A DRM Model for Copyrights Protection based on Hiding Information

Deok Gyu Lee
Electronics and Telecommunications Research Institute, Daejeon, Korea
deokgyulee@etri.re.kr

Jianhua Ma
Computer & Information Sciences, Hosei University, Japan
jianhua@hosei.ac.jp

Abstract

There have been researches into digital watermarking technology or Fingerprinting vigorously to safeguard 'Protective rights for knowledge and poverty' for digital contents. DRM, Digital Rights Management, is not only 'Protective rights for knowledge and poverty', but also management and systems that are necessary to put out, circulate and use for contents. This technology, DRM, encrypts contents to protect digital contents and they are sold users on. Sellers transmit contents with 'Usage Right' and a license including a key of encryption. The key of encryption decodes encoded files. The right of usage restricts users' application of contents. Even if digital contents that are applied the DRM are coped illegally and circulated, contents will be protected from that because a player of DRM checks existence of licenses and allows contents to be restored. However, this method might cause users to feel inconvenient since the users can only restore contents through the licenses offered by a player or a Smartcard. If radio as well as cable is used popularly in the future, there will be a lot of limits to use those kinds of players. In the method of that, the method using players need different players in order to work successfully in wired and wireless environment. In the case of using Smartcards, there might be a dangerous situation when the Smartcards disappeared. This paper proposes two kinds of ideas. One is protecting contents from illegal acts such as illegal copies when the contents are in the process of circulation. The other is the protocol that can give users convenience. Hidden Agents are used so that contents are protected from illegal copies and illegal use in the contents and cuts off those illegal acts. The Agent will be installed without any special setup. In addition, it can replace roles of Watermarking as a protection. Therefore, this paper shows the solution of illegal copies that happens frequently.

Keyword*: DRM, Hiding Information*

1. Introduction

To activate sales of digital contents in electronic commerce, 'protective rights for knowledge and property' should be studied at first. Digital contents can be copied and circulated unlike general off-line contents. Therefore, after a legal purchaser buys digital contents from a seller, the illegal redistribution of the contents should be considered to protect. There have been researches into digital Watermarking technology or Fingerprinting vigorously to safeguard 'Protective rights for knowledge and poverty' for digital contents.

Many models of the DRM that is based on those technologies have been proposed and used widely now. The DRM means those management and protection systems that are needed in publishing, circulating and using digital contents. And it means not only basic construct technology for building an integrated management system of contents, but also Infra technology of contents management such as DOI and INDECS, etc used all over the world. In a management session, another feature of DRM is a technology of application for protecting contents safely as a protection system.

To protect digital contents safely, there are some practicable technologies such as protective technology for copyright of circulation and service control, and cryptogram technology for copyright, ownership, the right of using and digital Watermarking technology. This paper will propose how to protect contents in the process of circulation and service for digital production among those technologies. This proposal will not only figure out illegal copies in circulation and service, but also protect copyright and the right of using. In existing proposed models, exclusive players, Smartcards or program installation has been used. In other words, the existing models should use a certain item to protect digital contents. It means that people are inconvenient to use that kind of models because of using the certain item. So this paper proposes the DRM model to prevent illegal copies without the above. Compared with the existing models like Smartcards and players, this proposed model could prevent illegal copies by using Agents included in contents. It never uses Smartcards and players.

2. Outline of Agents

Movable Agents are independent and autonomous so they can conduct many services by moving networks. This mobile Agents' motions of performance after moving from a local to a remote host. The Agent moves from host A to host B and collects the information that the Agent wants after approaching services and sources of the host B through defined interfaces. If finishing the job, it sends the information to the original server A. After acquiring the information an Agent wanted, the Agent moves other servers and do the same performance. The movable Agent is a processor that acts automatically for a user. If it starts to perform, it will leave the place that it was born at and collect the information that it wants by moving places through networks.

