Multimed Tools Appl (2015) 74:6255–6271
DOI 10.1007/s11042-014-2135-7

A novel approach to rights sharing-enabling digital rights management for mobile multimedia

Zhiyong Zhang · Zhen Wang · Danmei Niu

Received: 23 April 2014 / Revised: 22 May 2014 / Accepted: 27 May 2014 / Published online: 6 June 2014

Abstract Aiming at protecting the copyrights of audio, video and multimedia in mobile consumer electronics, a novel digital rights management (DRM) approach based on mobile Android terminal was proposed. Firstly, the solution adopted AES encryption and decryption algorithm to package multimedia contents, and meanwhile bound digital license to the hardware of the terminal device, as achieved the usage control and secure playback for mobile multimedia contents. Secondly, the license was written with Extensible Markup Language (XML), and especially a digital rights sharing between terminal devices was supported in the scheme. Thirdly, the times of reading and writing were reduced in the process of encrypting and decrypting multimedia contents by the way of introducing the appropriate size of the buffer, which effectively improved the encryption and decryption speed, and shortened the response time of the system. Finally, a prototype indicated that the solution has significant features of high security and faster cryptographic computation speed meeting the practical requirements for digital rights management and sharing by Android platforms.

Keywords Multimedia · Security · Digital Rights Management · Smart Mobile · Rights Sharing

1 Introduction

As digital contents (e.g., e-books, digital images, multimedia audio and videos, etc.) are easily copied and distributed without any damage or omission, as well as valuable digital content products protected by the intellectual property law can also be copied by batch without permission and be distributed, spread, and abused through various communication network carriers [16]. Therefore, undesirable outcomes and significant losses are incurred, affecting economic, social, and cultural development [5]. To address this technological problem, digital rights management (DRM) was adopted. The DRM comprises a series of technologies,

Z. Zhang (✉) · Z. Wang · D. Niu
Information Engineering College, Henan University of Science and Technology, Luoyang 471023, People's Republic of China
e-mail: xidianzzy@126.com

D. Niu
School of Computer Science, Beijing University of Posts and Telecommunications, Beijing 100876, People's Republic of China

methods, tools and applications mainly used for protecting the contents of digital products as well as the legal rights and benefits of copyright owners and users [12].

Since the middle 1990s, the research and applications of DRM have experienced offline use, Internet online, content distribution networks, and peer-to-peer network phases [4,23]. Early DRM service providers place a strict control on distribution of digital content and digital rights. Nowadays, when considering the distribution problems, the focus is often on the flexibility of control. The Digital Rights Sharing becomes a critical technology in the DRM system. The traditional DRM system focuses mainly on the transfer of rights between the copyright holders and the users, and put less attention to the sharing of rights among users [22]. In fact, the ability to support rights sharing has significant meanings in the DRM technology. A digital copyright protection system that supports sharing of digital rights between devices can effectively arouse users' desires to purchase and use a digital content, increase users' acceptance for a content protection system, and greatly reduce the users' intentions to attack a copyright protected system.

2 Related works

To protect the copyright of multimedia digital contents, solutions such as Windows Media DRM, which is based on the Windows Media Player by Microsoft, and Helix DRM for media streaming by Real Company, were developed and applied to PCs. But with the development of mobile Internet and the popularity of mobile devices like smart phones, more and more people use the mobile devices to access networks for recreational activities and digital content experiences [17]. Hence, the research and development of the DRM system oriented mobile terminals has become an important direction in the current mobile consumer electronics security.

2.1 Security technologies for digital rights management

Digital content protection mainly involves secure encryption and decryption, provable security for cryptographic protocols [7], and identity-based domain key distribution protocols [20]; whereas the usage control of digital rights covers the language description of the digital rights, usage control technologies, the transparent access based on the file system layer and content semantics [10]. Encryption is currently a popular method for protecting digital contents [19]. This technique encrypts common digital content documents (plain text) into ciphertexts to prevent valuable information from being illegally blocked or stolen, and to protect the copyright of digital contents. Bio-based fingerprint detection for copyright infringement authentication [11], and Traitor Tracing technologies have been also used for DRM system to strengthen digital media protection. For the validation of digital rights, Sachana implemented an effective method for checking rights consistency [15].

2.2 DRM systems based on mobile terminals

Bhatt et al. [2] proposed an individual DRM system based on the peer-to-peer model for the Motorola E680i smart phone to protect users' individual documents, such as photos and recorded videos. The native Android platform protects digital contents and applications through OMA DRM 1.0 solution [3]. Considering its inherent vulnerability, OMA DRM 1.0 solution cannot effectively protect the contents in the equipment. The above mentioned systems and solutions install the DRM system in several kinds of common smart phone systems. However, the DRM system that can effectively protect audio and video contents is

not installed in most popular Android smart phones. Therefore, a mobile DRM system that aims to protecting multimedia contents based on Android platform was proposed in this paper.

2.3 Digital rights sharing

With regard to the implementation mechanism of the digital content (rights) sharing, Digital Video Broadcasting Union first proposed the concept of Authorized Domain (AD) in order to facilitate content sharing between different devices. After that, the OMA DRM design applied this concept in its following versions V2.0 [14], and accomplished rights issuers' (RI) unified management of the domains, including domain creation and revocation, users' joining and leaving of a domain, and digital rights sharing between devices within the domain.

The current researches on DRM digital content sharing emphasize mainly on personal entertainment domains and home network domains [8]. Barhoush et al. [1] presented 11 security requirements of digital content multicast, and comprehensively analyzed available DRM commodity applications. Some disadvantages were identified and improved based on the proposed security standards. Feng and Tang et al. [6] adopted Ergodic Encryption and machine authentication to share purchased license with a result of significant reduction on the overhead caused by dependence on the authorized domain. Win et al. [18] proposed a secure and interoperable distribution mechanism enabling multiple authorized domains, which made the secure and effective content sharing among domains to be possible. Ling et al. [21] proposed JFE (combination of fingerprint and encryption) based on a tree structure conversion security mechanism that combines the fingerprint technology and the encryption technology to provide multiple layers of protection for media sharing. Ma et al. [13] proposed a proxy re-encryption technique to achieve digital rights sharing, and CEK is decrypted and then re-encrypted by the third-party. Lee et al. [9] took another approach that the valid users can distribute several shares from the M shares to other users after the rights are divided equally into M shares and each share is labeled uniquely.

