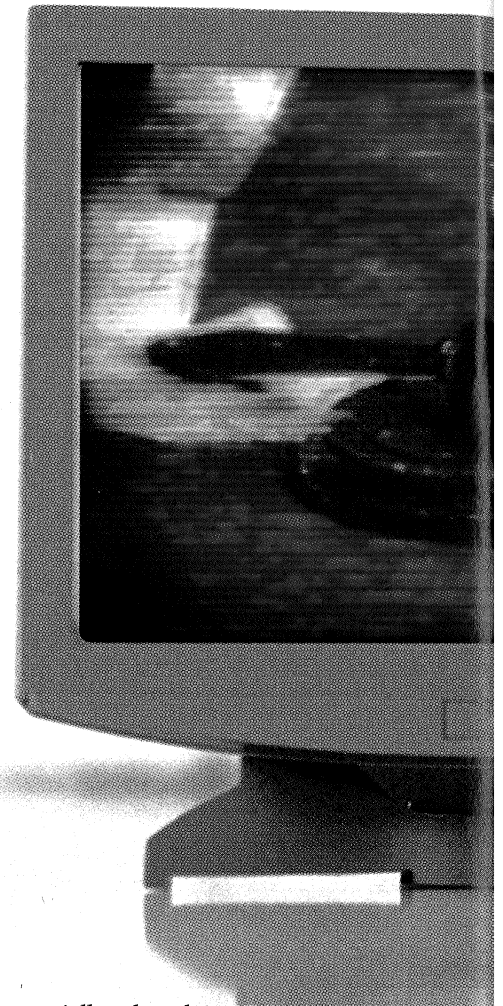
MAKING A CASE FOR DIGITAL VIDEO

Will your system stand up?



Digital video evidence has yet to be challenged in court, but questions about its admissibility are starting to surface. Experts offer their advice.

By Grant Buckler

Digital video surveillance is here to stay — nobody seems to dispute that fact. It's convenient and economical and makes it easier to find the video clip you need in a hurry. But compression techniques used with digital video raise some concerns about its usefulness in court.

Neither the fact that video is digital nor the fact that it is compressed is necessarily a problem in court. However, experts say, a lack of accepted standards means wide variation in quality, and some systems produce recorded images so poor they could be useless. Even with better systems, smart lawyers may ask tough questions about the output — though nobody can point to a case where video evidence has been thrown out of court because of compression.

The best advice is to choose digital surveillance systems carefully.

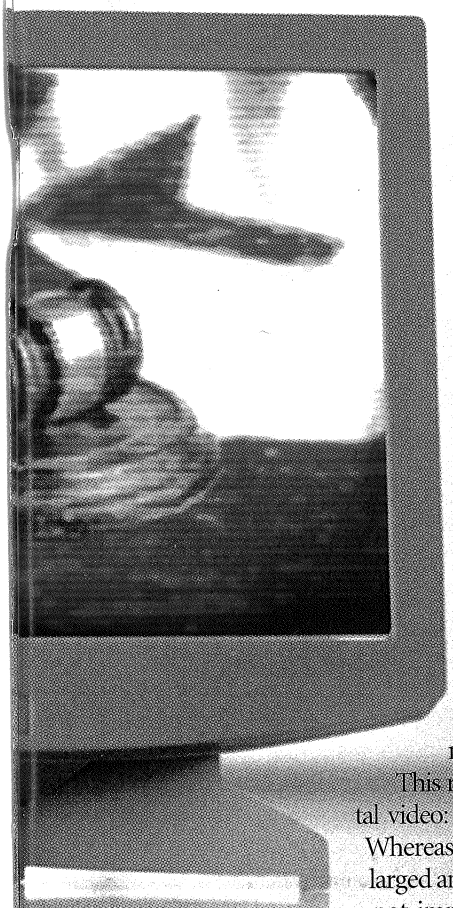
"The main problem with digital video is compression and artifacting and ghosting images," says Jonathan Hak, an Alberta Crown prosecutor who specializes in forensic video. Depending on the amount of compression, Hak says, data loss and artifacts — things appearing in the video that were not actually there — could be serious problems.

Individual video frames can be compressed by storing less detail — this is essentially what the JPEG compression standard for still images does. Motion JPEG uses JPEG to compress frames, and may also store fewer than 30 frames per second (the standard for television). MPEG video compression goes farther, analysing what parts of the image change over time and storing only the changes.

The problem is that the compression algorithm sometimes misses things, says Grant Fredericks, manager of forensic video solutions at Avid Technology Inc. of Tewksbury, Mass. Objects approximately the same colour as the background can disappear because the compression algorithm misses their movement. Fredericks says he recently saw surveillance video in which part of a white car vanished at it passed a light-coloured driveway.

Fredericks adds that compression usually changes the image's aspect ratio — it stretches it in one direction or the other, so objects appear taller and thinner or shorter and squatter. This can present problems with identification unless the aspect ratio is corrected.

The greater the compression, the more problems. Brett Hallgren, partner in North American Forensic Video Solutions in Delta, B.C., says 10-to-one compression yields quality comparable to standard VHS tape. But, says Gerry



Lanna, forensic audio/video specialist with the Ontario Provincial Police, "there are companies out there that are compressing video at 100 or 200 to one and they're bragging about it."

