Survey on the Technological Aspects of Digital Rights Management

William Ku and Chi-Hung Chi

School of Computing, National University of Singapore
3 Science Drive 2, Singapore 117543, Republic of Singapore
{kucheech, chich}@comp.nus.edu.sg

Abstract. Digitalization of content is both a blessing and a curse. While it allows for efficient transmission and consumption, the ease of copying and sharing digital content has resulted in rampant piracy. Digital Rights Management (DRM) has emerged as a multidisciplinary measure to protect the copyright of content owners and to facilitate the consumption of digital content. In this paper, we survey the technological aspects of DRM. We present a discussion of DRM definitions, formulate a general DRM model and specify its various DRM components. We also evaluated emerging trends such as the use of P2P in DRM and DRM for personal access control, some noteworthy issues such as content reuse and granularity, as well as citing some future directions such as frequent content key upgrades.

1 Introduction

The Internet has emerged as a vibrant information and digital entertainment hub. Other than being a hyper distribution channel for its easy and efficient dissemination of content, it also facilitates the synergy of digital technologies to provide a richer user experience. However, it has some drawbacks. The ease of copying and sharing of digital content such as music, without any deterioration in quality, has resulted in rampant piracy. Consequently, the content owners stepped in to tap on the unlimited potential of the Internet as well as to curb this piracy with technological and legal measures. One of such measures is Digital Rights Management (DRM).

DRM is basically an aggregation of security technologies to protect the interests of the content owners so that they may maintain *persistent* ownership and control of their content. A DRM system essentially specifies, manages and enforces "rules" in all aspects of the digital content, in particularly in its usage and distribution. The nature of these restrictions is such that existing DRM systems are typically closed proprietary systems. Digital content is packaged in proprietary data formats ("containment[1]") or/and marked and only accessible by proprietary trusted hardware/software, resulting in exclusion of certain users and non-interoperability between different DRM systems. In addition, the restrictions may hamper legitimate uses such as accessing the digital content on multiple devices or doing a backup.

[1] We would focus on the "containment" approach.

K. Zhang and Y. Zheng (Eds.): ISC 2004, LNCS 3225, pp. 391–403, 2004.

DRM systems do also present certain user issues such as privacy and the notion of fair use. Users may not be able to consume the digital content anonymously. In addition, DRM systems could be easily used to profile users' consumption behaviour.

Content reuse may be promoted in DRM but does the present infrastructure support it and if so, to what extent? How could the same content and DRM technologies cater to heterogeneous devices with varying computing capabilities. We hope to find out how DRM addresses these issues from a technological point of view.

2 Definition and Overview

In this section, we would first look at some definitions of DRM followed by an overview of a DRM system.

2.1 Definition

There is an apparent lack of a standard definition of DRM in current literature. Some definitions are:

- DRM refers to *controlling* and *managing* rights to digital intellectual property [27].
- DRM is the description, identification, trading, protection, monitoring and tracking of all forms of rights usages over both tangible and intangible assets including management of rights holders relationships [12].
- DRM must be about the "digital management of rights" not the "management of digital rights" [9,12].

The definition of DRM can be further classified into two categories namely *management* and *enforcement* [13,28]. Management has to do with the managing of digital rights. The rights holders have to be able to identify their content, provide the meta-data of the content (so that users can trace originality), specify the terms and conditions of usage and distribution of the content and etc. Enforcement is about the digital managing of the rights which is to ensure that the content is only used as stipulated in the terms and conditions associated with its usage.

