u-DRM: A Unified Framework of Digital Rights Management based on RFID and Application of Its Usage Data

Jong Hwan Suh,[1] and Sang Chan Park[1,2],

Dept. of Industrial Engineering[1], and Graduate School of Culture Technology[2], KAIST
Daejeon, Republic of Korea

Summary
In the Internet, the digital format of most contents has led to its increased piracy because of the ease of copying and sharing the digital contents. Moreover, the advent of new technologies such as ubiquitous computing seems to cause problems of piracy even more than before. Likewise it's going to be a more critical issue to control and manage rights of digital contents in the future. Therefore, in this paper, we propose a framework of u-DRM: a unified framework of DRM based on RIFD with watermarking and fingerprinting. The framework consists of two methods using digital mediums and digital contents. And we suggest ways for the application of usage data collected from the proposed framework of u-DRM.

Key words:
DRM, RFID, Usage data

1. Introduction

Today, digital contents such as movies and music are accessible without much difficulty to everybody through the Internet. And the Internet has become a paradise for those who are in pursuit of vibrant information and digital entertainment. However, the digital format of most contents has led to its increased piracy because of the ease of copying and sharing the digital contents. Although researches have been made to distribute digital contents with appropriate security mechanism, the piracy problem still remains unsolved. Moreover, there will be much more problems of piracy under the environment of ubiquitous computing where a huge amount of transactions of digital contents are expected.

Likewise, it is going to be a more critical issue to control and manage rights of digital contents in the future. Therefore, in this paper we propose a concept of u-DRM: a unified framework of DRM based on RFID. With present technologies such as watermarking and fingerprinting, the framework is suggested in two ways using digital mediums and digital contents. And we suggest ways for the application of usage data collected from the proposed framework of u-DRM. Based on usage data, we can pro-file users' consumption behavior, and thereby provide personalized services for content consumers. And we can improve quality of digital contents, and provide a new method of charging for the copied digital contents under supervision of payment system.

The organization of this paper is as follows. Section 2 begins by introducing related works with digital rights management. Section 3 gives a conceptual framework of u-DRM. And section 4 suggests conceptual ways of the application with usage data, providing a new charging method to secure rights of digital contents. Finally in section 5, we conclude the paper with a discussion of further works.

2. Related Works

DRM is basically defined as an aggregation of security methodologies to protect the interests of the contents owners so that they may maintain persistent ownership and control of their contents [1]. However, the definition of DRM can be further divided into two groups: management and enforcement [2, 3]. First, management is about managing of digital rights. The rights holders have to identify their contents, provide the meta-data of the content (so that users can trace originality), and specify the terms and contributions of usage and distribution of the contents. On the other hand, enforcement is about the digital managing of rights which is to ensure that the contents is only used as stipulated in the terms and conditions associated with its usage [1]. In this paper, u-DRM includes both definitions of DRM.

As preceding technologies, there are watermarking and fingerprinting applied for DRM. Watermarking is used for copy control, content identification, and tracing. In DRM, content is vulnerable to attacks at the end-user system. So watermarking can be taken advantage of to detect illegal copies of content that have been unprotected by such attacks [4]. On the other hand, fingerprinting is characterizing the content such as images, audio, and text based on its representation and matching it to an entry in a database [5, 6, 7]. Typically, fingerprinting has two processes. Firstly, in training phase, characteristic features of the content are extracted and compacted for an entry into a database. Secondly, in recognition phase, pattern recognition is performed to match the fingerprint of a given content to an entry in the database [1]. In this paper,

Manuscript received August 5, 2006.
Manuscript revised August 25, 2006.

we adopt both of watermarking and fingerprinting for the framework of u-DRM.

As one of researches on DRM with RFID, it is being developed a system comprised of DVDs embedded with RFID tags and DVD players embedded with RFID readers. The tagged DVD plays in the RFID-enabled players only if the reader authenticates the DVD's tag [8]. Likely, we adopt the approach of DRM with RFID. But we propose a modified DRM system from the previous research's framework so that we let digital contents consumed by users first and then ask the charges of uses later.

3. A Framework of u-DRM

In this section, we explain a framework of u-DRM which controls and manages rights of digital contents. As shown in the Figure 1, the proposed u-DRM is comprised of two components. Firstly, based on digital mediums (H/W), we adopt a player with a RFID reader and mediums of digital contents with RFID tags from [8]. And based on digital contents (S/W), we adopt fingerprinting of digital contents.

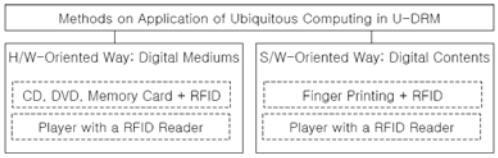

Fig. 1 Two methods in the proposed u-DRM

3.1 Method based on Digital Mediums (H/W)

In this subsection of 3.1, we describe a method adopted from [8]. As shown in Figure 2, a player is embedded with a RFID reader and mediums of digital contents are embedded with RFID tags. Through this structure, we authenticate digital contents and authorize its play.

