A Novel DRM Security Scheme and its Prototype System Implementation

Lili Zhang, Zhiyong Zhang, Danmei Niu, Tao Huang
Electronic Information Engineering College, Henan University of Science and Technology, Luoyang, China,
E-mail:lillyzh@126.com, xidianzzy@126.com, niudanmei@163.com, taohuang66@sohu.com

Abstract

A DRM system scheme based on PKI is proposed and designed in this paper, which can achieve effective user authentication, secure distribution of digital content and usage rights control. The architecture of system,secure mechanism, playback control mechanism are described in detail. Finally, against the offline usage control of the audio and video content in user terminal, we design a system framework mainly comprising the encryption and decryption of digital content, generation and distribution of license and secure usage control, and implement a prototype system -DRM Player in C++. This scheme and its prototype effectively assure authorized usages and copyright protections of the audio and video content in the whole life cycle.

Keywords*: Digital Rights Management, Encryption, Decryption, Security Mechanism, Usage Control*

1. Introduction

Along with the rapid development of Internet and digital technology, digital products including digital music, digital TV, E-Book and other various forms are more widely used. These digital products significantly facilitate our daily lives. Because digital contents provide much convenience like that it is easy to transfer and the copied contents are identical with the original，large copy of digital contents protected by Intellectual Property Right and unauthorized distribution, dissemination and abuse of them through various communication network carriers is a general phenomenon, which causes a series of increasingly serious problems of digital copyright. More seriously, in recent years, P2P networks, and the emerging social networks aiming at sharing multimedia content, such as YouTube, Myspace, Tudou etc, build a virtual socialized network based on broadband internet and wireless mobile communication network among the users, who can more easily transfer, share and use audio and video and other digital content. Flexible and versatile network admission modes enable convenient connections to existing and future digital resources "for anyone, anytime, anywhere, on any device." However, freely sharing and arbitrarily disseminating copyright-protected digital content not only damages the interests of copyright holders and dampens the creative passion of the original authors, but also brings serious injury to the management of the digital content and the benign development of digital content industry. So the providers of digital products need a technology to protect their digital content away from illegal use. Digital Rights Management (DRM) arises to solve the problem. It enables digital content to be used in the permissions granted by the provider of digital products.

DRM technology is a series of hardware and software technologies protecting intellectual property rights for all types of digital content. It ensures the legitimate use of digital content in the whole life cycle, balances the various interests and needs of each role in digital content value chain and promotes benign development of the digital markets and reliable dissemination of information[1-2]

DRM is a key problem concerning benign and healthy development of the digital content industry. DRM emerged in the early 1990s as a realistic response to the above threats. And also, it is multi-disciplinary research field involving the DRM security technology[3], Digital Copyright Act and technology implementation[4-7],DRM economics[8], business model[9-10], and DRM pricing（Pricing）policy [11-12], DRM trust and risk assessments [13-15] etc.

Typically, in recent years there are mobile DRM applications that have the capacity to solve the following problems for mobile e-commerce and e-content transactions, generation of digital content,

distribution and transmission, secure storage, usage control, as well as personal digital content/rights transfers [16],such as Mobile IPTV DRM [17].

Throughout the past decades, the study of DRM mainly focuses on cryptographic security and usage controls [18] on digital contents or rights, as well as on the reactive mechanisms of digital watermarking used for combating piracy. The emphasis on a DRM technical and managerial perspective has primarily been dealt with from a preventive approach to content protection.

Considering security and usage control technology comprehensively, this paper designs a DRM system based on PKI and describes system architecture, security mechanism , as well as playback control mechanism in detail. Against terminal usage control of digital content and copyright protection, this paper designs a system framework mainly comprising the encryption and decryption of digital content, generation and distribution of license and secure usage control. At last, a prototyping system-DRM Player is implemented in C++, consisting of two parts: server and user terminals. The system effectively assures authorized usage and copyright protection of the audio and video content in the whole life cycle.