2.2 Overview

Here, we present an overview of a typical DRM system. There are essentially three parties in the setup illustrated in Figure 1, namely the *Content Owner*, the *License Broker* and the *User*. The Content Owner usually owns all rights to the content. It may refer to a music label or a solo digital artiste. The License Broker handles all transactions, on behalf of the Content Owner, pertaining to the issue of a License that would specify exactly the permissions granted to an User on the use of the content, subject to certain terms and conditions. The User[2] here refers to a trusted hard-

[2] We would also refer it as the End-User Player (or Viewer) in this paper.

ware/software that is a proxy to the user (consumer). It is trusted in the sense that it would not allow the user unauthorized access to the content. It would also enforce the terms and conditions of the usage of the content. We outline the process of this DRM system:

1. The Content Owner would input the Content to the DRM system for Content Protection. In some cases, the Content Owner may be required to encode the Content in some proprietary data format. Here, the Content Owner may want to insert a digital watermark into the Content for purposes of identification. The DRM system would then encrypt and packaged for distribution. The Content Owner would need to specify, using a Rights Expression Language (REL), all applicable usage rights or rules that apply to this content.
2. The DRM system would return a Protected Content and a License (or one set of Licenses). The License contains a key that is needed to decrypt the Protected Content and must be used as a whole to access the content.
3. The Content Owner disseminates the Protected Content through various distribution channels including but not limited to the Internet, physical mediums such as CDROM/DVD, Email, Instant Messaging and P2P file-sharing. Distribution through the latter three media forms the notion of Superdistribution [17].
4. The Content Owner sends the License(s) to the License Broker. The License Broker is a trusted clearinghouse which would handle all requests for content access.
5. The User retrieves the Protected Content from a distribution channel. It examines its meta-data to identify the required License in order to access the content and the (location of) License Broker(s) that could provide the License.
6. If the user (consumer) does not the have the required (or a valid) License, the User would contact a License Broker to request for a License and making the requisite payment.
7. After the user has made payment, the License Broker would issue a License to the User. Depending on what the user (consumer) has paid for, the User would allow the user to access the content in a controlled manner.
8. The License Broker would remit to the Content Owner the proceeds from the transaction.

3 Components of DRM Systems

In Figure 1, we have a Content Protection "black box" that could be deciphered as shown in Figure 2 which also illustrate the main components of existing DRM systems:

1. The content is tagged with an unique identifier (identification) together with descriptive meta-data (meta-data).
2. A digital *watermark* is inserted into the content to serve as a proof of ownership identity in the event of a dispute.
3. A digital *fingerprint* is generated from the content. In addition to its forensic application for authentication (like watermarking), it has uses such as automatic content identification. This fingerprint is then stored in a database.

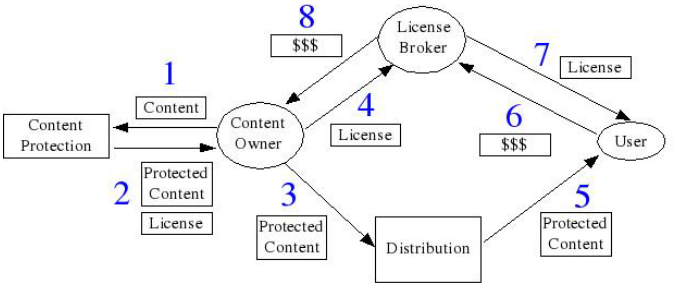

Fig. 1. Overview of a typical DRM system

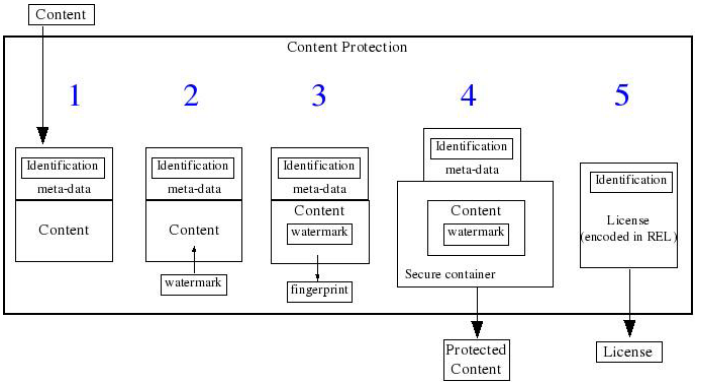

Fig. 2. The Content Protection Process

4. The content is enclosed by a *Secure Container* which would effectively prevent unauthorized access.
5. A License stating the rights and conditions of content usage is encoded in a Rights Expression Language (REL).

