Moderator
Jian Zhao
Fraunhofer CRCG
MediaSec Technologies LLC

Panelists

Eckhard Koch
MediaSec Technologies LLC

Joe O'Ruanaidh
Siemens Corporate Research

Minerva M. Yeung
Intel Corporation

Digital Watermarking: What Will It Do for Me? And What it Won't!

Digital watermarking has emerged as an enabling technology for protecting digital intellectual property rights. The technology is completing its trial phase and becoming mature in diverse markets, from electronic commerce and digital broadcasting to DVD. Several cross-industry organizations such as CPTWG (the Copy Protection Technical Working Group), DAVIC (the Digital Audio-Visual Council), and SDMI (the Secure Digital Music Initiative) are working hard to develop digital watermarking standards that will allow wide deployment and acceptance of this technology.

Digital watermarking embeds secure invisible or inaudible labels in multimedia data (such as images, audio, text, video, 3D graphics) for identifying copyright-related information such as origin, ownership, use-control, integrity, or destinations. The digital watermark is integrated with the multimedia and tightly bound with the quality of the content. The benefits of digital watermarking for content protection are twofold: it provides evidence of illicit copying after the event, and it discourages such misuse in advance.

Like any other emerging technology, digital watermarking has raised a number of questions both in research and business: Why is digital watermarking necessary? How does the technology work in the real world? What are the strengths and weaknesses of the technology? What data can be watermarked? How do you measure the security and robustness of digital watermarks?

This panel provides an opportunity to hear from some researchers as well as some startup entrepreneurs in the digital watermarking area. Panelists explain how to apply this technology in real-world applications and discuss where digital watermarking is likely to go in the future.

Eckhard Koch

Even though digital watermarking is still in its infancy and needs more research, the technology is already in commercial use. The main reason for this early adoption is that customers can't wait. Their bitter experiences with data pirating make them eager for protection.

Most customers for this technology are OEMs, system integrators, hardware manufacturers, and software vendors. They could add considerable value to their products and systems by licensing watermarking technology. The straightforward model for the watermark business is royalty-based licensing. An alternative model for large-scale mass-market products is to provide counter-based, off-the-shelf watermark packages. End users are charged by the number of watermarks locked in a software or hardware counter.

The major technical challenge is to develop a foolproof protection scheme while at the same time keeping the watermarks imperceptible. Absolute robustness is impossible, but digital watermarking can be useful as long as the process of tampering with and removing the watermark is costly and time-consuming.

Potential customers are pushing the digital watermark technology to enter the market faster than other new technologies. In fact, visionaries have adopted digital watermark products in some application domains where state-of-the-art technologies provide sufficient protection. For example, in the field of secure and invisible communications, where steganography has been accepted for centuries, watermark technology is considered ready for real-world applications.

Several cross-industry organizations such as CPTWG (the Copy Protection Technical Working Group) and DAVIC (the Digital Audio-Visual Council) are working hard to develop digital watermarking standards that will allow wide deployment and acceptance of this technology. Other visible initiatives are underway at the International Federation of Phonographic Industry (IFPI) and the Secure Digital Music Initiative (SDMI) for audio watermarking. and at the Digital Audio-Visual Council (DAVIC) for watermarking in e-commerce.

In the foreseeable future, in my personal opinion, it's unlikely that the digital watermark will be standardized for all markets. Instead, standardization will likely happen in different sectors such as physical media (DVD, CDs), online media delivery, broadcasting, and document authentication in the imaging industry.

Joe O'Ruanaidh

Watermarks. The term evokes visions of shady characters secretly beavering away in dark basements surrounded by forged $100 bills drying on clothes lines.

In a digital media context, away from the traditional world of inks and paper, the same old problem remains but it relates not just to forgery but also to outright theft, because one digital copy can spawn millions of others with the single click of a mouse button. It is hardly surprising that the notion of a digital watermark has stimulated avid interest amongst artists and publishers alike.

It is commonly recognized that digital watermarks must be as robust as the media in which they are embedded. For example, a rotated, cropped, and rescanned watermarked image should still be a watermarked image. However, this robustness requirement directly conflicts with the need for a digital watermark to be unobtrusive. The most effective techniques used to embed watermarks are the result of a combination of secret key-based techniques used for military communication and simple models of the human visual system.

The most familiar application for digital watermarks is for copyright protection and protection of intellectual property. On its own, a watermark does not provide any legal proof of ownership. In other words, the use of a given digital watermark to protect intellectual property must be registered with a trusted third party to be of any value. Any technique for embedding robust digital watermarks must be compatible with methods for registering copyright.

A watermark's resistance to intentional and unintentional degradation has been the main subject of interest in the watermarking community. The main challenges are geometric transformations such as change of proportion or simple rescaling. One watermark removal technique that is supplied on the Internet simply shifts a corner of the image. Lossy image compression such as JPEG and filtering are more easily overcome and, generally speaking, watermarks have evolved into very resistant forms. The results are impressive in the laboratory, but will they really work in the real world?

Digital Watermarking: What Will It Do for Me? And What it Won't!

Minerva M. Yeung

The Internet has been growing very rapidly, and the bandwidth available to users has increased as the Internet has grown. Digital subscriber lines and cable modems are becoming widely available at affordable prices. As transmission rates increase, the quantity and quality of available digital content (in the form of images, audio, video, graphics, and 3D models) will increase. However, this raises a major problem for content providers and owners: protection of their material. They are concerned about copyright protection and other forms of abuse of their digital content. On top of that, digital media content, coupled with Internet distribution, is subjected to instantaneous mass replication and distribution, resulting in severe loss of revenues or royalty payments.

Many of those involved in cross-disciplinary research on effective content protection technology for digital media believe that technology can play a major role in providing the infrastructure for content protection and distribution. But they are gradually realizing that a comprehensive digital content-protection infrastructure requires more than data encryption and embraces technical innovations plus in-depth study of the functionality, thread models, limitations, and applications across many disciplines, ranging from cryptography, computer science, signal processing, software and hardware architecture, public policy, and law.

This panel focuses on end-to-end protection of multimedia content in Internet-related applications, the role of digital watermarking in the media content protection infrastructure, potential benefits and limitations, possible attacks and remedies, and the current status of watermarking research in the computer graphics field.

Jian Zhao

High cost and user reluctance to establish the "use-control" trusted model encourage exploration of alternative solutions for content protection. Although the original motivation for digital watermarks was for copyright protection, this technology has found a multitude of potential applications not originally envisioned by pioneers in the field.

Digital watermarks can be used for creation of hidden labels and annotations in medical applications, in cartography, and for multimedia (video and audio) indexing and content-based retrieval applications. In a medical scenario, watermarks might be used for unique identification of patient records. Patient records could be embedded directly into the image data for each patient, which would both speed up access to records and prevent potentially harmful errors such as a mismatching of records and patients.

For proof of authenticity, digital watermarks are of particular interest in electronic commerce and distribution of multimedia content to end users. The surfaces of ID cards, credit cards, and ATM cards could be watermarked. So could bank notes, personal checks, and other bank documents. Scanners, printers, and photocopier could refuse to operate if they find a watermark that specifies permissions to manipulate the document and does not authorize scanning, printing, or copying.

As a robust covert communication channel, digital watermark technology has a wide range of applications in the defense and intelligence sectors, where traditional steganography has been employed for centuries. Also, digital watermarks may find potential markets in countries where strong cryptography is not permitted.