An Approach to Mobile Multimedia Digital Rights Management Based on Android

Zhen Wang, Zhiyong Zhang, Yanan Chang, and Meiyu Xu

Electronics Information Engineering College, Henan University of Science and Technology, Luoyang 471023, P.R. of China
z.zhang@ieee.org

Abstract. For digital rights management of mobile multimedia in mobile terminals, an Android based Digital Rights Management (DRM) approach to implementing mobile audio and video media usage control was proposed. The solution adopts 3DES encryption and decryption algorithm for protecting multimedia contents security as a whole. The usage of control and display for protected contents were completed in mobile terminal according to the acquired digital license. A prototype confirms that the solution has the features of high security and faster encryption speed, can be helpful to protect the copyright of digital multimedia contents on the highlighted Android of mobile platforms.

Keywords: Digital Rights Management, Mobile Multimedia, Encryption, Usage Control, Android.

1 Introduction

As the technologies for communication network and information dissemination rapidly develop, 3G mobile similarly enjoys increasing popularity while 4G is on its way to contributing to these advancements. Mobile terminals have become a primary electronic equipment and carrier for internet applications. In the realm of 4G networking, wireless data transmission will be as fast and as convenient as cable internet. Moreover, the convenience of mobility and hand holding is an advantage of smart phones over PC terminals. Data from the study of International Data Corporation (IDC) indicate that smart phones with an Android system account for at least half of the market shares of smart phones throughout the world. The Android system is a smart phone system preferred by many users at present. As digital contents (e.g., e-books, digital images, multimedia audio and videos, etc.) are easily copied and distributed without any damage or omission, valuable digital content products protected by the intellectual property law can also be copied by batch without permission and be distributed [1], spread, and abused through various communication network carriers. Therefore, undesirable outcomes and significant losses are incurred, affecting economic, social, and cultural development. To address this technological problem, digital rights management (DRM) was designed. The DRM comprises a series of technologies, tools, flow, and treatment methods mainly

J.-S. Pan et al. (eds.), *Genetic and Evolutionary Computing*,
Advances in Intelligent Systems and Computing 238,
DOI: 10.1007/978-3-319-01796-9_25,

used for protecting the contents of digital products as well as the legal rights and benefits of copyright owners and users [2].

2 Related Works

Encryption is currently a popular method for protecting digital contents. 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. To protect the copyright of 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.

Prompted by the growing significance of smart phones, personal digital assistants, and other mobile equipment, the new trend in the field of DRM research and development focuses on mobile terminals. A series of smart phones based on the Windows Mobile system of Microsoft [3], as well as smart phones and mobile equipment by Apple Inc., have been developed for and applied to commercial trade. The former supports Windows Media DRM solution and handles documents with Windows media video (WMV) and Windows media audio (WMA) formats. The latter utilizes the iTunes developed by Apple Inc. to secure the encrypted digital contents, the copyright of which is protected.

Bhatt et al. [4] 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 [5]. Given its inherent vulnerability, OMA DRM 1.0 solution cannot effectively protect the contents in the equipment. Shuo Zhang, Zhao-Feng Ma et al. [6] proposed a dynamic decryption and playing solution for MP3 documents. This solution encrypts MP3 documents frame by frame according to MP3 document structure. Therefore, it can realize the dynamic decryption and playing of ciphertext during document playing, without creating any temporary documents in the mobile terminal.

The abovementioned 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.

3 Audio and Video Protection Solution for the Android Platform

To solve the problems on the audio and video digital copyright protection of mobile terminals, the originally designed mobile DRM (MDRM) system is installed and realized by considering the Android system, which currently has the most market shares, as the object platform and the OMA DRM v2.0 [7] standard. The system architecture chart is shown in Figure 1.