In the RFID tags attached to digital mediums, we store information related to the digital contents such as a tag id, the content meta-data, and supply chain data. When the digital medium is put into the player with a RFID reader, the RFID reader checks whether the use of the digital contents contained in the digital medium is authorized or not. Of course, this confirmation process is on the basis of elements from the content meta-data. And the process also identifies how many times digital contents are used, and updates the information on it. Besides, using the URL of the license issuing system gotten from the content meta-data, we download more information about the digital contents on the web.

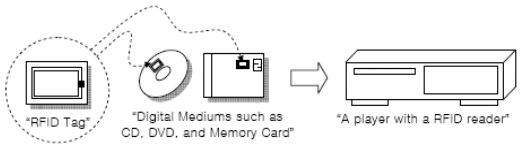

Fig. 2 Method based on digital mediums in the proposed u-DRM

3.2 Method based on Digital Contents (S/W)

In this subsection of 3.2, we give an account of a method based on digital contents, more precisely a method which uses fingerprinting. As described in the related works, the fingerprinting refers to content-based identification. It characterizes the digital content based on its representation such as feature or signals, and matches the result to an entry in a database. Actually, there have been already developed many robust ways for fingerprinting. So in this subsection, we do not develop a new fingerprinting algorithm but just assume that we adopt one of those fingerprinting algorithms, which is proper to our approach.

As shown in Figure 3, a fingerprint of an original digital content is created by using a function which is represented as a black box. This fingerprinting process is operated by a content provider. The fingerprint of the original digital content is stored as a reference in the content meta-data of medium's RFID tag, and the function used for fingerprinting is sent to a license administrator to be registered as an official function for the original digital content. When a medium is inserted into a player with a RFID reader, its RFID tag is identified by the player. And from the URL stored in the RFID tag, the player downloads the function which was used to create the fingerprint by the content provider. With the downloaded function, a fingerprint is calculated by the player from the digital content stored in the digital medium. And the player compares it to the fingerprint of the original digital content stored as a reference in the RFID tag.

By these steps, we check if a digital content in a digital medium is original or not. This method is effective in a sense that it guarantees the digital content's originality in a more precise way. If the copied digital content has a RFID tag copied from the RFID tag of the original digital content, the player may not be able to verify that it is an illegal copy only with a method based on H/W. That's because the copied RFID tag may have the same values of elements as the original one. However, if a player compares directly 'fingerprint of the original content stored as a reference in the RFID tag' to 'fingerprint calculated based on the digital content in the current digital medium with the downloaded function', we can avoid such a tragedy.

In this method based on digital contents, the RFID tag attached on the digital medium contains information

related to the digital contents such as a tag id, fingerprint of the original content as a reference. And it also stores the difference between the original fingerprint and the calculated fingerprint. The roles of a player here are similar to the ones for a method based on digital mediums in the subsection of 3.1. But, as mentioned in the previous paragraphs, additionally it downloads a function used for fingerprinting, calculates a fingerprint on the basis of current digital content in the digital medium, and compares it to the fingerprint of the original digital content stored as a reference in the RFID tag.

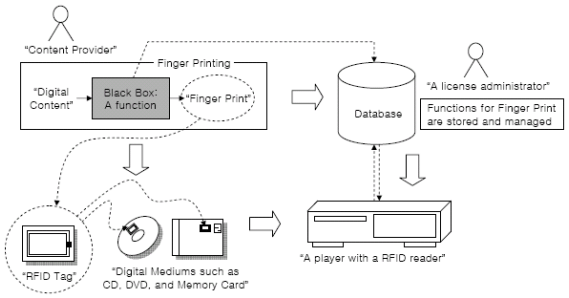

Fig. 3 Method based on digital contents in the proposed u-DRM

3.3 Process of Packaging Digital Contents

As a prerequisite to realize both methods of u-DRM in the subsections of 3.1 and 3.2, a process of packaging digital contents needs to be defined as shown in the Figure 4.

Firstly, digital contents are stored in some kinds of digital mediums such as CD, DVD, and a memory card. And the digital mediums are embedded with RFID tags, which contain information related to two methods of u-DRM described previously. To sum up from the subsections of 3.1 and 3.2, they are Tag ID, the content meta-data, supply chain data, fingerprint as a reference, and difference between a reference and the calculated fingerprint. In addition to the RFID tag, we insert watermarks to the physical bodies of the digital mediums such as CD and DVD if necessary.

