DIGITAL DIALOGUE

Highlights from a recent webcast on video surveillance

VIDEO SURVEILLANCE TECHNOLOGY: MORE THAN MEETS THE EYE

Pictures might tell the story, but a variety of emerging technologies are allowing investigators to delve even deeper into video evidence.

A picture is worth a thousand words, according to the old adage. But when it comes to video surveillance, a picture could be worth a whole lot more, as the technology for analyzing closed-circuit video grows increasingly sophisticated.

Video surveillance today is both ubiquitous and powerful, according to Grant Fredericks, owner of Forensic Video Solutions in Spokane, Wash., who spoke during a Dec. 10 webcast titled "Video Surveillance: Emerging Solutions for Securing Agency Assets."

Fredericks, who is also an adjunct instructor of forensic video analysis at the National Digital Multimedia Evidence Processing Lab at the University of Indianapolis, said that video images provide the richest source of evidence in criminal prosecution today.

Investigators still rely on more traditional forms of physical evidence such as fingerprints, DNA and tire tread analysis. But "they're actually finding more relevance and more information in video," Fredericks said. "Whether it's from a taxi cab, a school bus, a school itself, a private residence, a church, a convenience store or a bank, anywhere we can imagine the public has right of access, there's going to be video surveillance. We really are living in a surveillance society today and law enforcement agencies are taking advantage of that."

The global law enforcement market for video technology is expected to reach $23.5 billion in 2014 and to grow about 20 percent a year after that, he said.

This influx of technology is changing the field. In the past, for example, investigators would look at a videotape in a murder investigation to see if they could read the license number of a suspect car, or get a picture of a suspect. If they couldn't, they had to look elsewhere for evidence. But today, with the latest generation of software and forensics techniques, investigators do not have to give up so easily.

Fredericks described a cold case from Pennsylvania where the available video showed the suspected murderer, but not clearly. What seemed to be the victim, wrapped in a sheet in the passenger seat, was partially visible, but obscured by the driver.

Prosecutors refused to file charges in the case because the images were of poor quality. Investigators applied image averaging techniques to the video, and the image of the driver became very clear. Then, because the driver changed positions several times during the video, investigators were able to digitally remove his image and reveal a full view of the victim.

Ultimately, the forensic investigation provided enough evidence to convict the driver, who is now serving a 40-year sentence.

Such investigations have to be done carefully to make it more likely that a court will admit the results into evidence, Fredericks said.

"The admissibility of video is a decision made by any judge who's asked to

3 TIPS FOR EFFECTIVE VIDEO PLANNING

- **Define the purpose.** It's essential to match technology with the situation, said Grant Fredericks, owner of Forensic Video Solutions in Spokane, Wash. In the case of facility security, when dealing with hundreds of people constantly on the move and many areas to cover, compressed MPEG video will probably do poorly. When monitoring a dark parking lot, some sort of night vision is essential.

- **Set storage policies.** How long you should keep data depends, again, on what you plan to do with it. Organizations dealing with fraud investigation, for example, might keep the data stored for six months to two years.

- **Plan for interoperability.** Who is going to use the data? If it's for criminal evidence, for example, you should be able to share it with law enforcement in its original form to ensure the best chance of it passing the defense counsel's challenge.

make that evaluation," he said. "There is no such thing as evidence that is always admissible, so when an analytics company says 'Our material is admissible in court,' that's a misstatement. It may be admissible, it may not be."

That becomes an important consideration when the evidence to be presented is not obvious in the video itself, but comes from other data and techniques that judges and juries might not understand.

In one case of arson at a retail site, investigators were able to measure subtle changes of color in a security video to determine when and where the fire started – and they were able to link it to an individual, even though the fire itself was not visible until 20 minutes after the person was last seen in the frame.

"We're now kind of moving into an era where other technologies can assist us in interpreting the video information and in telling the story," he said. "When I testify in court, not only am I a scientist, I have to be a storyteller. I have to give voice to the video."

The possibilities are endless. Drew Gerber, president of G Technologies, based in St. Leonard, Md., said software also can bring functionality such as the ability to sound an alert when someone in the surveillance area leaves an object unattended, or to recognize license plates and check them against a whitelist, showing who should be allowed in, or blacklist, showing who should be kept out.

Here is a sampling of other capabilities offered by G Technologies' Intelligent Video Surveillance System:

• Camera loss detection: Detects the loss of video signal (e.g. cord cut) from any camera.

• Motion tracking: Compares relevant pixel changes between images and alerts on relevant motion while ignoring "background" motion (e.g. rain, snow, blowing objects, leaves on trees).

> "When I testify in court, not only am I a scientist, I have to be a storyteller. I have to give voice to the video."
>
> – *Grant Fredericks, owner, Forensic Video Solutions*

MARSHALING THE TEAM

The University of Indianapolis houses a facility that the Law Enforcement and Emergency Services Video Association (LEVA) owns and manages. While it mostly functions as a training center for investigators and analysts, it also can field emergency response teams to help member departments find useful information in data. The facility houses 20 advanced video forensics systems, all tied into an Avid ISIS management system with 64 terabytes of storage.

In 2011, hockey fans in Vancouver rioted after Vancouver lost the Stanley Cup playoffs to the Boston Bruins. Vancouver police sent teams to harvest video from cameras in the area, and also appealed to the public for mobile phone video of the riots. They ultimately developed 5,000 hours of evidence, well beyond their ability to analyze. At the department's request, LEVA activated the emergency team, which worked three shifts for two weeks to analyze the data.

Eventually, the team sent the data back with 15,000 separate criminal acts identified and tagged for easy retrieval, and the city filed more than 600 criminal charges, most of which led to quick guilty pleas, said Grant Fredericks, owner of Forensic Video Solutions in Spokane, Wash.

• Object classification: Distinguishes between people, vehicles and unknown objects.

• Virtual fence: Creates an invisible tripwire that can send an alert when crossed in one or both directions.

• Wrong direction: Detects motion going against the specified flow of traffic.

• Loitering/dwell time: Recognizes how long an object stays in a defined field of view.

• People/vehicle counting: Counts objects entering and leaving a field of view or crossing a virtual fence.

To improve the performance and the efficiency of intelligent video systems, many organizations are turning to another technology: Virtualization.

"Some of the biggest investments our customers have made are in their data centers, with data center virtualization, network virtualization," he said. "Leveraging those resources helps alleviate some of the costs associated with deployment." •