B19 New Methods for Linking Cameras on Social Media

Zeno J. Geradts, PhD, Netherlands Forensic Institute, Ministry of Justice, Laan van Ypenburg 6, Den Haag, SH 2497 GB, NETHERLANDS; Floris Gisolf, MSFS, Laan van Ypenburg 6, Den Haag 2497 GB, NETHERLANDS; Mark Vos, BS, Laan van Ypenburg 6, Den Haag 2497GB, NETHERLANDS; and Jonathan Stilkenboom, BS, Laan van Ypenburg 6, Den Haag, NETHERLANDS*

The goal of this presentation is to inform attendees about the possibilities and limitations of linking user profiles on social media to each other via images containing Photo Response Non-Uniformity (PRNU) patterns. An easy way to speed up the process of camera identification by using greyscale images will also be shown.

This presentation will impact the forensic science community by showing the effect that compression added to images by social media databases has on the ability to identify a common source of these images and by demonstrating a simple and effective way to decrease computation time by using grey scale images.

Many social media websites allow for the uploading of digital images. Sites like Facebook®, Flickr, Twitter, and Photobucket contain large numbers of images. Aside from their intended use, these sites are also used for illegal activities, such as spreading child pornography, scamming, fraud and terrorism. Generally these activities are done anonymously.

Using PRNU patterns images can be compared to each other to find out if they have a common source. Via this method a link can be established between an anonymous account used for illegal purposes and a normal user account on a social media website.

When an image is acquired with a digital camera light is captured with a camera sensor. Pixels on the sensor all have a slightly different sensitivity to light. This adds a systematic noise to an image which is approximately the same in each image taken with the same camera sensor. This noise is called the Photo Response Non-Uniformity and is caused by imperfections during the manufacturing process. By extracting and comparing the PRNU pattern from images it can be determined if they have a common source.

By comparing the PRNU pattern from images found on the social media page of a known user to the PRNU pattern from images found on the social media page of an anonymous user a link can be established. This can help identifying possible suspects.

Uploading an image to a social media website can severely reduce image quality by adding a layer of JPEG compression and resizing the image dimensions. During this presentation the possibilities and problems of determining a common source of images uploaded to these websites will be discussed.

Some sites add more compression than others. Furthermore, it is dependent on the settings used, image quality of the uploaded image before compression, and the camera. However, after such heavy compression it is often still possible to determine if images come from the same camera; even a comparison of two single images can still work.

Most images consist of three color layers: red, green and blue (RGB). Before extracting the PRNU pattern these layers have to be separated. This results in three layers with the same size as the original image. If the image was first converted to greyscale only one layer would have to be extracted, reducing calculation times and pattern size by a factor of three.

While this is not a new concept, as far as we know no data has been published to show the effects of converting to greyscale. During this presentation data of several RGB-to-greyscale ratios and their impact on camera identification will be discussed. It will be shown that using images converted to greyscale is at least as effective as using full color data.

PRNU, Social Media, Big Data

 ** Presenting Author*