SELECTED PAPERS FROM ISS 2000

Digital Rights Management and Watermarking of Multimedia Content for M-Commerce Applications

Frank Hartung and Friedhelm Ramme, Ericsson Research

ABSTRACT

E-commerce has become a huge business and a driving factor in the development of the Internet. Online shopping services are well established and will, with the advent of evolved 2G and 3G mobile networks, soon be complemented by their wireless counterparts. Furthermore, online delivery of digital media, such as MP3 audio or video, is very popular today and will become an increasingly important part of e-commerce and mobile e-commerce (m-commerce). However, a major obstacle for digital media distribution and associated business is the possibility of unlimited consecutive copying in the digital domain, which threatens intellectual property rights (e.g., copyrights). Digital rights management systems are required to protect rights and business. DRM systems typically incorporate encryption, conditional access, copy control mechanisms, and media identification and tracing mechanisms. Watermarking is the technology used for copy control and media identification and tracing. Most proposed watermarking methods use a so-called spread spectrum approach: a pseudo-noise signal with small amplitude is added to the host signal, and later on detected using correlation methods. A secret key is used to ensure that the watermark can only be detected and removed by authorized parties. Thus, watermarking is an essential component of modern DRM systems. Several standardization bodies are involved in DRM standardization. Some examples, (MPEG-4, SDMI, and DVD), are discussed in this article. Watermarking as an enabling technology is especially highlighted. Furthermore, the relation between DRM and m-commerce, and the impact on business models for m-commerce are discussed. A common experience today is that Internet e-commerce applications cannot always easily be adapted for mobile telecommunications systems. We emphasize, however, that DRM and watermarking can benefit from the additional information available in mobile telecommunications systems, and can thus help to improve rights management for digital media delivery.

INTRODUCTION

In a very short time, E-commerce has evolved to a huge business. Digital media distribution plays an important role in business-to-consumer (B2C) e-commerce. Digital music (e.g., MP3 encoded music) in particular has become extremely popular. Other media, like streaming video and e-books, are also becoming increasingly popular and important in terms of revenue. With the introduction of evolved second-generation and third-generation (3G) mobile networks like General Packet Radio Service (GPRS) and Universal Mobile Telecommunications Services (UMTS), mobile users will have fast access to the Internet and digital media wherever they are.

While there are many advantages associated with digital media and digital media distribution, clear disadvantages exist. A serious concern of multimedia content providers is the ease of producing digital copies, and their perfect quality. For rights holders, illegal copying implies serious financial loss. The International Intellectual Property Alliance (IIPA) estimates the annual lost revenues in the U.S. motion picture industry due to piracy at US$1.3 billion, and for the record and music industries at US$1.7 billion [1].

Thus, it is very obvious that multimedia distribution systems need to provide protection. This can be achieved by employing digital rights management (DRM) systems, designed to control and restrict access to multimedia data. This typically includes encryption, access control, and key management. Many DRM systems also include copy control mechanisms and interface billing systems. Copy control or prevention is difficult to achieve, especially in open systems. Identification and back-tracing of individual copies of multimedia data (similar to serial numbers for computer software) have been proposed as a last line of defense against unauthorized copying. It cannot prevent copying, but it can at least help identify the source of pirated copies, and thus enable legal action. A key technology used in DRM systems for data identification, and also for copy control, is digital watermarking.

0163-6804/00/$10.00 © 2000 IEEE

We will introduce the principles of digital media rights management systems, including the presentation of some recent DRM standardization efforts. The principles of watermarking technology are explained, and we clarify the relationship between DRM and watermarking, as well as e-commerce applications. Mobile DRM is specifically emphasized as we summarize and conclude the article.