2. DRM system architecture

DRM system architecture designed in this paper is illustrated in Figure1. The system is mainly composed of CA (Certification Authority), S (server), UD (User Domain) and Trading Center, constituting a PKI system.

These entities are the functional ones. In practical applications they may be separate and also be integrated.

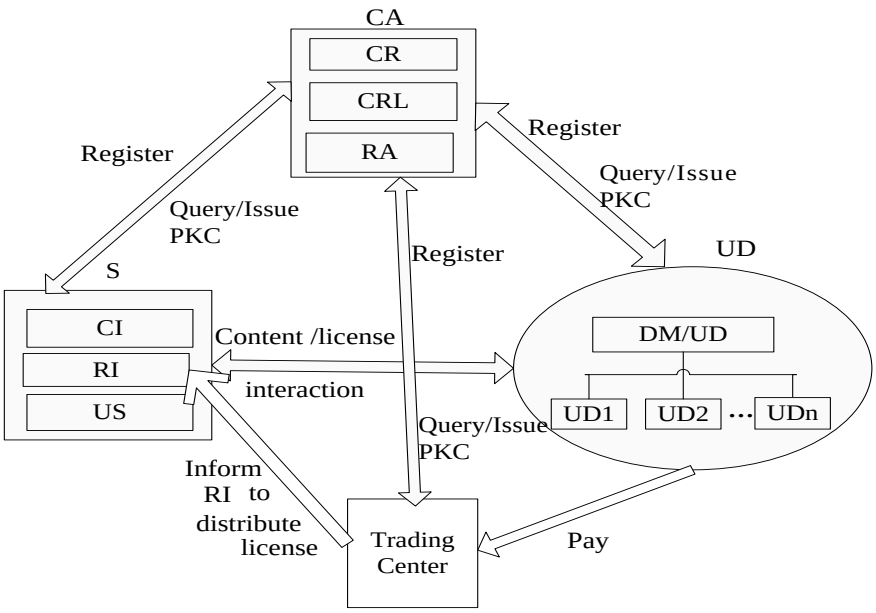

Figure 1. A DRM security architecture based on PKI

CA: CA integrates CR (Certificate Repository), CRL (Certificate Revocation List) and RA (Registration Authority). As the authority, CA receives and verifies the application information submitted by S and UD, then generates a unique PKC (Public Key Certificate) for the suitable entity, meanwhile backups and issues it. In addition, CA provides the inquiry service of PKC.

S: S consists of many servers. S is a provider of digital content and the issuer of corresponding DRM rights, the manager of UD as well. At least S includes CI (Content Issuer), RI (Right Issuer), US (User Server),CI provides the business of digital content distribution and download, RI is responsible for the generation and distribution of rights, US is used to store, update and manage the UD information.

CI usually includes content repository, production information database and "packaging" tool. It is mainly responsible for storage, maintenance and encryption of the digital content, as well as the embedding of digital watermarks in the digital content. Packaging the above processing results and the content identification metadata, CI sells or distributes them, ensuring the safe transmission of digital content on the network and copyright protection of digital content.

RI usually contains the right database, the content key database, the user identity database and DRM license generator. It is mainly used to generate and distribute content license. Content license includes rights to use digital content (play times, deadline and conditions of use etc), content encryption key, digital signature of license issuer and other information.

US is the user server and is used to store, update and manage the user information.

UD: UD (User Domain) is a collection of devices owned by the user. DM(Domain Manager) is the core device in UD. It is responsible for managing all the member devices in the domain and also responsible for communicating with the server uniformly. It has the eligibility for distributing the license for the digital content to the member devices. It is not necessary that DM is a specialized devices and it can be acted as by desktop, laptop or other devices. However, the device must have enough storage space and handling ability to accomplish the above function. User devices must support the DRM terminal with the corresponding DRM module to securely store DRM content and its corresponding license, and strictly comply with DRM security mechanisms. User devices can be PC, laptop, media player digital TV, set-top box or other digital devices.

