B3 Linking Persons Based on PRNU on Social Network Sites

Zeno J. Geradts, PhD, Floris Gisolf, MSc, and Dennie Verhoeven, BSc, Netherlands Forensic Institute, Ministry of Justice, Laan van Ypenburg 6, Den Haag, 2497 GB, NETHERLANDS*

The goal of this presentation is to learn possibilities and limitations of camera identification based on Photo Response Non-Uniformity (PRNU).

This presentation will impact the forensic science community by offering new methods to link persons on spoofed identities as a result of the massive expansion of social network sites and data it leaves behind.

Social media websites such as Facebook®, Flickr®, and YouTube® contain large numbers of photo and video material.

Photos and videos from databases, such as a child pornography database, can be linked with these social media websites, in order to find a potential suspect. It is also possible to determine if a suspect camera took certain images when a suspect camera is available. The linking of photos and videos is done by making use of the PRNU pattern.

A digital (video) camera consists of many electronic components. After the image has been formed on the image sensor, the image information will pass through all of the components before the final data file is written to flash memory. Each step in this process may add random noise to the image. Even during the image formation process itself, a noise-like pattern from the sensor may be introduced in the image. This noise-like pattern is a small but measurable systematic contribution to the signal, and is called the PRNU pattern. It is caused by small variations of pixel sensitivity to light. The visibility of this signal is limited, and may be a small difference depending on the intensity of the signal. In practice, this means that well-illuminated images will result in a better extraction of this signal compared to when the image is dark. The PRNU pattern itself can be determined from the image and is preferably done with images that have no discernible textures (flat field image for example, from a grey surface). Research so far seems to indicate that every camera has its own unique PRNU pattern. The examining of the PRNU pattern for forensic use is well researched by Jessica Fridrich and others.

The best situation would be to have the suspect camera so flat field images can be made. In practice, it is not always possible to have the camera for casework, such as when linking images in databases to social media websites. However, it is possible to determine if a set of images has been made with the same camera or a different camera based on the PRNU pattern. When the camera is available, the pattern from a questioned image can be compared with the pattern from a set of reference images made with a suspect camera. It can be determined whether the questioned image was produced with the suspect camera or not. This works when the image is authentic, but fails when the image underwent any spatial transformations (e.g., rotation, shearing, resizing) because the “fingerprint” is desynchronized, unless the same transformations are applied to the reference material. It is also possible to alter the image such that the PRNU pattern is filtered out, although this is complicated and time consuming.

Linking large image or video databases requires significant processing power and time. For a good comparison, it is important to have untampered, original images, or to know exactly what kind of operations have been conducted on the image. Since in casework the ground truth is not known, conclusions are given in a Bayesian framework.

In this presentation, an overview will be given of methods that can be used for faster calculation by using only a part of an image, as well as solutions for when the camera is not working by changing the camera module. Also, the possibilities of examining images and videostreams from social networks such as YouTube® and Facebook® are discussed.

Camera Identification, PRNU, Social Networks

 ** Presenting Author*