Digital Rights Management for Multimedia

Digital Rights Management Principles

Generally speaking, a DRM system enables the secure exchange of intellectual property, such as copyright-protected music, video, or text, in digital form over the Internet or other electronic media, such as CDs, removable disks, or mobile networks. DRM allows content owners to distribute securely to authorized recipients and gives them control over the whole distribution chain. This includes:

- Encryption of the content or parts in order to disallow uncontrolled access
- Decryption key management
- Access control (conditional access) according to flexible usage rules. A strength of modern DRM systems is that the usage rules can be adapted to the business models. For example, access can be restricted to certain users, a limited time, or a limited number of accesses. The access right can also be traded, for example, against customer information or the agreement of the customer to receive advertisements. Initial access to the data may even be free (e.g., the first playback of an audio track), while subsequent access has to be paid for.
- Interface to billing systems or mechanisms. Since most business models for media distribution involve monetary transactions, the DRM system must be able to trigger those transactions.
- Copy control or copy prevention. Depending on the usage rules, no/one/several/unlimited copies of the multimedia data are allowed, with or without the right to produce copies of the copies. The DRM system enforces those copy restrictions. For some usage rules, copy control is difficult to achieve and requires sophisticated technology like watermarking. Watermarking is discussed later.
- Identification and tracing of multimedia data. Since authorized users of multimedia usually have access at least to an analog version of the data (e.g., an audio track played back from a speaker, or a video rendered on a display), they could at least produce copies from that analog output. Thus, analog copies in general can hardly be prevented. For some applications it is a requirement to have the possibility to identify and trace back analog and digital copies of distributed media. This can be done by individual digital watermarking (fingerprinting) of the distributed data and is then also part of the DRM system.

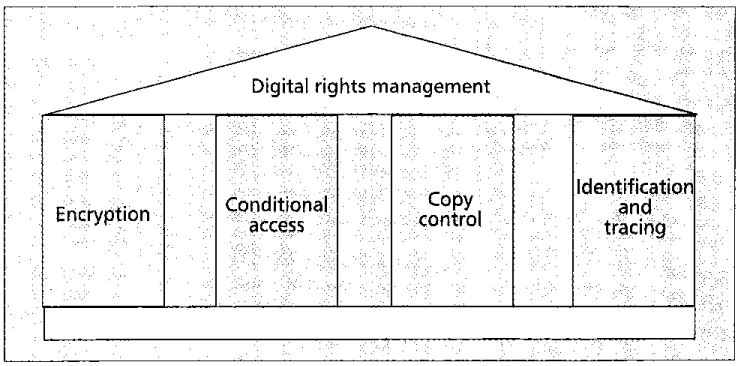


Figure 1. *The DRM pillar model.*

Figure 1 shows the main components of a DRM system. Like a cryptographic system, any DRM system is as strong as its weakest component.

It now has been widely realized that DRM is a required core ingredient of multimedia distribution, which is why several standards bodies are active in that area and complement the available proprietary solutions. They either define the whole DRM system, or interfaces and application programming interfaces (APIs). Some important standardization groups and bodies that have been working on DRM systems are the International Organization for Standardization (ISO) MPEG, Secure Digital Music Initiative (SDMI), DVD/Copy Protection Technical Working Group (CPTWG), *C, Open Platform Initiative for Multimedia Access (OPIMA), Digital Video Broadcasting (DVB), Digital Audio-Visual Council (DAVIC), Bluetooth Special Interest Group, and TV anytime.

MPEG-4 DRM Standardization

In MPEG-4 — ISO/International Electrotechnical Commission (IEC) 14496 — an Intellectual Property and Management (IPMP) framework has been standardized [2]. The idea is to tightly integrate *hooks* into the system to which a proprietary DRM system can attach. Content is generally either stored in a cryptographic container or encrypted in real time (for streaming applications). The decryption keys and rules for usage of the content can be either included in the container or distributed separately, depending on the requirements of the application. In MPEG-4, all encoded media objects (audio, video, video objects, 3D face animation streams, 3D objects, etc.) are accompanied by metadata called *object descriptors* (ODs). Part of an OD is the *IPMP descriptor* (IPMP-Ds) which carries information relating to rights management. General DRM information not related to specific objects is carried in *IPMP elementary streams* (IPMP-ESs). IPMP-Ds and IPMP-ESs provide a communication mechanism between IPMP systems and the MPEG-4 terminal. Certain applications may require multiple IPMP systems. When MPEG-4 objects require management and protection, they have IPMP-Ds associated with them. These IPMP-Ds indicate which IPMP systems are to be used, and provide information to these systems about how to manage and protect the content.