3.1 Content Identification and Meta-data

Before the rights of a content can be fully asserted, it has to be unambiguously identified so that users who want to access the content can purchase the usage rights of this content. The meta-data of the content may provide some non-sensitive information and may describe how to make use of the content identifier.

Content Identification. Other than being unambiguous, the content identifier has to be *persistent*. That is to say, even if the ownership of the content changes, the content identifier would remain the same. Existing uses of standard numbering schemes in DRM include ISBN, ISSN, ISAN and DOI [8].

Meta-data. Meta-data complements the use of the content identifier. The content identifier is likely to be an alphanumeric string which on its own, would not make any sense. The meta-data can provide more information on how to access the content. An example of a well-formed meta-data scheme is the <indecs> framework [14].

3.2 User Identification/Authentication

User identification/authentication is important in DRM as we would want only authorized users to be able to access the content. This is not an issue for certain closed systems such as mobile phone networks whereby the identity of the user is closely tied to his device but rather for semi-open networks such as the Internet. The significance here is that the difficulty in user identification resulted in most DRM systems for semi-open networks having to bind content to a specific device instead of to user.

User identification/authentication can be generally delegated to the License Brokers which could then use mature e-commerce technologies such as SSL to overcome user identification/authentication concerns.

Nevertheless, there are some work on user identification and authentication issues in the DRM context. [16,24] outline some sample applications where biometric technologies can successfully be applied to DRM applications. [7] presents a framework to hide the identity of an user by concealing the user's public key with a hash function.

3.3 Digital Watermarking

Watermarking is a technology that can be used for copy control, content identification and tracing. Most watermarking techniques use a spread spectrum approach which is essentially the insertion of a pseudo-noise signal with a small amplitude into the content (directly onto the content itself or onto its frequency domain). This watermark can be detected using correlation methods and often used in conjunction with a secret key so that the watermark can only be detected and removed by authorized parties.

In DRM, content is typically vulnerable to attacks at the end-user system. The content could be captured during its rendering (audio and video grabbing) or have its protection mechanism (its Secure Container) removed by direct attacks. Watermarking can be used to detect illegal copies of content that have been unprotected by such attacks. The basic requirements [11] of a watermark are:

- imperceptibility: the watermark must not affect the perceived quality of the content
- security: the watermark should only be accessible by authorized parties
- robustness: the watermark must be persistent and resilient to attacks

In the DRM context, the watermark must be able to survive indirect attacks such as audio and video grabbing. This requirement is not applicable in direct attacks since only the associated protection mechanism (the Secure Container) is removed but not the watermark. Nevertheless, the unprotected content at this junction could be subject to attacks to remove the watermark in it.

[3] provides an overview of data hiding in DRM. Firstly, in dealing with the proof of ownership, a watermark can be used to serve as a proof of ownership but is vulnerable to attacks such as average and collusion attacks. [33] highlights some possible collusion attacks and solutions. In addition to ensuring that a watermark cannot be removed, the DRM system has to ensure that a fake watermark cannot be inserted. [3] further discusses on how watermarking features in tracing and copy control mechanisms.

[1] introduces a formal framework that enables the rigorous assessment of the security of watermarks against protocol attacks. In addition, it shows how watermarking schemes can be secured against some protocol attacks by using a cryptographic signature of a trusted third party.

3.4 Content-Based Identification (Fingerprinting)

Content-based identification (Fingerprinting) refers to the characterization of the content based on its representation (signals or features) and matching it to an entry in a database. The term fingerprinting has been used interchangeably with watermarking in current literature and presents some confusion. We would differentiate these two terms here as tabulated in Table 1.

