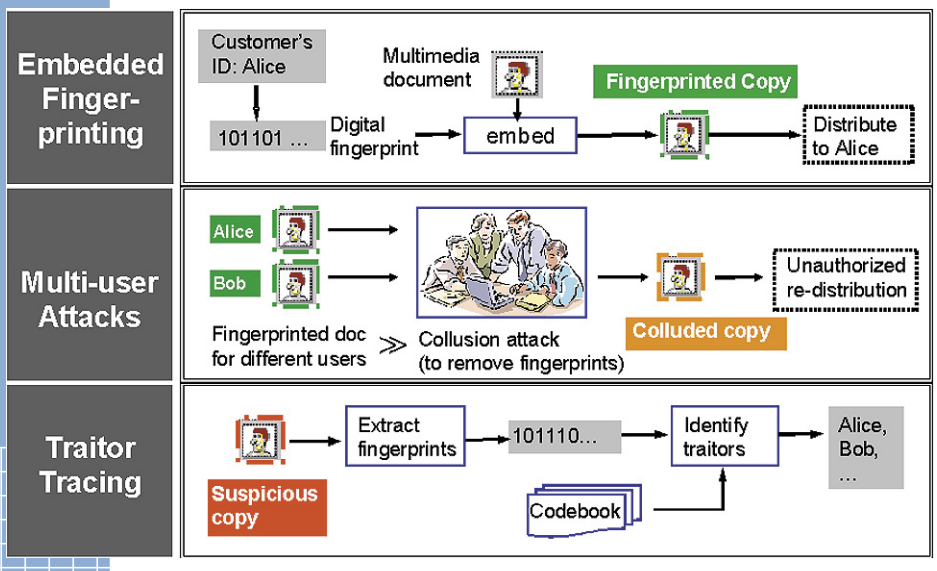
RESEARCHBRIEF
THE INSTITUTE FOR SYSTEMS RESEARCH

Digital fingerprinting for multimedia data

The potential

Ensuring that digital content is used for its intended purpose is extremely important to managing digital rights in commercial and military operations. To protect the sensitive nature of multimedia data shared among a group of users, solutions must be developed for tracking and identifying those involved in unauthorized redistribution of multimedia content.

Digital fingerprints are unique labels inserted in different copies of the same content before distribution. Each digital fingerprint is assigned to a "club member," and can be used to trace the culprits who use the content for unintended purposes. As a proactive forensic tool for gathering evidence and tracing the culprits of unauthorized information dissemination, it is essential that the fingerprints be difficult to remove.



Embedded fingerprinting for multimedia: how multimedia forensic fingerprints work against collusion attacks.

The challenge

A conventional way of embedding fingerprints into multimedia is through robust watermarking. Usually small in amplitude and imperceptible to humans, digital watermarks are integrated into the content itself and can survive compression, digital-to-analog conversion, and other moderate processing.

Unfortunately, conventional watermarking techniques do not shield well against "collusion," an attack by a coalition of users with the same content containing different marks. This frequent and cost-effective attack is a process in which several differently marked copies of the same content are averaged to disrupt the underlying watermarks. Another kind of collusion attack involves forming new content by selecting different blocks of pixels from among the colluders' content and piecing the new blocks together.

One key difference between fingerprinting generic and multimedia data is that multimedia data is sensually robust to minor disturbances in the data values. This makes it desirable and feasible to embed digital fingerprints within the media itself, rather than as external markers.

Unfortunately, some existing fingerprint codes designed for software and other generic data are too long to even *be* embeddable in multimedia data. The process of fingerprinting multimedia should, therefore, consider the design of appropriate fingerprints that are both effective and efficient.

The research

ISR-affiliated Assistant Professor Min Wu (ECE), Professor K.J. Ray Liu (ECE/ISR), and their research team are developing a method known as "digital fingerprinting" that protects watermarked documents from would-be colluders. This technique would make it possible to design fingerprints that resist collusion and identify users who try to use multimedia content for unintended purposes, thereby discouraging misuse of digital media and encouraging its future development.

continued...

Assigning mutually orthogonal watermarks to each user is a straightforward way to extend popular "spread spectrum" watermarking to fingerprinting. Their simple encoding and embedding structure makes them attractive to identification applications that involve a small group of users. The research team has developed a quantitative method to evaluate collusion resistance and provide operational guidelines.

However, the number of basis signals needed in orthogonal fingerprinting increases linearly with the number of users. This makes detection and bookkeeping much more complex. The research team strategically introduces correlations to the fingerprints that accurately identify which ones contribute to a collusion attack.

This has given birth to anti-collusion codes (ACC), a new fingerprinting scheme based on spread spectrum embedding and discrete-valued code. Based on combinatorial theory, the combination of a subset of code vectors uniquely identifies the guilty coalition. ACC code length is several magnitudes shorter in practical situations, a substantial advantage. By taking advantage of coding and embedding layers for high robustness and efficiency, ACC fingerprinting has demonstrated performance gain over previously known codes on colluder identification.

The team has developed a unified framework covering orthogonal, coded, and other correlated fingerprints. Under this framework, the fingerprinting technologies developed can be applied to images, video, audio, and special documents like maps. The team has proof-of-concept prototypes and pending patents on this research.

Award

A Collusion-Resistant Multimedia Fingerprinting Framework for Information Forensics, Air Force Research Laboratory Digital Data Embedding Technologies (DDET) award

Research team

Min Wu, Assistant Professor, Electrical and Computer Engineering Department and the Institute for Advanced Computer Studies

K.J. Ray Liu, Professor, The Institute for Systems Research and Electrical and Computer Engineering Department

Wade Trappe, Assistant Professor, Rutgers University Electrical and Computer Engineering Department and WINLAB, and former Ph.D. student of Dr. Liu.

Zhen Jane Wang, ISR Research Associate

Contacts

Min Wu
2457 A.V. Williams Bldg.
University of Maryland
College Park, MD 20742
Phone: 301.405.0401
Email: minwu@eng.umd.edu
www.ece.umd.edu/~minwu/

K.J. Ray Liu
2219 A.V. Williams Bldg.
University of Maryland
College Park, MD 20742
Phone: 301.405.6619
Email: kjrliu@isr.umd.edu
www.isr.umd.edu/Labs/CSPL/kjrliu/kjrliu.html

Web links

Multimedia fingerprinting
www.cspl.umd.edu/MMFP/

Communication and Signal Processing Laboratory, *www.cspl.umd.edu/*

"Anti-Collusion Fingerprinting for Multimedia," 2002 online research poster, *www.ece.umd.edu/RRD/onlineposters/Wu_AntiCollusionFingerprinting.pdf*

"Nonlinear Collusion Attacks on Independent Multimedia Fingerprints," 2003 research poster, *www.rrd.umd.edu/2003onlineposters/NonlinearCollusion.pdf*