Scanning the Issue

Special Issue on Enabling Security Technologies for Digital Rights Management

Modern advancements in communication infrastructure, signal processing, and digital storage technologies have enabled pervasive digital media distribution. Digital distribution allows the introduction of flexible, cost-effective business models that are advantageous to multimedia commerce transactions. The digital nature of the information also enables individuals to manipulate, duplicate, or access media beyond the conditions agreed upon for a given transaction. The latter issue has resulted in tremendous concern by content vendors. The large-scale success of legal digital media distribution rests, in part, on its ability to provide legitimate services to all parties. This requires allowing consumers convenient use of digital media while equitably compensating other members of the distribution chain such as content creators, aggregators and vendors.

Digital rights management (DRM) has been proposed to address these issues. DRM is the digital management of user rights to content. It links specific user rights to media in order to provide persistent governance of user activities such as viewing, duplication, and access. Ideally, a DRM system balances information protection, usability, and cost to provide a beneficial environment for all parties; this includes expanded functionality, cost effectiveness and new marketing opportunities. Overall, management is achieved through the interaction of effective economic models, social values, legal policy, and technology.

At the technological level, DRM systems incorporate encryption, copy control, tagging, tracing, conditional access, and media identification. The challenge is to engineer secure systems in an environment of dynamic applications and standards for which appropriate business models and consumer expectations are only now being identified. Furthermore, controversy over the ability of DRM to create atypical licensing policies and provide more control to content vendors than traditionally accepted practices has stirred much debate on the technology.

The goal of this Special Issue is to provide some principal tutorial papers and novel research contributions in the area of DRM technologies. Our objectives are to present an overview of the area by presenting papers of both practical and theoretical interest, focus on state-of-the-art and potential future technologies in order identify trends in DRM system evolution, and provide a good starting point for individuals entering this active research area by looking at both system- and algorithmic-level developments.

In the first paper of this Special Issue, Koenen *et al.* provide a high-level overview of DRM in their paper entitled "The Long March to Interoperable Digital Rights Management." Their work presents the DRM concept, outlines a basic reference model for current architectures, and discusses the importance and issues of DRM interoperability. The authors consider the significance of interoperable DRM systems and outline and compare three possible approaches to achieve this goal. Standardization of specific DRM-related technologies are detailed. The paper finally presents an experimental system that supports interoperability of heterogeneous DRM systems via online services and service orchestration.

Many existing DRM systems use handshake protocols to establish secured communication. Both the client and the server have public key certificates. After mutual authentication, the client and the server agree upon a unique secret key to encrypt further communications. This dependency on an online handshake protocol makes public key-based systems unsuitable for physical media or broadcast-based distribution. The handshake is undesirable, since it prevents disconnected operations and raises privacy concerns. Originally defined by Fiat and Naor, broadcast encryption was proposed as a key management scheme with revocation, but without the participating parties requiring a two-way handshake. In "Anonymous Trust: Digital Rights Management Using Broadcast Encryption," Lotspiech *et al.* discuss the concept of broadcast encryption for DRM. The authors provide an overview of this approach, discuss its application, and provide a comparison between broadcast encryption and public key cryptography. A cluster protocol for the home entertainment network is presented to illustrate a broadcast encryption based content-distribution system.

Encryption is also used to ensure confidentiality and access control for multicast communication applications. In a multicast environment, key management is essential and

Digital Object Identifier 10.1109/JPROC.2004.827336

yet represents one of the most challenging aspects to design and implement for content protection and rights management. The logical key hierarchy (LKH) algorithm is one well-known method for managing key exchanges when users in join or leave a multicast group. In "Efficient State Updates for Key Management," Pinkas describes several schemes for group rekeying that advances LKH to operational environments where members may not receive all of the group key updates. This is especially important when communication channels are lossy or group members go offline. The proposed schemes are detailed and are shown through analysis to be useful for rekeying large secure multicast groups.

In "Video Fingerprinting and Encryption Principles for Digital Rights Management," Kundur and Karthik provide a paper on digital fingerprinting and video scrambling algorithms based on partial encryption. Digital fingerprinting is the process of embedding a unique serial code into content streamed to each individual user in a multicast group. Partial video encryption involves the use of lightweight encryption principles to scramble select components of the video content. Straightforward application of digital fingerprinting and encryption of video increases communication bandwidth curtailing the scalability gains achieved through the use of multicast. The authors compare three potential architectures for video fingerprinting and encryption that make use of a "group key" for video encryption and integrate fingerprinting in different parts of the distribution end nodes. A novel methodology to integrate encryption and fingerprinting is proposed that exhibits some practical advantages.

The next two papers focus on authentication for content management. In "New Approaches to Digital Evidence," Maurer provides a foundation for understanding digital evidence systems and legislation. The paper reviews general physical and digital forms of evidence used in society to attach accountability to a given party in a contract. The limitations of traditional public key-based digital signatures and the legal system as a whole are then explored motivating the need for a paradigm shift in our thinking of digital evidence strategies. New ways of interpreting digital evidence are then presented, leading to the novel concept of digital declarations.

