D77 Digital Video 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 video 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 video forensics with implications to the Law, Media, Science, and Society.

Popular websites such as YouTube have given rise to a proliferation of digital video. Combined with increasingly sophisticated users equipped with cell phones and digital cameras that can record video, the Internet is awash with digital video. When coupled with sophisticated video editing software, we have begun to see an increase in the number and quality of doctored video. This technology is impacting 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 video forensics.

Digital watermarking has been proposed as a means by which a video can be authenticated. This approach works by inserting at the time of recording an imperceptible digital code (a watermark) into the video. With the assumption that tampering will alter a watermark, a video 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 a video, these forensic techniques can detect specific forms of tampering.

The MPEG video compression scheme has emerged as a virtual standard. This lossy compression scheme introduces specific spatial and temporal correlations into a compressed video. When a video is edited and re-compressed, static and temporal artifacts are introduced that are distinct from an originally recorded MPEG video. These double compression artifacts can be used to determine that a video was, at a minimum, subject to some secondary processing after recording.

Most video cameras do not simultaneously record the even and odd scan lines of a single frame. Instead, one-half of the scan lines are recorded at time T, while the other half are recorded at time T+1. In an interlaced video, these scan lines are simply combined to create a full frame. While this approach allows for better temporal sampling, it introduces spatial “combing” artifacts for quickly moving objects. In order to minimize these artifacts, a de-interlaced video will combine the even and odd lines in a more sensible way, usually relying on some form of spatial and temporal interpolation. For de-interlaced video, the correlations introduced by the camera or software can be quantified, and deviations of these correlations can be used as evidence of tampering. For interlaced video, the motion between fields of a single frame and across fields of neighboring frames should be equal. Deviations of this motion are used to detect tampering.

Sophisticated video editing software allows for objects and people to be added to complex and dynamic scenes. The camera motion can be estimated from individual objects or people in a video and any inconsistencies in camera motion are evidence of tampering.

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

Video Forensics, Video Tampering, Video Forgeries

 ** Presenting Author*