However, none of these designs provide an ideal solution because of few applications or complicated system structure. Therefore, the paper proposed a scheme including the rights sharing module. In this approach, the digital rights license is linked with the hardware profile, thus to achieve an arbitrary sharing between devices.

3 Audio and video protection solution for the mobile terminal

To solve the problems on the audio and video digital copyright protection of mobile terminals, a novel Android MDRM system is presented and realized based on OMA DRM V2.0 specification, as the Android platform currently has the most market shares. The MDRM system can not only effectively protect authorized users' usages of digital contents, but also enable authorized users to share a part of their licenses with other users or devices. The system architecture is shown by Fig. 1.

The MDRM system performs a cycle that starts from contents encryption, package and distribution to users, and ends at the contents decryption and usage control. It protects contents from abusing and sharing without any permission by separating protected digital contents from their usable permits. This step is done to achieve the flexible and secure use control and digital copyright protection of contents. This architecture consists of the server and the mobile terminal. For this MDRM system, the decryption and playing, including the usage control of multimedia audio and video contents on Android platform, are the emphases of the study.

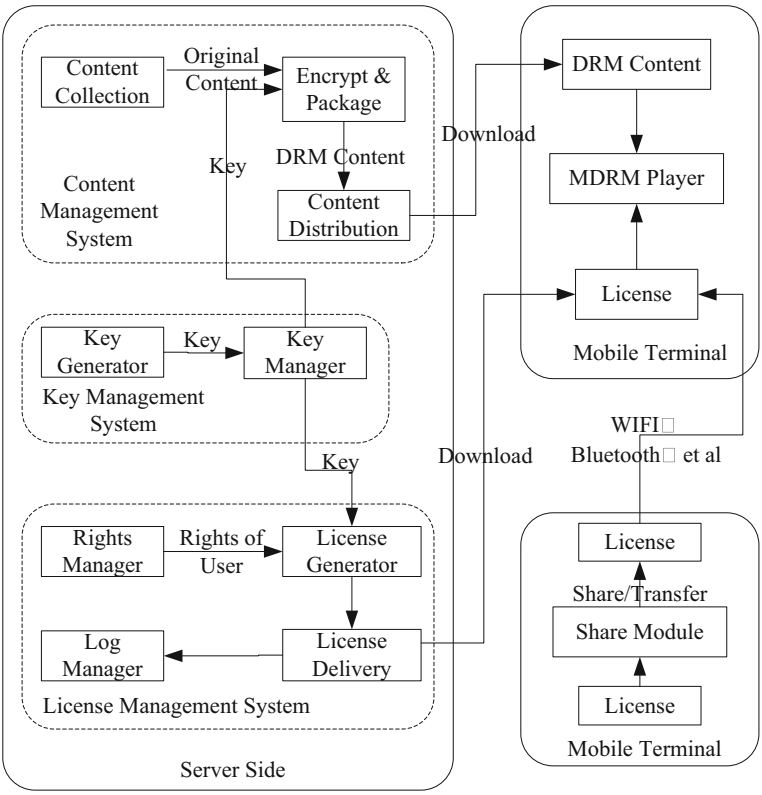


Fig. 1 System architecture of the MDRM

3.1 Digital rights license

The Digital Rights (DR) license is a document in the terminal to control the playing of copyrighted contents. It is generated and delivered by the server. The DR license can be written by using the Extensible Markup Language (XML).

The DR license contains a decryption key of the protected content and users' related permissions to the digital content. In this proposed scheme, the license is bound directly with the device's unique identification number; the license also contains message digests of the important data to prevent invalid dissemination and malicious tampering of the license during of its usage, so as to effectively protect content providers' and authorized users' rights and interests. Table 1 lists the major labels used in the proposed DR license along with their descriptions.

3.1.1 Main elements in the license

Some information in the license is not related to user authorization, but is indispensable for the license. License's unique identification number is provided by the server when the license is generated. When the license is issued, a record will be generated and saved on the server, and it can be accessed to when necessary. Message digests ensure that only the un-tampered digital contents can be rendered on the user device. Before playing the digital content, the calculated

Table 1 List of elements in the proposed DR license

Label	Description
<Rights>	A root element of the license, including<Asset>, <Permission>, and<Digest>.
<Asset>	A root element of some important information related to digital contents, and those are not relevant to user's authorization.
<ID>	The license's unique identification number provided by license management system in the server, when the DR license is generated.
<Content_hash>	The message digests of the digital content, and it is used to verify whether the digital content is tampered or not.
<Key>	The encrypted data of the CEK.
<Permission>	A root element of the user authorized privileges in the license.
<UID>	The unique identification number of the terminal device. It is generated by the DRM Agent in the terminal, and is used to bind license to a specified device.
<Usage_Rule>	Rules of how to use the authorized digital content.
<Count>	The authorized playing times of digital content.
<Deadline>	Expiration date of the license.
<Share>	Value "*T*" means to allow some rights to be shared with other devices; value "*F*" means to deny the operation.
<Transfer>	Value "*T*" denotes to allow the license to be transferred to another device; value "*F*" denotes to deny the operation.
<MD5>	The message digests of the important data in the license are used to verify whether the license is tampered or not.

message digest value will be compared with the reference value saved in the license, and the digital content will be displayed only when those two values are equal.

