

Security Stripes: Visible Seals for Robust Documentation and Authentication of Digital Images

Charles Bradley* and James Mancuso

Advanced Microscopy Techniques, 3 Electronics Ave., Danvers, MA 01923

* cbradley@amtimaging.com

Introduction

Digital images carry a great deal of information, but they should not stand alone. They need to be accompanied by experimental variables, equipment used, personnel involved, image-processing operations performed, and site information. It is essential to maintain a link between pixel data and experimental conditions associated with the picture.

Concern for the integrity of digital images presented in scientific studies has been growing in prominence [1, 2, 3, 4, 5]. Although manipulation of digital images is generally not malevolent, its relative ease exacerbates ethical and security issues that are less prevalent with film-based recording, where the common practice of pasting a print into a lab book and recording an exposure number creates a visible and permanent record. Permanence is important not only for maintaining organized, traceable, and intelligible records but also for supporting the authentication requirements of industry, medicine, and research funding.

We describe here the concept of a security stripe as a robust seal for recorded images. Like a product bar code, it is immediately visible and it contains information about the carrier. It can also authenticate the data collection process. The security stripe is compatible with all loss-less recording formats. So it can be widely adopted without compromising legacy files or obsolescing preexisting proprietary formats and the software that is dependent on those formats. In addition the security stripe can encode text in Unicode thereby permitting use of native character sets.

Current Image Recording Practices

A simple and common way of documenting an image is to create a companion file, which records instrument settings and experimental conditions. This can be in a notebook, although some instrument makers [6] create with each image a companion digital file containing this type of information. These digital files can be comprehensive, but they are vulnerable to being separated from the original or lost. Companion data can also be saved in a database, but this impedes information exchange as all collaborators and examiners of the image then need access to the database software and the database files. More importantly, neither companion files nor databases address validation as they are separate from their respective images.

Another approach to documentation is to include metadata containing the equivalent to a companion file within a proprietary image format [7]. Similar metadata can authenticate the image by the use of security keys or image self-consistency measures. The main drawback of proprietary formats is that they impede easy exchange of original data. When proprietary files are exported to a standard format, such as TIFF, the companion metadata and security metadata are often lost.

Standard format images can also embed experiment and authentication data within more standardized metadata structures such as TIFF tags (see Figure 1). Unfortunately, this approach is limited to a specific image file format. Even within a single protocol such as TIFF there can be serious problems in placing companion information into a tag. First, the TIFF standard requires reading programs to ignore tags that they do not use, which effectively strips them from the file when the image is re-saved. Second, most tags do not have a rigorous definition, and there is no provision for collisions where two applications interpret a given tag differently.

The weakness of this approach is illustrated when saving microscope companion data in the Image Description tag, one of Adobe's standard TIFF tags. The tag is defined in the Adobe TIFF 6 Standard as "A string that describes the subject of the image. . . . For example, a user may wish to attach a comment such as '1988 company picnic' to an image." [8] This is a very flexible specification, which can be, and has been, implemented differently by different programs. For example, ImageJ and Microsoft Paint write their version into this tag. The Open Microscopy Environment [9] has another recommended format for this tag for microscope data. However, in practice, it is used inconsistently by both camera suppliers and microscope vendors. Thus even loss-less saving in TIFF does not ensure preservation of companion data.

Authentication and Validation

Because concern for the integrity of digital images presented in scientific studies has been growing, government funding agencies and many journals are now adopting techniques from the rapidly emerging field of image forensics to detect image manipulation [10, 11, 12, 13, 14]. Several journals [3, 4, 5, 15]

