

DIGITAL FORENSICS: HOW EXPERTS UNCOVER DOCTORED IMAGES

By Hany Farid

Modern software has made manipulation of photographs easier to carry out and harder to uncover than ever before, but the technology also enables new methods of detecting doctored images

History is riddled with the remnants of photographic tampering. Stalin, Mao, Hitler, Mussolini, Castro and Brezhnev each had photographs manipulated—from creating more heroic-looking poses to erasing enemies or bottles of beer. In Stalin's day, such phony images required long hours of cumbersome work in a darkroom, but today anyone with a computer can readily produce fakes that can be very hard to detect.

Barely a month goes by without some newly uncovered fraudulent image making it into the news. In February, for instance, an award-winning photograph depicting a herd of endangered Tibetan antelope apparently undisturbed by a new high-speed train racing nearby was uncovered to be a fake. The photograph had appeared in hundreds of newspapers in China after the controversial train line was opened with much patriotic fanfare in mid-2006. A few people had noticed oddities immediately, such as how some of the antelope were pregnant, but there were no young, as should have been the case at the time of year the train began running. Doubts finally became public when the picture was featured in the Beijing subway this year and other flaws came to light, such as a join line where two images had been stitched together. The photographer, Liu Weiqing, and his newspaper editor resigned; Chinese government news agencies apologized for distributing the image and promised to delete all of Liu's photographs from their databases.

In that case, as with many of the most publicized instances of fraudulent images, the fakery was detected by alert people studying a copy of the image and seeing flaws of one kind or another. But there are many other cases when examining an image with the naked eye is not enough to demonstrate the presence of tampering, so more technical, computer-based methods—digital image forensics—must be brought to bear.

I am often asked to authenticate images for media outlets, law-enforcement agencies, the courts and private citizens. Each image to be analyzed brings unique challenges and requires different approaches. For example, I used a technique for detecting inconsistencies in lighting on an image that was thought to be a composite of two people. When presented with an image of a fish submitted to an online fishing competition, I looked for pixel artifacts that arise from resizing. Inconsistencies in an image related to its JPEG compression, a standard digital format, revealed tampering in a screen shot offered as evidence in a dispute over software rights.

As these examples show, because of the variety of images and forms of tampering, the forensic analysis of images benefits from having a wide choice of tools. Over the past five years my students, colleagues and I, along with a small but growing number of other researchers, have developed an assortment of ways to detect tampering in digital images. Our approach in creating each tool starts with understanding what statistical or geometric properties of an image are disturbed by a particular kind of tampering. Then we develop a mathematical algorithm to uncover those irregularities. The boxes on the coming pages describe five such forensic techniques.

The validity of an image can determine whether or not someone goes to prison and whether a claimed scientific discovery is a revolutionary advance or a craven deception that will leave a dark stain on the entire field. Fake images can sway elections, as is thought to have happened with the electoral defeat

DIGITAL FORENSICS: HOW EXPERTS UNCOVER DOCTORED IMAGES

By Hany Farid

of Senator Millard E. Tydings in 1950, after a doctored picture was released showing him talking with Earl Browder, the leader of the American Communist Party. Political ads in recent years have seen a startling number of doctored photographs, such as a faux newspaper clipping distributed on the Internet in early 2004 that purported to show John Kerry on stage with Jane Fonda at a 1970s Vietnam War protest. More than ever before, it is important to know when seeing can be believing.

Everywhere You Look

The issue of faked images crops up in a wide variety of contexts. Liu was far from the first news photographer to lose his job and have his work stricken from databases because of digital fakery. Lebanese freelancer Adnan Hajj produced striking photographs from Middle Eastern conflicts for the Reuters news agency for a decade, but in August 2006 Reuters released a picture of his that had obviously been doctored. It showed Beirut after being bombed by Israel, and some of the voluminous clouds of smoke were clearly added copies.

Brian Walski was fired by the Los Angeles Times in 2003 after a photograph of his from Iraq that had appeared on the newspaper's front page was revealed to be a composite of elements from two separate photographs combined for greater dramatic effect. A sharp-eyed staffer at another newspaper noticed duplicated people in the image while studying it to see if it showed friends who lived in Iraq. Doctored covers from newsmagazines Time (an altered mug shot of O. J. Simpson in 1994) and Newsweek (Martha Stewart's head on a slimmer woman's body in 2005) have similarly generated controversy and condemnation.

Scandals involving images have also rocked the scientific community. The infamous stem cell research paper published in the journal Science in 2005 by Woo Suk Hwang of Seoul National University and his colleagues reported on 11 stem cell colonies that the team claimed to have made. An independent inquiry into the case concluded that nine of those were fakes, involving doctored images of two authentic colonies. Mike Rossner estimates that when he was the managing editor of the Journal of Cell Biology, as many as a fifth of the accepted manuscripts contained a figure that had to be remade because of inappropriate image manipulation.

The authenticity of images can have myriad legal implications, including cases involving alleged child pornography. In 2002 the U.S. Supreme Court ruled that computer-generated images depicting a fictitious minor are constitutionally protected, overturning parts of a 1996 law that had extended federal laws against child pornography to include such images. In a trial in Wapakoneta, Ohio, in 2006, the defense argued that if the state could not prove that images seized from the defendant's computer were real, then he was within his rights in possessing the images. I testified on behalf of the prosecutor in that case, educating the jurors about the power and limits of modern-day image-processing technology and introducing results from an analysis of the images using techniques to discriminate computer-generated images from real photographs. The defense's argument that the images were not real was unsuccessful.

Yet several state and federal rulings have found that because computer-generated images are so sophisticated, juries should not be asked to determine which ones are real or virtual. At least one federal judge questioned the ability of even expert witnesses to make this determination. How then are we to ever trust digital photography when it is introduced as evidence in a court of law?

DIGITAL FORENSICS: HOW EXPERTS UNCOVER DOCTORED IMAGES

By Hany Farid

Arms

Race

The methods of spotting fake images discussed in the boxes have the potential to restore some level of trust in photographs. But there is little doubt that as we continue to develop software to expose photographic frauds, forgers will work on finding ways to fool each algorithm and will have at their disposal ever more sophisticated image manipulation software produced for legitimate purposes. And although some of the forensic tools may be not so tough to fool—for instance, it would be easy to write a program to restore the proper pixel correlations expected in a raw image—others will be much harder to circumvent and will be well beyond the average user. The techniques described in the first three boxes exploit complex and subtle lighting and geometric properties of the image formation process that are challenging to correct using standard photo-editing software.

As with the spam/antispam and virus/antivirus game, not to mention criminal activity in general, an arms race between the perpetrator and the forensic analyst is inevitable. The field of image forensics will, however, continue to make it harder and more time-consuming (but never impossible) to create a forgery that cannot be detected.

Although the field of digital image forensics is still relatively young, scientific publishers, news outlets and the courts have begun to embrace the use of forensics to authenticate digital media. I expect that as the field progresses over the next five to 10 years, the application of image forensics will become as routine as the application of physical forensic analysis. It is my hope that this new technology, along with sensible policies and laws, will help us deal with the challenges of this exciting—yet sometimes baffling—digital age.

This story was originally printed with the title "Digital Image Forensics"