Table 1. Fundamental differences between watermarking and fingerprinting

Watermarking	*Fingerprinting*
Embeds a signal into content, altering the content.	Does not embed a signal into content and hence does not alter content.
Not a function of the content.	A function of the content.
Usually invisible for non-intrusion and to avoid detection by adversaries.	No such requirement. Non-intrusive.
Requires prior access to content.	Does not require prior access (other than for database entry). May be used for "legacy content".
Can watermark individual copies.	Does not have this capability.
Have to reprocess all copies in event of new technology.	No such requirement.
No additional treatment for new content.	Have to store fingerprints of new content in database.

Typically, fingerprinting has two processes. The first is the training phase whereby characteristic features of the content are extracted and compacted for entry into a database. The second process is the recognition phase which is essentially a pattern recognition process to match the fingerprint of a given content to an entry in the database. Some essential requirements of fingerprinting techniques are robustness and compactness. Robust fingerprinting techniques would be able to associate content derivations or deviations with the original content. By being compact, fingerprinting will allow for fast fingerprint extraction, search and matching.

Watermarking and fingerprinting are meant to complement one another. Fingerprinting may prove to be of assistance when attacks against watermarking succeeded (for example in audio and video grabbing) and the watermarks are removed. Robust fingerprinting techniques would still be able to identify the content so long as the characteristics features of the content remain. This is useful considering that illegal content are usually lossy copies of the original content.

Some applications of fingerprinting are broadcast monitoring and filtering. Broadcast monitoring refers to the automatic playlist generation of content in the various distribution channels for auditing purposes such as royalty collection. Filter-

ing here refers to the identification of certain content for certain purposes. For example, Napster introduces a fingerprinting system to filter and remove copyrighted content in accordance with a court order.

Fingerprinting also has non-forensic uses. A popular use case in current literature is that of an user in a pub who likes the music being played, activates a personal device (possibly a mobile phone) to identify the music and to buy a copy of it. When the user goes back home, he would find the song downloaded (and billed for) into his digital music player.

Images. [18] presents a hash algorithm based on the observation that main geometric features in an image would remain approximately invariant under slight lossy changes.

Audio. Audio fingerprinting techniques fall into two main categories [31]. The first category refers to techniques that make use of the descriptive attributes of the content such as loudness, tempo, pitch etc while the second category includes approaches that are based on more intrinsic attributes of a recording with no explicitly identifiable descriptive qualities. An example technique of the first category is based on MPEG-7 [2]. Here, the *spectral flatness* (SFM) (related to the presence of tonal components within specified octave sub-bands) of the audio signal is used as a fingerprint. One example of an audio fingerprinting technique belonging to the second category is the MusicDNA system [30]. It essentially involves computing features from the time-frequency spectra of a recording. Further discussion of audio fingerprinting can be found in [4,5].

Text. Text fingerprinting have its roots in Natural Language Processing which has mature techniques for text and document feature characterization and classification. An example of text fingerprinting can be found in [30] which presents a way of fingerprinting text documents that can be used to identify content and expression similarities in documents, using surface, syntactic, and semantic features of documents. It claimed an accuracy of 90% and 67% for translated copies.

3.5 Secure Containers

Secure Containers are usually implemented in the use of cryptographic algorithms such as DES or AES. However, a combination of such algorithms (by way of obfuscation) may be used instead to provide further obscurity as shown in Microsoft audio DRM [29]. Coupled with the use of digital signatures and certificates, Secure Containers provides content confidentiality and integrity. The content integrity can be further enhanced by mechanisms generic to the content such as LAIR [9].

3.6 Rights Expression Languages

Rights Expression Languages (RELs) are used to articulate the usage rules of a content. These usage rules form the basis of the contract between the user and content owner pertaining to the use of the content. The usage of RELs can be mainly found in the meta-data of the content and its associated content. Thus, RELs have to be machine-readable (for interoperability) and extensible (in order to cater to all possible scenarios). Naturally, XML is the choice of language of existing RELs.