Unlike for MPEG-4, the properties of the DRM itself (but not the realization) are part of the specification. The SDMI specification is built around portable devices and portable media that store and play back protected audio content.

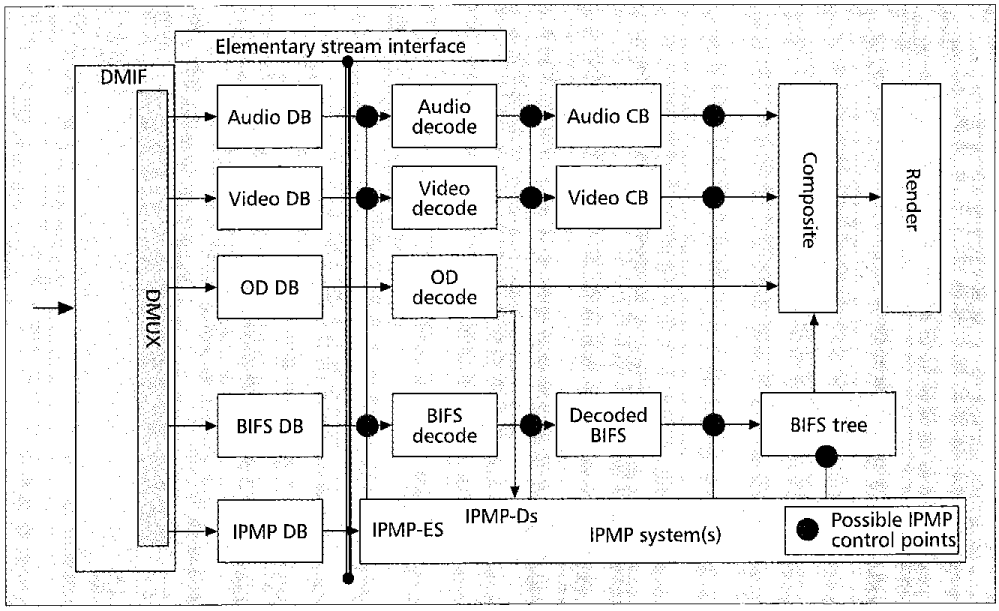


Figure 2. *The IPMP framework in the ISO/IEC 14496 terminal architecture.*

Figure 2 indicates a variety of hooks (control points) in the MPEG-4 terminal at which one might desire IPMP control. Many systems apply control between demultiplexing and the elementary stream decoders. There are also systems that need to apply control after stream decoding. For example, retrieval of watermarks introduced prior to content encoding can only be done after content decoding. In general, the IPMP control points involve different kinds of mechanisms ranging from rule processing to decryption to watermarking. The actual processing of this control occurs in the IPMP system.

Besides enabling owners of intellectual property to manage and protect their assets, MPEG-4 provides a mechanism to identify those assets via the *Intellectual Property Identification Data Set* (IPI Data Set). The IPI Data Set identifies content either by means of internationally standardized media numbering systems, such as International Standard Recording Code (ISRC), International Standard Audio-Visual Number (ISAN), ISBN, or Digital Object Identifier (DOI), or by privately generated key/value pairs (e.g. »Artist«/»The Beatles«). The IPI Data Set can be used by IPMP systems as input to the management and protection process. For example, this can be used to generate audit trails that track content use.