Trading center: Trading Center accepts payment information from the user, and then it informs RI to generate and distribute the license based on user requirements and fees the user has paid. Trading center and RI divide profits by a certain percentage.

3. DRM system security mechanism

3.1. Authentication mechanism

DRM system authentication mechanism is implemented via PKC(Public Key Certificate) service provided by CA. Server and user confirm the identity of each other by mutually verifying the digital signature of CA.CA first open its own PKC so that server and user acquire CA public key. When S communicate with DM in the user domain, they obtain PKC of each other in two ways: one way is downloading PKC of each one according to ID information provided by the opposite; the other one is that the opposite directly provides PKC. After obtaining PKC, the verifier verifies the identify of the provider. Firstly it is made sure CRL is up to date before verifying the opposite identity ，if necessary download the latest CRL. The authentication process is shown in figure 2 （P stands for provider ，V stands for verifier ）

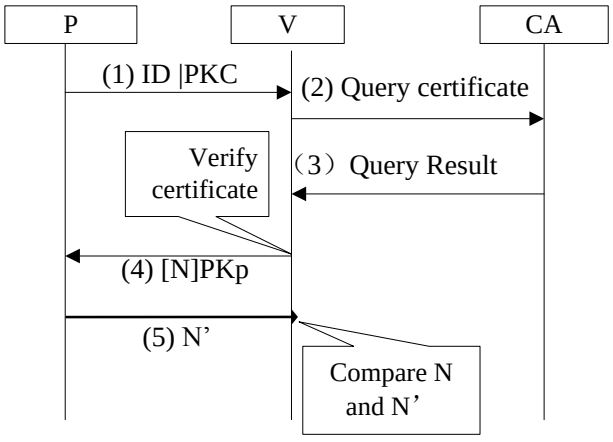

Figure 2. DRM system authentication process

Step1：P sends ID information and its own PKC to V.

Step2：V checks whether PKC of P is in CRL and queries the certificate of P.

Step3：CA sends query results to V.

Step4： After verifying PKC of P is not in CRL, V obtains the P's public key PKp, encrypts the random number N and sends the encrypted content to P.

Step5：After obtaining encrypted content, P decrypts it with its private key SKp and gets N', and sends N' to V.

At last V compares N and N', if N = N', V verifies the identity of P. if not, then fails.

3.2. Cryptography-based digital contents security

The confidentiality of DRM system is implemented via CEK (content encryption key) generated by S and the public key of the user together. CI encrypts data with CEK, while CEK is encapsulated in the license and is encrypted with the user public key. Thus, only those users with permission of the DRM content can get CEK in the license with their own secret key. After obtaining the license, user must first verify the server signatures to ensure the license real and effective.

3.3. Integrity protection mechanism

Integrity protection mechanism of DRM system is implemented by digital signature. Digital signature process is as follows: when the license is generated, the content of the license is hashed to generate a fixed length hash value. The hash value is encrypted with private key of RI to form a digital signature string attached the end of the license. When user terminal system resolves the license, it does the same hash operation to obtain the current hash value , and then decrypts the digital signature strings with the public key of RI to get a hash value, and at last compares the above two hash values, if the same license is valid, system can carry on the next resolving operation. Otherwise the license is considered invalid.

When the license is transferred to the intelligent terminal, firstly, complete the transfer of the license rights and transform the license signed by RI private key to the one signed by the user's private key .Each time after the user plays digital content, the intelligent terminal updates the information of the license, and then carry on the digital signature by the user's private key for the next check. This ensures the integrity of digital content in the client.

3.4. Security analysis of system

From the above system architecture, it can be seen that DRM system has the character that content encryption and key management is separable in time and position, comparing with traditional confidential communications. It is entirely due to use of the concept of "license". Similar to the attribute certificate in the PMI (Privilege Management Infrastructure), the digital license establishes a contractual relationship between users and RI.