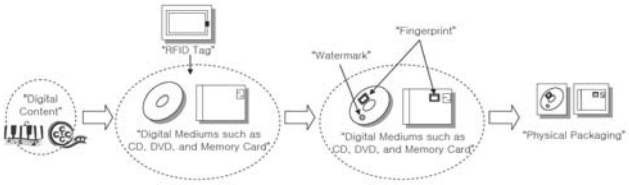

Fig. 4 Process of packing digital contents for u-DRM

3.4 Distribution of Digital Contents with u-DRM

In this subsection of 3.4, we explain a process to distribute digital contents with application of u-DRM. The overall picture is depicted in the Figure 5. There are six entities participated in the distribution of digital contents, and relationships among those entities are described.

In the Figure 5, the distribution process of digital contents is initiated by the creation of the digital contents. Content providers create digital contents such as music, movies, game, and etc. And they wrap up digital contents into physical bodies through the process described in the subsection 3.3. The physically packaged digital contents are sent to the content distributor, and the function used for fingerprinting is sent to the license administrator. Content consumers acquire the physically packaged digital contents on behalf of the content distributors. In order to experience those digital contents, content consumers utilize a player which is embedded with a RFID reader. And then, two methods of u-DRM described in the subsections of 3.1 and 3.2 are applied step by step to authorize the use of digital contents and identify the originality of the digital contents.

As seen in the subsection 3.1, firstly, the player checks if the medium of digital content has a right RFID tag, which proves the use is authorized. And then, as seen in the subsection 3.2, the player also checks if the digital content is copied or not with a function of the digital content's fingerprint downloaded from a license administrator. After consumption of digital contents, money is paid by content consumer through payment system and delivered to those who are participated in the processes from creation to distribution of the digital contents. Finally, usage data of content consumers is collected and sent to the content provider and content distributor by two ways: through a player connected to the web, and by getting back RFID tags embedded in mediums of digital contents.

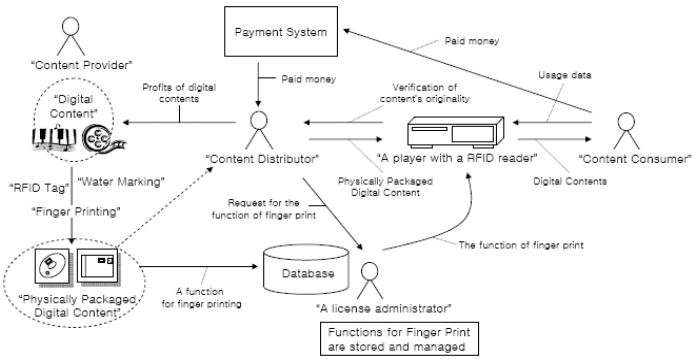

Fig. 5 Distribution of digital contents with u-DRM

4. Applications of Usage Data in u-DRM

In the section 3, we explained a framework of u-DRM on the basis of two methods, based on digital mediums and digital contents. In the section 4, we suggest possible ways for the application of usage data collected throughout the framework of u-DRM. According to the Figure 5 in the subsection of 3.4, usage data is collected in two ways: through a player connected to the web, and by getting back RFID tags embedded in mediums of digital contents. The collected usage data is delivered to the content provider and content distributor, and it is applied to provide many services customized to content consumers. From 4.1 to 4.3, applications of usage data are described based on scenarios.

4.1 Providing Personalized Services for Content Consumers

Each player has its id number and is connected to the user's id registered on the web. Each player records what kind of a digital content is played on the player, how many times the digital content is played by the user. And the player sends such information to the central system. Histories of usage are utilized to profile users' consumption behavior. Based on the identified consumption behavior, we provide personalized services for each user. For example, if it is found that a user likes watching soap drama, a free DVD related to the soap drama may be delivered to the user. And we also recommend similar kinds of digital contents for the user. Moreover, we charge fee differently according to how many times the digital contents are consumed.

4.2 Improving Quality of Digital Contents

According to the subsection of 3.4, RFID tags on the digital mediums store five elements of information throughout the distribution of digital contents with u-DRM. Among them, the content meta-data is applied to provide additional services customized to the user. Each medium has a RFID tag and it stores the content meta-data, and there are recorded usage data of how many times the digital content is used, and how much fee is charged for each user. Therefore, by using the usage data, we calculated how popular the digital content is. This result is sent to the content provider and used as a reference to create more popular contents.

4.3 Charging Later for Copied Digital Contents under Supervision

Among five elements which are stored in the RFID tags of the digital mediums, the element of 'difference between a reference and the calculated finger pint' is applied to develop a new method to secure the rights of digital contents. In this method, a player doesn't block the copied digital contents from being played, but it just lets the abuse go under supervision of payment system. With the help of fingerprinting, difference between a reference and the calculated fingerprint are used to check if copied digital contents are played illegally on the player. And if they are so, histories of such behaviors are sent to the central system and recorded in the payment system for the individual player. And later, those behaviors are investigated and analyzed on the basis of records in the payment system.