CEK's encryption *Key* is also included in the digital license, $E(S(UID), CEK)$, that is to say that $S(UID)$ is used as the key to encrypt *CEK*; $S(UID)$ means scramble string *UID* by using scrambling algorithm. This method ensures that only authorized devices can use *UID* to decrypt the encryption *Key* and get *CEK*. Besides, the approach of terminal devices to get *CEK* is denoted as $D(S(UID), Key)$, indicating $S(UID)$ as the key to decrypt value of element *Key*.

3.1.2 Authorization

In the DR license, the authorization rules and usage control determine the user's executable operations on the protected content. This scheme is flexible. Take element *Usage_Rule* for example, if its value is 1, the playing-times-based usage control policy is adopted, which means that the user can execute playing action, as long as the value of element *Count* is greater than 0; when the value is 2, the expiration-based usage control is employed, which means the user can execute unlimited play actions before the expiration date; and when the value is 3, there is the playing-times-and-expiration-based one, which indicates that the user can execute play action when *Count* is greater than 0 and before the expiration date.

The elements of both *Share* and *Transfer* in Table 1 were designed for license sharing and transfer polices, respectively.

3.1.3 Preventing license from tampering

In order to safeguard the license against malicious tampering, the scheme sets element *MD5*. The *MD5* value is the hash value after all the other elements integrate. When parsing the DRM

license, DRM Agent firstly calculates the value of *MD5*, and compares the calculated value with the reference value recorded in the license. If those two values are equal, the validity of the license is verified.

Figure 2 shows an example of the DR license. Here *Usage_Rule* value is 3, which means the playing-times-and-expiration-based security rule, and both of the values of *Share* and *Transfer* are *T*, representing the license can be transferred and shared between devices. The following experiments are based on this scenario.

3.1.4 Protecting license against reusing

Besides the problem of preventing license from tampering, another illegal operation in the process of using license is a license reusing. The operation means that when a user gets a legal license, the user will backup it firstly and intend to further use the backup license after the legal license has been invalid. To avoid this illegal operation, the MDRM Player in this paper creates a database with only one table, which contains two important fields, like *ID* and *MD5*, to storage the unique serial number ID and the hash value of the license separately.

Assume that the license is legal and un-tampered, so the anti-reuse steps can be described as follows:

