May 2006, Vol.21, No.3, pp.366–369 J. Comput. Sci. & Technol.

Basic Considerations on AVS DRM Architecture

Tie-Jun Huang[1] (黄铁军) and Yong-Liang Liu[2] (刘永亮)

[1] *Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100080, P.R. China*

[2] *Department of Computer Science and Engineering, Harbin Institute of Technology, Harbin 150001, P.R. China*

E-mail: tjhuang@ict.ac.cn; ylliu@jdl.ac.cn

Received November 1, 2005; revised March 14, 2006.

Abstract Digital Rights Management (DRM) is an important infrastructure for the digital media age. It is a part of the AVS (Audio and Video coding Standard) of China. AVS Trusted Decoder (ATD) that plays back digital media program according to rights conditions is the core of AVS DRM architecture. Adaptation layers are responsible for translating or negotiating between ATD and peripheral systems. The Packaging Adaptation Layer (PAL), Licensing Adaptation Layer (LAL) and Rendering Adaptation Layer (RAL) will help ATD to gain the interoperability in various DRM environments.

Keywords digital media, digital rights management, AVS (Audio and Video coding Standard)

1 Introduction

The "Advanced Audio and Video coding standard" (AVS for short) being established by the Audio and Video coding Standard workgroup of China (AVS workgroup) is a fundamental standard in the information technology field. In technical aspect, AVS includes four parts — system, video, audio, and digital rights management (DRM)[1]. AVS DRM aims to offer a universal and open interoperable standard for digital media industry. One of the most important principles in AVS standardization is that the patents in standard must be clear. This is also the case in Digital Rights Management part.

In the process of media industry transferring from analog to digital age, the end decade in the last century could be named as semi-digital period. Although the content on CD, VCD and DVD is in digital, it is the disc that determines the distribution method and business model. Although the program in TV broadcasting maybe is digital and the rights can be controlled by Conditional Access System (CAS), the TV network itself is the key limitation of the TV business.

Since the beginning of the new century, the technical evolvement—the PC with higher performance and the broadband widely deployed—made it easier and easier to record, store, process, deliver and exchange digital audio and video with low cost. The media content can exist in the digital form without any limitation of the physical carriers. MP3 audio being exchanged in the Internet push the Digital Rights Management into massive view. The discussion about DRM in this paper will focus on audio and video media but not general purpose such as e-book application.

A normal definition on DRM from American National Institute of Science and Technology (NIST) is that "DRM is a system of IT components and services along with corresponding law, policies and business models which strive to distribute and control IP and its rights"[3]. In our opinion, DRM is a synthesis of rights protection technology and trust management that runs through the whole life circle of digital media[4]. DRM will be an important part of the infrastructure in digital media age in that the media industry will develop favorably and the consumers can get more innovative experience. The design of AVS DRM part is at the view of infrastructure for digital media.

2 Progress in Digital Media Rights Management

The efforts on DRM for digital media in the past years can be divided into four kinds: CAS enhancement, the content protection technology in consumer electronics, the solutions for IT companies and the standardization initiatives.

More and more conditional access systems for digital TV are enhanced by protecting AV output of the decoder. Operators can define different rights for their programs. For example, the normal programs can be output without any restriction but the movie cannot be output without encryption. In order to support the requirement, the security digital output interface between the decoder and the render device become necessary. HDCP (High Bandwidth Digital Content Protection) that supports protection for data on the two typical digital outputs of DVI (Digital Visual Interface) and HDMI (High definition Multimedia Interface) is requested in USA.

There are many separated efforts on digital content protection in consumer electronics field. CSS (Content Scramble System) from DVD Content Control Association, Secure Digital Music Initiative with the aim to resolve MP3 download issue, DTCP (Digital Transmission Content Protection) focusing on compressed content in home network, CPRM (Content Protection for Removable Media) that protects recording on removable media, Secure Video Processor (SVP) that keeps content

Short Paper

Supported by the National High Technology Development 863 Program of China under Grant No. 2004AA119010.

encrypted until final rendering and AACS (Advanced Access Content System) for high definition optical media. These technologies are focusing on special product or application but not general DRM system.