Biometric information can be used in several different ways for authentication of users in DRM systems. Biometric-based authentication is currently a potential candidate to replace less-secure password-based authentication systems. The paper "Biometric Cryptosystems: Issues and Challenges" by Uludag *et al.* provides an overview of the issues and challenges facing biometric cryptosystems. The authors introduce biometrics, summarizing the different stages of generic biometric technologies. Examples of proposed biometric information include content from a user's face, fingerprint, iris, hand geometry, signature, keystroke pattern, and voice. Furthermore, the paper discusses details of a few state-of-the-art biometric user authentication systems and shows their related challenges.

For a security technology to be effective, it must take into account the specific content distribution architecture employed. Many distribution architectures have been recently proposed and are for use in DRM. The focus of the next paper in this Special Issue is on peer-to-peer (P2P) information systems. In "Music2Share—Copyright-Compliant Music Sharing in P2P Systems," Kalker *et al.* show how the peer-to-peer distribution systems can be an easy-to-use distribution system for music and also respectful of digital rights protection and management. The authors propose a system called Music2Share that uses among other technologies audio fingerprints and watermarking to ensure the fair behavior of the users. A certification architecture allows the use of equitable protocols between contents providers and end users.

The next paper in this issue also involves digital watermarking technology. There is an overwhelming amount of literature proposing digital watermarking algorithms for copyright protection. It appears that digital watermarking is the only means to pass copyright information through analog-to-digital or digital-to-analog conversion of media. However, the effectiveness of the technology is still under much research discussion. The paper entitled "Benchmarking of Image Watermarking Algorithms for Digital Rights Management" by Macq *et al.* attempts to assess a number of watermarking algorithms through benchmarking suites. The authors focus on image watermarking algorithms and conclude that the use of open-source Web based approaches are highly beneficial for such challenging assessment design.

Some legal aspects of DRM technology of importance to the technical community are addressed by the next two contributions. DRM represents a class of technologies that aspire not only to enforce content usage controls, but also to provide governance for a broader set of organizational and public policies. Erickson and Mulligan's paper entitled "The Technical and Legal Dangers of Code-Based Fair Use Enforcement" reviews the concepts and architecture for policy specification and enforcement. Specific examples for DRM are cited, leading to a detailed discussion of how usage control policies are evaluated in DRM systems focusing on the issue of rights expression languages. The authors also consider the role of trusted computing systems in ensuring that computing agents interpret policies in reliable and deterministic ways.

The final paper in this issue provides an introduction to the legal and policy aspects of DRM targeted at the technical community. The tutorial paper "Legal Policy and Digital Rights Management" by Owens and Akalu provides an introduction to the laws and treaties that relate to DRM. These laws are currently a dynamic phenomenon, changing with both technology and social norms. The trends and policy contentions shaping these laws are discussed by the authors. In addition, the authors assert that given the social nature of DRM, technologists must be aware of the sensitive legal aspects of their work to be able to design broadly accepted technologies.

It is clear that DRM is a field of growing activity in which innovation interacts with emerging business models, legal policy and social norms. This Special Issue is intended to

provide an overview of the area through the introduction of comprehensive tutorial and research papers in the field. We hope that this collection inspires continued technologic progress, greater debate, and increased interaction between the many forces affecting and affected by DRM.

DEEPA KUNDUR, *Guest Editor*
Texas A&M University
College Station, TX USA
77843-3128

CHING-YUNG LIN, *Guest Editor*
IBM T. J. Watson Research Center
Hawthorne, NY 10532 USA

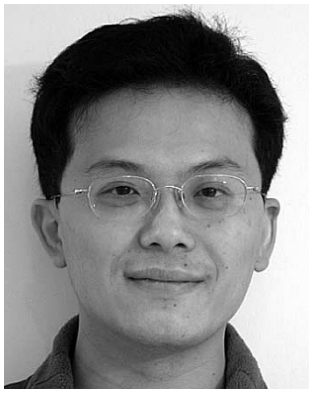
BENOIT MACQ, *Guest Editor*
Universite Catholiqué de Louvain
Louvain-la-Neuve B-1348, Belgium

HEATHER YU, *Guest Editor*
Panasonic Digital Networking Laboratory
Princeton, NJ 08540 USA

Deepa Kundur (Senior Member, IEEE) was born in Toronto, ON, Canada. She received the B.A.Sc., M.A.Sc., and Ph.D. degrees in electrical and computer engineering in 1993, 1995, and 1999, respectively, at the University of Toronto, Toronto.