S1. Check the serial number of the license and the table of the database. If the serial number has not been written in the database, and then write the serial number and the hash value of the license into the database (that is to say the license has not been used in this device before), and return *True* as the result. Otherwise, the following step S2 is executed.
S2. Check the hash vale of the license and the MD5 value in the database. If they are consistent, that means a legal license, and the step S3 is followed. Otherwise, the license would be a backup, and return *False* for the checking result.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<rights>
  <asset>
    <ID>unique_serial_number_of_license</ID>
    <Content_hash>hex_value_of_hash</Content_hash>
    <Key>hex_value_of_encrypted_CEK</Key>
  </asset>
  <permission>
    <UID>unique_serial_number_of_device</UID>
    <Usage_Rule>3</Usage_Rule>
    <Count>65</Count>
    <Deadline>2014-01-01</Deadline>
    <Share>T</Share>
    <Transfer>T</Transfer>
  </permission>
  <Digest>
    <MD5>hex_hash_value_of_license</MD5>
  </Digest>
</rights>
```

Fig. 2 A sample of the DR license

S3. Check the deadline of the license. If it is due, and then delete the record from the database and return *False*, and else return *True*. (This step can limit the size of the database expanding.)

In the runtime of the MDRM Player system, if some operations have resulted in a change of hash value of the license, a synchronous update on the database is needed.

3.2 Use control over multimedia at mobile terminals

The mobile terminal, i.e. the client side, plays multimedia audio and video through the MDRM Player installed in the Android platform. The MDRM Agent that is a core module in the system runtime library identifies, decrypts, and controls the usage of protected contents. Figure 3 illustrates the implementation of this module in the Android platform.

In the original system of the Android platform, the Media Player class directly initiates the multimedia modules in the runtime for processing when the superior multimedia application calls the Media Player class of the application framework layer. In the designed Android player, MDRM Agent module is integrated in the system runtime. When the user utilizes the MDRM Player to play audio and video, the MediaPlayer class in the application framework layer first calls the MDRM Agent module, and then processes the parameters from the MediaPlayer class and activates the operation of the multimedia module. Figure 4 presents the details of the parameter transmission procedure.

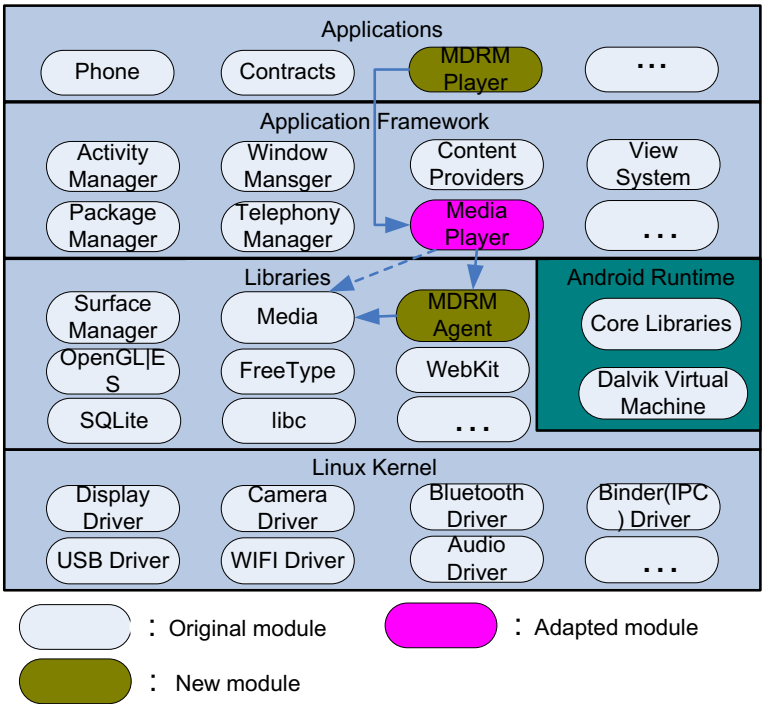


Fig. 3 MDRM Player in Android platform

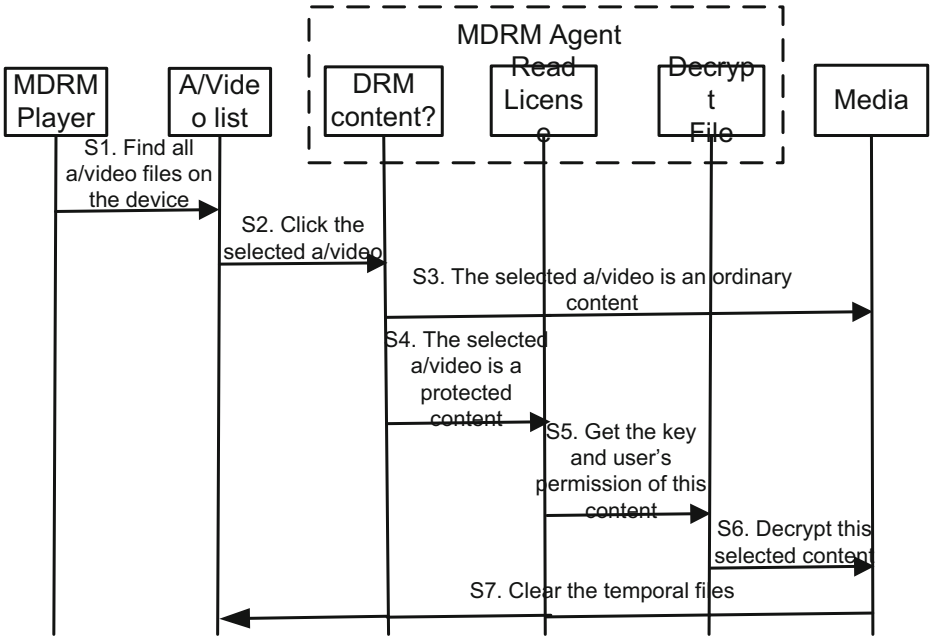


Fig. 4 Information processing by the MDRM Player

Step S1 The user opens the MDRM Player application, and then the player scans the memory space of the equipment to find audio and video documents with the supported formats. After scanning, the audio and video documents are shown in different lists, respectively.

Step S2 The user could select a favorite digital content to play according to those listed audio and video information.

Step S3 After receiving the parameters from the superior framework, the MDRM Agent module in the system runtime layer evaluates whether the selected content is protected. If the content is not protected, the module will directly initiate the multimedia modules to play and render it.

Step S4 If the module finds that the content is copyrighted, it will search for the correct permissions on the contents.

Step S5 After detecting the usable permissions, the MDRM Agent reads its sub-modules to validate related information on the user's right and decryption key. The process of parsing the license is as follows:

1) Read all elements values except *MD5*, and conduct a hash calculation after integrating these values. Next, based on a comparison between the calculation results and the *MD5* value saved in the license, the next step begins, or the system ends with an error.
