematical relationships not found in original, undoctored images. When analyzing the global structure, techniques focus on compression schemes, interpolation, the color filter array, RGB color distributions, quantization tables, error level analysis, and DCT coefficients. Techniques that examine the statistical relationships that exist between neighboring pixels, such as copy and paste detection, photo-response non-uniformity comparisons, correlation or probability maps, histogram equalization, and JPEG error level analysis, are included in the analysis of the local image structure. Additionally, source image identification exploits small imperfections in the image sensor, such as its Photo-Response Non-Uniformity, where pixel defects are imprinted onto the output image file consistently occurring from one image taken by the camera to the next. These irregularities can be used to determine if the image in question could have come from a specific acquisition device.

By combining techniques that examine visual image inconsistencies with different areas of a digital image structure, the probability that manipulations in a digital image will go undetected are greatly reduced. To assure quality in image authentication examinations, cross-verifying conclusive findings using a minimum of two different methods is recommended. Furthermore, when employing automated algorithms, it is necessary to verify their performance on realistic databases and image manipulation techniques before applying them in real cases. It is important to note that these techniques can only provide positive proof of image tampering. It is extremely difficult, or even impossible, to prove that an image is free of modification; the best that an analyst can do when authenticating digital images is to search for indications that support the hypothesis that the image was generated without modification. In addition to inconclusive findings, the conclusions an expert can reach shall be that the evidence is either consistent or inconsistent with an original image.

Media Forensics, Image Authentication, Media Authentication

 ** Presenting Author*