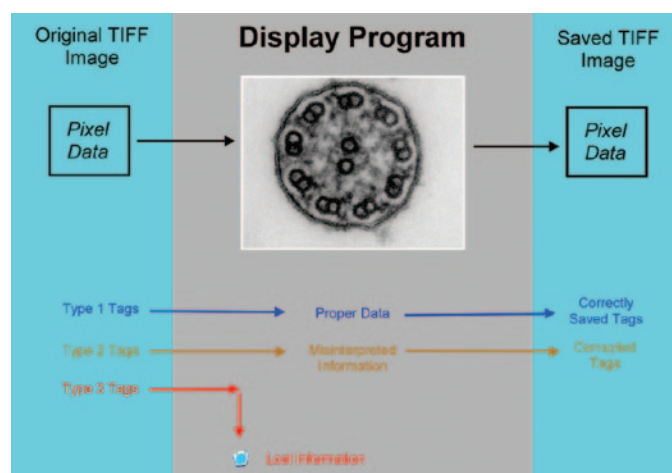


Figure 1: Possible fates of TIFF tags. Information stored in a tag in a TIFF header can be used properly or improperly, or it can be silently stripped from the file. Because tags are not visible, this silent stripping of image data may go unnoticed for long periods.

DiATOME

DIAMOND KNIVES

40 YEARS

OF DEVELOPMENT, MANUFACTURING, AND CUSTOMER SERVICE

What have we achieved in this period?

ultra 45° the first diamond knife with an absolutely score-free, hydrophilic cutting edge.

semi the first diamond knife for alternating sectioning ultrathin/semithin.

cryo the diamond knife for sectioning at low temperature.

histo the first diamond knife for semithin sections for light microscopy.

ultra 35° the diamond knife for optimized sectioning results in almost all applications.

STATIC LINE II the ionizer for eliminating electrostatic charging in ultramicrotomy.

cryo-P a cryo knife with a patented platform for section pick up.

cryo immuno the optimized cryo diamond knife for the Tokuyasu technique.

ultra sonic the oscillating diamond knife for room temperature sectioning.

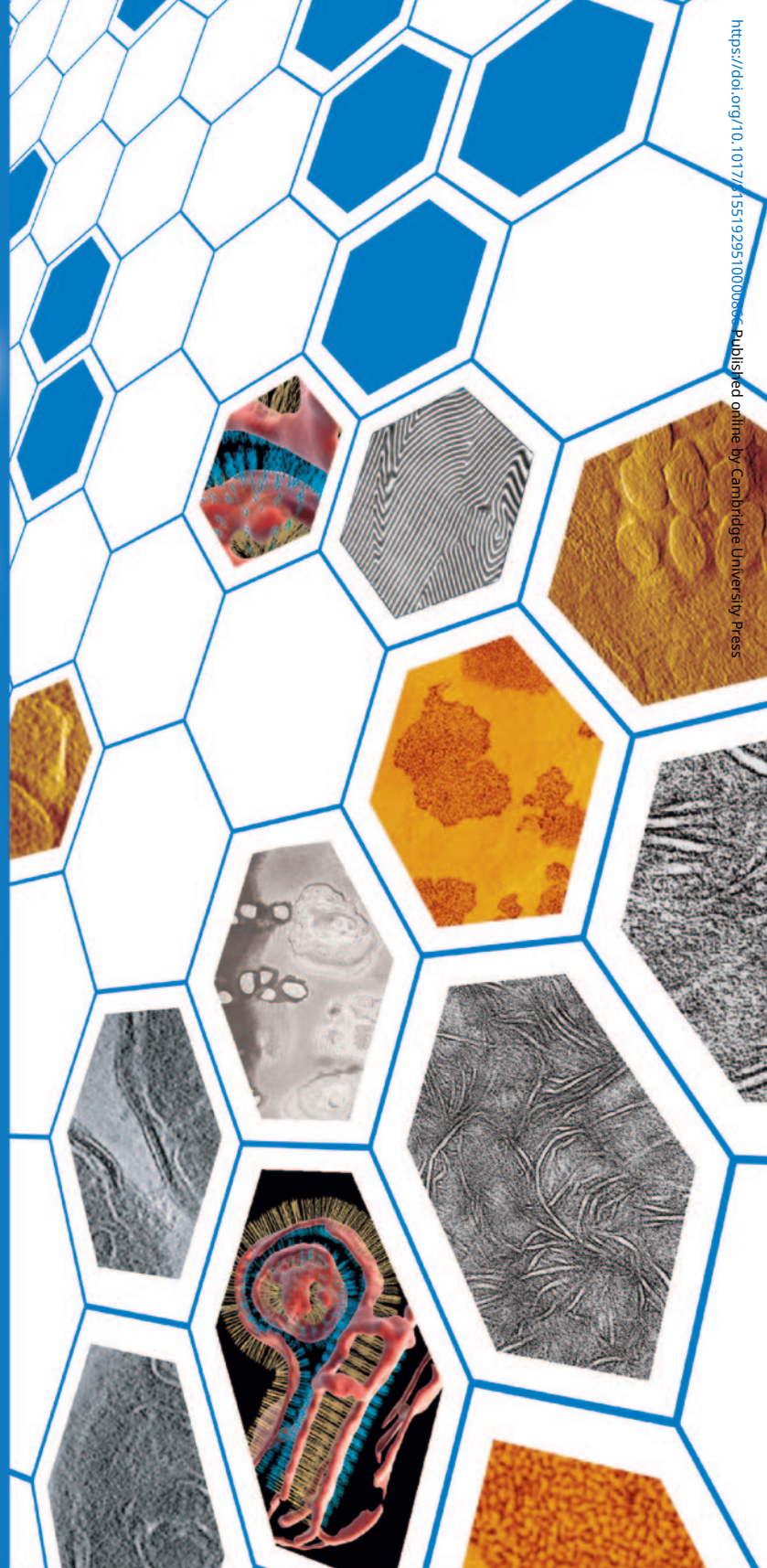
cryotrim 45 and 25 optimizing trimming with diamond blades.