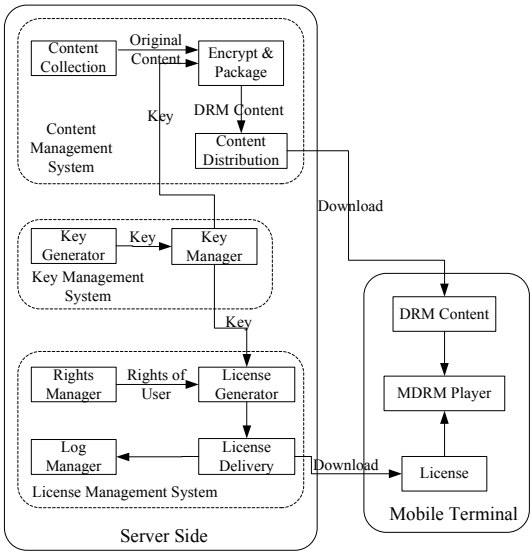

Fig. 1. System architecture of the MDRM system

The MDRM system performs a cycle that starts from content encryption, package, and issuance to the distribution of permits by the content provider and the decryption and content use right control by the users. It prevents contents from being abused and shared without permission by separating protected digital contents from the applicable permit, distributing the same, and controlling the authorized use. This step is done to achieve the safe use control and digital copyright protection of contents. This model consists of the server and the mobile terminal. For this MDRM system, the decryption and playing, including the use control of multimedia audio and video contents based on Android platform, are the emphases of the study.

3.1 Server Side

The server side is composed of the management systems for content, key, and license to perform the encryption and for the issuance of multimedia audios and videos, generation and management of content encryption key, and generation and issuance of multi-media videos and audios.

Content Management System

The triple data encryption standard (3DES) cryptographic algorithm is used for the content management system to encrypt and pack video and audio documents. It is a transitional cryptographic algorithm from DES to advanced encryption standard (AES), and it uses three 56-digit keys to process data thrice.

For audio and video documents requiring encryption for protection, the encryption and package program of the content management system reads the data from the source document through a module with fixed size, initiate the 3DES encryption program to encrypt the read data, and input the encrypted data into the new document. The process is repeated until all the data in the original document are encrypted. The main codes for the encryption program are as follows:

```
/* len refers to the length of the source document; buffer_size refers to the data
  module with a fixed size read every time; fileIn refers to the source document; and
  fileOut refers to the protected document encrypted */
    long j=len/buffer_size;
    for(i=0; i<=j; i++)
    {memset(buffer,'\0',buffer_size);
     fread(buffer,1,buffer_size,fileIn);
     3DesEncrypt(key,buffer,buffer,buffer_size);
     fwrite(buffer,1,buffer_size,fileOut1);}
```

Key Management System

One of the tasks of the key management system is to generate a random character string key for each of the original content to be encrypted and packed, and to supply the generated key to the content management system for encrypting and packing the original document. Another task of this system is to manage effectively these generated keys and return to the encrypting key of the applicable protected content after receiving the request from the license management system in order to generate a license.

License Management System

The license management system generates and distributes the license of the protected contents to legally authorized users. The license is composed of the decryption key of the protected contents and the right of the user to the digital contents. As a prototype system, the license management system defines the right of the user to the protected contents as the authorized times of playing the protected contents in the mobile equipment.

3.2 Mobile Terminal

The mobile terminal, that is, the client side, plays multimedia audio and video through the MDRM player installed in the Android platform. The MDRM Agent module in the system runtime library identifies, decrypts, and controls the use of protected contents. Figure 2 illustrates the implementation of this module in the Android platform.