In the following, an example is given of how an MPEG-4 IPMP systems may work for an MPEG-4 stream being delivered to a client. The client contains an MPEG-4 IPMP system, or, in our terminology: a DRM system. First the client is initialized. This includes initialization of the audio-visual scene description (BIFS), ODs, and IPMP-ESs. The client contains a DRM system that includes a certified public/private key pair used to establish and maintain a cryptographic relationship between client and server. The DRM system also includes a public key decryption engine, a block cipher for bulk decryption, and cryptographic hash functions. The system may contain mechanisms to securely oversee various rules for managing use of the content. It also contains implementations of the client side of key management protocols. When the client requests the delivery of the MPEG-4 scene (consisting of MPEG-4 objects and their spatio-temporal relations), the client and server execute a bilateral authentication protocol to establish an authenticated secure channel. As part of the authentication, a session key is exchanged. Once the channel is established, the content decryption keys and any other required information (e.g., payment and consumer preference information) can be transmitted securely and confidentially (encrypted with the session key). The server delivers the content decryption keys to the client (encrypted with the session key). These keys are delivered via IPMP-ESs. The mapping of keys and content is accomplished by IPMP-Ds associated with the content. The client's DRM system extracts the content decryption keys from the IPMP-ESs. They are subsequently used to decrypt content protected with these keys.

Once all keys are exchanged and established, the stream managers parse the relevant ODs and determine which content streams are protected. The DRM system will handle the IPMP-Ds associated with these streams. Contained information is, for example, which keys or usage rules to use to manage the particular stream. After the usage rules are successfully processed, the content is decrypted and the clear-text content is forwarded to the appropriate decoders for further rendering.

The SDMI Portable Device Specification

SDMI is an industry consortium that has been defining an open standard for audio DRM. The initial focus was on portable hardware devices. This is also reflected in their first specification, the Portable Device Specification Part 1, Version 1.0 [3], which specifies a system for secure

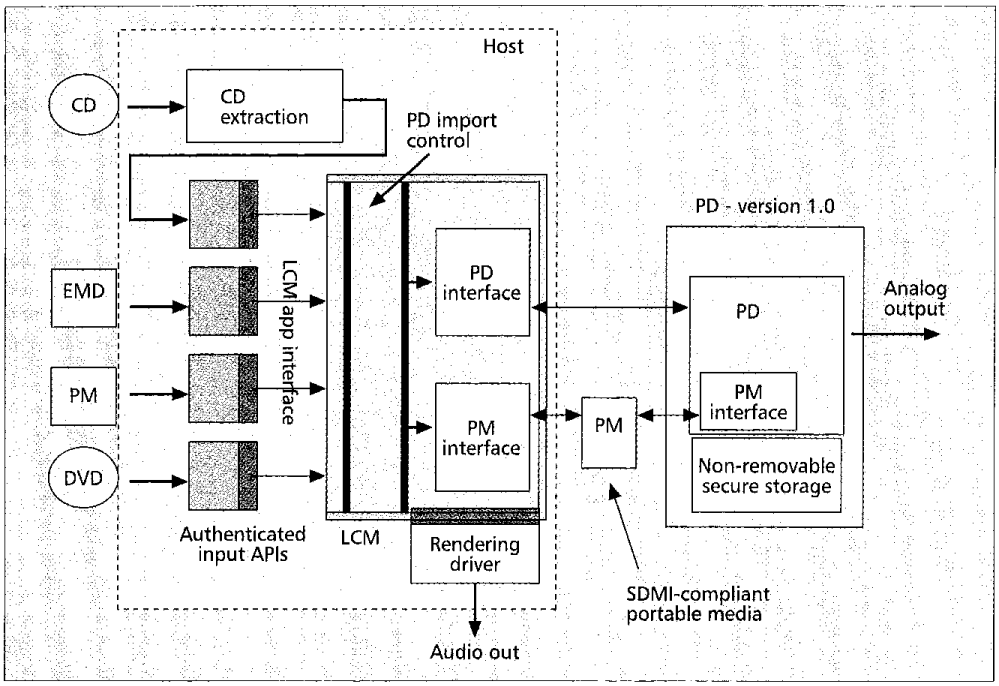


Figure 3. *An architectural overview of the SDMI portable device concept.*

Some of the required functions of a comprehensive DRM system are that unremovable information be attached to multimedia data. A digital watermark is such information invisibly attached to multimedia

