# Evolvement of DRM Schema: From Encryption to Interoperability and Monitoring

Tiejun Huang

Institute for Digital Media, Peking University,
100571 Beijing, China
tjhuang@jdl.ac.cn

**Abstract.** By reviewing DRMs up to now and two typical examples – AVS DRM and DMP IDP, the paper tries to find out the fundamental challenge of content protection approach from technical and social viewpoints. Not only it is difficult to deploy and update content encryption and security infrastructure, but also the content diffusion is limited and Fair Use is affected. The new schema for DRM should content monitoring system in public space that prevents illegal diffusion of content in copyright but permits content being used freely in private space or for social liberty. The traditional rights in analog times will fluently move to digital space under the proposed schema.

**Keywords:** DRM, Protection, Interoperability, Authentication, Monitoring.

## 1 Introduction

Although it isn't a normal way to start a technical paper by a literary quotation, I want to start the discussion on digital rights management (DRM) by the famous gnome from Charles Dickens -

*It was the best of times, it was the worst of times, it was the age of wisdom, it was the age of foolishness, it was the epoch of belief, it was the epoch of incredulity, it was the season of Light, it was the season of Darkness, it was the spring of hope, it was the winter of despair, we had everything before us, we had nothing before us, we were all going direct to heaven, we were all going direct the other way - in short, the period was so far like the present period, that some of its noisiest authorities insisted on its being received, for good or for evil, in the superlative degree of comparison only.*

*(From A Tale of Two Cities)*

The DRM story came into the view of public and mass media from the transition to the new millennium when more and more audio and video contents in copyright or out of copyright were digitized and bestrewed into Internet to be shared by public. The PC with higher performance and the broadband widely deployed – made it easier and easier to record, store, process, deliver and exchange digital content with low cost.

When someone cheer for the best of times in digital, some others despair for the lost of control on their content in the worst of times for copyright.

N. Sebe, Y. Liu, and Y. Zhuang (Eds.): MCAM 2007, LNCS 4577, pp. 65 – 75, 2007.

The fundamental reason for this is media content in digital can exist and be spread without limitation of the physical medium. In analog times of last millennium and before that, physical medium shapes the content (e.g. characters and figures on bones, stone, metal) and become the measure to control it's copyright (e.g. paper book, audio and video tape and movie on plastic DVD). DMCA (The Digital Millennium Copyright Act) seem to be signed by US President at the end of last millennium to prove specially the forecast of Charles Dickens. After DMCA, the MP3 on Internet strongly crashed the record industry and MP4 and others online digital video technology began to strike video industry.

Digital rights management was expected to save the content industry. Various DRM technologies, solutions, standards were proposed in last several years and partly deployed but effect is limited. From Conditional Access System for DTV to HDCP (High Bandwidth Digital Content Protection) that protects data from STB to TV monitor, more and more separated efforts appeared to protection in consumer electronics field. CSS (Content Scramble System) from DVD Content Control Association, Secure Digital Music Initiative for MP3 player, DTCP(Digital Transmission Content Protection) for home network, CPRM (Content Protection for Removable Media) for recording on removable media, Secure Video Processor (SVP) for decoder and AACS (Advanced Access Content System) for high definition optical media. The Coral Consortium launched in the end of 2005 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 by converting from one DRM format to another by accessing a conversion service.

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 solution. Then Apple DRM system entered into the market with the success of iPod and iTunes. Microsoft provided its DRM solution with Microsoft Media. 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.

Fairplay – the DRM system from Apple - is the most successful one in the market. Facing the complaint about a private solutions like Fairplay may be used to monopolize market in last year, Apple is appealed to open it's DRM so that music purchased from iTunes can be played on digital devices purchased from other companies, and protected music purchased from other online music stores can play on iPods. Steve Jobs fights back by "thoughts on music" [2] with the following key points:

(1) Only 22 out of 1000 songs, or under 3% of the music on the average iPod, is purchased from the iTunes store and protected with DRM. In other words, Fairplay and his congener from Microsoft and Sony etc doesn't divide the market into several unconnected garden, 97% world of the music world is open without DRM.

(2) There is no theory of protecting content other than keeping secrets...one must still "hide" the keys which unlock the music on the user's computer or portable music player. If Apple doesn't keep the secret itself but license it to its competitor, the security of DRM will come down.