In order to ensure secure transmission and legitimate use of content license, the content encryption key (CEK) is protected using asymmetric encryption algorithm. CEK is written in the license after being encrypted by the public key of the user who purchases the digital content. After decrypting CEK by the private key, the player can only play the content. This mechanism ensures that the content can only be played by the user who purchases the digital content. This mechanism has been described in detail in 3.2. The system implements integrity protection by digital signature, ensuring that the content and the corresponding license are not changed in the process of transmission and preservation.

4. Playback control based on cryptography and license

Playback control mechanism of digital content is implemented through the content encryption and the license together. When playing the audio and video files, user can only decrypt and play them through exacting the content encryption key CEK in the license. User terminal gets the encrypted resources package through the download module and the license through purchase module, and gives

the above two to the play module when playing digital content. Usually DRM system fulfills playback control through the following rights such as play times, the valid play period and play time to prevent any abuse and arbitrary sharing of digital contents.

When playing the audio and video content, firstly the system checks the license to ensure the integrity of the license through verifying signature and then resolves the license to determine if it is in the valid period, if the license is integral and also in the valid period, system takes the content encryption key to decrypt the content for playing.

After playing the digital content every time, license needs to be updated because the change of the rights in the license and needs a new signature with the user public key. System will delete the invalid license (expiring or being damaged). If the license is invalid, user can only get a new license file only through repaying fees. The entire process including check, analysis, update and delete of the license is shown in figure 3.

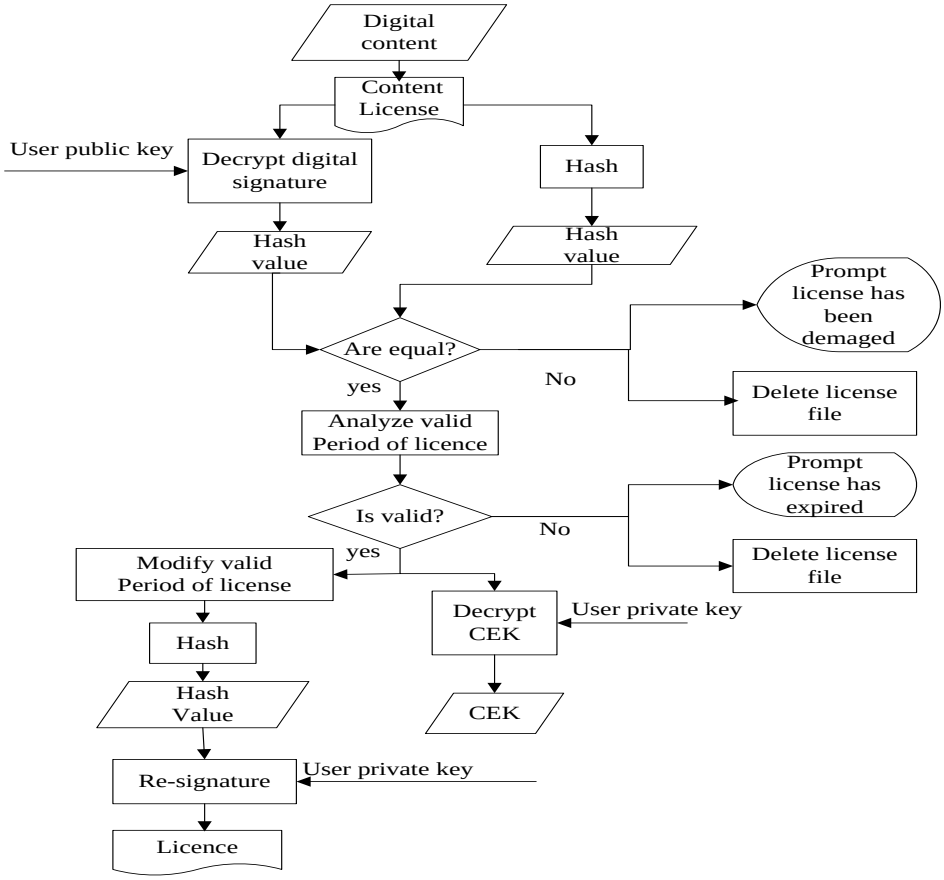

Figure 3. License handling process

5. Implementation of DRM prototype system

5.1. DRM player system framework

In this paper, we implement digital content security control prototype system--DRM Player in C++ language, containing digital content server and user terminal. Figure 4 depicts the framework of the prototype system-DRM player.

