D73 Digital Image Forensics

Hany Farid, PhD, Dartmouth College, 6211 Sudikoff Lab, Hanover, NH 03755*

After attending this presentation, participants will learn about cutting edge techniques in digital image forensics and how they can be applied in real-world settings.

This presentation will impact the forensic science community by describing the new and important field of digital image forensics with implications to the Law, Media, Science, and Society.

Today's technology allows digital media to be altered and manipulated in ways that were impossible twenty years ago. The impact of this technology is being felt in nearly every corner of our lives, from the courts to the media, politics, business, and science. As this technology continues to evolve it will become increasingly more important for the science of digital forensics to keep pace. This presentation will describe state of the art techniques in digital image forensics.

Digital watermarking has been proposed as a means by which an image can be authenticated. This approach works by inserting at the time of recording an imperceptible digital code (a watermark) into the image. With the assumption that tampering will alter a watermark, an image can be authenticated by verifying that the extracted watermark is the same as that which was inserted. The major drawback of this approach is that a watermark must be inserted at precisely the time of recording, which limits this approach to specially equipped digital cameras.

In contrast, recent advances in digital forensics operate in the absence of any watermark or specialized hardware. With the assumption that tampering disturbs certain underlying statistical properties of an image, these forensic techniques can detect specific forms of tampering.

Air-brushing or re-touching can be detected by measuring deviations of the underlying color filter array correlations. Specifically, virtually all digital cameras record only a subset of all the pixels needed for a full-resolution color image. Instead, only a subset of the pixels are recorded by a color filter array (CFA) placed atop the digital sensor. The most frequently used CFA, the Bayer array, employs three color filters: red, green, and blue. Since only a single color sample is recorded at each pixel location, the other two color samples must be estimated from the neighboring samples in order to obtain a three-channel color image. The estimation of the missing color samples is referred to as CFA interpolation or demosaicking. In its simplest form, the missing pixels are filled in by spatially averaging the recorded values. Since the CFA is arranged in a periodic pattern, a periodic set of pixels will be precisely correlated to their neighbors according to the CFA interpolation algorithm. When an image is re-touched, it is likely that these correlations will be destroyed. As such, the presence or lack of these correlations can be used to authenticate an image, or expose it as a forgery.

A digital composite of two people can be detected by measuring differences in the direction to the illuminating light sources from their faces and body. By making some initial simplifying assumptions about the light and the surface being illuminated, we can mathematically express how much light a surface should receive as a function of its position relative to the light. A surface that is directly facing the light, for example, will be brighter than a surface that is turned away from the light. Once expressed in this form, standard techniques can be used to determine the direction to the light source for any object or person in an image. Any inconsistencies in lighting can then be used as evidence of tampering.

Duplication or cloning is a simple and powerful form of manipulation used to remove objects or people from an image. This form of tampering can be detected by first partitioning an image into small blocks. The blocks are then re-ordered so that they are placed a distance to each other that is proportional to the differences in their pixel colors. With identical and highly similar blocks neighboring each other in the re-ordered sequence, a region growing algorithm combines any significant number of neighboring blocks that are consistent with the cloning of an image region. Since it is statistically unlikely to find identical and spatially coherent regions in an image, their presence can then be used as evidence of tampering.

These and other image forensic techniques will be described. In addition, demonstrations of their use in exposing digital tampering will be provided.

Image Forensics, Image Tampering, Digital Forgeries

Copyright 2008 by the AAFS. Unless stated otherwise, noncommercial *photocopying* of editorial published in this periodical is permitted by AAFS. Permission to reprint, publish, or otherwise reproduce such material in any form other than photocopying must be obtained by AAFS. ** Presenting Author*