(3) DRMs haven't worked, and may never work, to halt music piracy. To abolish DRMs entirely so that every online store sells DRM-free music encoded in open

licensable formats. This is clearly the best alternative for consumers, and Apple would embrace it in a heartbeat.

Is Jobs right? For thought of music, maybe right. For thought of DRM, partly wrong. But anyway, Job's thought provide an exact point to review the short history of DRM and foresee its long future.

This paper try to find an answer by analyzing and comparing the three DRM schemas – protection by cipher technology, interoperable DRM infrastructure and content-based media authentication and monitoring in public space.

Firstly, this paper will review the AVS DRM from the Audio and Video coding standard of China for which the author is a major designer. The sample DRM shows that it is possible to design a DRM standard by which all the players in a market can focus on respective DRM products at different chains and inter-operate without comedown of security. In fact, there are many other successful cases outside of DRM field that doesn't control by one company. For example, e-business and its security infrastructure are open and secure in practical sense.

For the more, it is also possible to construct a worldwide interoperable DRM infrastructure also. Starting from the Digital Media Manifesto[6] published in Sep.,2003, Leonardo Chiariglione lead the Digital Media Project (DMP)[7] 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 works, 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 released the "Interoperable DRM Platform" Phase I specification (for Portable Audio and Video Devices) in 2005 and Phase II specification (for Stationary Audio and Video Devices) in 2006. Phase III specification that tries to be media infrastructure will be release in 2007.

The fact that under 3% of the music is protected with DRM Fairplay pricks a bubble that protection approach is an effective measure for rights management. In the last section, by analyzing the disadvantages of current DRM, this paper will clarify the simple target for digital rights management is to prevent the diffusion of content in copyright in the public space like Internet and allow the Fair Use in the private space of consumer and commonweal space like library and classroom. To meet this target, content-based media authentication and monitoring for plain content should replace cipher-based media encryption and watermarking. And as a result, media usage in analog times will be back. The analog holes in current DRM will be blocked also.

## 2 AVS DRM: Simple But Typical DRM

Among dozens of DRM solution today, AVS DRM is a sample but typical one. Alike the video and audio coding standard from the Audio and Video coding Standard Working Group of China tries to provide an uniform AV format for the country to avoid possible bulwark between different AV systems such as DTV broadcasting systems, IPTV and storage AV player, the DRM part of the national standard tries to avoid possible rampart generated by different cipher technology in DRM. Uniform AV coding and DRM standards will decrease the total cost for media industry and consumers by boosting competition at products level.

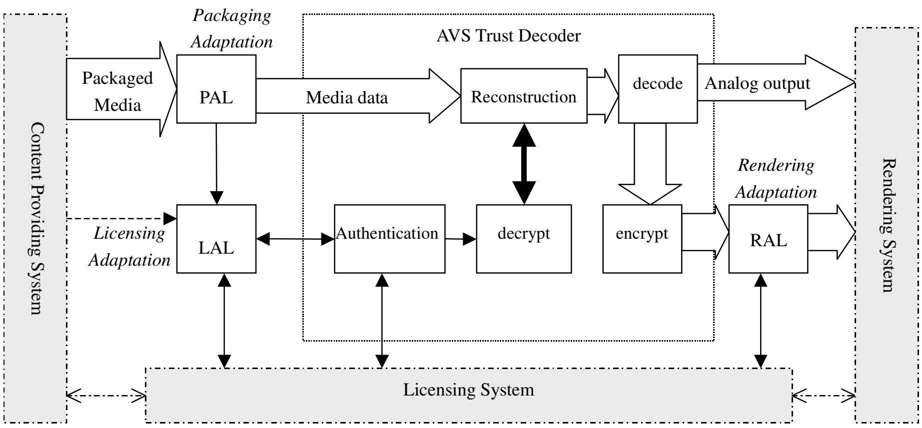


**Fig. 1.** Architecture of AVS DRM Core profile

Fig.1 shows the Architecture of AVS DRM Core profile which consists of the AVS Trusted Decoder (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).

The ATD should be strongly protected as a whole, for example, as an ASIC chip with physical anti-track shell. Licensing system can communicate with it through an security channel setup by authentication model in ATD and counterpoint in licensing system such as smartcard for end user or AAA (authentication, authorization, and accounting) server at head-end system.

