Abstract—Digital rights management allows content providers to control the distribution and usage of digital contents for their e-commerce applications. Most of previously proposed digital rights management mechanisms focus on the protection mechanisms for digital contents and pay less attention to the discussion on business models and users’ convenience. It will decrease effective distribution for digital contents and the intentions of users’ usage. With the superdistribution model, we first propose a digital rights management system that increases distribution channels to increase the efficiency of distribution for digital contents. Then, we implement the proposed digital rights management system by using the API Hook with Microsoft Foundation Classes (MFC) as a wrapper. The implemented digital rights management system can achieve content protection without sacrificing user’s convenience. In addition, the proposed digital rights management system satisfies the following requirements: description, identification, transaction, protection, monitoring, tracing, superdistribution, transparency, and portability.

Keywords-component: Digital Rights Management, API Hook, Wrapper, Transparency

I. INTRODUCTION

With the rapid development of Internet and computers, more and more digital contents including text files, audios, and videos can be distributed through public network channels. However, it is easy for a pirate to illegally copy, use and distribute those digital contents from public channels. Intentional piracy of digital contents has become a serious problem. The consequence of pirating has brought large amount of revenue loss to the digital content providers [12]. Digital Rights Management (DRM) is a mechanism which applies cryptosystem to defend against unauthorized copy or usage and protects the rights of digital content providers [8, 12]. DRM can be used to track and manage the utilization of digital contents, including copy permission, distribution, and legal issues.

In 2001, Iannella [9] proposed a DRM architecture, and the architecture describes how core entities interact with each other to protect a digital content and its distribution. The architecture points out that a successful DRM must consider both content protection and content distribution. Since then, a variety of research works have been published [2-3, 5, 7-8, 10-11, 13-14, 18-21, 24-26, 28]. However, most of them only focus on content protection and do not consider effective content distribution in order to earn more profits.

Liaw et al. [13] proposed a complete digital rights management process design. However, they do not specify any method for offline tracking. Furthermore, their scheme does not support rights transfer and the rights revoking as they package all files including digital contents, rights expression language, and monitor module into a single protected file. Their mechanism does not support superdistribution either.

Sun et al. [24] introduced an improved system to rectify privacy deficiencies of the identity-based DRM system proposed by Conrado. Moreover, their system retains users’ privacy by removing the relationship between users and digital contents. Nonetheless, they only mentioned that digital contents are protected by using secure memory and their work does not monitor the use of digital contents.

Sun et al. [25] designed a ticket based DRM to solve user privacy problem. Although their scheme introduces a new role as service provider and uses the ticket issuing mechanism to protect users’ privacy, this system may encounter unavailability problem and require enormous computing cost from users as it consumes considerable computing power to perform a partial blind signature mechanism.

In view of currently existing multimedia application systems, such as Windows Media Rights Manager, iTunes, Adobe Systems, the vendors only support their own digital content types and thus do not offer system transparency for the sake of users’ convenience. System transparency is an important feature for users who can use a new system without changing their using behaviors and habits [27].

A successful DRM system heavily relies on its support capability to business models of digital content providers as well as potential customers. In 1990, Mori and Kawahara [18] introduced the concept and architecture of superdistribution for software distribution. Under such architecture, the chosen target of software can be available
freely in various distribution channels without restriction in an encrypted format. Lately, Hwang [8] successfully employed superdistribution into the design of a DRM system for digital contents in a more creative and effective manner [12, 15-16]. A DRM system with superdistribution has the advantages of increasing distribution channels, reducing costs, and forming strong partner networks [12, 15-16]. Thus, a DRM system is successful if the following requirements are satisfied [8, 12, 15-16, 18, 23]:

**Description:** For consumers to know what the digital content is before they buy it, content information description and preview should be provided in the system.

**Identification:** A digital content must be uniquely identified. Thus, each digital content should be assigned a unique number.

**Transaction:** To support transactions of the protected digital content, various transaction processes should be defined or provided.

**Protection:** Only an authenticated consumer can use the corresponding digital content. In our system design, cryptosystem is adopted to encrypt the digital content and only legal and authenticated user owns the decryption key.

**Monitoring:** To assure every action from a user is valid, a DRM system should provide monitoring feature. In our system, API HOOK technique is adopted to monitor consumer’s behaviors on content usage.

**Tracing:** Content provider may want to know how consumers use purchased digital contents, so the system should be able to transfer usage records of consumers from their devices to the content provider.

