

# Digital camera 'fingerprinting' developed

**Child pornographers will soon have a harder time escaping prosecution thanks to a stunning new technology in development at Binghamton University, State University of New York, that can reliably link digital images to the camera with which they were taken, in much the same way that tell-tale scratches are used by forensic examiners to link bullets to the gun that fired them.**

"The defense in these kind of cases would often be that the images were not taken by this person's camera or that the images are not of real children," said Jessica Fridrich, associate professor of electrical and computer engineering. "Sometimes child pornographers will even cut and paste an image of an adult's head on the image of a child to try to avoid prosecution.

"But if it can be shown that the original images were taken by the person's cell phone or camera, it becomes a much stronger case than if you just have a bunch of digital images that we all know are notoriously easy to manipulate."

Fridrich and two members of her Binghamton University research team – Jan Lukas and Miroslav Goljan – are coinventors of the new technique, which can also be used to detect forged images.

The three have applied for two patents related to their technique, which provides the most robust strategy for digital image forgery detection to date, even as it improves significantly on the accuracy of other approaches.

Fridrich's technique is rooted in the discovery by her research group of this simple fact: Every original digital picture is overlaid by a weak noise-like pattern of pixel-to-pixel non-uniformity.

Although these patterns are invisible to the human eye, the unique reference pattern or "fingerprint" of any camera can be electronically extracted by analyzing a number of images taken by a single camera.

That means that as long as examiners have either the camera that took the image or multiple images they know were taken by the same camera, an algorithm developed by Fridrich and her co-inventors to extract and define the camera's unique pattern of pixel-to-pixel non-uniformity can be used to provide important information about the origins and authenticity of a single image.

The limitation of the technique is that it requires either the camera or multiple images taken by the same camera, and isn't informative if only a single image is available for analysis.

Like actual fingerprints, the digital "noise" in original images is stochastic in nature – that is, it contains random variables – which are inevitably created during the manufacturing process of the camera and its sensors. This virtually ensures that the noise imposed on the digital images from any particular camera will be consistent from one image to the next, even while it is distinctly different.

In preliminary tests, Fridrich's lab analyzed 2,700 pictures taken by nine digital cameras and with 100 percent accuracy linked individual images with the camera that took them.

Fridrich, who specializes in all aspects of information hiding in digital imagery, including watermarking for authentication, tamper detection, self-embedding, robust watermarking, steganography and steganalysis, as well as forensic analysis of digital images, says it is the absence of the expected digital fingerprint in any portion of an image that provides the most conclusive evidence of image tampering.

In the near future, Fridrich's technique promises to find application in the analysis of scanned and video imagery. There it can be expected to make life more difficult for forgers, or any others whose criminal

pursuits rely on the misuse of digital images.

"We already know law enforcement wants to be able to use this," Fridrich said. "What we have right now is a research tool; it's a raw technology that we will continue to improve."

Source: Binghamton University

*This document is subject to copyright. Apart from any fair dealing for the purpose of private study, research, no part may be reproduced without the written permission. The content is provided for information purposes only.*