Investigating Digital Images; What's real and what's phony?

July 1 2004

"Seeing is no longer believing. Actually, what you see is largely irrelevant," says Dartmouth Professor Hany Farid. He is referring to the digital images that appear everywhere: in newspapers, on Web sites, in advertising, and in business materials, for example. Farid and Dartmouth graduate student Alin Popescu have **developed a mathematical technique to tell the difference between a "real" image and one that's been fiddled with**.

Consider a photo of two competing CEOs talking over a document labeled "confidential - merger," or a photo of Saddam Hussein shaking hands with Osama bin Laden. The Dartmouth algorithm, presented recently at the 6th International Workshop on Information Hiding, in Toronto, Canada, can determine if someone has manipulated the photos, like blending two photos into one, or adding or taking away objects or people in an image.

"Commercially available software makes it easy to alter digital photos," says Farid, an Associate Professor of Computer Science. "Sometimes this seemingly harmless talent is used to influence public opinion and trust, especially when altered photos are used in news reports."

Photos have been altered in the past, from airbrushing in fashion magazines, to aliens in tabloid newspapers, to giant lizards in the movies, but computers make it easier for more and more people to manipulate images. Farid explains that "regular" photos are hard to change without special expertise in altering negatives or dark room privileges that would

allow someone to influence the printing process. However, once images have been digitized, translated into the computer language of ones and zeros, it's easier to manipulate them.

A digital image is a collection of pixels or dots, and each pixel contains numbers that correspond to a color or brightness value. When marrying two images to make one convincing composite, you have to alter pixels. They have to be stretched, shaded, twisted, and otherwise changed. The end result is, more often than not, a realistic, believable image.

"With today's technology, it's not easy to look at an image these days and decide if it's real or not," says Farid. "We look, however, at the underlying code of the image for clues of tampering."

Farid's algorithm looks for the evidence inevitably left behind after image tinkering. Statistical clues lurk in all digital images, and the ones that have been tampered with contain altered statistics.

"Natural digital photographs aren't random," he says. "In the same way that placing a monkey in front of a typewriter is unlikely to produce a play by Shakespeare, a random set of pixels thrown on a page is unlikely to yield a natural image. It means that there are underlying statistics and regularities in naturally occurring images."

Farid and his students have built a statistical model that captures the mathematical regularities inherent in natural images. Because these statistics fundamentally change when images are altered, the model can be used to detect digital tampering.

"This technology to manipulate and change digital media is developing at an incredible rate," says Farid. "But our ability to contend with its ramifications is still in the Dark Ages. I'm always asked if this technology would stand up in a court of law." He explains that the simple

answer is, "eventually." Farid predicts there will be skepticism and a great deal of scientific and legal debate. But eventually, he believes that some form of his technology or someone else's will be incorporated into our legal system.

Farid, whose research is funded by an Alfred P. Sloan Fellowship, the National Science Foundation and the U.S. Department of Justice, also works with law enforcement officials, government representatives, and corporate leaders on this issue of authenticating digital images.

"There is little doubt that counter-measures will be developed to foil our detection schemes," says Farid. "Our hope, however, is that as more authentication tools are developed it will become increasingly more difficult to create convincing digital forgeries."

Soruce: Dartmouth College

Citation: Investigating Digital Images; What's real and what's phony? (2004, July 1) retrieved 26 April 2024 from https://phys.org/news/2004-07-digital-images-real-phony.html

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