**Superdistribution:** It can increase the distribution channels when a DRM system supports superdistribution. In our system, we separate content usage license from the content itself to facilitate content distribution.

**Transparency:** In our system API HOOK is implemented to achieve monitoring feature and allows consumers to keep using his favor media player.

**Portable:** In our system, online authentication and smart card authentication mechanisms are provided for consumers to use contents in different devices.

In this paper, we propose a novel DRM system that adopts the superdistribution model to increase distribution channels and consequently support more versatile business models. We also implement a prototype for the proposed DRM system using the API Hook technique from Microsoft Foundation Classes (MFC) as a software wrapper to achieve system transparency and provide user’s convenience. Note that our implementation is under Windows 32-bit platform.

II. THE PROPOSED THEME

In this paper, we propose a secure, fair and effective DRM system to support the distribution and management of digital contents through Internet.

Our system model is shown in Fig. 1 and stakeholders of this whole system model are introduced as follows.

Consumer (C): A consumer who utilizes this system is to consume digital contents. A consumer buys digital contents from the digital content rights issuing management platform, and then completes the payment. Later, the consumer can download the digital contents and obtain the license. Following this, the consumer enjoys his digital contents and can distribute digital contents or get digital contents through superdistribution.

Certificate Authority (CA): CA is the TTP of this mechanism. Its services are as follows: registration of applicants, licenses issuing, licenses revoking, and licenses management. Moreover, it will store evidence during the process of transactions for future judgment should arguments occur.

Digital Content Provider (CP): His alias is the provider. His major tasks are to provide contents produced by the government or publishers and to digitalize authors’ works. Then, he provides these digital contents for distribution.

Digital Content Rights Issuing Management Platform (MP): Its alias is management platform and its services are (1) providing a website to advertise and market providers’ digital contents. This website must contain functions that include flexibility with regard to transaction, licenses issuing, and tracing (2) identifying banks, consumers, and providers. Moreover, it serves as a bridge and manages cash flow.

Bank (BK): Providing financial transactions and related business.

![Figure 1. The proposed DRM system model](image)

The following describes the detailed processes of our mechanism. Our mechanism contains seven phases: Initial Phase, Superdistribution Phase, Content Selection and Authentication Phase, Flexible Payment Phase, License Issuing Phase, Tracking Phase, License Reissuing Phase. We show system notations in this paper as follows:

- ID:<sub>X</sub>: Identity of user X
- PW: Password
- TID:<sub>X</sub>: Temporary identity generated with KryptoKnight
- PM: The selected method of payment
- DID:<sub>X</sub>: Serial number of X’s device. The device may be CPU, smart card, etc.
- MID: MP’s Server ID
- PID: CP’s Server ID
- DCSN: Serial number of the digital content
- L: License of the digital content
- tk: Verification code of the license
- SIG:<sub>X</sub>: Signature with key X
- E:<sub>X</sub>: Encryption with key X
- UR: Grants of the digital content
- UD: The use data of the consumer
- GM:<sub>X</sub>: Rates of X
- AP:<sub>X</sub>: Accounts payable of X
Message 3-2, of the desired content and the desired grants to
Initial Phase
During the initial phase, all participants within this mechanism must register with CA and request certificates. After registration, CP decides on marketing and basic grants for superdistribution. If consumers wish enjoy these digital contents, they must register MP by sending a self certificate, device serial number or smart card. Then, CP registers his content as the following step:
Message 1-1, CP → MP: ID ‖ CON ‖ UR
CP transfers his grants of digital contents in XrML format and sends the digital contents and XrML to MP through a secure channel. MP saves the above information upon receiving it. Figure 2 shows the processes for uploading.

Superdistribution Phase
Potential consumer CN can receive a protected digital content shared by original consumer CO through emails, instant messages, or P2P connections. CN can test the content with the basic grants. If CN is interested, he can buy the content through a DRM controller.