ultra AFM & cryo AFM the first diamond knives for AFM at room and low temperatures.

cryo 25° for sectioning frozen hydrated specimens.

What services can we offer you?

- Technical assistance in all fields of ultramicrotomy.
- Free sectioning tests for all types of samples.
- Make use of our many years of experience in perfecting our knives.
- Custom knives, tools, and boats.
- Special purchase programs.
- Workshops and training.



DiATOME

for all your sectioning requirements

For more information, please call or write us today,
or visit us online at: www.emsdiasum.com

P.O. Box 550
1560 Industry Rd.
Hatfield, Pa 19440
Tel: (215) 412-8390
Fax: (215) 412-8450
email: sgkcck@aol.com
www.emsdiasum.com

note cases where images have been manipulated beyond what their editors considered ethical. For example, the *Journal of Cell Biology* recently reviewed papers accepted over a period of 42 months. Although only 1% of acceptances were revoked, 25% of submitted papers contained at least one image that had to be redone before publication because they conflicted with image presentation guidelines [4].

The need for standards is now obvious to the scientific community. In fact, U.S. government regulations such as CFR 11 Part 21 give image integrity preservation the force of law [16] for pharmaceutical research. However, as intimidating as the CFR regulations may be, they do not specify a protocol. In fact, such detailed specification may not be generally possible within the CFR.

Although there is general agreement that image file formats should be loss-less, most else is up for grabs. Today there is a vast legacy of proprietary protocols (numbering over 50) and file formats that must be reduced to a few. Standards have been proposed by the Open Microscopy Environment, which endorses an OMEXML format, and a TIFF format that includes the non-image data in the ImageDescription tag as an XML file. OME also provides a Bio-Formats function library that can be used to read and write most of the proprietary formats and translate these into the OME-XML format [17]. In addition, the Microscopy Society of America ethics committee supports TIFF6 as a recording standard [1]. Still, neither these nor any other standard or protocol has gained dominance. More importantly, most do not address authentication.

Security Stripe Goals

One possible solution to these difficulties is a security stripe that embeds image information into the image itself. The specific goals for developing the security stripe are:

- 1) Preservation of experimental conditions plus sample and authorship information.
- 2) Compatibility with native character sets.
- 3) Compatibility with standard imaging applications.
- 4) Flexibility to include new types of information without needing to revise the standard.
- 5) Authentication of both pixel data and the attached description of experimental conditions.
- 6) Extension to any loss-less image storage format, open or proprietary.
- 7) Preservation through image format conversion.

