INFORMATION TECHNOLOGY

Easy-to-Alter Digital Images Raise Fears of Tampering

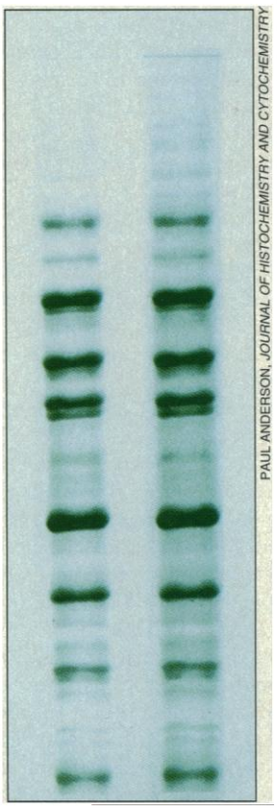
In 1982, *National Geographic* created a furor when, for purely aesthetic reasons, it moved the pyramid at Giza a little closer to some palm trees. The feat was quite simple: *Geographic* technicians digitized an image of the scene and "moved" the pyramid over a little. The result looked stunning on the cover of the magazine, but sharp-eyed readers quickly spotted the digital manipulation and protested the magazine's efforts to improve on reality. Nowadays, anybody with access to a desktop computer, cheap off-the-shelf software, and a little skill can perform a similar feat—and the chances are the manipulations won't be detected.

That's a worrying prospect to some scientists, journal editors, and even officials at federal agencies such as the Food and Drug Administration (FDA), which relies on scientific images in evaluating drugs for approval. Because digital imaging—computer photography—gives researchers the ability to edit scientific images without leaving a trace, "the opportunity for 'adjusting' the photographic representation to fit the hypothesis is very tempting," says Paul Anderson, a Mt. Sinai School of Medicine neuropathologist and editor of the *Journal of Histochemistry and Cytochemistry*. So far, the threat is entirely hypothetical; there have been no known cases of deceptively doctored digital images in the scientific literature. But Anderson and his colleagues think it's time to prepare for the digital era by developing policies to guard against digital image fraud and setting acceptable boundaries between "cleaning up" images and using the technology to deceive. As Steven Erde, director of academic computing at Cornell Medical School, points out, one researcher's noise is another's data. "Should we allow any image manipulation or cleanup? This is becoming a big topic, a real source of anxiety."

The issue of digital images was the focus of a session at a conference held at the National Institutes of Health last year on plagiarism and scientific misconduct, and it has come up since then in meetings of scientific editors, including those of the Council of Biology Editors. Among the safeguards under discussion is a requirement that researchers preserve an electronic history of an image, including all changes, or that papers alert readers to the technology that generated the image. But agreement about solutions—or about the severity of the threat—has been slower in coming.

The concerns are mounting as computer photography becomes ubiquitous in clinical and biological laboratories. Scientists use electronic cameras to record everything from microscopic images of tissue samples to cell counts and DNA bands on gels. The principal advantage of the cameras, which convert light to digital data with a high-resolution optical sensor known as a charged-coupled device, is that they deliver instant results. A researcher can view the final image on a monitor as soon as it is taken, to see if it shows what it is supposed to show. The images, stored on magnetic or optical disks, are also easy to analyze by computer, transmit, and incorporate into documents. They don't fade. And, for good or bad, they are easy to modify.

"I can now sit here with an image editor and manipulate results as easily as I can with a table of numbers," says Erde. A click of a computer mouse can create a gel electrophoresis band or, just as effortlessly, remove one. Likewise, a scientist can change the contrast in some parts of an image, but not in others, to make weak data look stronger, as has been done in the image above.



PAUL ANDERSON, JOURNAL OF HISTOCHEMISTRY AND CYTOCHEMISTRY

Digital liberties. Faint bands on an electrophoretic gel *(left)* can be emphasized without altering the darker bands *(right)*.