Content Selection and Authentication Phase
After the consumer finishes registration and receives the certificate, he can browse the website of MP or get the content by superdistribution to find contents of interest.
Message 3-1, C → MP: DCSN
The Consumer C sends a request containing the identity of the desired content and the desired grants to MP.
Message 3-2, MP → C:
DCSN ‖ UR ‖ CON ‖ OD ‖ EPKC (UMP)

MP decides upon a temporary private key dMP and generates a public key UMP with Elliptic Curve Diffie-Hellman (ECDH). Next, MP sends the encrypted message PKC to C.
UMP = dMPG

C receives the message and checks the content. If the message is correct, C decides upon a temporary private key dC and generates the private key Uc with ECDH[1]. Next, C generates a temporary identity TIDC with KryptoKnight[17].
dC . Uc = dCG
TIDC = EPKMP (UMP ‖ IDC ‖ Uc ⊕ DIDC ‖ Uc)

Then, C sends the message to MP, including TIDC, the serial number of the content, and the payment method. The payment method may be credit transfer, micro-payment, or credit card payment.

Finally, MP decrypts the message with his own private key. Then, MP identifies C by checking the Database (DB) to see if it has TIDC or not. The process maintains the anonymity of consumers by using a temporary identity that does not involve the personal information of C to avoid the consumers’ privacy leaking.

Flexible Payment Phase
Consumers can buy licenses from online services after authentication. Figure 5 shows the details of the processes:
Message 4-1, C → MP:
UMP ‖ DCSN ‖ PM ‖ EK (SigMP (H (r ‖ UMP ‖ Uc)) ‖ CertMP)
MP decides the temporary private key dMP and generates a public key UMP with ECDH after C requests the desired digital content. Then, MP selects a random number r and generates a session key K (K = H(dMPUC ‖ r)) between MP and C by hashing. After this, MP sends the encrypted messages to C.
Message 4-2, MP → C:
EK (SigC (H (Uc ‖ UMP ‖ CertC) ‖ PM)
C can generate the same session key K (K = H(dC UMP ‖ r)) of MP by using the parameter sent by MP and check the validity after receiving a message from
MP. After checking the validity of K, C returns the related message as a response to MP.

Message 4-3, MP → BK:
\[ DCSN \parallel PM \parallel E_{PK_{MP}}(ID_C \parallel AM_C) \]

MP sends the related message to BK for payment, including the serial number of the content, the payment method, the identity, and the payment amount.

Message 4-4, BK → C:
\[ DCSN \parallel E_{PK_{MP}}(ID_C \parallel TO_C) \]

Message 4-5, BK → MP:
\[ DCSN \parallel E_{PK_{MP}}(ID_C \parallel TO_C) \]

When completing the transaction, BK sends a successful message to inform C and MP that the transaction has been completed, including the serial number of the content, the consumer’s identity, and the message.

Message 4-6, MP → BK:
\[ DCSN \parallel E_{PK_{CP}}(ID_{CP} \parallel GM_{CP} \parallel GM_{MP}) \]

MP sends the profit distribution agreed upon by MP and CP to BK. BK processes the transaction after receiving the above message.

In addition, the TO_C contains a hash of the serial number of the content, the consumer’s identity, and the timestamp. The above messages are also signed with BK’s private key.

**License Issuing Phase**

After payment, the consumer can request the license as to enjoy the content. The details of the process are shown in Figure 6:

Message 5-1, C → MP:
\[ U_C \parallel DCSN \parallel PM \parallel E_{PK_{MP}}(ID_C \parallel TO_C) \]

C sends TO_C to MP for requesting the license. At the same time, they start to agree on the session key K.

Message 5-2, MP → C:
\[ U_{MP} || r \parallel E_K(\text{Sig}_{MP}(H(r \parallel U_{MP} \parallel U_C) \parallel ID_C \parallel E_{PK_C}(L)) \parallel \text{Cert}_MP) \]

MP checks the validity of the TO_C, it issues the license encrypted with K to C.

\[ L = \{DCSN \parallel H(DID_C \parallel MID) \parallel r \parallel UR \parallel OD \}
\]
\[ \text{Sig}_{MP}(DCSN \parallel H(DID_C \parallel MID) \parallel r \parallel UR \parallel OD) \]

Message 5-3, C → MP:
\[ E_K(\text{Sig}_{C}(H(U_C \parallel U_{MP} \parallel OD) \parallel DCSN \parallel tk)) \]

C decrypts the message and receives the license and hashes the identity of C’s device and the license as a token for checking validity in the future. Finally, C sends the token to MP and MP saves the token.

\[ tk = H(DID_C \parallel L) \]

In order to avoid the confusion which results in users’ licenses being reissued if CP requests for license transferring, we do not include CP’s identity in the license. Moreover, we can protect user privacy by eliminating it in the license. Furthermore, users cannot change the grants or other information because they are signed with MP’s private key.