In achieving these goals the security stripe has become a visible addition to a digital image. It contains companion information, can authenticate the data collection process, and serves as a robust seal. It acts similarly to a product bar code, as it is immediately visible, while at the same time it encodes experimental information and authentication data. Because it contains data, the security stripe is similar to the invisible metadata often contained in headers of digital records. However, the stripe differs by being visible and not confined to a unique file format.

The stripe should not make obsolete progress made by standards organizations or manufacturers who have dealt with these issues using specific loss-less formats and databases. It should provide a mechanism for exchange of data that can be used in conjunction with all loss-less protocols.

Security Stripe Implementation

There are many ways one might design a security stripe, and although flexibility is valuable, some general guiding principles will make exchange of information much easier. We propose that the following features be included in building a security stripe to be used for microscopy.

- 1) The security stripe should use Unicode text data to encode the gray scales along a stripe corresponding to the width of the image. Unicode is a widely used format that permits standard encoding of native scripts.
- 2) The text data should include experimental conditions as well as security keys for image authentication and validation. The keys may be simple codes, can refer to image characteristics, be self-consistency checks, or a combination of these.
- 3) The stripe should be appended to the picture section of the original digital image file in the form of pixels. This will create a single file where the companion experimental conditions and authentication information are permanently and visibly attached to the pixel data.
- 4) The security stripe cannot be an overlay, as many lossless formats do not support overlays.
- 5) The security strip should appear as a caption or part of a caption to the image. A prototype is shown in Figure 2.

The security stripe shown in Figure 2 clearly meets its goals of compatibility. Current TIFF reading programs can

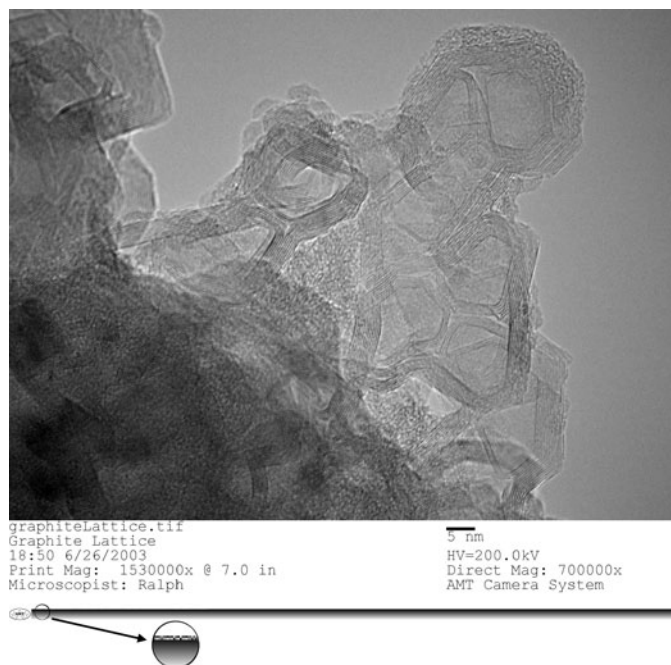


Figure 2: Encoded contextual information and security keys incorporated as part of an image. This is a prototype version of the Security Stripe, which is 40 lines high. Companion and authentication data are encoded into grayscale values in a reserved region of caption portion of a single image. In this example each pixel is given an 8-bit ASCII character value (in an 8-bit image). In this 2k wide image, the strip can incorporate 2,000 characters per line, so this data strip has a capacity of 80 kB. A Unicode version would typically require 4 pixels to represent a character. However this is more than enough space to record typical experimental conditions, sample information, facility, and authorship.

be used “as is” because the companion data field is simply another part of the picture. One need not be concerned about which subset of TIFF tags the program (or version) supports. The image can be converted to any other loss-less format. There is no need to carry and keep a track of companion files. Stripe removal is immediately apparent, because the strip is visible.