AVS DRM is an open solution that any company can provide decoder with ATD and any content provider can publish its content through any transmission system as long as they obey the same AV coding and DRM standard. Although ATD contains “secret” components that should be touched only by authorized entity or only by itself (e.g. private key), it doesn’t mean the system must be kept “secret”. All the players in a market know there is a secret but at the same time they can produce respective DRM products at different chains and inter-operate without comedown of security.

Just like Fairplay is workable in Apple world, AVS DRM with uniform cipher technology is workable in a country like China. But for worldwide, we must look for super solution for co-existence of different cipher technologies, content format and so on.

## 3 DMP Interoperable DRM Platform

The Digital Media Project (DMP) is a non-profit Association registered in Geneva, Switzerland. Its mission is “to promote the successful development, deployment and use of digital media that respect the rights of creators and rights holders to exploit their works, the wish of end users to fully enjoy the benefits of digital media and the interests of value-chain players to provide products and services, according to the principles laid down in the Digital Media Manifesto” [6] [7].

The DMP is the first attempt at achieving an end to end Interoperable DRM Platform (E2E IDP). Its objective is to achieve consensus between representatives of all traditional value chain players (including end users) using standard technologies. It is E2E because it represents content throughout the chain including representation of all entities digital or not that are relevant to the value chain and to which rights are attributed for. This initiative presents an opportunity for minimizing differences between value chain players focusing on use cases that support the interests of all.

DMP approaches the problem of DRM Interoperability by specifying technologies – that DMP calls Tools – required to implement what DMP calls “Primitive Functions”. These are “smaller” functions obtained when the functions value-chain users perform when they do business between themselves are broken down into more atomic elements. DMP provides specifications of Tools enabling Primitive Functions along with examples of how Value-Chains serving specific goals can be set up using the standard Tools. The ensemble of all standardized DRM Tools is called “Interoperable DRM Platform (IDP)”.

A Value-Chain is a group of interacting Users, connecting (and including) Creators to End-Users with the purpose of Delivering Content to End-Users. In general Users require Devices to perform the Functions proper of their role in the Value-Chain. Fig. 2 shows the Devices mentioned above in a generic Value-Chain and identifies their principal relationships.

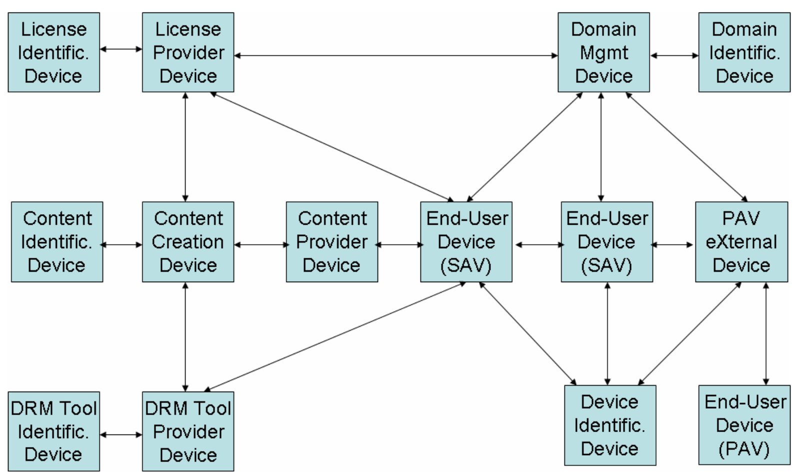


**Fig. 2.** Devices in a Value-Chain defined by DMP

## 4 Challenges from Technical Perspective

There are three approaches used in DRM to protection content up to now: Cipher-based model, Watermarking and Digital fingerprinting.

Cipher-based approach employs encryption tools to protect content and key management infrastructure to delivery encryption key and other sensitive information. Encryption is the process for controlling access to confidential data, known as plaintext, by scrambling the data into an unintelligible form [8]. The key used by encryption and other sensitive information like license which stores usage rules about specialized content for specialized end user(s) can be transferred between value chain participants one by one through a trusted key management and delivery infrastructure which need to authenticate all of the participants or their devices.

Watermarking [9][10] has been proposed as a means for content protection evenafter data has been decrypted. A watermark is a signal that is embedded into an original content to produce the watermarked content. Content owner related information can be inserted to identify the ownership of the copyright. Usage rules can be embedded to direct the watermark-enabled device how to use the content.