2) Read and calculate device's unique identification number *UID*, and compare the calculated value with the *UID* value in the license. If both are consistent, and then go to the next, otherwise give an error hint.
3) Execute the procedure of anti-reuse.
4) Calculate the message digests of the digital content, and verify the calculated value by using the *Content_hash* value located in the license.

5) There is a decrease on the authorized play times, recalculation on the MD5 value, and rewriting the *Count* and *MD5* values back to the license.
6) Update the corresponding record in the database.
7) Decrypt the element *Key* to obtain *CEK*.

Step S6 The decryption sub-module of the MDRM Agent analyzes the key gained in Step 5 to decrypt the protected content, and initiates the multimedia to play the decrypted temporary file.
Step S7 After the multimedia module has been played, the temporary document created before is cleared.

The system does not require the user to place protected contents in a specific area in mobile equipments, and not limit the protected contents from the downloadable sources through the specific browser installed in the equipment. Instead, the user may store the protected contents in any area in the equipment. Moreover, the source of protected contents may be downloaded by the user through the same or other equipments, or from a PC through Wi-Fi, USB, Bluetooth, and so on, provided that the protected contents are complete and free of damage. However, the DR license of the protected contents should be stored in a specific location in the equipment.

3.3 Sharing and transferring of digital rights

The main characteristic of XML makes data exchanges easier between different types of devices. Combined with the PC-based DRM Player previously designed, the rights sharing module of this proposed scheme can achieve rights sharing and transfer not only between mobile devices, but also between mobile devices and PCs, which expands the application scope of the rights sharing module. In the DR license, the hardware profiles of the mobile device and PC are extracted by the MDRM/DRM Agent, respectively. The different UIDs ensure to identify different devices. The sharing and transferring of digital rights between devices is as shown in Fig. 5. The DR license directly from the license server was referred to as RO (Rights Object), while the transferred or shared DR license from a user's device was written by TRO (Transferable Rights Object).

3.3.1 Digital rights sharing between devices

In the scheme, the rights license can be shared and transferred between devices at liberty. Therefore, when needed, the user can share some of device A's playing times of content C to the device B, and device B obtains the valid authorization of content C.

Assuming that device A is authorized to play content C with M times, and N times ($N <= M$) would be shared to device B, the sharing process is as shown in Fig. 6.

The detail procedure is described as follows:

1) Open the player and select content C for sharing; check whether device A has a valid license for this content. Here, a valid license means that it has ever not been tampered maliciously, the UID saved in the license is equal to the one extracted from the equipment, the current date is before the expiration date, the value of element *Count* is greater than 0, and the result of the anti-reuse is *True*.
2) Enter into the license sharing interface, and input the sharing times N and device B's unique identification number UID_B.
3) Recalculate $Count_A$ by changing M to $M-N$, recalculate $MD5_A$, and write them back to the license.

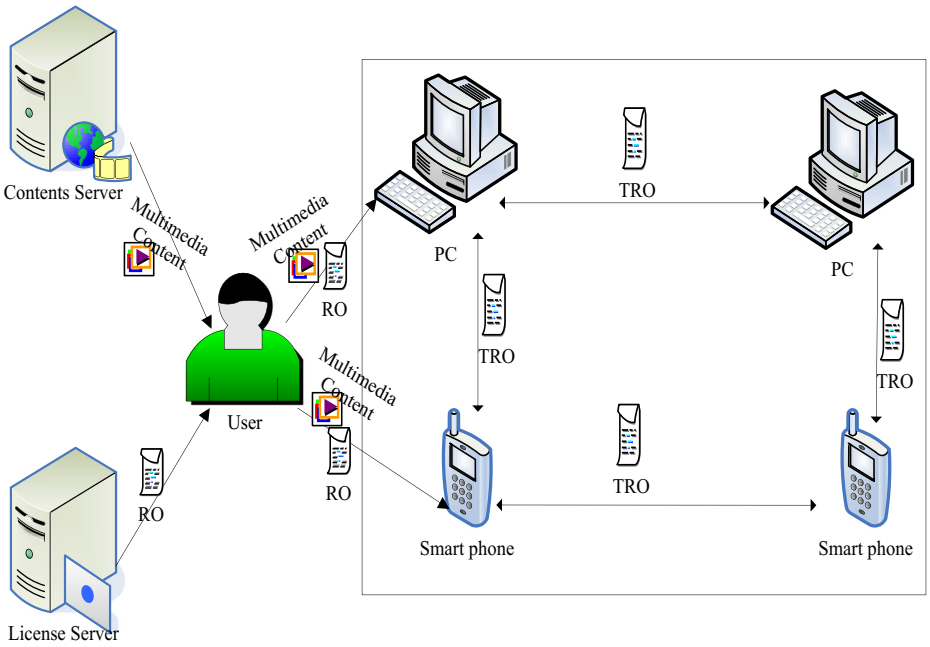


Fig. 5 Sharing and transfer of digital rights between terminal devices

4) Update the record of the database.
5) Read Key_A value, use Key_A and UID_A to calculate $CEK=D(S(UIDA),KeyA)$, and then use UID_B and CEK to calculate $Key_B=E(S(UIDB),CEK)$.

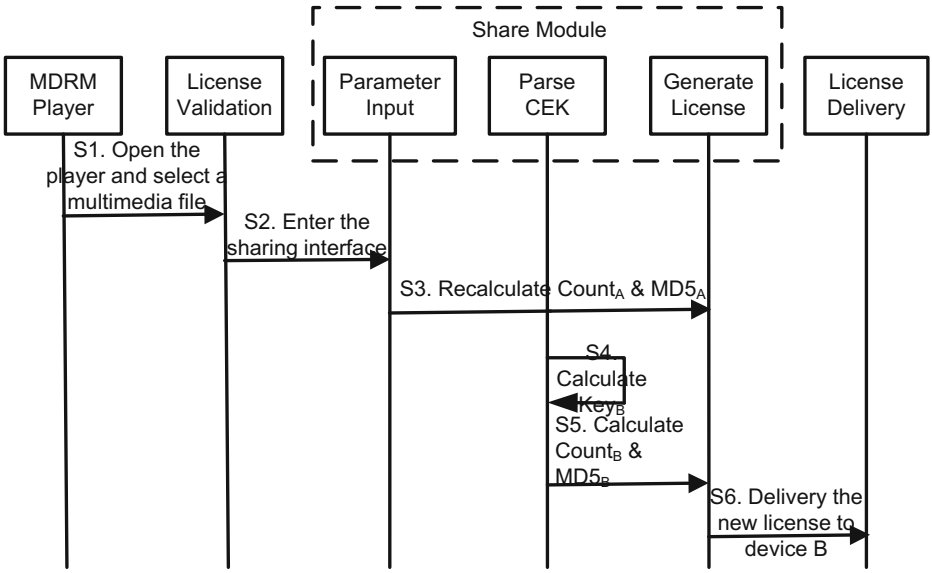


Fig. 6 Information flow diagram for rights sharing between devices