music distribution with built-in DRM capabilities. Unlike for MPEG-4, the properties of the DRM itself (but not the realization) are part of the specification. The SDMI specification is built around portable devices (PDs) and portable media (PM) that store and play back protected audio content. *Licensed compliant modules* (LCMs) act as interfaces between applications and PDs/PM. The specifications require that any SDMI content be protected at all times after it first gets imported into an SDMI application or LCM, or recorded onto an SDMI PD. Subsequent storage or transfer of the content must be done such that the protection is maintained. SDMI applications, PDs, or LCMs must respect any usage rules connected to the content. Unknown content (like the audio content existing today) can be checked in into an SDMI PD, but it cannot be copied again. The specification also contains requirements related to authentication of applications or devices, secure communications between SDMI-compliant components, portable media, built-in microphones, copy mechanisms, and screening methods. The purpose of screening is to provide mechanisms to detect illegal copies. SDMI screening technology is still under evaluation and will provide mechanisms that enable SDMI components to recognize illegal copies. Such components will then refuse to import, transfer, or play illegally distributed SDMI content. Screening technology will be based on digital watermarking.

Figure 3 shows the architecture of an SDMI system with server (host), portable playback device (PD), PM, and LCM interfaces.

Currently, the SDMI consortium is evaluating how mobile devices like mobile phones fit into the SDMI concept and PD specification. Basically, this means mapping a mobile network structure onto the SDMI server-LCM-PM-PD model and defining special rules allowing built-in microphones (which are not allowed in the portable device specification).

Watermarking Technology

Some of the required functions of a comprehensive DRM system, such as copy control and data identification and tracing, require that unremovable information be attached to multimedia data. A digital watermark is such information invisibly attached to multimedia data. The basic requirements it has to fulfill are:

- *Imperceptibility* — The watermark must not impair the perceived quality of the data.
- *Security* — The watermark should only be accessible by authorized parties.
- *Robustness* — The watermark must persist in the data after manipulation, including malicious manipulation with the intent to remove the watermark.

Related techniques for secret and unsuspicious hiding of information in other host data are well known for analog and digital media. These are referred to as *steganography* or *data hiding* techniques. The main difference from watermarking is that watermarking has the additional notion of robustness against attempts to remove the information. This robustness is typically paid for by a much lower amount of information that can be hidden within the host multimedia data.

The basic idea of watermarking is to apply very slight changes to the individual basic entities (samples, pixels, etc.) of the data in order to ensure imperceptibility. On the other hand, small changes are potentially vulnerable to manipulations and attacks. Therefore, the watermark information is spread over the host data.

Watermarking is not a "stand-alone" technology. It is only useful as a system component, with the most important application being DRM and copyright protection in general.

Figure 4. *A digital image (left) and the watermarked version (right).*

For example, 1 bit of watermark information may be embedded into several thousand (or even millions) of pixels of an image. In order to prevent the watermark from being accessible by unauthorized parties, since such access would also potentially allow attacks, some sort of secure cryptographic key is typically used. It is also for that reason that watermarks are usually pseudo-random and noise-like. The noisiness prevents the watermark from being detected. Since real-world signals like images and video typically also contain some noise, the watermark can be hidden in that noise.

Most practical watermarking schemes employ so-called spread spectrum methods. The idea of spread spectrum communications, as used in code-division multiple access (CDMA) radio communication systems, was originally developed for secure and unobtrusive radio communication. The underlying problem there is similar to that in watermarking: a narrowband signal (the watermark information) has to be transmitted via a wideband channel that is subject to noise and distortion (the multimedia host data, e.g., video or audio). The basic principle of spread spectrum watermarking involves the following steps:

- Repetition of the watermark information bits[1] to be embedded
- Modulation (i.e., multiplication) of the resulting bit sequence with a pseudo-noise signal drawn from a random number generator
- Addition of the resulting signal to the multimedia signal to be added

Figure 4 shows, as an example, a digital image and its watermarked version (in this case, the watermark amplitude is around 1 percent of the image luminance amplitude). Recovery of the embedded watermark information is only possible with knowledge of the pseudo-noise signal that has been used for modulation. The basic principle of spread spectrum watermark recovery employs a correlation principle and involves the following steps:

- Subtraction of the original host signal from the watermark-host signal mixture, if available
- Demodulation (i.e., multiplication) of the resulting signal with the same spread spectrum signal used for embedding
- Summation over all samples of the resulting signal that belong to 1 bit of watermark information
- Threshold decision: if the sum is negative, the watermark bit is –1; otherwise, it is +1

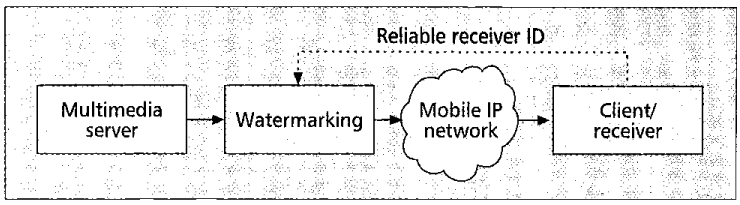
Building on the basic spread spectrum principle, various watermarking methods have been proposed. Many of them embed the watermark into transform coefficients of the signal, rather than into the signal itself; for an overview, see [4–8]. Also, several extensions for increased robustness against malicious attacks have been proposed, and today mature methods exist that are reasonably robust against malicious attacks [6] and modifications like format conversion or digital-to-analog conversion.

Watermarking for E-Commerce Applications

Watermarking is not a standalone technology. It is only useful as a system component, with the most important application being DRM and copyright protection in general [8]. MPEG-4 IPMP and SDMI screening are only two examples of DRM systems that use watermarking or are favorably used with watermarking. DVD is another example [1, 9]. The DVD copy control mechanism uses watermarking to embed in-band signals carrying such information as "copy once" or "copy never" flags. The watermark is tied to the individual serial number of the disk. Standard-compliant players will then refuse to play back unauthorized copies. It should be pointed out that today's watermarking methods have reached a certain level of maturity, but they are not as secure as modern cryptography. Thus, they should still be regarded as the weak pillar

[1] *As usual in spread spectrum communications, the two possible states of a bit are denoted by -1 and +1, in order to receive mean-free signals. For details, see [6].*

of a DRM system. Another problem for DRM systems is that the identity of the receiver is often either unknown or unreliable (e.g., in Internet media distribution systems). Individual identification of distributed multimedia copies only make sense, however, if the receiver can be identified reliably. The situation is fortunately different for mobile media distribution.



