Images as Evidence

A look at a British study examining the use of digital images in court

By Elliott Goldstein

Q Have there been any studies of the use of digital images as evidence?

A Yes. The Select Committee on Science and Technology of the House of Lords in England released a report in February 1998 entitled "Digital Images As Evidence."[1] The report examined some of the legal issues that go towards proving the accuracy of a digital image and assessing its weight.

The aforementioned committee also looked at some suggestions for establishing requirements for the use of images in court. And it made recommendations to the British government [2] that were later reflected in the *Data Protection Act* 1998.[3]

The report observed "there is no legislation which expressly covers digital images used as evidence, nor any reported cases in which the fact that an image was collected in digital form was at issue."[4] It also pointed out that the fundamental problem with digital images is the potential for image tampering.

How can the court be sure that an image has not been unfairly modified? What, if any, image "enhancement" is justified? The person or party tendering the digital images must provide the court with evidence about the following:

- the source of a digital image;
- its processing;
- any "enhancement" it has undergone; and
- its storage since it was first recorded.

This evidence will satisfy the chain of custody requirement and prove continuity of possession.

In Canada, the courts require that the "original" image accompany an "enhanced" image. This allows the court to compare the two and opposing counsel to object to the "enhanced" version if so instructed by his or her client.

The report also discusses the problem of establishing that a digital image is authentic. This problem arises for three reasons:

- the nature of digital processing of images;
- the potential for image modification; and
- the problem of defining what is an "original."

As a solution, the report suggests two methods of establishing authenticity: to have an "audit trail which records everything that happens to the image from its capture to its presentation in court; and to have a technological solution that 'watermarks'" the image at the time of its capture and can subsequently show that it is authentic.

Audit trail methodology is already in use with other forms of evidence (for example, accounting records and physical exhibits) in Canada and the United Kingdom. This methodology involves proving that the evidence has been treated fairly; that any processing (in a forensic or testing laboratory) it has undergone has been well documented; that its location is always known; and that all those who have had contact with the evidence have the necessary authorization. (In Canada, this is known as proving the chain of custody of the evidence.)

"Watermarks" can provide an extra level of security

"Watermarks" can provide an extra level of security to an image if they are added at source when the video surveillance camera captures the image. Watermarking, as the process is known, involves adding an identifying code or logo to the image data.

Usually, the watermark is hidden within the image data with a form of encryption. The watermark may be present in all parts of the original image (down to pixel scale). To the viewer, the image looks normal and the watermark can only be viewed with the appropriate decryption key. It is also possible to encrypt the entire image so that it cannot be seen without the appropriate equipment and decryption key.

The report distinguishes between the two types of watermarks. The permanent or "tattoo" watermark is hidden within the image and remains there no matter how many times the image is copied, altered, changed, modified or otherwise processed. This kind of watermark is very useful in copyright cases. It permits identification of the source of images that have undergone significant modification, alteration or copying.

The other kind of watermark is known as a "fragile" watermark. It is so called because any processing, modification or alteration of the digital image destroys it. However, simple viewing of the image does not destroy the fragile watermark.

Fragile watermarks have a significant potential for authenticating images used in evidence. For example, a digital image that should have a watermark but does not — or has a damaged or corrupted watermark — would probably not pass the test of authentication. That is, a witness could not verify under oath that the digital image is a true and accurate reproduction of the original scene if the watermark was missing or damaged.

The same would apply to a digital image recorded, without human intervention (for example, by an automatic surveillance camera), on a digital surveillance recorder. As most digital surveillance recorders "copy" the image onto a digital tape or other media, and then erase the original, the "copy" image should be identical to the original.

If the watermark indicates that it is not, then either the copying process was defective or the digital image (or file) has been tampered with. The latter is the more likely explanation if the digital surveillance recorder employs an error-correction process, which ensures the copying process is successful.

The report also discusses the advantages of making duplicate originals using WORM (write once read many) memory

devices (for example, CD-ROMs). These are plastic discs coated with a reflective material into which pits have been physically etched. The CD's laser reads the information stored in the etching but cannot change or delete it. As well, the report discusses the use of digital signatures that incorporate encryption and make the signature unique to the specific document or its originator.

In response to the report, the British government recommended that the use of authentication techniques be encouraged and that members of the legal profession be made aware of the benefits of these techniques, their value in adding weight to evidence, and the possible significance of their omission. In addition, and among other things, the following recommendations were also put forward:

- that consideration be given to measures to reduce the uncertainty over the use of digital images in court;
- that the government encourage the adoption of technological measures for the authentication of images as evidence by giving type approval to them; and
- that the Judicial Studies Board consider establishing a program of education on the implications of digital technology for the judicial system.

This report is a major step forward towards allowing digital evidence in common law courtrooms. The other major issue addressed in the report, the civil liberty implications of public surveillance systems, will be the subject of a future column.

Elliott Goldstein, BA, LL.B., is a lawyer, visual evidence consultant and author based in Toronto, Ontario.

Author's Notes

1 See House of Lords, Select Committee Science and Technology — Fifth Report, February 3, 1998, "Digital Images As Evidence"© Parliamentary Copyright 1998, available on the Internet from www.parliament.the-stationery-office.co.uk.

2 The British government responded in a later report of the House of Lords. See Select Committee Science and Technology — Eighth Report, June 22, 1998, "Digital Images As Evidence: Government Response"© Parliamentary Copyright 1998, available on the Internet from www.parliament.the-stationery-office.co.uk.

3 1998 Chapter 29, available on the Internet from www.hmso.gov.uk.

4 This is still true in the United Kingdom today, and in Canada.

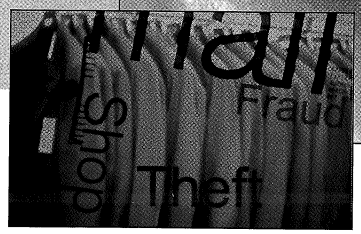
CANADIAN Security
The Publication for Professional Security Management

Contents

June/July 2001 Volume 23 Number 5

Cover Photo: Custom Protection Canada Inc. and Wyco Security Ltd.

page 14



page 18

In Each Issue