



## Adobe eyes fraud-busting tools for Photoshop

03 / 08 / 07 |

**In the near future, it could be a lot easier to see if those pictures of the person you've been talking to on Match.com have been retouched.**

Adobe Systems' Advanced Technology lab is working on plug-ins for Photoshop that would detect whether a photo has been tampered with, according to an Adobe representative. So far, the company has two plug-ins that are in a fairly advanced stage of development. Adobe is working with Dartmouth professor Hani Farid, an expert in photo fraud detection.

One tool from Adobe, called Clone Tool Detector, determines whether a section in a picture, such as a patch of sand or a field of grass, has been recopied from another part of the picture. Last year, Reuters admitted that a photographer cloned a smoke plume in a shot of wartime Beirut. The tool can't ascertain with absolute certainty whether two items, say a pair of clouds or other images, have been cloned, but it will say that the two images are "improbably similar."

The other tool, informally known in the lab as Truth Dots, determines whether pixels are missing from a photo, a sign that the image has been cropped. Even if the images were greatly magnified, the human eye could not detect these.

The representative said that Adobe has not made a final determination of whether or when to add these tools to Photoshop, but added that Adobe is very interested in photo authentication, which has become a hot topic with the proliferation of blogs, photo sharing Web sites and online news.



Adobe is currently beta testing a new version of Photoshop, called CS3, that will be announced at the end of March and is expected to ship later this spring. The company has become more aggressive in its development and marketing of Photoshop, seen by many as the standard professional photo-editing tool. New Photoshop variations, such as a free online version and an "extended edition" with advanced 3D tools, are planned.

Farid has worked with Adobe, the FBI and news agencies for several years on

detecting photo and image fraud. Informally, he also gets a constant stream of requests from people asking whether the picture of an item on eBay is real, or from people who want the picture of their potential date on dating sites to be verified. (He and the researchers at the Dartmouth Image Science Group have also worked with art museums to determine the authenticity of certain masterpieces.)

More recently, Farid has also begun to develop tools that could sniff out video and audio forgeries, a much more difficult task.

Probability plays a significant role in fraud detection. The software essentially looks for anomalies and discontinuities in pictures and flags them. An underlying understanding of the hardware and software used by photographers also helps.

Different cameras from the same manufacturer operate under different JPEG quantization tables, which determine the rate at which a camera will drop data in compressing a photograph. Farid's group has come up with software for examining the quantization tables across different cameras.

Adobe Photoshop, meanwhile, has its own distinct quantization table. As a result, the software can tell whether a photo has been run through Photoshop or came from a source other than that claimed.

"I can't tell you the serial number of the camera, but I can tell you this did not come from a Canon PowerShot. It came from a Nikon," he said in an interview last fall. "You can also tell if it came through Photoshop. It won't tell you what happened to the image, but it tells you it did not directly come out of the camera."

In an e-mail interview today, Farid did not comment on the exact nature of what Adobe might include in Photoshop but said it would likely be less powerful than the software he provides to law enforcement agencies.

"The primary reason for this is that some of our tools still require a fair amount of expertise to use," he wrote.

Making more authentication tools will likely help consumers sniff out fraud, but it could also help people interested in concocting fraudulent or doctored pictures. Child pornographers regularly exploit photo doctoring tools to develop composite pictures that allow them to get around criminal statutes. The 2004 presidential campaign also showed how doctored photos--remember the fake photo of John Kerry and Jane Fonda sitting next to each other--can influence a campaign.

"Educating fraudsters' is a real issue, but also an inevitable one in this type of game. I do believe that although we publish all of our results, the combination of techniques that we and others are developing will make it increasingly more difficult to create convincing forgeries," Farid wrote. "Whether we publish our results or not, the best

forgers will always be able to create forgeries that go undetected. The average person, however, will likely not be able to circumvent all of our techniques."

---

ZDNet | Copyright © 2006 CNET Networks, Inc. All Rights Reserved