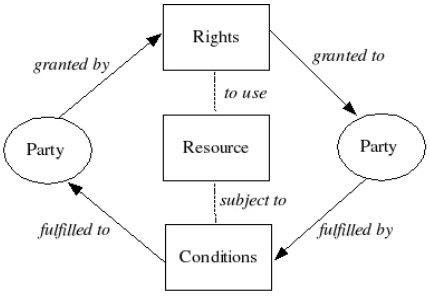

Fig. 3. Building blocks of the rights language concept in a REL

A REL has two distinct components: the *rights language concept* (syntax) and the *rights data dictionary* (semantics). The rights language concept refers to the grammar rules while the rights data dictionary refers to the ontology that provides meanings to the terms used in the grammar rules. Generally, the basic building blocks in the rights language concept of most RELs are enumerated as follows:

- Rights: the permissions allowed in the usage of the *resource*. This includes the *restrictions* of usage such as limited times of usage etc.
- Conditions: the prerequisites that need to be fulfilled before the *rights* can be exercised
- Resource: the content in question, which is to be unambiguously identifiable.
- Parties: the principals involved.

These basic building blocks and their relationships are illustrated in Figure 3.

Two widely accepted RELs are XrML [34] and ODRL [22]. XrML is being used by MPEG-21 [19], the OASIS Rights Language Technical Committee [21] and the Open eBook Forum [23] while ODRL is employed by the Open Mobile Alliance [25] as the standard REL for all mobile content.

License. A License can be generally encoded in a REL and contains the following elements:

- Content Identifier
- Optional user information
- Rights and restrictions: The exact terms and conditions of usage.
- Stateful information: To monitor the use of the content, possibly for the purpose of restrictions (for example limited number of access).
- Content key(s): To be kept secret.
- Authentication information: To provide for the decryption of the content key(s) and the binding of the License to the End-User Player. This may also allow the License to be modified by authorized parties. The integrity of the License is also based on this.

The License has to specify the rights accorded to the user, which have to be expressed in a REL. The License is to be bound to a device so that the License is not directly transferable across devices. Thus, individualization of the End-User Players is required so that Licenses can be constructed uniquely to the End-User Players.

The End-User Player

The End-User Player[3] (EUP) is a trusted unit in the DRM system (illustrated as the User in Figure 1) that enforces the rights of the content. With reference to Figure 3, the End-User Player assists the user to procure the *rights* to access the contents by getting the user to fulfill the required *conditions*. It also make sure that any *restrictions* to the *rights* are adhered to. It can be a hardware (for example Apple's iPod) or software (Microsoft Media Player). The key technical requirements for the EUP are:

- Closed specifications: It is proprietary by extension as the content data format is usually proprietary.
- Individualization: This would bound the EUP to the device and allow for ease of user identification/authentication as well as provides for Licenses to be uniquely bound to the EUP.
- Tamper-resistant: It should be difficult to reverse engineer and be able to resist manipulations.
- Security upgradeable: It should be easily upgraded for security fixes or new security mechanisms.
- Able to detect illegal content: The EUP should be able to detect illegal copies and refuse to render these illegal content.
- Separation of compliant and non-compliant EUPs: Non-compliant EUPs should not be able to render legal content.

We observed that there is little attention paid to the EUP in current literature, despite its relative importance in the DRM system.

4 Trends, Noteworthy Issues, and Future Directions

In this section, we look at some emerging trends in DRM, some noteworthy issues and cite some possible directions in future DRM research.

4.1 Mobile DRM

Mobile devices will form an integral backend for content consumption. There are several issues whereby DRM would have to address. Firstly, there is a wide spectrum of heterogeneous mobile devices that need to be able to interoperate with one another and with other devices such as the PC. Standardization of DRM would help here. Secondly, these mobile devices usually have limited and varying computing capabilities, content granularity (please see Section 4.5) becomes an issue. The DRM containment mechanism (Secure Container) essentially is a one-size-fit-all approach. Thus, what may be rendered in one device may not be similarly rendered in another device.