This method is different from the current DRM system so far, because it does not focus on blocking the illegal uses of digital contents. It is similar to a monitoring system for the overspeeding vehicles, where charging is decided later. Thus using these usage data, it is possible to change the basic concept of current DRM into a new way: monitoring first, and then charging later for the abuse. Under the ubiquitous computing, it is not the best solution for securing rights of digital contents to block the uses of copied digital contents. Therefore, this method is appropriate because it provides an opportunity to activate the transactions of the digital contents among many users, but still securing the rights of the digital contents.

5. Conclusion

In this paper, we proposed u-DRM: a unified framework of DRM based on RFID with preceding technologies such as watermarking and fingerprinting. The framework of u-DRM is divided into two methods based on H/W and S/W. In the method based on digital mediums (H/W), a player is embedded with a RFID reader and mediums of digital contents are embedded with RFID tags. When a digital medium is put into a player with a RFID reader, the RFID reader checks the RFID tag's authenticity to know whether the use of digital contents contained in the digital medium is authorized or not. In the method based on digital contents (S/W), fingerprinting is adopted, and it is used to verify the originality of the digital content stored in the digital medium. Through this, problems which may be caused by using the method based on digital mediums (H/W) alone are prevented. Processes of packaging and distributing digital contents for the proposed framework of u-DRM are described as well.

And we suggested ways for the application of usage data collected from the proposed framework. Using the RFID-enabled player and the RFID tag of the digital medium, we can collect usage data about digital contents. And those histories are used to profile users' consumption behavior, and thereby to provide digital contents in more customized ways for the content consumers. And we also discussed how u-DRM can help contents providers to

improve quality of digital contents. Finally, we suggested a new paradigm beyond the current DRM system. Like a monitoring system for the overspeeding vehicles, it watches the illegal uses of the copied digital contents firstly, and then it charges fee later according to the records. By this new approach, though under the ubiquitous computing environment, we expect it would be possible to activate the transactions of the digital contents among many users, but still securing the rights of the digital contents.

Acknowledgments

This research is supported by the KAIST Graduate School of Culture Technology.

References

[1] William Ku, Chi-Hung Chi: Survey on the Technological Aspects of Digital Rights Management. In: K. Zhang and Y. Zheng (eds.): ISC 2004. Lecture Notes in Computer Science 3255 (2004) 391–121
[2] Iannella, R., Higgs, P.: Driving Content Management with Digital Rights Management (2003), URL: http://www.iprsystems.com/whitepapers/CM-DRM-WP.pdf
[3] Rump, N.: Definition, Aspects, and Overview. In: E. Becker et al. (eds.): Digital Rights Management. Lecture Notes in Computer Science 2770 (2003) 3-15
[4] Barni, M., Bartolini, F.: Data hiding for fighting piracy. Signal Processing Magazine, IEEE, Vol. 21, Issue 2 (2004) 28-39
[5] Mihcak, K., Venkatesan, R.: New Iterative Geometric Methods for Robust Perpetual Image Hashing, Security and Privacy in Digital Rights Management. Proc. of ACM CCS-8 Workshop DRM 2001 (2002) 13-24
[6] Allanmanche, E., Herre, J., Helmuth, O., Frba, B., Kasten, T., Cremer, M.: Content-Based Idnetifiction of Audito Material Using MPEG-7 Low Level Description, Proc. of the Int. Symposium of Music Information Retrieval (2001)
[7] Cano, P., Battle, E., Kalker, T., Haistsma, J.: A review of algorithms for audio fingerprinting, Proc. of Int. Workshop on Multimedia Signal Processing (2002)
[8] http://www.rfidjournal.com/article/articleview/1589/1/1/

Jong Hwan Suh received the B.S. degree of industrial engineering from Korea Advanced Institution of Science and Technology (KAIST) in 2004, and the M.S. degree in 2005 at KAIST. He is now a Ph.D. candidate in industrial engineering at KAIST. His current interests include the application of artificial intelligence, especially machine learning or neural network methodologies, to the design of knowledge based systems for various management principles. He has expanded his research domain into TQM, B2B EC, CRM, Financial Engineering, and Ubiquitous Computing.

Sang Chan Park received the M.B.A. degree from the University of Minnesota, Minneapolis, in 1985 and the Ph.D. degree in MIS from the University of Illinois, Urbana, in 1991. He was an Assistant Professor of information systems design and analysis with the School of Business at University of Wisconsin, Madison, for six years before joining the faculty of KAIST. His current interests include the application of artificial intelligence, especially machine learning or neural network methodologies, to the design of knowledge based systems for various management principles. He has expanded his research domain into TQM, B2B EC, and educational technology for the gifted and Ubiquitous Computing. He has published in the areas of data mining, quality information systems, BPR, workflow analysis, and financial engineering. He has contributed papers to many scientific publications.