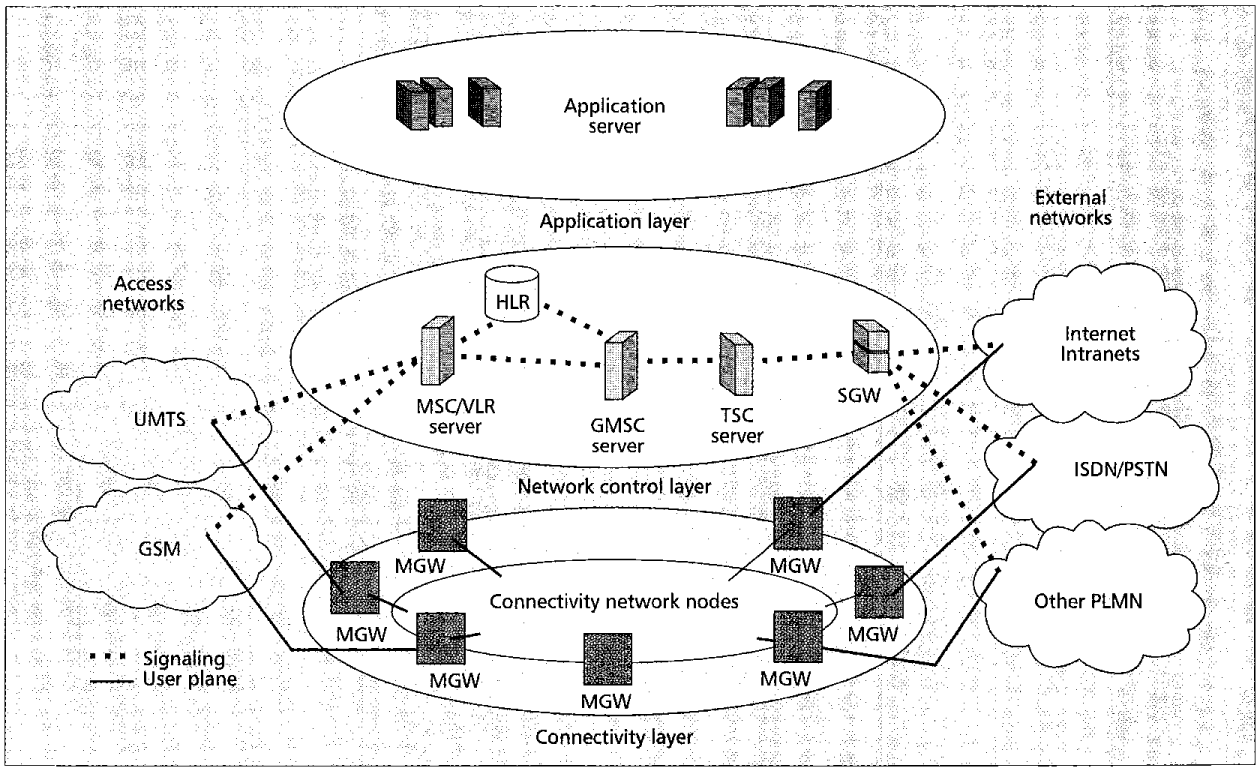
■ **Figure 5.** *Embedding a reliable receiver ID in media distribution applications in mobile networks.*

MOBILE DRM

With the increasing popularity of wireless data services, especially in high-rate mobile networks like GPRS and UMTS, mobile e-commerce (m-commerce) is also becoming increasingly important. An important ingredient of m-commerce is wireless media download and streaming, such as video, audio, or e-books, that can be purchased from and downloaded to a wireless terminal like a smart phone, a communicator, or a laptop connected to the mobile network.

Unlike in the fixed Internet, mobile terminals provide much more reliable information about the identity of the user. The mobile terminal serial number (e.g., the IMEI in the Global System for Mobile Communications, GSM) and, even more, the phone number or identity (e.g., the International Mobile Subscriber Identity, IMSI, in the GSM system) are usually tightly bound to an individual user known to the network provider. This information can be used for watermarking and data identification purposes (Fig. 5), thus avoiding a weakness of Internet DRM systems. In the layered mobile network model, as depicted in Fig. 6, this would imply that the application server which provides the multimedia distribution system, including the DRM system, requires information present in the network control layer. The mobile switching center/visitor location register (MSC/VLR) stores information about roaming mobile users, including their IMEI and IMSI in the GSM system, or similar information in other mobile systems. If the application server has access to that user information, and maybe even additional geographic location information, this information can be used for better enforcement of media rights using DRM systems.

Thus, watermarking for media individualization and identification makes much more sense in wireless networks and for m-commerce than in the fixed Internet, where reliable customer identification is often not possible. This has an impact on business models for media distribution. Due to the feasibility of individual watermarking, pirated copies of data can be traced back to the individual pirate, unlike in the Internet. Thus, fraud and illegal copying can be prevented to a higher degree, and lost revenues due to pirated copies are likely to be lower than in the fixed Internet. Thus, mobile networks are, from a DRM point of view, an



■ **Figure 6.** *A layered mobile network model.*

Watermarking for media identification and copy control is feasible in mobile networks, and is likely to decrease piracy of media distributed over mobile networks. This impacts business models for digital media distribution.

attractive distribution channel for multimedia content providers. This will be even more evident with the convenient bit rates available for multimedia services in future networks like GPRS and UMTS.

Another advantage of mobile DRM systems compared to Internet DRM systems is that rights management and protection is potentially more secure in more closed environments. This means that telecommunications devices like phones are potentially less vulnerable to attacks against DRM systems than totally open systems, like PCs as used in the Internet.