[3] It is also referred as the device in this paper.

However, mobile devices form a more tightly knitted network than the PCs/Internet. User identification/authentication is almost a non-issue as the mobile device (especially mobile phone) is usually bound to the user. They follow proprietary hardware specifications, making them more tamper-resistant than PCs. Their heterogeneous nature also means that attacks on one platform may not necessarily work on another platform. As such, DRM should be more easily enforced with mobile devices. There are already existing DRM implementations for mobile devices with more to come with the advent of the OMA and market forces.

4.2 DRM Integration with P2P

P2P provides DRM an excellent content delivery platform. There are some pioneer implementations that pave the way for this new paradigm. [26] presents the details of a P2P protocol based on broadcast encryption that supports and enforces renewable content protection for home networks and providing for a careful balance between the needs of content owners and consumers' expectations. [32] presents a similar P2P architecture of set-top boxes. The Potato system [20] is a DRM-enabled P2P system that provides incentives for users to redistribute content.

Integrating DRM into P2P systems is not a trivial exercise. [15] presents a study of some of the issues involved in such a setup. There is certainly much more work left in this aspect. Most probably, a DRM hybrid of P2P networks, the Internet and mobile networks would evolve.

4.3 DRM for Everyone

Existing DRM systems are set up for the benefits of large music labels, Hollywood movie studios and Fortune 500 content providers. There is no provision for the amateur artiste or any individual to make use of DRM to distribute their content.

DRM can be a great way to impose access control over personal content. For example, one may want to share his vacation photos and video among his friends. DRM can actually provide this functionality easily. Taking for instance a DRM-enabled P2P network, the user uploads his content and specifies some usage rules. He may specify that only his intimate friends may access certain photos and the video while others may view the rest. He passes the content to some friends who relay it to his other friends or even some strangers. Those who try to view the content would request for the license automatically. In this way, access control over personal content is achieved.

4.4 Content Reuse and Granularity

We look at the impact of DRM on content reuse and granularity. Content reuse refers the use of caches to minimize retrieval latency of the content while content granularity refers to the availability of the content in multiple resolutions.

Content reuse. Multimedia content accounts for only 20% of web content [6] although this percentage is expected to increase. Content owners often restrict distribution as they do not have access control over the content once it becomes available

in the Internet. DRM offers a new dimension in content delivery both in the Internet and P2P in the notion of Superdistribution. With the assurance from DRM, content owners would release more content into the Internet and P2P, content reuse through the use of caches will have to be re-examined. These content would be large in size and caching large objects is expensive. How then are DRM and the web caches going to accommodate one another?

Content granularity. Granted that there is pervasive use of DRM, content granularity would play a significant role. It would not be practical to expect the Secure Container, a one-size-fits-all approach, to be able to cater to the wide spectrum of heterogeneous devices. For example, a handheld device with limited capabilities would not be able to render a large multimedia content. How can the device take it from there and locate a scaled-down version. Existing DRM systems do not address this. Conversely, a content received from a handheld device may not fully make use of the capabilities of a PC. One possibility is the use of the Content Identifier to locate other versions of the content..

The data format of the content would also play an important role as well. It has to be able to support multiple resolutions. It would not be practical to distribute a content of the highest quality so as to provide multiple granularity as the large file size of the content would impede its distribution (and availability to small devices).

4.5 Frequent Content Key Upgrades

DRM systems need frequent security upgrades. This could be easily done so for the various components so long as there is Internet access except for the Secure Container component. The Secure Container has a fixed content key. The distribution nature of the content makes it difficult to change its content key. Certainly, the same content could be protected with different keys but this not only complicate the retrieval of the correct content key, it does not solve the problem of the content having the same key for an indefinite period of time, providing fodder for a brute-force attack.

