W13 Forensic Multimedia Authentication: Real-Life Problems and Solutions

Zeno J. Geradts, PhD, Netherlands Forensic Institute, Den Haag, SH 2497 GB, NETHERLANDS; Catalin Grigoras, PhD*, National Center for Media Forensics, Colorado University Denver, Denver, CO 80204; Leonid I. Rudin, PhD*, Cognitech, Pasadena, CA 91117; Cole Whitecotton, MSc*, National Center for Media Forensics, Colorado University Denver, Denver, CO 80204; Gregory S. Wales, MS*, National Center for Media Forensics, Colorado University Denver, Denver, CO 80204*

Learning Overview: After attending this workshop, attendees will: (1) be familiar with the latest developments in forensic video and audio authentication and enhancement and restoration; (2) understand criteria used for media authentication; (3) understand how to conduct analysis within a forensic framework; and (4) explore the latest technologies in the generation of synthetic imagery, including deepfakes, face2face, and others.

Impact on the Forensic Science Community: This workshop will impact the forensic science community by: (1) explaining the scientific approach in forensic media authentication, enhancement, and restoration; (2) demonstrating an authentication investigation framework; and (3) discussing tools used to create and combat multimedia forgery.

Digital Multimedia Authentication seeks to determine the validity of digital multimedia containers and contents by investigating their format, structure, time, frequency, pixel and/or sample level features. This workshop will discuss the multimedia authentication process providing the user with methods of authenticating both video and audio, including deepfakes and deepvoices, and audio compression history assessment. It will also demonstrate the incorporation of multiple tools and techniques into unified frameworks appropriate in forensic examinations where reducing examiner bias and error is crucial.

The goal of this workshop is to provide an overall view of conducting comprehensive examinations that rely on the results of multiple analyses to inform an ultimate finding or opinion. First covered is a video authentication framework, focusing on camera verification/identification and image and video attack detection. This includes a quick overview of a digital video file creation chain for contextual information of the artifacts that influence the final digital media streams based upon the general description of camera sensor noises for both complementary metal-oxide-semiconductor and charge couple device type sensors. Photo Response Non Uniformity (PRNU) are small artifacts of the sensor and can be used as a sort of fingerprint for the sensor. For video and images, it can be determined with a high likelihood that a certain image or video has been made with a specific camera. PRNU can also be used for detecting deepfakes. Splicing, copy-move, and removal artifacts are also investigated in a complex video authentication process and will be discussed and exemplified with original and manipulated videos.

The 3D scanned models of vehicles can be misused to make geometrically accurate fake video implicating false suspect(s). But it also can be used to photogrammetrically authenticate a make and model of the vehicle captured in the Closed-Circuit Television (CCTV) recording. This workshop will present a novel computational method for video-based Forensic (i.e., with mathematically accurate error estimates) vehicle Make/Model Authentication (FMMA) through Height-Preserving Constraints (FMMA-HPC). Given a sufficient number of identifiable vehicle features-set, and a required 3D vehicle scan, the FMMA-HPC yields an accurate authentication/disparity error measure between the observed image of an unknown vehicle and the conjectured vehicle make and model, as presented in the 3D scan model. This workshop will demonstrate the application of FMMA-HPC technique on several examples. One of the examples comes from expert-witness forensic photogrammetry testimony utilizing an earlier Height Preserving Projection (HPP) method, which photogrammetrically concluded a "Features-Insufficient or 3D Inconsistent video data, for a positive vehicle Make/Model Authentication vs. Merritt Truck 3D Model," from the evidentiary CCTV video, during the 2019 Charles Merritt death penalty trial in San Bernardino, CA. This scientific public data should be peer-review studied and scrutinized by the forensic science community, using similar and alternative computational methods, given its enormous social implications.

In the second section of the workshop, real-life audio challenges and solutions will be presented. The proposed audio authentication framework combines both container and content analysis to determine authenticity of the recording as well as the purported source. Audio container analysis will exploit characteristics of the multimedia file format and structure while content analysis will cover time and frequency domain techniques, including quantization level, power, direct current offset, butt splice, spectral, Modified Discrete Cosine Transform (MDCT) map, MDCT frame offset analysis, and microphone attribution.

Forensic Multimedia Authentication, Deepfake, Deepvoice