3. Elements of DRM and Analysis of existing Model

3.1 Elements of DRM

A digital content goes through the step of formation, circulation, and consumption as writers' creature. In order to protect digital information, the function of DRM should be added to the each step above. In the preparatory stage of creation and flowing, Packagers are needed to encode and protect contents. In the stage of circulation and sales, Financial Clearinghouses and licensees that take charge of finance and the issue of license are needed. In the stage of consumption, the DRM of Agents are needed to control restoration according to the encryption and the right of usage. The packager protects contents through the encryption. An encryption Algorithm is sent to a license clearinghouse in order to make a key needed in encrypting. Packaged contents are sent to the purchasers who paid the bills in electronic commerce such as on-line shopping Malls, CD, E-mail (reference to step 2,3 out of the Figure 2). The purchaser will get contents with license (reference to sep 4 out of the Figure 2). The license has the information of the right that the purchasers can use contents legally and the

cipher-keys that can decode encoded files. It means that the key decodes the cryptogram of contents and abstracts contents under the right of usage. The rights include the frequency of usages, the period of usages, the term of validity, and transfer to other tools, moving to other storing item. Clearinghouses have been consisted of trade and finance, as well as a license clearinghouse. Financial Clearinghouses conduct necessary jobs of financial approval and the settlements of accounts followed by the approval in contents commerce including consumption, sales and circulation. License Clearinghouses, as it was mentioned before, might as well a general term as a server for issuing a license. It issues a license needed to decode a message of contents in code. Business models like IMPRIMATUR and MPEG, have been using a technical term, 'Monitoring Authority'.

3.2 Analysis of existing models

DRM technology is necessary for digital contents to be circulated in a market and there is a conflict between the owners who has the copyright of contents and the Internet users who want to use contents on free. Therefore, there has been a slow development of that. Early DRM manufactures were aimed to make the Internet charged for, but they failed to do so. Now they have been developed many kinds of markets, for example, electronic mail, electronic documents, and circulation of software, etc.

Besides, there are two sales methods. One is an existing solution sales method. The other is the sales method that applies DRM, ASP models. Two kinds of methods support the total process of DRM application. In the side of working method, targets models have been introduced into a market. The target models are divided into license servers and Financial Clearinghouses that have a license and a bill system. Korean DRM solution is consisted of three kinds of solution such as Intertrust, MS and Koreans' own technology. Firstly, there are some companies, Pasu.com and Trusttechnology, adopting Intertrust solution. Pasan.com has used the API supplied by Intertrust.co and provided a financial service by using Financial ClearingHouse and E-Book, A/V (Audio/ Video) contents solution accepting the complicated preservation algorithm. Trusttechnology.co operates a license server by offering preservation of documents as well as E-mail solution to enterprises. It is necessary to set up exclusive client software on every media such as E-Book, Audio/Video, Image, etc. Secondly, DRM Korea Co. is one of companies providing DRM as based on Microsoft. The company has offered contents solution to a small size of an A/V Entertainment market, charged a fee whenever it authenticates licensees for encoded contents. However, it could not prepare the Financial Clearinghouse linked with licensees. This solution uses the Window Media Player of Microsoft as client software. It does not need another S/W for A/V contents but it should have exclusive client software for E-Book. Thirdly, domestic companies of DRM solution such as Markany Co. and Dreamintech Co. have supported DRM solution on the basis of Watermarking and Public key infrastructure as cipher special enterprises.

4. Proposal Scheme

This paper prevents illegal copies by using a Hidden Agent and encourages existing systems to figure out problems of inserting Watermarking and payment for early contents.

4.1 Terms desired of the proposal scheme

Hidden Agents should satisfy the terms desired as fallow.

- The proposed a Hidden Agent should be in the contents.

The Hidden Agent that exists in the contents cannot be removed by optional request of users. If the Hidden Agent is deleted, all contents will be deleted together.

- Hidden Agents will fulfil after offering contents.

The Hidden Agent that exists in the contents is provided with contents.

- As soon as the contents practice on user's computer, Agents load.

- Hidden Agents will be loaded in booting.

After an operating system starts, Hidden Agents will be loaded to prevent illegal copies of contents.

- Hidden Agents include a factor.

To prevent illegal copies of contents, a factor should have its ID and value of key.

4.2 Illegal copies of contents

- In the case of copying contents without the authority of usage or in the case of copying contents without acquiring the authority of the usage.

- The contents are obtained illegally on the Internet.