In the original system of the Android platform, when the superior multimedia application contacts the MediaPlayer class of the application framework layer, the MediaPlayer class directly initiates the multimedia modules in the system runtime for processing. In the designed Android player, MDRM Agent modules are integrated in the system runtime. When the user utilizes the MDRM Player to play audio and

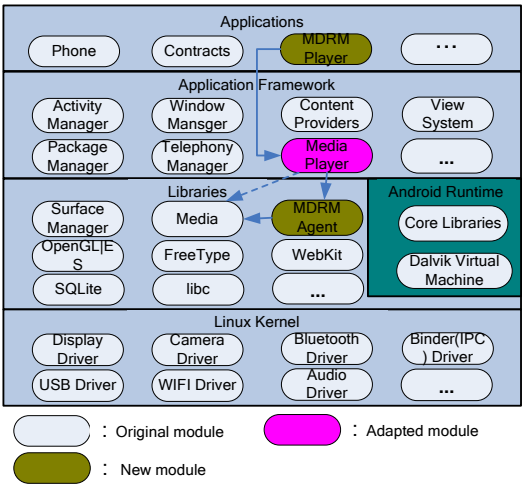

Fig. 2. Android system architecture

video, the MediaPlayer class in the application framework layer first contacts the MDRM Agent module, which then processes the parameters from the MediaPlayer class and initiates the operation of the multimedia module. Figure 3 presents the details of the parameter transmission course.

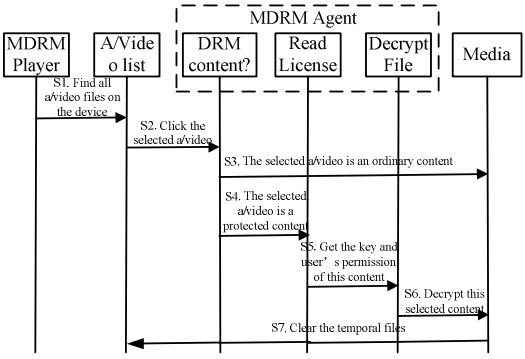

Fig. 3. Information processing by the MDRM player

Step S1. The user opens the MDRM player application, which scans the memory space of the equipment after searching for audio and video documents with the supported format. After scanning, the audio and video documents are shown to the user in list form. For audio document, the list presents not only the document name but also its protection status and the right of the user to it (playing times).

Step S2. The user selects a favorite content to play according to the information indicated in the document list of the audio and video.

Step S3. After receiving the parameters from the superior framework, the MDRM Agent module in the system runtime layer evaluates if the selected content is protected. If the content is protected, the MDRM Agent module will directly initiate the multimedia module to resolve and play the document.

Step S4. If the MDRM Agent assesses that the content selected by the user is protected, it will search for the correct permit.

Step S5. After detecting the correct permit, the MDRM Agent reads its sub-modules to validate the information on the user's right and decryption key.

Step S6. If the right of the user to the protected content is valid (the playing times is higher than zero time), the decryption sub-module of the MDRM Agent will analyze the key acquired in Step 6 to decrypt the protected content and will initiate the multimedia to play the decrypted temporary file.

Step S7. After the multimedia module is played, the temporary document created is cleared and Step S2 is repeated.

The system neither forces the user to place protected contents in a specific area in the equipment nor limits the protected contents to the download sources through the specific browser installed in the equipment. Instead, the user may store the protected contents in other areas in the equipment. Moreover, the source of protected contents may be downloaded by the user through the same or other equipment, or from a PC through Wi-Fi, USB, Bluetooth, and so on provided that the protected contents are complete and damage-free. However, to manage the right permit of the protected contents, it should be saved in a fixed folder in the equipment.

4 Performance Assessment

To test the system performance of the design, the content decryption and encryption speeds of the MDRM system and system safety are respectively tested and analyzed.

4.1 Speed Tests of Decryption and Encryption

The test environment for the encryption package program was a common PC with i3-2130 CPU. The test environment of the MDRM player program was the Android simulator run by a PC-based UBUNTU system virtual computer. Block sizes were set to 1024000, 102400, and 10240 to test the two programs.

