D72 The Detection and Authentication of Real Digital Photographic Images in Light of Ashcroft, Attorney General, et al. vs. Free Speech Coalition

Michael J. Salyards, PhD, DC3/DCFL, 911 Elkridge Landing Road, Linthicum, MD 21090*

The goals of this presentation are to (1) report current state-of-the-art in Computer Graphics (CG) technology, (2) report current legal precedence including Ashcroft v. Free Speech Coalition and subsequent cases, (3) provide an explanation of the JPEG image structure, (4) describe artifacts found in real (i.e., non-CG) digital images, and (5) describe artifacts found in CG digital images

In ASHCROFT, ATTORNEY GENERAL, et al. v. FREE SPEECH COALITION (April 16, 2002) the Supreme Court of the United States decided to overturn parts of the Child Pornography Prevention Act (CPPA) of 1996. Specifically the Court ruled that in order to prosecute child pornography cases, the Government must prove that a real child was harmed. This presentation will impact the forensic science community by demonstrating how since this decision, this "virtual child pornography" defense has been frequently used by accused parties, and has been a challenge to address.

The Department of Defense Computer Forensic Laboratory (DCFL) Image Authentication Process (IAP) has shown that real (non computer generated) digital photographic images contain numerous detectable artifacts.

In ASHCROFT, ATTORNEY GENERAL, et al. v. FREE SPEECH COALITION (April 16, 2002) the Supreme Court of the United States decided to overturn parts of the Child Pornography Prevention Act (CPPA) of 1996. Specifically the Court ruled that in order to prosecute child pornography cases, the Government must prove that a real child was harmed. Since this decision, this "virtual child pornography" defense has been frequently used by accused parties, and has been a challenge to address. Confounding the issue, many fact witnesses (investigators, support councilors, etc) who are currently able to testify to victim identity are aging and in some cases passing away.

The Department of Defense Computer Forensic Laboratory (DCFL) Image Authentication Process (IAP) has shown that real (non computer generated) digital photographic images contain numerous detectable artifacts.

The process consists of four major steps. First, a unique mathematical "fingerprint" of the image called the message digest version 5 (MD5) value is calculated and compared against values stored in the National Center for Missing and Exploited Children (NCMEC) database. Each picture in the NCMEC database contains an identified known child victim.

Second, the metadata contained in the image is extracted and analyzed for artifacts of origin. This includes both metadata that is statically available such as camera make and model as data in the image and metadata that is calculated from the properties of the picture file itself.

The third step in the process is to extract and analyze the image quantization table for artifacts of origin. Each JPEG image contains a quantization table that is generated during the second of three compression steps (discrete cosine transform, quantization, Huffman coding). This table varies from camera to camera and program to program.

During the fourth and final step a discriminatory examination of the Red, Green, and Blue (RGB) values for each pixel is mapped and incorporated into a number of mathematical equations. These equations compare each pixel to its neighbors in order to detect such things as flatness, lighting differential and human skin depth.

Data produced by the process shows that there is a significant, quantifiable difference between real and computer generated (CG) images.

Computer Graphics, Child Pornography, Image Authentication

 ** Presenting Author*