6) Set $Count_B$ value as N, using element values that are associated B to calculated $MD5_B$, and generate and store a new license in the specific location.
7) Deliver the new license to device B, and the sharing is ended.

After those above mentioned, device B starts to have the valid and usable permissions of content C, and the other authorization rules are same to the license in device A before sharing.

3.3.2 License transferring between devices

During of the usage, the DR license may encounter the situation of device replacement, in which an old device is replaced by another new one. In this scenario, if the license in the older device is still valid, the user may require the valid license to be moved from the old device to the new for continue usages. Based on the sample in Fig. 2, the license transferring between devices is as shown in Fig. 7.

We described the above information flow as follows:

1) Open the player and select content C for sharing; check whether device A has a valid license for this content.
2) Enter into the sharing interface, and input device B's unique identification number UID_B.
3) Parse the license and delete it from device A.
4) Update the record of the database.
5) Read Key_A value, use Key_A and UID_A to calculate $CEK=D(S(UIDA),KeyA)$, and then use UID_B and CEK to calculate $Key_B=E(S(UID_B),CEK)$.
6) Use element values that are associated B to calculated $MD5_B$, as well as generate and save a new digital rights license in the specific directory.
7) Deliver the new license to device B, and the sharing is completed.

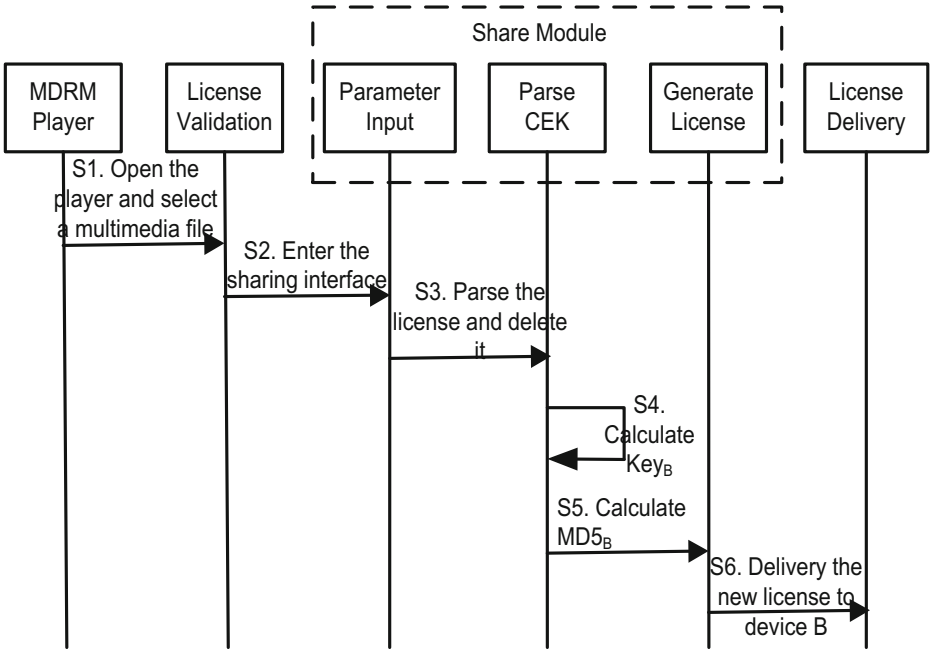


Fig. 7 Information flow diagram for license transferring between devices

Similarly, after those above mentioned, device B starts to have the valid and usable permissions of content *C*, and the other authorization rules are same to the license in device A before transferring.

4 Performance analyses

The experimental tests shows that this prototype can support three kinds of file formats, including MP3, MP4, and 3GP. After importing a valid license, the encrypted files in these

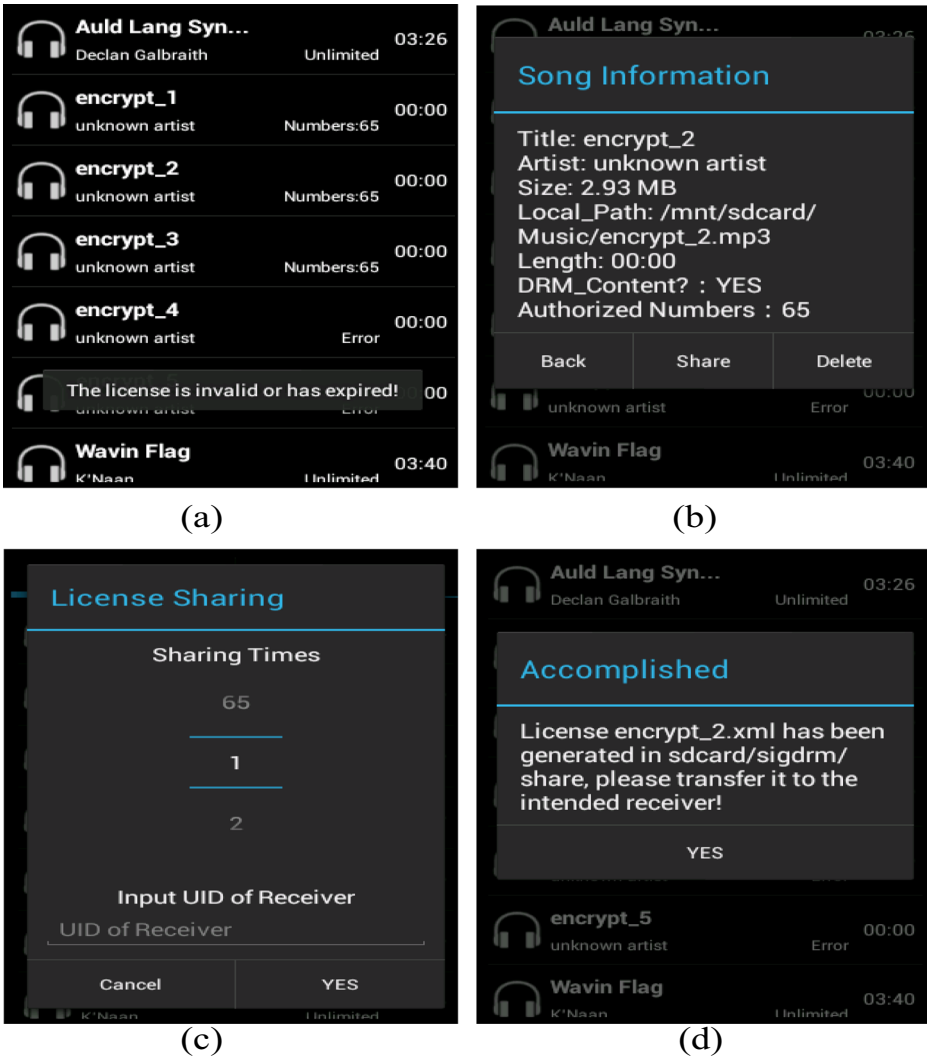


Fig. 8 Screenshots of MDRM implementation **a** License of clicked content is invalid **b** Basic information interface **c** License sharing interface **d** Hint information after a license for receiver has been generated

three formats can also been played normally. Besides, if the license of a multimedia content is invalid, a hint for the user is illustrated as Fig. 8a. Tests and analyses have also been done for rights sharing between Mobile DRM devices, and for the speed of content encryption and decryption.

4.1 Functionality test on rights sharing

In the rights sharing test, device A is a mobile phone with an operation system Android 4.01, and device B is a PC machine. Device A shares the authorized playing times of content *C*. During of sharing, the basic information of a digital content *C* on the list is as shown in Fig. 8b, and clicking the "Share" button to enter the License Sharing interface is Fig. 8c. The two parameters that need to be entered are Sharing Times and the unique identification number UID_B of device B. Finally, a DR license is generated under a specified directory of device A, and this license is the only one that fits device B to decrypt and play content *C*. This license can be imported to a specified directory in device B, and then device B can decrypt and play content *C* properly.

4.2 Efficiency tests on encryption and decryption

The test environment for the encryption package program was a common PC with i3-2130 CPU. The test of the MDRM Player program was located at the Android simulator run by a PC-based UBUNTU virtual machine. Block sizes were set to 102400, 10240 and 1024 to test the two programs, respectively.

This experiment selected two kinds of symmetric encryption algorithms, such as AES and 3DES, commonly used to package and encrypt multimedia contents. Finally, the best encryption algorithm would be used for the scheme was determined by comparing the experiment results. Results of experiment confirmed that the encryption speed and decryption speed of

