Technology
AN MIT ENTERPRISE Review

Monday, December 11, 2006

Forensic Watermarks in Mobile Devices

Researchers are working on a new watermarking scheme to deter people from illegally sharing videos.

By Kate Greene

As video content shows up on more and more cell phones, content providers are looking for new ways to curb illegal distribution. Researchers at Cinea (http://www.cinea.com/) , a subsidiary of Dolby, are working on a system that embeds a unique digital signature called a forensic watermark into a video after it's downloaded. The watermark, explains Robert Schumann, general manager of Cinea and board member of the Digital Watermarking Alliance (http://www.digitalwatermarkingalliance.org/) , contains bits of data, hidden from view, that allow content providers to trace a video back to the phone or device on which it was downloaded. The goals, he says, are to deter people from widely distributing a downloaded video and to have a method of finding individuals who illegally share video.

The most common way to deter illegal distribution of music and movies is through digital rights management technology (DRM): instructions embedded in the files that limit their use. For instance, music bought from Apple's iTunes music store uses the DRM scheme called FairPlay, which allows songs to be played only on an Apple iPod MP3 player and a limited number of authorized computers.

Schumann says watermarking technology could offer a less restrictive alternative to DRM. "People are not happy with how DRM works today," he says. The limits imposed by DRM are not necessarily because content owners don't want an individual to make five or six copies of a CD, he says, but because content owners are looking for a way to keep people from making one million copies. Watermarking, Schumann says, could potentially give people more freedom than some current DRM schemes, allowing consumers to shuttle video or music from device to device, and to share copies with friends. "If you use the video [on your own electronic devices], then nobody knows the [watermark] is there," he says. "But if we find a million copies of [the video containing your unique watermark] out on the Internet, then we might come looking for you."

Embedding a forensic watermark is typically a computationally intense task. Pixels of the video need to be altered to create the watermark, and ideally, those alterations are invisible. Each scene must be analyzed to determine which pixels to alter. Cinea wants to create a system that can embed these watermarks using the limited processing power of devices such as mobile phones.

Cinea believes the solution lies in doing some of the computer processing before the video is downloaded. Then, when the video is sent to a mobile phone, Schumann says, the file contains a few extra kilobits of data that essentially point to the pixels that need to be changed in order to embed a watermark.

"It's conceptually easy," Schumann says, "but hard to do in practice." The researchers are trying to tweak the algorithm so that the watermarking data added to the file isn't excessive. "Bandwidth is precious," he says.

Some researchers don't see forensic watermarking technology being easily accepted by consumers. "In extremely dynamic, mobile media consumer environments, fingerprinting makes a lot of sense only if you want to alienate your customers," says Radu Sion (http://www.cs.stonybrook.edu/%7Esion/) , professor of computer science at Stony Brook University, in New York. The problem, he says, is that if you give a song or video to one of your friends, the forensic watermark that identifies you travels with it. What happens after it leaves your possession is out of your hands. Suppose your friend gives it to her friend, who puts it on a file-sharing site on the Internet, Sion says. The forensic watermark still traces it back to you. "Customers would now be reluctant to buy into such a technology," he adds.

There are also problems in keeping forensic watermarks from being removed, says Min Wu (http://www.ece.umd.edu/%7Eminwu/) , professor of electrical and computer engineering at the University of Maryland. Wu researches methods for allowing watermarks to stand up to these attacks. If multiple people purchase the same video, for instance, and compare those files, they could detect the unique pixel alterations in each person's file. These could be averaged out to reveal a watermark-free video.

Securing forensic watermarks is still an active area of research, says Cinea's Schumann. Perfecting the technology is still a few years out: he expects to see the first field tests for forensic watermarking on mobiles in 2007 and 2008. But he's confident that within the next decade, technology can change the way content providers protect their digital goods and the way people share and use them.