IT industry is playing a more and more important role in providing end-to-end DRM solution. At first, Intertrust, ContentGuard and other small companies proposed respective DRM solutions[5]. Then Apple DRM system entered into the market with the success of iPod and iTunes. Microsoft provided its DRM solution with Microsoft Media. The trouble is that these solutions are private and may be used as a tool to segment the media market. As a different approach, Sun Microsystems announced DReaM initiative to develop a DRM solution focusing on open-standards-based-solutions that will be open source and royalty-free[7].

As the response to IT companies' success, consumer electronics companies begin to cooperate under the flag of interoperability. The Coral Consortium launched at the end of 2004[7] and the Marlin Joint Development Association started in the beginning of 2005 announced to develop standards ensuring that copy-protected content can be played on any kind of consumer electronics device.

MPEG is the AV source coding standard[8] that is adopted by digital television system and DVD. The MPEG specific term for DRM is Intellectual Property Management and Protection (IPMP). MPEG-2 contains a few tools for the Identification as well as the Protection of copyright on content. While MPEG-2 enabled conditional access systems to be integrated with MPEG-2 technology, there are no provisions for interoperability. In MPEG-4, representatives of rights holders communities raised the problem of protection of content in an early stage. MPEG-4 IPMP covered: identification of content; automated monitoring and tracking of creations; prevention of illegal copying; tracking object manipulation and modification history; supporting transactions between Users Media Distributors and Rights Holders. The aim of MPEG-21 IPMP Components that define structures for expressing information relating to the protection of content, including tools, mechanisms and licenses, is to allow controls on the flow and usage of Digital Items throughout their lifecycle. Even now, the main challenge for MPEG IPMP is still the goal of MPEG—interoperability.

OMA (Open Mobile Alliance) formed in 2002 won the widespread involvement in recent years. DRM is the core of OMA specifications. The scope of OMA DRM 1.0 released in June 2004 is to enable the controlled consumption of digital media objects by allowing content providers to express usage rights. Only basic DRM features — preview and copy protection — are included but not a complete DRM technology. OMA DRM 2.0 released in Sept. 2005 defines the protocols, messages and mechanisms necessary to implement a robust, end-to-end DRM system that takes into account the need for secure distribution, authentication of Devices, revocation and other aspects. Out of specification scope, the Content Management Licensing Administrator (CMLA) was established by four companies to implement a "trust model" that defines a compliant implementation of OMA DRM 2.0 for use with a wide variety of digital client devices and applications (e.g., cell phones, PDAs and PCs). OMA DRM 2.0 is the first real DRM system although it targets to mobile application.

Following the Digital Media Manifesto[9] published in Sept. 2003, Leonardo Chiariglione lead the Digital Media Project (DMP)[10] with the mission to "promote continuing successful development, deployment and use of Digital Media that respect the rights of creators and rights holders to exploit their work, the wish of end users to fully enjoy the benefits of Digital Media and the interests of various value-chain players to provide products and services". DMP finalized the "Interoperable DRM Platform" Phase I specifications (for Portable Audio and Video Devices, PAVs) and will release Phase II specifications (for Stationary Audio and Video Devices, SAVs). DMP specifications draw the outline of the ideal DRM solution in the future.

From the view of AVS, DMP, OMA and other interoperable DRM system will be the environment for AVS standards. As a result, AVS DRM will define not only an end to end solution specification but also the mappings and interfaces that an AVS-compatible device can act as a module in DRM ecosystem.

3 AVS DRM Architecture

3.1 Three Design Principles

Following the other three parts in AVS standard, that only define the features that an AVS decoder should provide, AVS DRM part should define the features that AVS decoder has to satisfy the requirement about rights management. An AVS decoder being conformable with AVS DRM is named as AVS Trusted Decoder (ATD). The basic function for ATD is to replay digital audio and video programs according to the rights claim of the content provider. Here we have the first principle (so called Minimum Principle) for AVS DRM specification that the core of AVS DRM standard is ATD.

ATD should try to satisfy the requirements of various application environments and business models. In other word, AVS DRM should assign strong interoperability to ATD. The peripheral systems of ATD include the content providing system, the licensing system and the rendering system. Consequently, AVS DRM Standard should design the corresponding adapter for them, i.e., the packaging Adaptation Layer, the licensing Adaptation Layer and the rendering Adaptation Layer, to support the interoperability with other DRM specifications that cover these systems. AVS DRM Adaptation Layers should have enough capability to support all kinds of applications. Here we have the second design principle—maximum principle.