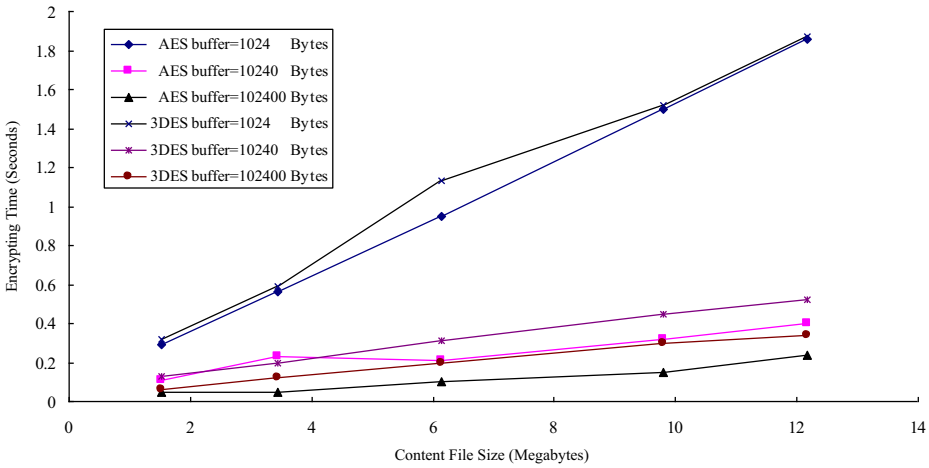


Fig. 9 Test of the encryption package program

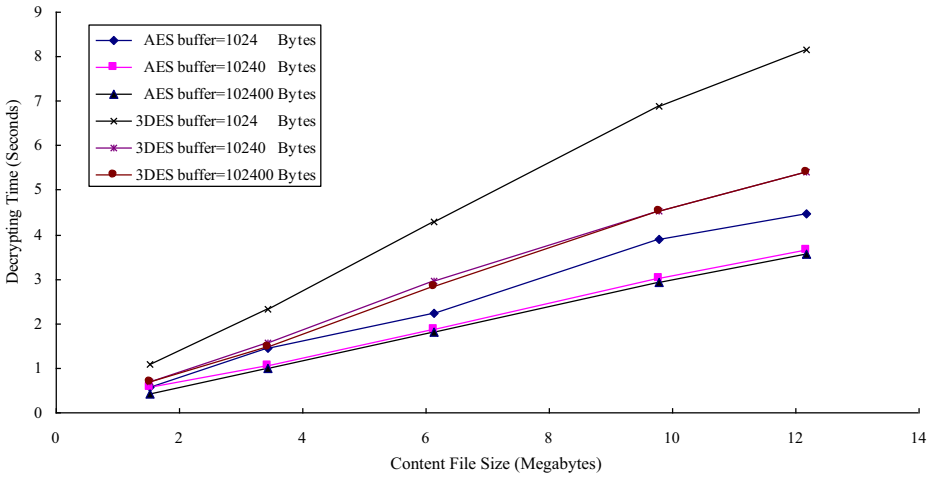


Fig. 10 Test of the decryption program

AES algorithm were both higher than 3DES algorithm under the same hardware environment and block size.

Figures 9 and 10 present the test results of the encryption package program and the decryption program, respectively, in different algorithms and block sizes. The block size of 102400 has the best performance in the AES encryption package program with an average speed of 55.16 MB/s, and it still has the best performance in the AES decryption with an average speed of 3.44 MB/s. Therefore, the AES algorithm was adopted to protect mobile multimedia contents when implementing this scheme.

5 Conclusions

For audio and video digital copyright protection in mobile terminals, the paper employed the Android system, which currently has the most market shares, as the DRM scheme platform. The source codes and compiling rules of Android 4.01 were analyzed. A prototype system was realized according to OMA DRM V2.0 Specification. The experimental results indicates that the MDRM Player can protect copyrighted contents by the users' right and the security rules set in the server side of the MDRM architecture, meanwhile digital rights sharing between devices can be executed securely and freely, which meet the basic requirements of DRM system and users for digital rights sharing.

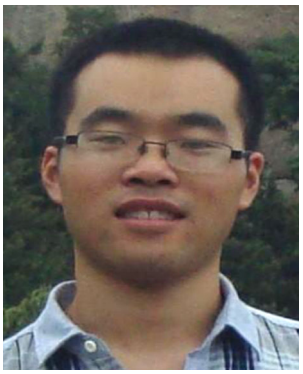
Acknowledgments The work was sponsored by National Natural Science Foundation of China (Grant No. 61370220), Plan for Scientific Innovation Talent of Henan Province (Grant No. 134100510006), Program for Science & Technology Innovation Talents in Universities of Henan Province (Grant No. 2011HASTIT015), and Key Program for Basic Research of The Education Department of Henan Province (Grant No.13A520240, No.14A520048). We give thanks to the reviewers and editors for their valuable comments, questions, and suggestions.

References

1. Barhoush M, Atwood JW (2010) Requirements for enforcing digital rights management in multicast content distribution. Telecommun Syst 45(1):3–20
2. Bhatt S, Sion R, Carbunar B (2009) A personal mobile drm manager for smartphones. Compu Secur 28(6): 327–340
3. Chuang CY, Wang YC, Lin YB (2010) Digital right management and software protection on Android phones. In Proceedings of IEEE 71st Vehicular Technology Conference, May 16–19, Taipei, Taiwan, China: 1–5
4. Diaz-Sanchez D, Almenarez F, Marín A, Proserpio D, Arias Cabarcos P (2011) Media cloud: an open cloud computing middleware for content management. IEEE Trans Consum Electron 57(2): 970–978
5. Fan YC, Shen JH (2009) DFT-based SoC/VLSI IP protection and digital rights management platform. IEEE Trans Instrum Meas 58(6):2026–2033
6. Feng X, Tang Z, Yu Y (2009) An efficient contents sharing method for DRM. In Proceedings of 6th IEEE Consumer Communications & Networking Conference, Jan 10–13, Las Vegas, Nevada, USA: 1–5
7. Koushanfar F (2012) Provably secure active IC metering techniques for piracy avoidance and digital rights management. IEEE Transac Inf Forensic Secur 7(1):51–63
8. Lee J, Jeong Y, Yoon K, Park J (2009) DRM applied contents share in digital home. In Proceedings of IEEE 13th International Symposium on Consumer Electronics, May 25–28, Kyoto, Japan: 64–66
9. Lee S, Kim J, Hong SJ (2009) Redistributing time-based rights between consumer devices for content sharing in DRM system. Int J Inf Secur 8(4):263–273
10. Lee S, Lee HR, Lee S, Kim J (2012) DRMFS: A file system layer for transparent access semantics of DRM-protected contents. J Syst Softw 85(5):1058–1066
11. Lian S, Chen X (2010) Secure and traceable multimedia distribution for convergent Mobile TV services. Comput Commun 33(14):1664–1673
