D75 Blind Verification of Image and Video Authentication Examinations

Richard W. Vorder Bruegge, PhD, Federal Bureau of Investigation, Operational Technology Division –Forensic Audio, Video and Image Analysis Unit, Building 27958A, Pod E, Quantico, VA 22135*

After attending this presentation, attendees will learn how image analysts authenticate images and videos as depicting real people and events. They will also learn of multiple instances in which subsequent investigation verified conclusions reached by FBI examiners.

This presentation will impact the forensic science community by documenting instances in which the results of image and video authentication examinations have been verified after the fact, thus meeting the *Daubert* criterion that this technique be tested.

Blind verification is recognized by the forensic science community as an excellent way to demonstrate that examiners and laboratories – as well as specific forensic techniques and processes – produce results that are accurate and reliable. Blind verification is particularly relevant to many image and video authentication examination requests handled by the FBI's Forensic Audio, Video and Image Analysis Unit (FAVIAU). FBI personnel have been conducting authentication examinations of images for decades.

This paper will describe how the results of multiple FAVIAU image and video authentication examinations have been confirmed through investigative work performed after the examinations were completed. Included among these confirmations are: (1) authentication of a beheading video as real (confirmed through the subsequent recovery of the victim's headless torso and head), (2) identification of a "snuff film" as a forgery (confirmed by disclosure of the forgery by the creator as a demonstration of his ability in the realm of special effects), and (3) authentication of multiple child pornography images and videos as being real (confirmed by the subsequent identification of previously unidentified victims depicted as real children). It is proposed that such confirmations effectively constitute "blind verification," thereby demonstrating the validity of not just the individual examinations, but the validity of the techniques and processes used in these examinations, as well. Furthermore, such a demonstration provides a direct way of addressing the *Daubert* criterion regarding whether a technique has been tested or is capable of being tested.

The Scientific Working Group on Imaging Technology (SWGIT) describes forensic image authentication as "…the application of image science and domain expertise to discern if a questioned image or video is an accurate representation of the original data by some defined criteria….Questions involved…include issues of image manipulation, image creation, and consistency with prior knowledge about the circumstances depicted."[1] This type of authentication differs from the necessity to authenticate evidence as a precondition to acceptance in court (e.g., testimony from a fact-witness that a photograph is a "…true and accurate depiction of the scene at the time the photograph was taken…"). Likewise, image and video "authenticity" should not be confused with image and video "integrity," which specifically addresses whether an image or video recording has been altered or modified from its original state, regardless of whether such alteration changes the intrinsic meaning of the recording.

The question raised in forensic image authentication exams effectively comes down to "Did the events depicted occur as they appear in the picture or pictures?" Currently, FAVIAU is most frequently asked to perform image authentication examinations in cases involving child pornography. In such instances, the defense may claim that the images or videos charged in the case do not, in fact, depict real people and events. This may include the suggestion that the images or videos are computer- generated (CG) or that images have been manipulated in some way to make it appear that children were engaged in sexually explicit behavior, when they actually were not. For example, it might be suggested that the face and/or body of a minor was inserted to replace that of an adult in a sexually explicit scene that originally involved only adults.

Another type of case in which image authentication exams are requested involves purported executions or murders depicted in videos. While execution videos have become something of a staple on the Internet as a propaganda tool of terrorists, there remains a subset of videos known as "snuff films" that have nothing to do with terrorism, per se. In either case, investigators are anxious to determine whether a real crime is depicted in the video, or whether the video is merely an attempt at misdirection or some other purpose.

The process by which such images and videos are examined to determine authenticity can involve multiple tasks. As SWGIT notes, "…[t]hese tasks include…evaluation of image structure and content."[2] Evaluation of image structure may include observation of detailed characteristics of an image to detect artifacts of manipulation, or it may involve analysis of metadata to determine the source or provenance of an image, such as camera make and model, or date and time information. Content evaluation may involve observation to detect manipulation in continuity, or specific characteristics of the content, such as staging or features that are out of place or time. For example, when conducting an examination to determine whether a human being depicted in an image or video is real and not CG, there are specific characteristics of human beings that are known to be difficult to recreate in a CG depictions. Such features include fine details of the skin, eyes, and hair.

This paper will describe some of the specialized software tools used to assist in the detailed examination of the images and videos, including those used to examine the metadata and structure of individual digital files. Finally, the criteria used to establish authenticity will also be discussed. References:

 ** Presenting Author*

[1] SWGIT, “Best Practices for Image Authentication”, available on line at theiai.org/guidelines/swgit/guidelines/section_14_v1-0.pdf.

[2] Ibid.

Image Authentication, Image Manipulation, Blind Verification