The paradigm of *forward security* can be applied here to alleviate the above issue. In a *forward-secure* scheme, secret keys are updated at regular periods of time. These keys are supposedly independent of one another such that knowledge of one key does not divulge the other keys. In the DRM context, the content key can be updated at certain time intervals, probably at point of access.

5 Conclusion

We hope we have presented a comprehensive survey of the technological aspects of DRM. We had looked at some definitions and examined a generic DRM model and dissect them into various components, each of which was individually discussed. We concluded by evaluating emerging trends, noteworthy issues and future directions.

References

1. ADELSBACH, A., KATZENBEISSER, S. and VEITH, H. 2003. Watermarking schemes provably secure against copy and ambiguity attacks, Proceedings of the 2003 ACM workshop on Digital rights management, 2003, pp. 111-119.
2. ALLAMANCHE, E., HERRE, J., HELMUTH, O., FRBA, B., KASTEN, T. and CREMER, M. 2001. Content-Based Identification of Audio Material Using MPEG-7 Low Level Description, Proceedings of the International Symposium of Music Information Retrieval, 2001.
3. BARNI, M. and BARTOLINI, F. 2004. Data hiding for fighting piracy, Signal Processing Magazine, IEEE, Volume 21, Issue 2, March 2004, , pp. 28- 39.
4. CANO, P., BATLLE, E., GMEZ, E., GOMES, L. DE C. T. and BONNET M. 2002. Audio fingerprinting: concepts and applications, Proceedings of 1st International Conference on Fuzzy Systems and Knowledge Discovery, Singapore, November 2002.
5. CANO, P., BATLLE, E., KALKER, T. and HAITSMA, J. 2002. A review of algorithms for audio fingerprinting, Proceedings of International Workshop on Multimedia Signal Processing, US Virgin Islands, December 2002.
6. CHI, C. H., WANG, H. and KU, W. 2003. Proxy-Cache Aware Object Bundling for Web Access Acceleration, Proceedings of Eighth International Workshop on Web Content Caching and Distribution, 2003.
7. CONRADO, C., KAMPERMAN, F., SCHRIJEN, G. J. and JONKER, W. 2003. Privacy in an identity-based DRM system, Proceedings of 14th International Workshop on Database and Expert Systems Applications 2003, 1-5 Sept. 2003, pp. 389-395.
8. DOI. The Digital Object Identifier (DOI) System. http://www.doi.org/
9. ERICKSON, J., IANNELLA, R. and WENNING, R. 2001. Workshop Report, W3C Workshop on Digital Rights Management for the Web, 22-23 January 2001.
10. GOODRICH, M. T., SHIN, M., STRAUB, C. D. and TAMASSIA, R. 2003. Distributed data authentication, Proceedings of DARPA Information Survivability Conference and Exposition 2003. Volume 2 , 22-24 April 2003, pp. 58-59.
11. HARTUNG, F. and RAMME, F. 2000. Digital rights management and watermarking of multimedia content for m-commerce applications, IEEE Communications Magazine, Volume 38, Issue 11, Nov. 2000, pp. 78-84.
12. IANNELLA, R. 2001. Digital Rights Management (DRM) Architectures, D-Lib Magazine, June 2001, Volume 7 Number 6, ISSN 1082-9873. http://www.dlib.org/dlib/june01/iannella/06iannella.html
13. IANNELLA, R. and HIGGS, P. 2003. Driving Content Management with Digital Rights Management, Apr 2003. http://www.iprsystems.com/whitepapers/CM-DRM-WP.pdf
14. INDECS. The <indecs> framework. http://www.indecs.org
15. IWATA, T., ABE, T., UEDA, Y. and SUNAGA, H. 2003. A DRM system suitable for P2P content delivery and the study on its implementation, Proceedings of The 9th Asia-Pacific Conference on Communications, APCC 2003, Volume 2, 21-24 Sept. 2003, pp. 806-811.
16. KANG, Y. K. and KIM, M. H. 2001. Real-time fingerprints recognition mechanism-based digital contents protection system for interaction on the Web, Proceedings of Pacific Rim International Symposium on Dependable Computing 2001, 17-19 Dec. 2001, pp. 304-309.
17. MORI, R. and KAWAHARA, M. 1990. Superdistribution: the concept and the architecture. Technical Report 7, Inst. of Inf. Sci. & Electron (Japan), Tsukuba Univ., Japan, July 1990.
18. MIHÇAK K. and VENKATESAN R. 2001. New Iterative Geometric Methods for Robust Perceptual Image Hashing, Security and Privacy in Digital Rights Management: Proceedings of ACM CCS-8 Workshop DRM 2001, Philadelphia, PA, USA, November 5, 2001, pp. 13-24.