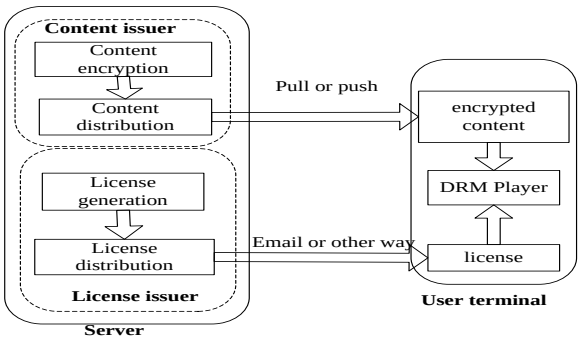

Figure 4. DRM Player system framework

Content issuer achieves encryption and distribution of the audio and video content; license issuer achieves generation and distribution of the license; user terminal or client implements the decryption of the encrypted content and the usage control by the DRM player. Through the separated distribution of the encrypted content and license, DRM system prevents arbitrary abusing and sharing of the digital content, achieving secure usage control and digital rights protection. For this DRM prototype system, the main study point is decrypting and playing audio and video content encrypted in the user terminal, as well as usage control, implementing a playback system supporting digital rights protection.

5.2. Design and implementation of server

Server side mainly consists of two modules: (1) server-side encryption module of digital content (The name of the software is *DRM Player Server Contents Encrypt for Win7.exe*) (2) server-side generation module of digital license (The name of the software is *DRM Player Server Generate Licenses for Dos.exe*).

5.2.1. Encryption of digital content

Encryption of digital content is oriented to C / S mode. The server adopts 3DES cryptographic algorithm to encrypt digital content with the overall encryption method. The overall encryption means many files can be selected and encrypted one time. Tested, with this method, system overhead is relatively small in the hardware environment of the existing mainstream PC. So it does not affect the normal operation of the server system. Encrypted file name begins with “encrypt_”; for example, if the audio file “you are not alone.mp3”is encrypted, the name of the generated file is “encrypt_you are not alone.mp3”. In addition, we achieve a encryption speed of about 27 megabits per second with the overall encryption method.

5.2.2. Distribution of digital content

Content distribution system is oriented to B / S model, and it is a logic function entity responsible for DRM content distribution. After encrypting and packaging digital content, the content provider distributes them to the digital content management platform. At the same time, content operators can also provide packeted content to end-users in various ways, such as Pull (HTTP Pull, OMA Download), Push (WAP Push, MMS), or streaming transmission etc.

5.2.3. License generation mechanism

Generation of the license is achieved by license generation module, and license includes content encryption key and the play rights. The name of the license generation software implemented in the paper is *DRM Player Server Generate Licenses for Dos.exe*. Generation process of license is as follows: Firstly input the audio or video file name. The file is generated by encryption module of digital content and is started with “encrypt_”; then input the encryption key. The key is the one which

is used to encrypt the original audio or video file. The two keys must be consistent; otherwise the encrypted file will not be played; finally, input the play rights, such as play times, play period and play time. The resulting license is text files existing in encrypted form.

5.3. Implementation of the user terminal

5.3.1 Mplayer Profile

Mplayer is currently the most widely used open-source audio and video playback software written in C, and it has an excellent implementation framework. It has low CPU occupancy rate during playback, and its source code is directly used by many open source projects such as ffdshow, xine , producing lots of software based on it.

.

5.3.2. Implementation of DRM Player based on Mplayer

Through analyzing the source codes of open source software MyPlayer and researching their feature characters, we implement a prototype system-- DRM Player on the base of Mplayer, which can encrypt digital content in server side and achieves the offline usage control of encrypted audio and video contents in user terminal. DRM Player controller is the core control module of DRM Player and its location is shown in Figure 5. Program carries on this module before the audio and video file is read into the stream separator. We implement the encryption and usage control of digital content through adding a lot of function codes in the module of DRM Player controller.In addition, DRM Player supports a variety of common non-encrypted audio and video formats.