From 1999 to 2002, she was an Assistant Professor in the Edward S. Rogers Sr. Department of Electrical and Computer Engineering, University of Toronto, where she held the title of Bell Canada Junior Chair-holder in Multimedia. In 2003, she joined the Electrical Engineering Department at Texas A&M University, College Station, where she is a member of the Wireless Communications Laboratory and holds the position of Assistant Professor. She is the author of over 60 papers. Her research interests include multimedia and network security, video cryptography, sensor network security, data hiding and steganography, covert communications, and nonlinear and adaptive information processing algorithms.

Dr. Kundur is the recipient of several awards, including the 2002 Gordon Slemon Teaching of Design Award. She has been on numerous technical program committees and has given over 30 talks in the area of digital rights management, including tutorials at ICME 2003 and Globecom 2003.



Ching-Yung Lin received the B.S. and M.S. degrees in electrical engineering from National Taiwan University in 1991 and 1993, respectively, and the Ph.D. degree in electrical engineering from Columbia University, New York, in 2000.

From 1993 to 1995, he was a 2nd Lieutenant in the Taiwan, R.O.C., Air Force. From 1995 to 1996, he was an Instructor in the Network Communication Lab, National Taiwan University. Since 2000, he has been a Research Staff Member in IBM T. J. Watson Research Center, Hawthorne, NY. He is also an Affiliate Assistant Professor at the University of Washington, Seattle. He has pioneered the design of video/image content authentication systems and since 2003 has led a semantic video annotation project which involves 23 worldwide research institutes. He is the author of more than 80 journal papers, book chapters, conference papers, and public release software. He is the primary author of the IBM Video Annotation System software system. He holds three patents and 12 pending patents. His current research interests include multimodality information analysis, multimedia understanding and multimedia security.

Dr. Lin is a recipient of the 2003 IEEE Circuits and Systems Society Outstanding Young Author Award and the 1993 Acer Lung-Terng Thesis Award. He received IBM Invention Achievement Awards in 2001 and 2003. His IBM multimedia semantic mining project team performed best in the NIST TREC video semantic concept detection benchmarking in 2002 and 2003. He is a Guest Editor of this Special Issue of the PROCEEDINGS OF THE IEEE, the Technical Program Cochair of IEEE ITRE 2003, and the Cochair of the Watson Workshop on Multimedia 2003.

Benoit Macq (Senior Member, IEEE) was born in 1961. He received the electrical engineering and the Ph.D. degrees from the Université Catholique de Louvain (UCL), Belgium, in 1984 and 1989, respectively. He did his Ph.D. thesis on perceptual coding for digital TV under the supervision of Prof. Paul Delogne at UCL.

He is currently Professor at Université Catholique de Louvain (UCL), Louvain-la-Neuve, Belgium, in the Telecommunication Laboratory, where he is teaching and doing research in image processing for visual communications. He has been a Guest Editor for the *Signal Processing Journal*, and was a Guest Editor for a Special Issue on security for image communications for *Image Communications*. His main research interests are image compression, image watermarking, and image analysis for medical and immersive communications.

Prof. Macq received the Bell Telephone award in 1990. He has held leadership positions for several IEEE and SPIE conferences. He was a Guest Editor for a Special Issue on watermarking for the IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, and a Guest Editor for this Special Issue of the PROCEEDINGS OF THE IEEE on digital rights management. He is also Associate Editor of the IEEE TRANSACTIONS ON MULTIMEDIA. He is a Member of the IEEE Technical Committee on Image and Multidimensional Signal Processing (IMDSP).

Heather Yu received the M.A. and Ph.D. degrees in electrical engineering from Princeton University, Princeton, NJ, in 1996 and 1998, respectively.

In 1998, she joined Panasonic, where she is a Senior Scientist at the Panasonic Digital Networking Laboratory, formerly the Panasonic Information and Networking Technologies Laboratory, Princeton, NJ. She has served as reviewer for many renowned international journals in the area of multimedia communication and processing. She has published nearly 50 technical papers, holds three U.S. patents, and has more then 20 patents pending in the multimedia communication and multimedia information access area. She is an Editor for *Computers in Entertainment* (ACM) and an Associate Editor for *Informing Science*. Her major focus is multimedia communication and multimedia information access research and development.

Dr. Yu is Chair of IEEE COMSOC Multimedia Communications Technical Committee, Conference Steering Committee Member of IEEE International Conference on Multimedia and Expo and IEEE Consumer Communications and Networking Conference, Technical Program Cochair of IEEE International Conference on Communications 2004 Multimedia Technologies and Services Symposium and IEEE International Conference on Communications 2005 Multimedia and Home Networking Symposium, and Conference Technical Program Vice Cochair of the IEEE International Conference on Multimedia and Expo 2004. From 1998 to 2002, she served as conference technical program chair, associate chair, session chair, technical committee member, best paper award committee member, keynote speaker, panelist, panel chair, and steering committee member for many conferences. She is an Associate Editor for IEEE TRANSACTIONS ON MULTIMEDIA and IEEE MULTIMEDIA.