Digital fingerprinting was proposed by [11] more than twenty years ago. Fingerprinting is the process of embedding a distinct set of marks into a given host signal to produce a set of fingerprinted signals that each "appear" identical for use, but have a slightly different bit representation from one another. These differences can be used to track of a particular copy of the fingerprinted signal. The marks, also called the fingerprint *payload*, are usually embedded through the process of robust digital watermarking.

The above technology was studied for many years. It is expected that more strong or robust protection to appear in the future. But no matter what the protection technology is or would be, there are more fundamental problems that must be faced. Here are some most important that were pointed out in last several years (partly from [8]):

(1) Cipher-based approach encryption techniques do not offer any protection once the encrypted data has been decrypted. As an extreme but popular case, analog hole always exist. It is always possible to make analog copy from the end device through the use of "legacy" devices that are not DRM compliant. Once the content flows from DRM world into analog world, it can be converted into digital without DRM.
(2) Despite the considerable effort that has been spent on developing robust watermarks for digital video, the robustness and security of current watermarking techniques may not be sufficient for some DRM applications. Removal attacks and spatial and temporal synchronization attacks remain challenging for watermark detection. Security is also an issue.
(3) Digital fingerprint faces most problems of watermarking. For the more, privacy infringing is challenge when end user related information is embedded in the content.
(4) For DRM systems are required and must govern all access, use, and copying of protected content and do so securely, a enormous infrastructure is needed to construct. Who should be charged to do this? Content owners, providers, operators or

consumers? Although it is always consumers to pay for everything, it is impossible for DRM to be afforded when it limits Fair Use space or infringes the privacy of the consumers.
(5) Beside the cost for constructing a DRM system, renew an attacked system means more cost and more complex tasks. Some challenging questions remain for using device revocation also.
(6) Protection technology cumbers Fair Use of content. Encryption makes fair share in family, library and classroom impossible or very difficult.

## 5 Challenges from Social Perspective

Before technical guys can find more sophisticated protection artifices, although his iPod and Fairplay gained amazing success, Steve Jobs already has been beyond endurance on DRM and announced that “DRMs haven’t worked, and may never work, to halt music piracy.”

Another thought from librarian [12] mentioned that DRM is perceived as a barrier for it does build in obsolescence, end equitable access, invades user privacy and enable censorship.

DMP thought DRM by Digital Media Manifesto [6] which is the foundation for it interoperable infrastructure. After analysis on disadvantages of current DRM, DMP proposed the following steps to remove the hurdles to a fuller digital media experience. Although DMP approach is ahead of current protection approaches and standards, it isn’t difficult to notice that DMP solution is influenced by protection methodology also. By protection approach, it is not possible or affordable to Map Traditional Rights and Usages (TRUs) to the Digital Space [13].

DMP TRUs should be listed in the most important contributions to media. It is the start point for next generation rights management. The 88 TRU picked out by DMP are classified into five categories as following:

(1) Already-established legislative TRUs of content creators (21)
(2) Already-established legislative TRUs belonging to end-users (7)
(3) Commercial and remuneration TRUs of direct economic significance (22)
(4) TRUs related to general social liberties (13)
(5) Fundamental TRUs from historical practice and interaction with analogue media (14)
(6) Consumer-choice TRUs relevant to the high-tech environment (12)

You can find the protection approach satisfies few of them but make most of them impossible or excessive complex to implement in digital space.

Content protection should not forget the primary goal of content itself. Technology should accelerate the diffusion of knowledge and culture but not limit it. Let’s image a scene many years later, when our descendants excitedly discover the digital content piece in our age, they find it was locked in black box by encryption but key is not there because the complex key management system designed by us disappeared or crashed like dinosaur, we should be ashamed for our short see on rights management to make our descendants disappointed.

## 6 Monitoring Rights in Public Digital Space by Contentprint

Although amount of effort was taken to protect digital content, the real situation is most of the content in copyright still go around everywhere and the protection is revolted by many consumers and organizations. Contrasting with stronger and stronger protection technologies, more and more contents in copyright without DRM are exchanged in Internet. Now Apple and Microsoft decided to provide DRM-free music on their online store. It is the time to consider new approach for rights management.

The origin of content protection is digital content in copyright was released into cyberspace. The involuntary reaction of media industry is to protect the content by encryption, prove the ownership by watermarking and track the user by fingerprinting. An important fact ignored by most people is the cyberspace. The cyberspace is a kind of public space. It is illegal to spread content in public space without permission of the content owner. So the real question is how to prevent illegal spreading activities.