If compression is too high, it may be impossible to see what a judge or jury needs to see for the video to be useful evidence. This depends on what must be proven. A compressed image may show people as little more than blocks of video pixels, Hak says, but if all you need to show is how many left the scene, that could be enough. On the other hand, "if you get a vehicle that is eight pixels, you're never going get a license plate off eight pixels no matter what you do."

This raises another point about digital video: what you see is what you get. Whereas analogue video can be enlarged and enhanced to bring out details not immediately visible, digital stores no more than the eye can see and can't be enhanced, Lanna says.

The lack of digital video standards is another issue, Fredericks says. Technology-dependent evidence is subject to tests that ask whether the technology that obtained it is generally accepted by scientists and uses a process that has undergone peer review — Canadian courts rely on the Daubert test, while some U.S. states use Daubert and others use the similar Frye test. Since there is no standard, Fredericks says, digital video passes neither. This does not make it inadmissible, though — just more open to question.

Because most digital systems use proprietary software to compress and display video, police usually lack the equipment to view the stored video. Many surveillance systems can transfer the relevant clips to a CD, but Lanna dislikes this because there could be questions about whether what appears on the CD is exactly what was recorded. In some cases, Hallgren says, police seize entire systems to be able to view video in its native format.

Despite these concerns, Toronto lawyer Elliott Goldstein says compressed video is acceptable in court. "I'm not aware of any Canadian case in which digital video has been rejected simply because it was digital video," he says.

However, Lanna says, plenty of compressed video never goes to court because it is not of good enough quality to be useful as evidence. This can happen with poor-quality analog video too, he adds, but is more common with digital today.

Goldstein says the reliability of any video evidence, whether analogue, uncompressed digital or compressed digital, is open to question. In court, the party presenting the evidence must support it either with an eyewitness who will testify that the events on the video are what he or she saw happen, or in the case of automatically recorded video, with an expert witness who will explain what measures have been taken to ensure the image has not been altered.

Digital video can be edited, as can analogue video, says Brett Beranek, product manager for Genetec Information Systems, Inc., a Montreal company that provides video surveillance systems using various technologies. But digital has an advantage in the ability to use watermarking or digital signatures to show whether the video has been altered.

Goldstein says the second issue is what information is relevant to the case. Compression — like other factors, such as resolution, lighting and colour calibration —may be an issue if it affects the ability to distinguish something critical to a decision. For instance, some systems take fewer frames per second than full-motion video, resulting in jerky playback that may not accurately reproduce the speed of movements. Such video might be questioned if the speed of motion is an issue, Goldstein says.

"It's not enough that there's a problem," Goldstein adds. "The problem's got to affect the result." His advice to anyone bringing video evidence in court: "Take a good look at what you're trying to use the tape to show." If there can be a legitimate question whether the tape shows that, it may be inadmissible.

Mark Holik is director of safety and security at West Edmonton Mall. The mall moved from an analogue tape system to a fully digital one in August 2003, and Holik has no regrets. "We have taken digital video evidence into court," he says, "but we haven't had it contested."

Fredericks advises testing digital equipment before buying. If a vendor touts 30 days of video on a single hard drive, he says "you want to say 'will you please set the compression so the hard drive holds 30 days of video,' record five minutes and then examine the image." Record the video under the worst conditions in which you need the system to work, he adds — for instance, if you may ever need video recorded at night, test at night.

Hak stresses that it's vital to evaluate the recorded image, not the uncompressed image shown on a monitor as you record, which in systems with high compression may be very different from what is stored.

Given a choice, Hak prefers analogue video. "Analogue is the best," he says, "there is no question." But he recognizes the attractions of digital, and expects its use to increase. "I've seen great quality, medium quality and poor quality," he says. The trick is to buy a system that delivers good enough quality for your needs.

Grant Buckler, is a Kingston, Ont.-based freelance writer.

CANADIAN SECURITY
THE PUBLICATION FOR PROFESSIONAL SECURITY MANAGEMENT

November 2004 | Volume 26 Number 8

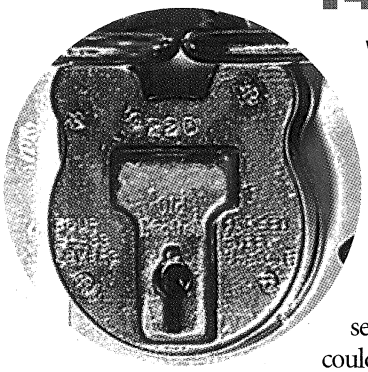
COVER: JEFF KIRK

COVER STORY |

10 Securing the Identity of the People

Wayne Simmerson takes on the role of Chief Security Officer in the Office of the Registrar General. In an age of identity theft, his department is beefing up measures to reduce risk.
By Jennifer Brown

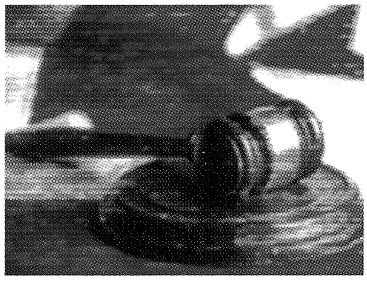
FEATURES |



14 Do you know where the CFO has left his laptop?

Wireless devices have given employees the ability to work anywhere, but they also pose a liability if they are not properly secured. Safeguarding mobile hardware could be critical to protecting your company's information assets.
By John Shoesmith

18 Making a case for digital video. Will your system stand up?



Digital video evidence has yet to be challenged in court but questions about its admissibility are starting to surface. Experts offer their advice.
By Grant Buckler

DEPARTMENTS |