4.3 Whole system model

The follow schematizes the whole system of DRM.

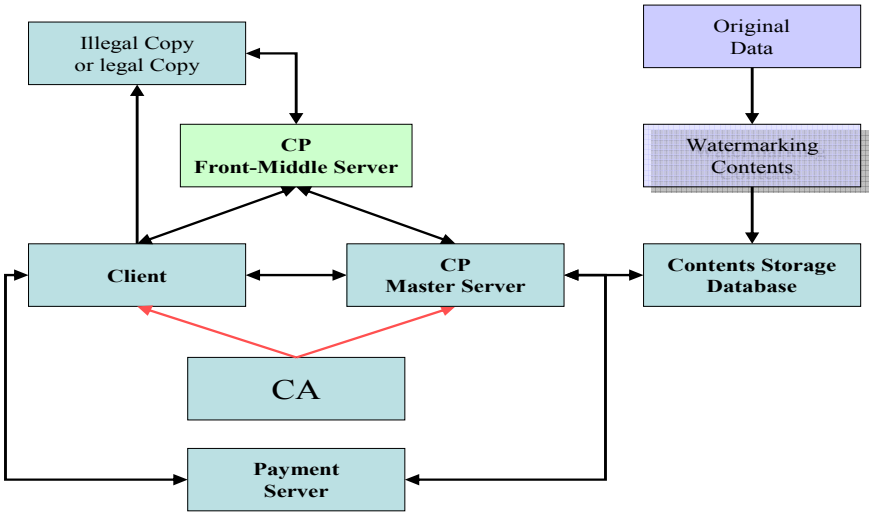

Figure 1. Whole System Model

4.4 Constituents

Explanation of constituent items in this system is followed by next.

A User : wants to purchase contents has a bill and the right of usage. Contents providers create a key for offering contents with Master Servers.

CP Master servers : cover user's registration and have the right of ownership. Also, it creates a key for offering contents as a user does so.

CP Front-Middle servers : communicate with Hidden Agents offered within contents to prevent illegal copies. This item receives user's information from CP Master servers. A user is authorized by Hidden Agents can copy on the basis of user's information.

Payment Server : is located between users and CP Master servers as an item for payments.

Contents Database : is offered contents undergone Watermarking by a writer. In case that a writer is a CP, the CP will get copyright. On the other hand, just in cast of existing a writer, the Contents Database will get copyright.

CA (Certificate Authentication) : is constituted to use signature and put to practical use with payment system and Contents Database afterward.

4.5 System Parameters

This paper explains exchange of keys for offering contents. Hidden Agents need a system coefficient.

- ID : Identify
- K : Contents offer to Encryption Key
- KA : Agent in Encryption Key
- Sig : the Key exchange in signature for Confidential

- user : Signature of User

  - MS : Signature of CP Master Server

- D : authority class
- L : Hash Value
- T : Time-Stamp
- S : Contents class
- M : the Amount paid

4.6 Explanation for each stage of protocols

In this paragraph, this paper gives an explanation for each stage of protocols. The Figure 4 diagrammatizes the way in which Hidden Agents are offered in the contents and the picture shows general contents of Hidden Agents.There are three steps totally, 'contents offering stage', 'contents payment stage', and 'verification stage of contents' through illegal copies. The rest except 'contents payment stage' will follow the existing system for the matters of payment. You can see the detail explanation for each stage.

4.6.1 Contents offering stage: The next paragraph explains exchanging keys between users, CP master Servers and CP Front Middle servers, as well as the process of providing user's information.s

Phase 1. A user sends a sort (S) of contents that the user wants, and values for payments to CP Master Servers.

Phase 2. is a process of transferring user's keys to supply contents.

- gx, siguser(ID || gx || S)
- D = S + M
- L = H(ID || D)

Phase 3. sends a server key after making the value of a key by using the value received from a user.

- K = gx + gy
- gy, sigMS(gx || S || M)

Phase 4. sends a massage of finishing exchanging keys by using the value received from a user.

- K = gx + gy
- Finish_Message

Phase 5. sends the factors created in the master servers to Front-Middle servers.