This approach does not preclude other protocols for incorporating information into a file. Manufacturers can continue to embed experimental information in the TIFF header; those who have proprietary (loss-less) file formats can continue to use them. Thus backward compatibility can be maintained and an incremental path toward a real standard is available. There is adequate space for additional comments and the recording of additional image processing operations—like a continuing lab book.

Note that there is a complication. It is necessary to obtain encoding and decoding programs to read, write, and validate the information contained in the stripe. Technically, this is a simple process. A stand-alone application can read or write the encoded information. Better implementations would employ plug-ins to provide this functionality within image display programs. The authors propose that this method be publicly available so that all suppliers of digital imaging equipment can freely implement the reading and writing of the Security Stripe. Example code will be made available by the authors at <http://www.amtimaging.com/sampleCode.html>.

Where to Go From Here

Digital imaging is virtually forcing scientific records to be paperless, but security and documentation become problems when protocols for data storage are not standardized. The security stripe concept takes its cue from the more traditional film-based approaches where magnification information is ‘burned’ into a plate and images are pasted into a notebook with companion data. Its essential purpose is to locate relevant image data in single place and do so in a fashion that inhibits modification after the fact.

We would like to encourage the Microscopy Society of America to define a standard format for recording that uses this type of visible seal containing experimental conditions and authentication data as one tool for data documentation. This approach to dealing with digital information is different from what has been done in the past, so it can serve as a fresh start, enabling the definition of a standard while at the same time avoiding issues that orphan proprietary formats would generate.

References

- [1] JM MacKenzie et al., *Microscopy Today* 14(1) (2006) 40.
- [2] U.S. Food and Drug Administration, “CFR 21 Part 11,” http://www.fda.gov/ora/compliance_ref/Part11/.
- [3] CSE’s *White Paper on Promoting Integrity in Scientific Journal Publications*, http://www.councilscienceeditors.org/editorial_policies/whitepaper/3-4_digital.cfm (Accessed Nov., 2009).
- [4] M Rossner, *The Scientist* 20(3) (2006) 24–25.
- [5] I Hames, *The Journal of the European Medical Writers Association* 17(4) (2008) 164–67.

- [6] Kevin McIlrath, Hitachi High Technologies America, Pleasanton, CA, personal communication.
- [7] TS Baker, <http://cryoem.ucsd.edu/microscopes/DM3.shtm> (accessed 2009).
- [8] Adobe Developers Association, Adobe Systems Incorporated, TIFF Revision 6.0 (1992), page 34, <http://partners.adobe.com/public/developer/en/tiff/TIFF6.pdf>.
- [9] J Swedlow, I Goldberg, K Eliceiri, and OME Consortium, *Annual Review of Biophysics* 28 (2009) 327–46.
- [10] H Farid, *IEEE Spectrum*, 46(8) (2009) 42–47.
- [11] H Farid, *IEEE Signal Proc Mag* 26(2) (2009) 16–25.
- [12] W Wong, *Digital Video Forensics*, Ph.D. thesis, Dartmouth College, June 2009.
- [13] M Richardson, *Am J Roentgenol* 164 (1995) 228–29.
- [14] I Avcibas, S Bayram, N Memon, B Sankur, and M Ramkumar, *Proc of IEEE ICIP* (2004) 2645–48.
- [15] SK Suvarna, MA Ansary, *Histopathology* 39 (2001) 441–46.
- [16] U.S. Food and Drug Administration, CFR – Code of Federal Regulations Title 21, <http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=11>.
- [17] The Open Microscopy Environment, <http://www.openmicroscopy.org/site>.


MT

PELCO®


Silicon Nitride Membranes

Next Generation
Si₃N₄ TEM Support Films

- Durable and inert planar 50 and 200nm substrates
- 3.0mm circular frame
- EasyGrip™ edges
- Free from debris
- Complimented with Holey Membranes and Silicon Dioxide Substrates



Holey
Si₃N₄
Membrane



Silicon
Dioxide
Membrane

TED PELLA, INC.
Microscopy Products for Science and Industry

sales@tedpella.com 800-237-3526 www.tedpella.com