



Finding the truth behind photographs

Nasir Memon

New digital forensic techniques provide source, integrity, and authenticity verification for photographic images.

In the analog world, photographic images have generally been accepted as ‘proof of occurrence’ of the depicted events. But today, the creation and manipulation of images is made simple by digital processing tools that are widely available and easily obtained. As a result, we can no longer take the authenticity of any images, analog or digital, for granted.

This is especially true when they are used as photographic evidence by law enforcement agencies. In this context, the field of image forensics is concerned with uncovering underlying facts about an image: by using its techniques, we attempt to provide authoritative answers to several questions about the content and source of an image. Is this an ‘original’, or was it created by cut and paste operations from different images? Was it captured by a camera manufactured by vendor X or vendor Y? Did it originate from camera X as claimed? At time Y? At location Z? Does this image truly represent the original scene or was it digitally altered to deceive the viewer: is this coffee stain a re-colored blood stain?

These are just a few of the questions faced routinely by investigators and others in law enforcement. However, existing techniques are often insufficient to provide authoritative answers. Although digital watermarks have been proposed as a tool to verify the authenticity of images, the overwhelming majority of images captured today do not have one. This situation is likely to continue for the foreseeable future, so in the absence of their widespread adoption, we believe it is imperative to develop techniques that can generate definitive statements about the origin, veracity, and nature of digital images.

The past few years have seen a growth of research in this area. Work in the field has focused mainly on solving two types of problems: image source verification and tamper detection. The aim of the former is to determine through what means a given image was generated (e.g., digital-camera, computer graphics, scanner, etc.) and associate it with a class of sources that have

common characteristics, or match it to a specific source. Meanwhile, the goal of tamper detection is to determine whether a given image has undergone any form of modification or processing since it was initially captured. Our research at the Information System and Internet Security (ISIS) laboratory at Polytechnic University, NY, has resulted in the development of many techniques that address these two types of problems. We briefly summarize this work here.

When the source of an image is identified as being a digital camera, the ability to identify its make and model requires an understanding of the image formation process. Although many of the details of the camera pipeline are considered proprietary information by manufacturers, the basic structure remains the same in all digital cameras.

In our initial approach to the problem, we identified a number of relevant features. These included energy in sub-spectral bands; higher-order statistics of sub-band coefficients, which can be used to demonstrate statistical inconsistencies between natural and unnatural images; image quality metrics; and inter-band correlations. Also, deviations from the ‘gray world’ assumption—which states that, in a natural image with a sufficient amount of color variation, the values of each of the basic color components of the image (red, green, and blue) should average to gray—were identified as possible indicators of alteration.

Based on these features, we used a classification-based technique to capture the characteristics of each camera examined.¹ This approach was also applied to cell phone camera images with reasonable success.² We further enhanced our results by detecting interpolation artifacts in smooth and non-smooth parts of the image. These were introduced using a color-filter array, which necessitates a de-mosaicing operation.³

Our approach to the detection of image-tampering stems from the idea that a digitally altered image would have undergone one or more image-processing operations (e.g., scaling, rotation, blurring/enhancement, brightness/contrast adjustments). For this purpose, we designed classifiers that can distinguish between images that both have and have not been processed us-

Continued on next page



ing these basic operations. To ensure that the classifier only responds to the aforementioned types of operation and that it will not be eclipsed by the image's content, we introduced features that are, under some assumptions, content independent. Experimental results demonstrate the ability to determine, with a high level of accuracy, if some part of an image has undergone a particular or a combination of processing methods.⁴

In order to identify images generated by a computer graphics program, we approached the problem from two directions. First, we enhanced a previous method that classifies based on the inherent statistics of natural (unaltered) images. The added features capture binary texture characteristics within the bit planes of an image. We based the second approach on the premise that 'synthetic' images should not exhibit the characteristics of those from a digital camera, as the methodology that governs generative algorithms is fundamentally different. Our results indicate that sensor noise can be used to differentiate between computer-generated and natural images.⁵

The need to determine the integrity and authenticity of digital images is ever increasing. At the present time, however, there is a severe lack of available techniques that can satisfactorily do this. The development and improvement of image forensic techniques is therefore of the utmost importance. Our research to date has shown promise in solving the problems of image source identification and tamper detection. However, satisfactory solutions are still far off, and will require the incorporation of many different approaches. We are currently expanding our research to better model the image-acquisition process and tampering operations.

Author Information

Nasir Memon

Computer and Information Science Department
Polytechnic University
Brooklyn, NY

References

1. M. Kharrazi, H. T. Sencar, and N. Memon, *Digital camera model identification*, **Proc. IEEE ICIP**, 2004.
2. O. Celiktutan, I. Avcibas, B. Sankur, and N. Memon, *Source cell -phone identification*, **Proc. ADCOM**, 2005.
3. S. Bayram, H. T. Sencar, and N. Memon, *Source camera-model identification based on CFA interpolation*, **Proc. IFIP WG 11.9 International Conference on Digital Forensics**.
4. I. Avcibas, S. Bayram, N. Memon, M. Ramkumar, and B. Sankur, *A classifier design for detecting image manipulation*, **Proc. IEEE ICIP**, 2004.
5. S. Dehnie, H. T. Sencar, and N. Memon, *Identification of computer generated and digital camera images for digital image forensics*, **submitted to IEEE ICIP**, 2006.