Scientists are divided on how much—if any—editing is acceptable in digital images. "Some say it's a departure from truth and that's wrong," says Anderson. "Others say, why not make it easier to read?" As Erde puts it, "Everybody crops and cleans up analog images [photographs] and nobody gets bent out of shape. Should you hold digital images to a higher standard?" But Anderson answers that with digital technology, unlike conventional photography, it's just as easy to fabricate or eliminate data as it is to crop and clean up an image. Most of those concerned about the issue aren't looking for an outright ban on electronic editing; they just want some record of what's been done.

So far scientific journals have received only a trickle of digital photographs (as opposed to computer-generated digital images of molecular structures, which are ubiquitous). As a result, only a few journals have set policies for handling digital photographs. *Nature* does not yet have such a policy, but its two spin-off journals, *Nature Genetics* and *Nature Structural Biology*, have both adopted the requirement that authors submitting a digital image list what software and hardware they used in the methodology section and in the caption. *Science* has discussed but not adopted a policy, according to managing editor Monica Bradford. *Cell* editor Benjamin Lewin declined to comment on his journal's policy.

Anderson's journal, too, "is still wrestling with the issue of digital images," he says. Meanwhile, as a member of the Council of Biology Editors and chairman of a committee on standards for scientific illustrations, he's pushing the council to issue general guidelines for editors. The proposed policy statement would stipulate that digital images are acceptable, but that scientists must maintain some archival record of how the graphic was obtained and what has been done to it. Such a record should be available for the inspection of journal editors, reviewers, or other scientists.

That proposed policy is similar to regulations adopted 2 years ago by the FDA to deal with other kinds of computer-generated data. Because FDA officials need to be able to audit scientific data as part of the drug and product approval process, the agency needed to ensure that changes to digital data would leave an indelible record. "In the old paper system, we had a whole audit force that would go out to the clinical investigator's site to certify that the data we have been given is the same as that on site," says Robert Bell, who runs FDA's computer-assisted new drug application program. But when computer-generated data from analytical instruments began pouring into the agency in the mid-1980s, officials realized that the audit trail was in danger of vanishing.

For example, chromatographs, which are images of peaks that indicate the presence of certain chemicals, have traditionally been generated on paper by a strip chart recorder. But over the last decade, drug company scientists switched to generating digital chromatographs in computers. "Before, FDA was confident in the strip chart recorder because there's no way to tamper with that," says Rohit Khanna, vice president and general manager for data products at Waters Chromatographics. "But now with computers, they're not so sure. How

Technology for Turning Seeing Into Believing

"Photo editors and journalists have been sounding the panic alarm for 10 years," says Gary Friedman of the advanced information systems division at the Jet Propulsion Laboratory in Pasadena. "You can't trust what you see any more. We all should be worried about the credibility of photographic images." Now, with the proliferation of digital cameras in clinical and biological laboratories, Friedman's concerns extend to science—to digital images in scientific papers or stored in electronic lab notebooks. While journal editors and officials contemplate guidelines to discourage digital fraud (see main text), Friedman and some of his colleagues are dreaming up technical fixes.

These researchers say that no feasible technology can discriminate between acceptable manipulation of a digital image—such as cropping or cleaning up—and falsification. Instead, investigators are developing systems that automatically store an audit trail. These technologies create a tamper-proof record of the original image, with which later versions can be compared if any questions arise about the data.

One such system is already available: Kodak's Digital Camera System. Snap a photo and, like any digital camera, it captures the image on light-sensitive semiconductors, which convert the light to a digital form. Special software then stores the data on a compact disc in what Kodak calls a proprietary image—a write-once-read-many-times format. Although the data can be copied from the camera system into a personal computer, then manipulated freely, the original archived data can't be altered by a casual user. "Let's say an editor wanted to check the original data," says Kodak's Philip Amato. "All [a scientist] has to do is supply the original compact disc with the camera archive on it and [the editor] could access the original image in its raw form."