Different with DRM specifications that come from legacy version or DRM solutions that must be compatible with running infrastructures, AVS DRM part is specified synchronously with the audio and video coding parts. It is possible to accommodate new technical features in the architecture to provide stronger security, lower complexity and more flexibility. One example is the rights put on AV compressed stream based on its syntax or semantic structure to make the content be rendered partly to users without license but fully rendered to users with license. Encouragingly, these advanced features of AVS DRM make it prior to other standards or specifications. As a result, Innovative Principle is the third design principle that encourages new DRM modules to be proposed to AVS DRM.

As for technical decision, the above three principles should be considered in order. That is, the Maximum Principle should not violate the Minimum principle, and the Innovative Principle should not violate both the prior two.

3.2 AVS DRM Architecture

According to the former principles, AVS DRM Architecture, shown in Fig.1, consists of the ATD, the Adaptation Layers and the peripheral systems.

AVS Trusted Decoder is an extension of the traditional decoder with the addition of an authentication module, a decryption module, a data reconstruction module and an output encryption module.

AVS DRM peripheral systems consist of the content providing system, the licensing system and the rendering system. They are related but not essential components of AVS DRM.

The adaptation layers between the ATD and the peripheral systems are responsible for the interaction and negotiation among them. There are three adaptation layers — Packaging Adaptation Layer (PAL), Licensing Adaptation Layer (LAL) and Rendering Adaptation Layer (RAL).

3.3 AVS Trusted Decoder

To make itself trusted in a DRM ecosystem, a trusted decoder contains some new modules based on a traditional AV decoder. The authentication module provides the identification of the decoder and the security channel between the decoder and the peripheral systems. Typically, the authentication module is based on Public Key Infrastructure. The decryption module is responsible for decrypting the encrypted content by the key received from the authentication module. The design of the decryption module should take into account as many encryption algorithms (such as AES) of the various content provider systems as possible. The data reconstruction module will reconstruct the data with encryption part into plain data that can be decoded by the decoding module. That means a traditional decoder can be put into the ATD as a whole without any change. The output encryption module encrypts the decoded data and then output the result to the rendering system. The selection of the encryption module should consider the decryption algorithm supported by the secure display interfaces.

The ATD should be strongly protected as a whole, for example, as an ASIC chip, or as a software core with the special protection.

3.4 Packaging Adaptation Layer (PAL)

PAL is a middleware between the decoder and the applications that can extract necessary information from various packaging formats. PAL identifies packaging format and extract media data to the ATD, extract licensing data to the License Adaptation Layer and throw other information in the package to the high level applications.

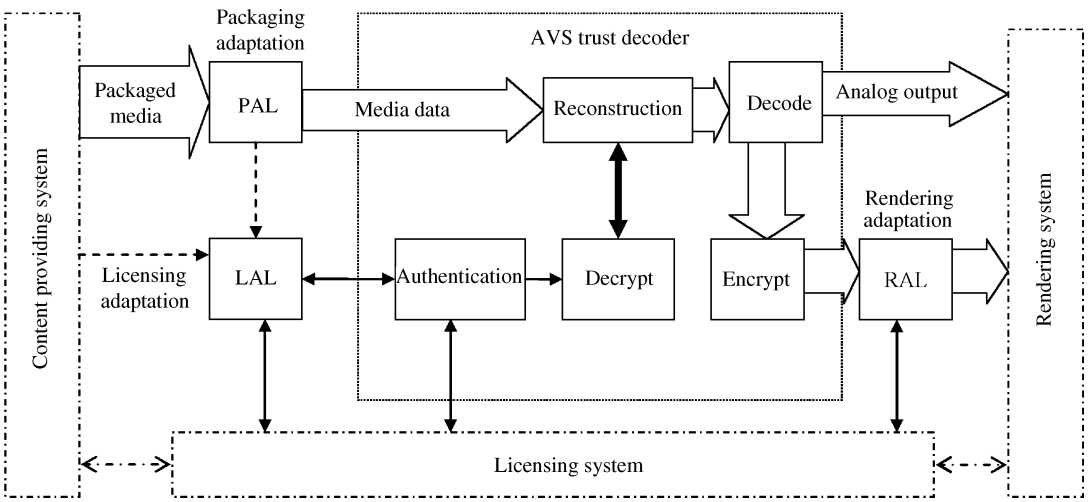

Fig.1. AVS DRM architecture.

