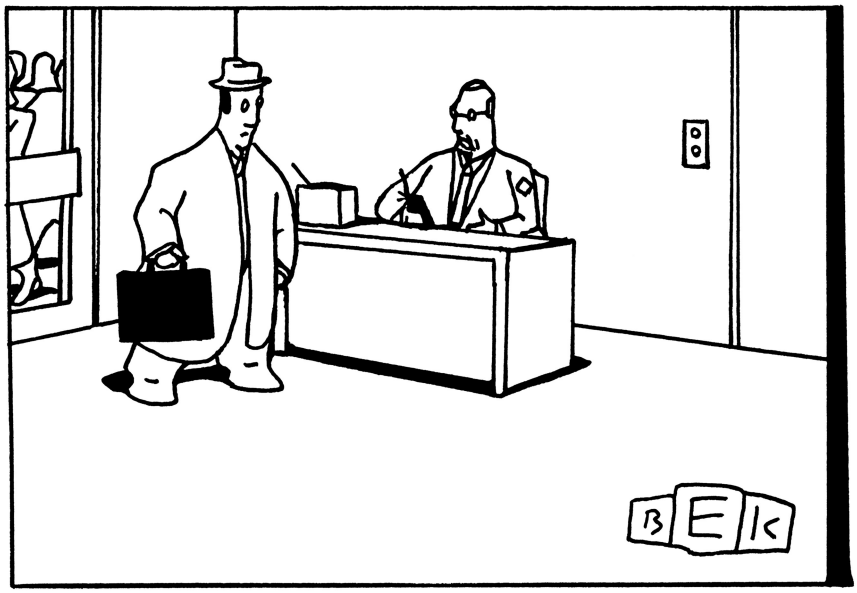
A false sense of security

Mike Rossner

Executive Director, The Rockefeller University Press

Some journals are using ineffective software to screen images for manipulation. In doing so, they are creating a false sense of security in the research community about the integrity of the image data they publish.



"I'm sorry, but we're going to have to act as if we have some kind of security system."

"There must be an easier way!" It's the mantra of anyone performing a labor-intensive task, and the motivation behind the human desire for automation. Apparently, it also holds true for image screening.

At the Rockefeller University Press, we screen all images in all accepted papers for evidence of manipulation (1). We do this by visually inspecting every image using basic adjustments in Photoshop. When editors from other publishers see a demonstration of our process, they often assert, "There must be an easier way!"

The possibility of automating the image screening process was described in a *Nature* news article more than two years ago (2). About a year ago, one of the largest publisher services providers, Cadmus Communications, started offering an automated image screening service using a program called Rigour, which they publicize as "the world's first automated Image Manipulation Analysis Software" (www.suprocktech.com).

Cadmus demonstrated an early version of this software at the Press, but we found that it could not detect blatant examples of band deletions, band intensity adjustments, large regions of duplication, or composite images. In an e-mail to Cadmus dated September 11, 2007, I expressed my concern, "I am worried about causing a setback in the publishing community if editors think the current Rigour software is effective at detecting problems in biomedical images (specifically gel images). I have already heard of editors saying they will not initiate visual screening because they will just use the Cadmus software. This is creating a false sense of security in the community, because the software is not yet an effective screening tool." I received no response to this e-mail.

I was surprised to learn that, within a couple of months, Cadmus had started to sell an image screening service to publishers using this software. But given the availability of such a service, I was not surprised to learn that editors at two very prominent journals were using it. Publishers were clearly looking for a less labor-intensive solution to an image problem, in two senses of the word—image data, and public image. They wanted to be seen by the public to be actively addressing the problem of image manipulation.

I asked these publishers if they had tested the service before they started to use it. Both had done so, but one of them declined to send the results of their tests; the other indicated that the Cadmus service had a 20% success rate. It seems that these publishers were not really concerned if the screening process they used actually worked.

Problems with the service were still evident recently when I was consulted by a third party about a case of image manipulation in a paper published in one of these journals. The paper made a surprising claim with important clinical implications. Given that journal's policy of only screening a fraction of papers for

The Rockefeller University Press $30.00
J. Cell Biol. Vol. 183 No. 4 573–574
www.jcb.org/cgi/doi/10.1083/jcb.200810172

image manipulation, one might expect that they would at least select those with important clinical implications. In fact, the papers are selected at random, and this one had not been screened. After questions were raised, the figures were screened by Cadmus using their software, but they did not detect problems with the images that were easily revealed with visual screening.

In personal communications, publishers have argued that using the Cadmus service must be better than doing nothing. In fact, it is worse than doing nothing. These publishers are creating a false sense of security in the community about the integrity of the image data they publish.

A recent test of the Cadmus image screening service showed some improvement, with the software detecting manipulation in 10 out of 22 images (45%) in which image manipulation had previously been detected by visual inspection. However, when multiplied by the small fraction of images being screened by these journals, the percentage of images that are effectively screened is dramatically lower. At the very least, these journals should fully disclose their screening practices (and their efficacy) to their readers.

Although complete protection against manipulated images cannot be guaranteed, it is incumbent on journal editors to screen the images they publish using the best available method, not just to some known (and low) percentage of efficacy. The issue of data integrity should not be left to chance and probability. This is scholarly publishing, not blackjack.

There are others developing software to detect image manipulation, and it is possible that these applications may eventually prove to be useful and effective tools for editors. But journal editors should not rely on an automated method for image screening unless they know it is as effective as the visual method. Otherwise, readers are left to hedge their bets.

Conflict of interest statement: The Rockefeller University has licensed the author's know-how for visual screening of images using adjustments in Photoshop. The author received a one-time share of the income from the license. Notwithstanding the license, the know-how is distributed freely, on request, to editors of all scientific journals, commercial or non-commercial.

References

1. Rossner, M. 2002. Figure manipulation: assessing what is acceptable. *J. Cell Biol.* 158:1151. DOI: 10.1083/jcb.200209084.

2. Pearson, H. 2006. Forensic software traces tweaks to images. *Nature*. 439:520–521. DOI: 10.1038/439520b.