19. MPEG-21. MPEG-21. http://www.chiariglione.org/mpeg/standards/mpeg-21/mpeg-21.htm
20. NUTZEL, J. and GRIMM, R. 2003. Potato System and signed media format - an alternative approach to online music business, Proceedings of Third International Conference on Web Delivering of Music, 2003. 2003 WEDELMUSIC, 15-17 Sept. 2003, pp. 23-26.
21. OASIS. OASIS Rights Language Technical Committee. http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=rights
22. ODRL. Open Digital Rights Language (ODRL). http://www.odrl.net/
23. OEBF. Open eBook Forum. http://www.openebook.org/
24. OMA. Open Mobile Alliance (OMA). http://www.openmobilealliance.org/
25. ORTEGA-GARCIA, J., BIGUN, J., REYNOLDS, D., and GONZALEZ-RODRIGUEZ, J. 2004. Authentication gets personal with biometrics, Signal Processing Magazine, IEEE, Volume 21, Issue 2, March 2004, pp. 50- 62.
26. PESTONI, F., LOTSPIECH, J. B. and NUSSER, S. 2004. xCP: Peer-to-Peer content protection, Signal Processing Magazine, IEEE, Volume 21, Issue 2, March 2004, pp. 71- 81.
27. ROSENBLATT, B., TRIPPE, B. and MOONEY, S. 2001. Digital Rights Management: Business and Technology, John Wiley & Sons, 2001, ISBN 0764548891.
28. RUMP, N. 2003. Definition, Aspects, and Overview, E. Becker et al. (Eds.): Digital Rights Management, ISBN 3-540-40465-1, LNCS 2770, 2003, pp. 3-15.
29. "SCREAMER, B". 2001. "Beale Screamer"'s crack of Microsoft DRM Version 2. http://cryptome.org/ms-drm.htm
30. UZUNER, Ö. and DAVIS, R. 2003. Content and expression-based copy recognition for intellectual property protection, Proceedings of the 2003 ACM workshop on Digital rights management, 2003, pp. 103-110.
31. VENKATACHALAM, V., CAZZANTI, L., DHILLON, N. and WELLS, M 2004. Automatic identification of sound recordings, Signal Processing Magazine, IEEE, Volume 21, Issue 2, March 2004, pp. 92- 99.
32. WALKER, J., MORRIS, O. J. and MARUSIC, B. 2003. Share it! - the architecture of a rights-managed network of peer-to-peer set-top-boxes, EUROCON 2003. Computer as a Tool. The IEEE Region 8, Volume 1, 22-24 Sept. 2003, pp. 251-255.
33. WU, M., TRAPPE, W., WANG, Z. J. and LIU, K. J. R. 2004. Collusion-Resistant Fingerprinting for Multimedia, Signal Processing Magazine, IEEE, Volume 21, Issue 2, March 2004, pp. 15- 27.
34. XRML. eXtensible rights Markup Language (XrML). http://www.xrml.org/