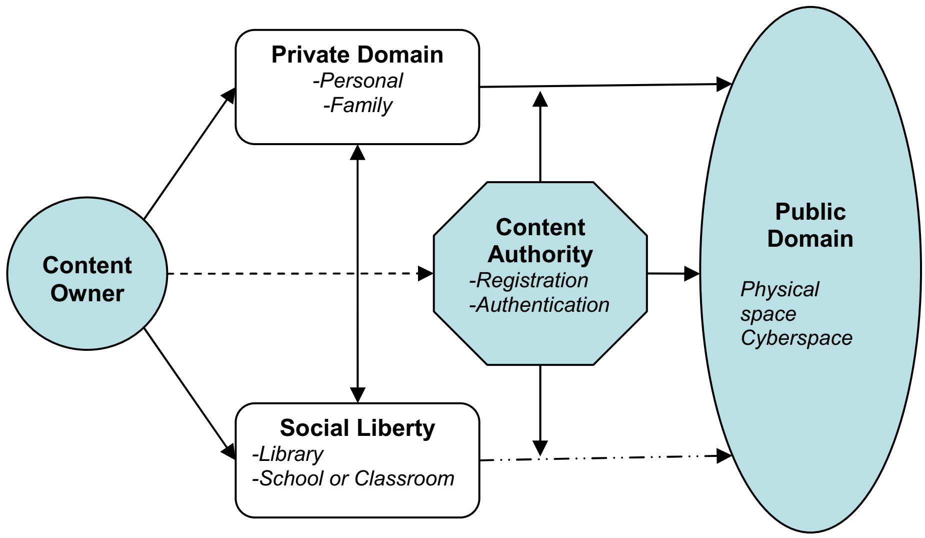


**Fig. 3.** Content diffusion

Fig.3 shows the question in detail. After a content is created, it should be registered on a authority organization. A person buys the content from the rights owner or middle-man and uses it by himself/herself or shares it in his/her private space (e.g. family). Library can collect and loan it to its readers for social liberty. After the expiration of the copyright, the content enters the public space as a part of human knowledge or culture. In analog ages, pirate is controlled by legal measure. In digital space, pirate can be controlled by legal measure also. For the technical community, the most important that should be invented is not the tool for content owner to protect their content but the tool for authority or police to trace and prevent the pirate activities in digital space.

The shift of DRM schema from content protecting by owner to pirate monitoring by public authority follows typical social evolvement. Not like previous DRM that modifies the content by scrambling or marking, the content authentication-based DRM doesn't change anything. For the more, once a content is registered in authority database, its pirate copy (even though with artificial or other change) will be monitoring in public space. If someone attempts to spread a content in copyright to others, he or she will be found and the activities will be stopped. The monitoring only operates in public space, the Fair Use of content in private space or sharing for social liberty purpose is outside of the monitoring.

The new schema is better than cipher-based model and watermarking model. The advantages are following:

(1) Content without change: maximum freedom for the content diffusion not only for today but also for the future.
(2) Consumers friendly: anyone can get a copy from the content owner. The consumer only pays for the content. No DRM-enable device is needed. All traditional right usages are reserved.
(3) No analog hole: The monitoring system is designed to block analog hole. Although anyone can get a copy but he or she can't spread it for the monitoring system in the public space will stop any illegal transmission.
(4) Flexible right management: content in copyright that is registered will be monitored in public space. Once expiration of the copyright, it will be out of monitoring and be released to public space automatically.
(5) Cost can be controlled: monitoring system need cost also. But the cost is from content owner who wants to protect the content that can bring him revenue. If the content owner believes his/her content is necessary to be monitored, the means he or she wants to pay for it. That is to say, there are enough money to construct a monitoring system and maintains it.

To monitor digital content in digital space, a content-related identifier is needed. The identifier is called contentprint. Contentprint is a new word which is created to identify a content just like fingerprint, voiceprint to identify a person. It is abstracted from a media content. Content should be robust enough - constant to various variations (compression, analog to digital or contrariwise, zoom etc.) and should be unique – different content should generate different contentprint. When special feature is regarded, contentprint can be reified as visualprint, auralprint and so on.

