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