- (ID, L, D, M, S, T)

Phase 6. Master servers send the Hidden Agent that is suitable for users after inserting in the contents.

- EK(C(A)|| T)

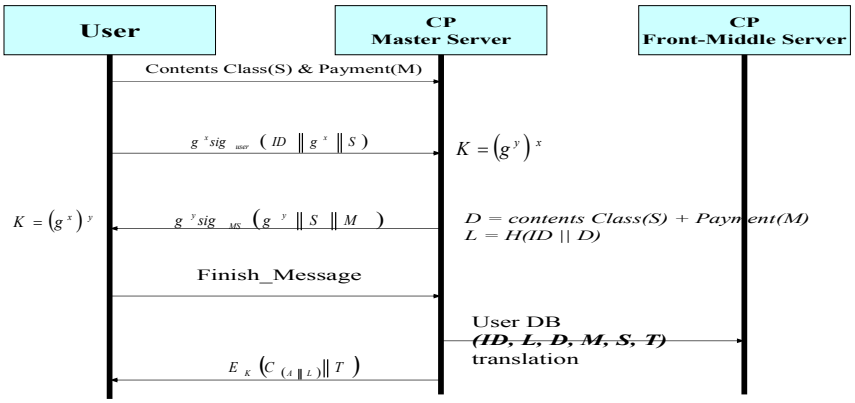

Figure 5. Contents offering Stage

4.6.2 Verification stage of contents illegally copied: In case that a user wants to copy contents illegally, what kind of reaction from Hidden Agents is explained as follow: As it was explained previously, Hidden Agents conduct after supplying contents. If a user commands orders like 'COPY' and 'MOVE' on an operating system, a Hidden Agent will start to work by using the keys received from a server. The Agent encrypts ID, S, M, T, L, R and sends them to Front-Middle Servers. The Front-Middle sever will work only with a Hidden Agent. If the Agent cannot connect with a server, the right of copy won't be provided for a user.

Phase 1. If the order of copy acts on user's computer, a Hidden Agent will not only run automatically, but also encode S, M, and T. Then the Agent will send them to a Front-Middle server.

- EKA(ID || S || M || T)

Phase 2. The Front-Middle sever will calculate 'D' and 'L' by using ID, S, and M, and compare them with its database. It allows a user the right of copy.

- D = S + M
- L = H(ID || D)
- EKA(ID || YorN)

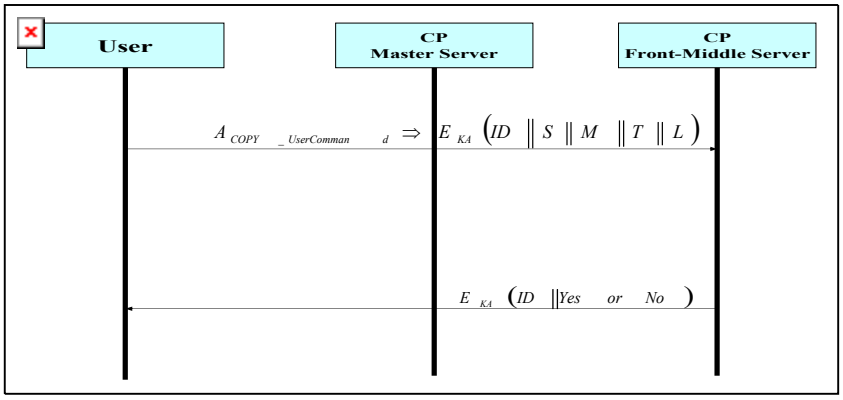

Figure 6. Verification stage of contents illegally copied

5. Inquiry into proposed system

This paper proposes how to prevent illegal copies by using a Hidden Agent. Through inserting a Hidden Agent in the contents, a user has the limitation of the right of usage of contents. A user can receive the right of ownership only from CP and use contents with copyright. Even if a user copies contents illegally, the user cannot get the value of 'R'. It means that Hidden Agents and Front-Middle severs cannot calculate 'D', 'L' so the illegal copy won't be verified. When a user copies all contents illegally, the value of 'R' will be changed to distinguish itself from original value. Through this process, illegal copies will be prevented. Even if a user tries to copy contents with a legal way, the user cannot copy it successfully since Hidden Agents have the right of copy for a Front-Middle server. Another feature of preventing illegal copies is that when a Hidden Agent doesn't have the right of a Front-Middle server, a user cannot delete illegal copy because it doesn't allow contents to be copied. If some files circulated by illegal copies, a Hidden Agent locating in the contents will check its ID and verify responsibility for the fulfillment of contents.