There are some similar concepts for contentprint. The first is perceptual hashing[14]. Hash mean satisfies the unique characteristic but doesn't satisfy the constant characteristic. Another is video or audio fingerprint. For fingerprinting is used to describe embedding user-related information into original content, we prefer to create the new word to describe abstracting features from the content.

There are many works on content authentication [15~18] for different purpose. For need to authenticate content that has experienced legitimate editing in addition to potential tampering attacks, [19] develop one formulation based on a strict notion of security, and characterize and interpret the associated information-theoretic performance limits.

Although there are many algorithms for contentprint abstracting, research on robust abstracting algorithm for ultra amount content dataset is needed. Benchmark for contentprint abstracting is needed also. For the more, normative contentprint is needed to setup open contentprint management and monitoring system.

## 7 Conclusion

By reviewing state of art DRMs including two DRMs that the author involves in, the paper checked the challenges of DRM from technical and social perspectives. The conclusion is that protection approach solved few problems for rights management but lead to more new problems (e.g. block the Fair Use). The fact that under 3% of the music is protected with Apple Fairplay is an auspice for replacing it with new schema.

This paper points out a simple fact that the origin and final target for rights management is to prevent illegal spread in public space. Content-based media authentication and monitoring will play more important role in new generation DRM. To construct such a new rights management, more efforts on contentprint abstracting, authentication, identification and high performance contentprint monitoring are neeed.

## References

1. The U.S. Copyright Office. The Digital Millennium Copyright Act. (1998) http://www.copyright.gov/legislation/dmca.pdf
2. Fernando, G., Jacobs, T., et al.: Project DreaM: An Architectural Overview. Sun Microsystems White paper (September 2005)
3. Jobs, S.: Thoughts on Music. (February 6, 2007) http://www.apple.com/hotnews/thoughtsonmusic/
4. China national standard GB/T 20090.2. Advanced Audio and Video coding Part 2: Video (2006)
5. Tie-jun, H., Yongliang, L.: Basic Considerations on AVS DRM Architecture. J. of Computer Science and Technology 21.3, 366–369 (2006)
6. The Digital Media Manifesto (2003/09/30). http://www.dmpf.org/manifesto/dmm.htm
7. Digital Media Project. http://www.dmpf.org/
8. Eugene, T.L., Ahmet, M.E., Rgginald, L.L., Edward, J.D.: Advances in Digital Video Content Protection. In: Proceedings of the IEEE, vol. 93, pp. 171–183 (2005)
9. Doërr, G., Dugelay, J.-L.: A guide tour of video watermarking. Signal Process. Image Commun. 18(4), 263–282 (2003)
10. Cox, I., Miller, M., Bloom, J.: Digital Watermarking. Morgan Kaufmann, San Francisco, CA (2002)
11. Wagner, N.R.: Fingerprinting. In: Proceedings of IEEE Symp. Security and Privacy, pp. 18–22 (1983)
12. Hill Slowinski, F.: What Consumers Want in Digital Rights Management (DRM): Making Content as Widely Available as Possible in Ways that Satisfy Consumer Preferences. AAP/ALA White Paper (March 2003) http://dx.doi.org/10.1003/whitepaper
13. DMP0270. Collection of TRU templates (November 11, 2004). http://www.dmpf.org/open/dmp0270.zip
14. Kalker, T., Haitsma, J.A., Oostveen, J.: Issues with digital watermarking and perceptual hashing. In: Proceedings of SPIE 4518, Multimedia Systems and Applications IV (2001)

15. Du, R., Fridrich, J.: Lossless Authentication of MPEG-2 Video. In: Proceedings of 2002 International Conference on Image Processing, vol. 2, pp. 893–896 (2002)
16. Pröfrock, D., Richter, H. Schlauweg, M., et al.: H.264/AVC video authentication using skipped macroblocks for an erasable watermark. In: Proceedings of Vision Communication and Image Processing, pp. 1480–1490 (2005)
17. Queluz, M.P.: Towards robust, content based techniques for image authentication. In: Proceedings of the 2nd Workshop on Multimedia Signal Processing, pp. 297–302 (1998)
18. Lin, C.-Y., Chang, S.-F.: Issues and solutions for authenticating MPEG video. In: Proceedings of SPIE Storage and Retrieval for Image and Video Databases, San Jose, CA, USA (1999)
19. Martinian, E., Wornell, G.W., Chen, B.: Authentication with Distortion Criteria. IEEE Transactions on Information Theory 52(7), 2523–2542 (2005)