Friedman has developed what he thinks is an even more sophisticated solution. Instead of storing the original image in a separate archive, his system appends to each image a digital "signature" of the original data. It does so by generating a pair of files: "One is the standard image file," says Friedman, which can be altered freely. To create the other, the system takes the image and first compresses it by what's called a one-way hash function, which turns the image into a unique number of about 160 bits. That number is then encrypted by a "public key" scheme. The private key, needed to encrypt the data, is built into the camera and then destroyed at the time of manufacture; the public key, needed to decode it, is printed in the frame of the image.

An editor or anyone else who wanted to authenticate the image, says Friedman, "would use public domain verification software, which takes three inputs: the digital image that's in question, the encoded digital signature of the original image, and the public key. First it takes the public key and decrypts the hash. Then it takes the image file in question and makes its own hash, and then it compares the two results. If they match, the picture hasn't been manipulated." If the hash values don't match, and the author can supply an image file that does pass this test, an editor can compare the two images to learn the extent of manipulation. The technology, says Friedman, is ready to be commercialized, and he says he has been approached by several companies interesting in licensing it.

For laboratories without an image-verifying camera, there's already a way to authenticate images or pages in an electronic lab notebook: digital time stamping. The scheme—the electronic equivalent of signing and notarizing a document—relies on the same algorithms that Friedman would like to put in a camera. To authenticate, say, a page of notes and images in an electronic notebook, explains Steve Kent, chief scientist for security technology at Bolt, Beranek, and Newman in Boston, a researcher would run the data through a hash function, then encrypt the resulting digital string.

The encoded number would then go to a timestamp notary service—something that already exists for authenticating other kinds of digital data (*Science*, 9 July 1993, p. 162). The timestamp notary takes the encoded hash value, adds a time and date stamp, signs the result and sends it back. The result is a unique, encoded string of digits representing the entire notebook page, its authenticity guaranteed by the notary's time stamp. Any suspicions about the integrity of the notes or images can be resolved by running the data through the hash function again and seeing if the result matches the time-stamped value.

None of that would help, of course, if the original image or notebook entry was faked. Observes Earl Boebert, chief scientist of the Secure Computing Corp. in Minneapolis, "There's no defense against fraud except the traditional scientific one of somebody duplicating the experiment." Still, he adds, "it's not necessary in the electronic world that one has to rely any more upon the honesty of the individual researcher than is the case already."

–Gary Taubes

do you validate your work?"

So FDA moved to set some standards, culminating in 1991 when it completed a set of guidelines called Good Automated Laboratory Practices (GALP). In the case of the chromatographs, for example, GALP requires laboratories to archive the original, unedited data display and a trail of any changes. GALP also includes guidelines for writing laboratory software that can preserve this kind of evidence. (Similar guidelines for international regulatory bodies have been developed by the International Standards Organization.)

FDA is considering similar requirements for the digital images now being submitted to the agency. And officials at other agencies are thinking along the same lines. At NIH's National Library of Medicine, for example, deputy director Michael Ackerman is responsible for several projects (including an ambitious "Visible Human" initiative) that are generating huge databases of computer photographs, radiographs, MRI scans, and other digital images. The proliferation and easy availability of such images, Ackerman worries, could open the door to extensive digital modifications. Medical researchers who want to illustrate a certain condition have traditionally had to search high and low until they found a perfect example to photograph. With digital images, Ackerman points out, they only have to "find one that's close and edit it to make it optimum."

As long as nobody's misled, he says, that's fine for educational purposes. But he also sees the need for a clear record of what's been done to an image, from editing to data compression. Without such a record, the image's scientific value becomes questionable. "What's redundant to one person is data to another," he says.

Guidelines and codes of conduct won't always keep the data stream pure, of course. So some researchers and digital imaging companies are exploring technical fixes—such as special cameras and electronic notaries—that create tamperproof records of the original image (see box). These safeguards, too, are only half-measures. As Ackerman puts it, "locks only keep honest people out." But as computers bring a brave new world of digital imagery—and its dangers—into the lab, scientists like Ackerman believe that even the barest of precautions are better than no precautions at all.

–Christopher Anderson