A drawback is that mobile DRM implies additional data traffic between the network and the terminal (e.g., for cryptographic key management), and additional complexity in the terminal, mainly due to decryption and deciphering. For compressed multimedia data (e.g., MPEG-4 video), applying only partial encryption of the media may reduce decryption complexity.

CONCLUSIONS

With digital media taking a steadily increasing share of the media market, digital rights management has been recognized as a required system component that protects businesses and business models. DRM systems allow content providers and publishers to control the whole distribution chain and apply flexible usage rules. Copy control and media identification and tracing are also important components of DRM systems. Watermarking is the key technology used for copy control and media identification. One major reason that watermarking for media individualization/identification and prevention of piracy is not much used in the Internet is that information about the identity of Internet users is usually not reliably available.

This is different for mobile networks and mobile media distribution, because in mobile networks the identity of the user is known (in terms of subscriber identity). Thus, watermarking for media identification and copy control is feasible in mobile networks, and is likely to decrease piracy of media distributed over mobile networks. This impacts on business models for digital media distribution, and it seems that mobile networks are specifically suitable for media distribution from the media security and DRM points of view. The complexity of DRM systems, mainly of decryption/deciphering, is still a technical challenge, but will become less important with increasing processing capacity of mobile devices.

REFERENCES

[1] M. Miller, I. J. Cox, and J. Bloom, "Watermarking in the Real World: An Application to DVD," *Proc. Wksp. Multimedia and Security at ACM Multimedia 98*, Bristol, U.K., Sept. 1998.

[2] J. Lacy, N. Rump, and P. Kudumakis, "MPEG-4 Intellectual Property Management & Protection (IPMP) Overview and Applications," MPEG doc. ISO/IEC JTC1/SC29/WG11/N2614, Dec. 1998.

[3] SDMI, "SDMI Portable Device Specification, Part 1, Version 1.0," SDMI doc. pdwg99070802, July 1999; http://www.sdmi.org/.

[4] M. Kobayashi, "Digital Watermarking: Historical Roots," Tech. rep., IBM Research, Tokyo Res. Lab., April 1997.

[5] F. Petitcolas and S. Katzenbeisser (Eds.), *Information Hiding Techniques for Steganography and Digital Watermarking*, Artech House, 2000.

[6] F. Hartung and M. Kutter, "Multimedia Watermarking Techniques," *Proc. IEEE*, vol. 87, no. 7, pp. 1079–1107, July 1999.

[7] J. K. Su, F. Hartung, and B. Girod, "Digital Watermarking of Text, Image, and Video Documents," *Computers & Graphics*, vol. 22, no. 6, Feb. 1999, pp. 687–95.

[8] F. Petitcolas, R. Anderson, and M. Kuhn, "Information Hiding — A Survey," *Proc. IEEE*, vol. 87, no. 7, July 1999.

[9] I. J. Cox and J. P. Linnartz, "Some General Methods for Tampering with Watermarks," *IEEE JSAC*, vol. 16, no. 4, May 1998, pp. 587–93.

BIOGRAPHIES

FRANK HARTUNG [M] (frank.hartung@eed.ericsson.se) received a Dipl.-Ing. degree from the Technical University of Aachen, Germany, and a Ph.D. from the University of Erlangen, Germany, both in electrical engineering. Since 1999, he has been a senior researcher with Ericsson Research, Ericsson Eurolab Deutschland GmbH, Aachen, Germany. His research interests include video streaming, mobile multimedia systems, mobile digital rights management, mobile e-commerce, and video compression.

FRIEDHELM RAMME is manager of applications research at Ericsson Eurolab Germany and coordinates mobile e-commerce research at Ericsson on the corporate level. He studied computer science at the University of Paderborn. From 1991 to 1998 he was employed at the Paderborn Center for Parallel Computing, where he finished his Ph.D. in April 1997. He has published several papers on parallel computing topics at international conferences and in scientific journals. His research interests include services infrastructure solutions for telecommunication networks, design of parallel multimedia systems, and mobile e-commerce applications.