PAL should understand the basic format about the media data to find above information. ISO Base Media File Format is the typical baseline format adopted by several media package formats (e.g., OMA DRM, DMP and MPEG-4 IPMP). In this case, PAL can find the format type from File Type Box (ftyp), content from Media Data Box (mdat) and license from License Box (licb). A more flexible approach is to define a DRM ontology as the semantic bridge between different formats. The ontology-based PAL (LAL and RAL in the following subsections) can act as the uniform middle layer between ATD and various packaging formats.

3.5 Licensing Adaptation Level (LAL)

LAL defines the security connection between ATD and the licensing system. The first function of LAL is to establish trust relationship between the ATD and the licensing system by specifying the trust establishment procedure (includes certification) between them in different application environment that can be classified into three conditions: bi-direction connection (such as Internet), uni-direction (such as broadcasting) and non-connection (such as portable MP3 player).

Another function of LAL is to parse the license or negotiate on the licensing condition with the license issuer. LAL may receive a license from PAL or just get a license address or license issuer address. Then LAL extracts right terms from the license or negotiate with the license issuer. At the end, the encryption key and other security data are transferred to ATD. Please notice that the key and other data from license system to ATD should be in encryption form. LAL just transfers them but not understands them.

It is possible for LAL to understand different licenses. The most important component for license is the language that expresses the rights. Two famous languages are ODRL (Open Digital Rights Language) and MPEG-21 REL. [11] implemented the translation and interoperability between them. If a native language embedded in LAL, then other rights language can be translated into the native language at least at the range of expression ability of the native language. Therefore, an AVS DRM implementation can download corresponding translation tool to support new type of license.

3.6 Rendering Adaptation Layer (RAL)

The goal of AVS Rendering Adaptation Layer (RAL) is to support the security communication between ATD and various rendering systems. If the decoding result is requested not in plain by the license issuer, ATD will encrypt the result and send it to the rendering system. What RAL should do is to negotiate with ATD and the rendering system about the encryption algorithm and interaction protocol. The authentication module in ATD can be used to establish trust relationship between ATD and the rendering system by RAL.

4 Conclusion

Under the former architecture, AVS working group is specifying an open digital media rights management standard. There will be more details on AVS Trusted Decoder and the three adaptation layers. AVS Trusted Decoder can be embedded in various DRM applications for its comprehensive security features and flexibility to various business models. The three adaptation layers enable AVS DRM to communicate with any current and future DRM systems. The design will make AVS DRM play an active role in the future infrastructure of digital media world.

Acknowledgement The authors would like to thank the Audio and Video coding standards working group, especially the DRM subgroup, for providing a well environment for the paper.

References

[1] Huang Tiejun, Gao Wen. AVS-background and IPR. *Television Technology*, 2005, 7: 4–7. (in Chinese)
[2] Lyon G E. A Quick-Reference List of Organizations and Standards for Digital Rights Management. NIST Special Publication 500-241. October 9, 2002.
[3] Lyon G E. The Internet Marketplace and Digital Rights Management. Gaithersburg, 2001.
[4] Huang Tiejun, Gao Wen. Basic idea and trend of DRM. *Modern Television*, 2004, 12: 19–21. (in Chinese)
[5] Austin Russ. Digital rights management overview. Security Essentials v1.2e, July 2001, http://www.sans.org/rr/papers/48/434.pdf.
[6] Fernando G, Jacobs T *et al.* Project DreaM: An architectural overview. Sun Microsystems White Paper, September 2005.
[7] Coral Consortium. http://www.coral-interop.org/.
[8] MPEG standards. http://www.chiariglione.org/mpeg/standards.htm.
[9] The digital media manifesto. Sept. 30, 2003, http://www.dmpf.org/manifesto/dmm.htm.
[10] Digital Media Project. http://www.dmpf.org/.
[11] Josep Polo, Jose Prados, Jaime Delgado. Interoperability between ODRL and MPEG-21 REL. In *Proc. the First International ODRL Workshop,* Renato Iannella, Susanne Guth (eds.), Vienna, Austria, April 22–23, 2004, pp.65–76.