5.1 Analysis and compare with existing method

In this section, a proposed method will be compared and analyzed with an existing method.

The Table 1 shows the result after comparing and analyzing a proposed method with existing one. Some existing systems can prevent illegal copies of MP3, but there is a bad situation that a devil user can distribute data and keys of MP3. In such case, it is hard to prevent those illegal copies. However, this proposed system could prevent even that damages

when such illegal distribution happens because it has keys of a Hidden Agent and CP Front-Middle severs. In addition, since there is the value of 'R' that is created in the Hidden Agent, illegal distribution of MP3 data can be prevented.

[Table 1] Analysis of Proposal Scheme

	Contents illegal copy protection	Contents illegal distribution protect	Contents eavesdropping	License Server working	On/Off-Line Application	Contents robustness	Independence player
Pasu.com	O	×	O	O	×	×	O
TrustTech	O	O	O	O	△	×	×
DRM Korea	O	O	×	O	△	O	×
DreamIntech	O	×	O	O	×	×	O
MarkAny	O	×	×	O	×	O	O
Proposal Scheme	O	O	O	×	O	O	×

Existing systems such as Pasu.com, Dreamtech, and Markany have used independent players to prevent that kind of situation, but it seems to be difficult for existing systems to expand into wireless environment and to be impossible for original contents to be potent because of frequent ciphers. Besides the proposed method has convenient feature, compared with existing systems. The great feature is that the proposed Agent just restricts the right of copy however the old systems should pass all time-consuming processes of Authentication for each content and then it can play the contents. After a user purchases contents at first, he/she has to get authentication every time. This process makes the user feel irritated. However, the proposed method only has some limitation to use some orders like 'COPY' and 'MOVE'. It means that a user can use contents as the same as regular contents.

6. Conclusion

There have been many researches into DRM. Protection of contents in distributing and managing is the most important part of processes. An existing method using a exclusive player and a Smartcard has some obstacles that a user feel inconvenient because of frequent authentication for getting contents. This proposed method has made effort to solve the problems. This paper proposes the DRM models for preventing illegal copies by using a Hidden Agent. Users can use an existing system without alteration and even they don't know the existence of a Hidden Agent. Moreover, this method can be used wired and wireless environment since it is different from an existing system, especially an exclusive player. A user doesn't have to make effort to install a Hidden Agent in the contents. Through a Hidden

Agent, illegal copies will be prevented and people easily can approach whole DRM models. To improve the proposed method more efficient and convenient, this paper suggests homework like how to connect the right of ownership of original contents with payments, and how to supply anonymous users contents. Those DRM technologies will encourage the changes of current software circulation system in which people can purchase products like CD off-line, as well as on-line sales such as digital contents for entertainment and amusement.

7. References

[1] Wanger N. R, 1983. "Fingerprinting", IEEE Symposium on Security and Privacy

[2] Lee K. H. 2001 "A Contents Protection Technology based on Mobile Agent", Korea Multimedia Society review. pp 164-171

[3] Vigna A., 1998, "Cryptographic traces for Mobile Agents", In:G.Vigna(Ed.), Mobile Agents and Security, Springer-Verlag, Lecure Note in Computer Science 1419, pp 99-113

[4] Hohl F., 1998, "Time Limited Blackbox Security: Protecting Mobile Agents from Malicious Hosts", In:G.Vigna(Ed.), Mobile Agents and Security, Springer-Verlag, Lecure Note in Computer Science 1419, pp 137-153

[5] Sander T. & Tschudin, 1997, "Toward Mobile Cryptography", International Computer Security Institute (ICSI), TR-97-049

[6] http://www.intertrust.com

[7] http://www.uspto.gov

[8] http://www.markany.com

[9] http://www.dreamintech.co.kr