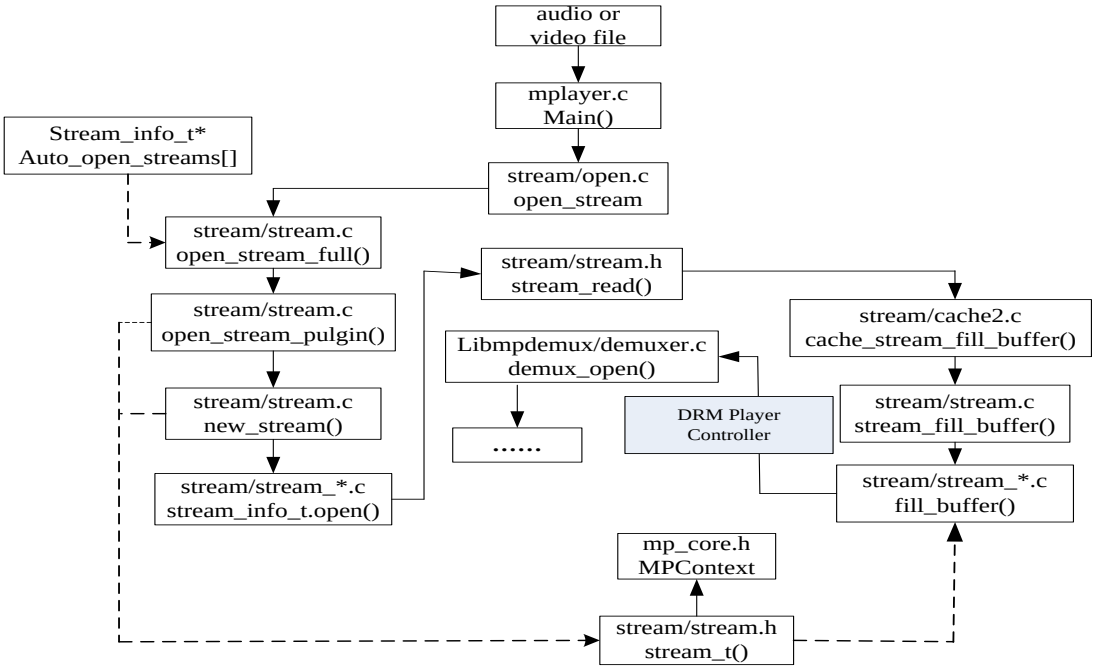

Figure 5. Achieving position of DRM Player Controller

Usage control of DRM Player includes two steps: Firstly, read the corresponding license of encrypted audio or video content, and determine whether there are play rights; then, if there are play rights, DRM Player gets CEK in license, decrypts and play the digital content. When running the kernel software --DRM Player Client Kernel V1.0.exe in a DOS environment, you can see rights in license change. For example, play times change when playing the decrypted file.

6. Conclusion

In this paper, DRM system scheme based on PKI is proposed and designed, which can achieve effective user authentication, secure distribution of digital content and usage rights control. Then against usage control of digital content and copyright protection in open network environment, this paper focuses on usage control technology based on cryptography and implement digital content security control prototype--DRM Player containing digital content server and user terminal in C++ language. DRM player supports the common audio and video format such as RMVB, RM, WMA, WMV, AVI, MKV, MP3, MP4, FLV etc. By the overall encryption method, the server encrypts content with 3DES cryptographic algorithm. Tested, with this encryption method, system overhead is relatively small in the environment of the currently mainstream PC hardware. In addition, we achieve a encryption speed of about 27 megabits per second in server, and a decryption speed of approximate 17 megabits per second when playing the audio and video content with DRM player. The research of authorized usage control of digital content, effectively ensures the authorized usage and copyright protection in the whole life cycle of digital content.