**Tracking Phase**

Regardless of online or offline patterns, the DRM controller must record and trace the processes whereby users enjoy contents so as to protect the contents. Figure 7 shows the details of the process:

Message 6-1, C → MP:
\[ E_{PK_{be}}(U_C \parallel r \parallel \text{Sig}_{C}(H(U_C \parallel r) \parallel UD) \parallel DCSN \parallel tk) \]

When consumers connect to the Internet and enjoy the digital contents at the same time, the DRM controller will verify the validity of the user and usage through MP. The DRM controller sends a request for identification which includes token, using data, and information to MP.

Message 6-2, MP → C:
\[ U_{MP} \parallel \text{Sig}_{MP}(H(U_C \parallel U_{MP} \parallel r) \parallel \text{Sig}_{MP}(H(U_C \parallel U_{MP} \parallel r \parallel UD)) \]

After MP receives the request and determines the validity, it sends information which contains the current state
of information and this is signed with MP’s private key to C. Then, C saves the above information.

License Reissuing Phase

Consumers may lose their licenses. This mechanism allows consumers to request license reissuing. The details of the process are shown in Figure 8:

Message 7-1, C → MP: DCSN || PM || TIDC

C decides the temporary private key dc and generates a temporary public key Uc with ECDH. Then, C computes the temporary identity TIDc and sends the serial number of the content, the payment method for reissuing, and TIDc to MP to request license reissuing.

Message 7-2, MP → BK:

DCSN || PM || EPKc(IDc) || AMC || GMMP

P checks the validity of DIDc by searching its DB after receiving the request. Next, MP notifies BK that C shall pay for the amount of fees.

Message 7-3, BK → MP: DCSN || EPKc(IDc) || TOC

BK processes the transaction and sends a message to indicate that the transaction has been completed to MP.

Message 7-4, MP → C:

UMP || r || EK(SigmP(H(r || UMP || UC)) || IDc || EPK(L) || CertMP)

MP revokes C’s original license and computes the session key K after receiving the message showing that the transaction has been completed. Next, MP reissues the license and encrypts it with K. Then, MP sends the above to C.

Message 7-5, C → MP: EK(SigmC(H(Uc || UMP || L) || tk))

C computes a session key and then generates a token. After that, C sends the token to MP. MP saves the token after receiving it.

III. IMPLEMENTATION

This paper implements a sample of DRM system for protecting digital contents. The implementation contains the following features: attainment of integrity and security by wrapping; monitoring of processes by API HOOK and description of digital rights language with the XrML format. Moreover, this system allows various authentications, including both online and offline authentication with device identity of hardware or smart card. This section provides the architecture of this system.

There are four functional modules in this system, shown in Figures 9 and 10: Digital Content (DC) Management, DC Package, DC Wrapper, and DC Rights Exchange (DCRE). Furthermore, DC Management, DC Package, and DCRE are the modules of digital content rights issuing management platform. DC Wrapper is the module of clients and it starts when we use the services of digital contents.

The following describes the functions of each module:

**DC Management:** This module provides content uploading and rights setting, such as the printing rights, times of use, durations of use.

**DC Package:** What providers hope for is to distribute their contents effectively in order to earn money. Furthermore, consumers must be authenticated and paid for their contents. This system decrypts digital contents to avoid unauthorized use. Moreover, we package the contents to a new file, which includes encrypted content, copyright information, rights expression language, and API HOOK module. Moreover, we support marketing grants and basic grants for supporting superdistribution as well. In addition, the above mechanism makes rights exchanging and rights revoking more easily. Besides, this implementation provides a convenient and the user-friendly interface under an API HOOK by adopting MFC.

**DCRE:** This system supports rights exchanging and rights revoking. As mentioned before, this paper allows providers to pay more attention on business models.

**DC Wrapper:** In this system, we adopt an API HOOK to monitor processes. In addition, consumers need not install plug-in and change their habits.
when getting the proposed DRM support. In other words, this prototype achieves system transparency and thereby inherits all system advantages proposed by Liaw et al. [13]. Furthermore, we propose the concept of DRM controller to solve tracing issue without the need of installing plug-in program.

![Diagram](image.png)

Figure 10. The functions of DC Wrapper

ACKNOWLEDGMENT

This research is supported by the “Digital Convergence Service Open Platform” project of the Institute for Information Industry which is subsidized by the Ministry of Economy Affairs of the Republic of China.

REFERENCES