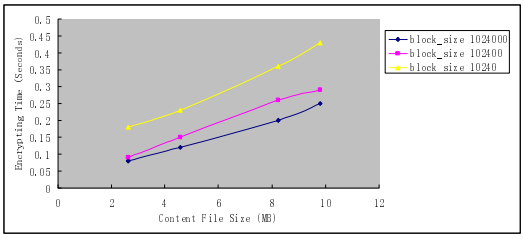

Fig. 4. Test of the encryption package program

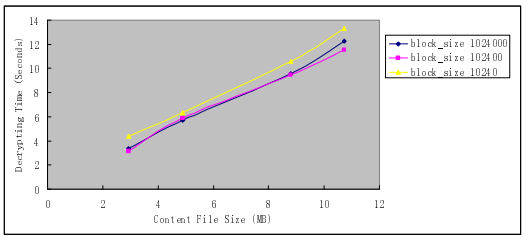

Fig. 5. Test of the decryption program

Figures 4 and 5 present the test results of the encryption package program and the decryption program, respectively, in different block sizes. The block size of 1024000 had the best performance in the encryption package program with an average speed of 38 m/s, and the 102400 block size had the best performance in the decryption program with an average speed of 0.906 m/s . Therefore, in different hardware environments, the scales of the block size of the same encryption and decryption programs vary in terms of the highest speed. Block size scale should be adjusted according to actual conditions during deployment to enhance decryption.

4.2 System Safety Analysis

In the designed MDRM Agent module, the directory of the decrypted temporary document of the protected contents is specified as a folder under the "data" of the system directory. Considering safety, common users of the Android system do not have the right to access and directly manipulate the document under the "data" directory [8]. The temporary decrypted document of protected contents in the Android system is also deleted immediately after being played. Accordingly, the designed system can finish protecting the encrypted contents in the mobile terminal. In this study, temporary document refers to the document created when protected contents are played.

Table 1. Comparison among solutions

	Our system	Literature2	Literature3	Literature 4
Encryption algorithm	3DES	RC4	Unspecified	AES
Save contents in the equipment	Encrypted contents	Encrypted contents	Original directory Specific location	Encrypted contents
Temporary document	with	with	without	Without
Object platform	Android	Mobilinux	Android	Windows mobile

5 Conclusion

For audio and video digital copyright protection in mobile terminals, the author of this paper selected the Android system, which currently has the most market shares, as the

object platform. The source codes and compiling rules of Android 2.3 were analyzed. The designed prototype system was realized and installed based on the Android platform according to OMA DRM v2.0 standards. Results confirm that the MDRM player, one of the system components, can present protected contents by playing within the users' right and according to the rules set in the server-side of the Android platform, thus complying with the basic DRM demands.

Acknowledgments. The work was sponsored by National Natural Science Foundation of China Grant No. 61003234, 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. We would also like to thank the reviewers for their valuable comments, questions, and suggestions.

References

1. Security, Z.: Trust and Risk in Digital Rights Management Ecosystem. Science Press, China (2012)
2. Zhang, Z.Y.: Digital Rights Management Ecosystem and its Usage Controls: A Survey. International Journal of Digital Content Technology & Its Applications 5(3), 255–272 (2011)
3. Toma, C., Boja, C.: Survey of Mobile Digital Rights Management Platforms. Journal of Mobile, Embedded and Distributed Systems 1(1), 32–42 (2009)
4. Bhatt, S., Sion, R., Carbunar, B.: A Personal Mobile DRM Manager for Smartphones. Computers & Security 28(6), 327–340 (2009)
5. Chuang, C.Y., Wang, Y.C., Lin, Y.B.: Digital Right Management and Software Protection on Android Phones. In: IEEE Vehicular Technology Conference, Taipei, Taiwan, pp. 1–5 (2010)
6. Zhang, S., Ma, Z.F., Lu, X.F., Yang, Y.X., Niu, X.X.: Design and Implementation of Music Content Dynamic Encryption and License Authorization System. Computer Science 38(12), 43–48 (2011)
7. Open Mobile Alliance™, OMA DRM Requirements Candidate Version 2.0, OMA-RD-DRM- V2_0-20040715-C
8. Liu, C.P., Fan, M.Y., Wang, D.W., Zheng, X.L., Gong, Y.F.: Light-weight access control oriented tow and Android. Application Research of Computers 27(7), 2611–2613 (2010)