12. Lian S, Chen X, Wang J (2012) Content distribution and copyright authentication based on combined indexing and watermarking. Multimedia Tools Appl 57(1):49–66
13. Ma G, Pei Q, Wang Y, Jiang X (2011) A General Sharing Model Based on Proxy Re-encryption. In Proceedings of 7th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Oct 14–16, Dalian, China: 248–251
14. Open Mobile Alliance™ (2008) OMA DRM Requirements Candidate Version 2.0.1. http://technical.openmobilealliance.org/Technical/release_program/docs/DRM/V2_0_2-20080723-A
15. Sachan A, Emmanuel S, Kankanhalli MS (2009) Efficient license validation in MPML DRM architecture. In Proceedings of the 9th ACM workshop on Digital rights management, Nov 9–13, Chicago, IL, USA: 73–82
16. Thomas T, Emmanuel S, Subramanyam AV, Kankanhalli MS (2009) Joint watermarking scheme for multiparty multilevel DRM architecture. IEEE Trans Inf Forensic Secur 4(4): 758–767
17. Toma C, Boja C (2009) Survey of mobile digital rights management platforms. J Mob, Embed Distrib Syst 1(1):32–42
18. Win LL, Thomas T, Emmanuel S (2012) Secure interoperable digital content distribution mechanisms in a multi-domain architecture. Multimedia Tools Appl 60(1):97–128
19. Wu CC, Lin CC, Chang CC (2010) Digital rights management for multimedia content over 3G mobile networks. Expert Syst Appl 37(10):6787–6797
20. Yan XX, Ma ZF, Yang YX, Niu XX (2012) Identity-based domain key distribution protocol in the E-document security management. J Commun 33(5):12–20
21. Ye C, Ling H, Zou F, Liu C (2012) Secure content sharing for social network using fingerprinting and encryption in the TSH transform domain. In Proceedings of 20th ACM International Conference on Multimedia, Oct 29-Nov 2, Nara, Japan:1117–1120
22. Zhang ZY (2011) Digital rights management ecosystem and its usage controls: a survey. Int J Digit Content Technol Appl 5(3):255–272
23. Zhang ZY (2012) Security, trust and risk in digital rights management ecosystem. Science Press, Beijing

Z. Zhang born on Oct 31, 1975, at Xinxiang City, Henan, China, and received his Master, Ph.D. degrees in Computer Science from Dalian University of Technology and Xidian University, respectively. He was ever post-doctoral fellowship at Xi'an Jiaotong University, China. Nowadays, he is a full-time professor with Department of Computer Science, College of Information Engineering, Henan University of Science & Technology. He is ACM Senior Member, IEEE Senior Member, IEEE Systems, Man, Cybermetics Society Technical Committee on Soft Computing, World Federation on Soft Computing Young Researchers Committee, Membership for Digital Rights Management Technical Specialist Workgroup Attached to China National Audio, Video, Multimedia System and Device Standardization Technologies Committee.

Prof. Zhang and research interests include digital rights management and multimedia social networks, trusted computing and access control, as well as security risk management and soft computing. Recent years, he has published over 60 scientific papers on the above research fields, and held 5 authorized patents. Besides, he is Topic Editor-in-Chief of International Journal of Digital Content Technology and Its Applications, Associate Editor of Social Network Analysis and Mining, and Guest Editor of The Computer J., Journal of Multimedia. And also, he is Chair/Co-Chair and TPC Member for numerous international workshops/sessions on Digital Rights Management and contents security.



Z. Wang born on Feb 27, 1989, at Wuyang County, Henan, China. He is currently a postgraduate majoring in Computer Science, College of Information Engineering, Henan University of Science & Technology. His research interest focuses on digital rights management and mobile consumer electronics security.

D. Niu born on Dec 18, 1979, at Luoyang City, Henan, China. She is currently a Ph.D. candidate majoring in Communication, Communication Network Institute, Beijing University of Post & Telecommunication. Her research interest focuses on computer network security and usage control, and she has published above 10 papers in the above fields.