7. Acknowledgment

The work was sponsored by the National Natural Science Foundation of China (Grant No.61003234), Program for Science & Technology Innovation Talents in Universities of Henan Province (Grant No.2011HASTIT015), China Postdoctoral Science Foundation (Grant No.20100471611), and Henan University of Science & Technology Doctors Research Fund (Grant No.09001470).

8. References

[1] William Rosenblatt, William Trippe, Stephen Mooney, Digital Rights Management: Business and Technology, USA, 2002.
[2] Nic Garnett, "Digital right s management , copyright , and napster", ACM SIGecom Exchanges , vol.2, no.2, pp.1-5, 2001.
[3] Yajun Jiang, Bo Yang, "A Privacy-preserving Digital Rights Management Protocol based on Oblivious Transfer Scheme", International Journal of Digital Content Technology and its Applications, vol.5, no.5, pp.337-341, 2011.
[4] Lili Zhang, Zhiyong Zhang, Danmei Niu , Sen Shen, Chuanqi Ye "A DRM System Based on PKI", The Fourth International Conference on Genetic and Evolutionary Computing, pp.522-525, 2010.
[5] Hinkes, Eric Matthew , "Access Controls in the Digital Era and the Fair Use/First Sale Doctrines", Santa Clara Computer and High-Technology Law Journal, vol.23, no.4, pp.685-726, 2007.
[6] Bill Rosenblatt , "DRM, Law and Technology: an American Perspective", Online Information Review, vol. 31 no.1, pp.73-84, 2007.
[7] Shiguo Lian, Multimedia Content Encryption: Techniques and Applications, Auerbach Publication, UK, 2008.
[8] Shiguo Lian, Multimedia Communication Security: Recent Advances, Nova Publishers, USA, 2009.
[9] Bill Rosenblatt, "DRM, Law and Technology: an American Perspective", Online Information Review, vol.31, no.1, pp.73-84, 2007.
[10] Kiema, llkka, "Commercial Piracy and Intellectual Property Policy", Journal of Economic Behavior & Organization, vol.68, no.1, pp.304-318, 2008.
[11] Tobias Regner, Javier A. Barria, Jeremy V. Pitt, Brendan Neville "An Artist Life Cycle Model for Digital Media Content: Strategies for the Light Web and the Dark Web", Electronic Commerce Research and Applications, vol.8, no.6, pp.334-342, 2009.
[12] Michael E. Lesk, Stytz M R, Trope R L, "Digital Rights Management and Individualized Pricing", IEEE Security and Privacy, vol.6 no.3, pp.76-79, 2008.
[13] Yung-Ming Li, Chia-Hao Lin, "Pricing schemes for digital content with DRM mechanisms", Decision Support Systems, vol.47, no.4 , pp.528-539, 2009.

[14] Zhiyong Zhang, Shiguo Lian, Qingqi Pei, Jiexin Pu, “Fuzzy Risk Assessments on Security Policies for Digital Rights Management”, Neural Network World, vol. 20, no.3, pp.265-284, 2010.

[15]Zhiyong Zhang, Qingqi Pei, Lin Yang, Jianfeng Ma, "Establishing Multi-Party Trust Architecture for DRM by Using Game-Theoretic Analysis of Security Policies", Chinese Journal of Electronics, vol.18, no.3, pp.519-524, 2009.

[16]Siddharth Bhat, Radu Sion, Bogdan Carbunar, “A Personal Mobile DRM Manager for Smartphones”, Computers & Security, vol.28, no.6, pp.327-340, 2009.

[17]Nishimoto Y, Imaizumi H, Mita N, “Integrated Digital Rights Management for Mobile IPTV Using Broadcasting and Communications”, IEEE Transactions on Broadcasting, vol.55, no.3, pp.419-424, 2009.

[18]Zhang Zhiyong, “Digital Rights Management Ecosystem and its Usage Controls: A Survey”, International Journal of Digital Content Technology & Its Applications, vol.5, no.3, pp.255-272, 2011.