CHAPTER 26

Digital Rights Management Issues for Video

Sabu Emmanuel, Nanyang Technological University, Singapore
Mohan S. Kankanhalli, National University of Singapore

1. INTRODUCTION

A huge amount of digital assets involving media such as text, audio, video etc. are being created these days. Digital asset management involves creation, transfer, storage and consumption of these assets. It is chiefly in the transfer function context that the digital rights management (DRM) becomes a major issue. The term DRM refers to a set of technologies and approaches that establish a trust relationship among the parties involved in a digital asset creation and transaction. The creator creates a digital asset and owner owns the digital asset. The creators need not be owners of digital asset as in the case of employees creating digital asset for their company. In this case, though the employees are the creators, the ownership of the digital asset can reside with the company. The digital asset needs to be transferred from the owner to the consumer, usually through a hierarchy of distributors. Therefore the parties involved in the digital asset creation and transaction are creators, owners, distributors and consumers. Each of these parties has their own rights namely, creators have *creator rights*, owners have *owner rights*, distributors have *distributor rights* and consumers have *consumer rights*. We lay down the requirements of these rights in section (4). A true DRM system should be able to support all these rights. It is to be noted that there can be multiple creators jointly creating a digital asset and likewise, multiple owners jointly owning a digital asset. There can also be a hierarchy of distributors and also distributorships allocated by geographic regions or time segments. The consumer can also be either an individual or a group of individuals or a corporate entity. Tackling DRM issues in this multiparty, multilevel scenario is a very challenging problem. We continually point out challenges that can be the basis for further research in this chapter.

The digital rights requirements vary with the kind of digital asset being transferred. Digital assets can possess different transaction values. Some can be free while others can be of a high value (digital cinema,

high valued digital arts). And some can be truly invaluable especially archival and historical photographs, audios and videos. The creation/production cost of a digital asset is different from the transaction value. The transaction value is most often assigned by the owner (which is usually higher than the production cost). The transaction cost consists of the distribution cost and cost of setting-up of the DRM (DRM cost). Designing an economically viable DRM system is particularly challenging for low-valued digital assets.

The framework of DRM consists of technical, business, social and legal components [31][37][48][53]. The business aspect of DRM involves new business models such as a free evaluation copy first for few days followed by a full permission or a downloadable stream for immediate use followed by a DVD copy in mail. The social angle of DRM is governed by societal norms concerning fair use, privacy management, and the education of consumers so as to inform them on the risks associated with using pirated content. The legal aspect deals with the laws of the license jurisdiction and that include legislation, compliance, investigation, and enforcement. The technical DRM perspective deals with the technical standards and infrastructure, which consists of protection mechanisms, trading protocols and rights language. We, further in this chapter, will discuss the business, social, legal, and technical aspect of DRM in detail.

Consider a digital commerce transaction completed over the Internet for DVDs (Digital Versatile Discs). In such a transaction, usually the consumer and the seller are geographically far apart and possess scant knowledge of each other. To initiate the transaction, the consumer browses the web for DVDs. In this scenario, a few typical issues are raised. Can the consumer trust that the online stores are legitimate and possess the right to distribute the copyrighted DVDs? Can the consumer be guaranteed that the payment information and order information are secure? Can the consumer trust that the digital content he/she is about to download is authentic, untampered material from the original author or owner or distributor? Can the consumer trust that the content will work on his/her usage devices and whether he/she can give the content to his/her friend? Can the consumer trust that his/her privacy regarding his/her buying behavior is secured? The questions that the legitimate online DVD seller would ask are: Can I trust the consumer that he/she would not create unauthorized copies and redistribute? In the event of a copyright violation, can the

seller identify and trace the consumer who did it so as to bring him/her to justice? Without proper DRM, answers to most of these questions are in the negative.

Let us look at the example of a new business model where a consumer wants to buy a DVD over the Web. The e-mall could straight away stream out the video to the consumer which could be watched on the Personal Computer (PC) or sent to the Liquid Crystal Display (LCD) projectors of the home theater system immediately and a physical DVD could be dispatched for viewing and possession. However the rights usage of the streamed version should be limited. The stream should be allowed to play on the machines indicated by the consumer and also may be allowed to be diverted to the systems as specified by the user. And the DVD should be allowed to play as and when required and on any machine. The DRM system should support these usage requirements. We discuss various usage requirements in section (3).

Already products and services are available which support DRM. But these products are often not interoperable, do not support newer business models, and support only limited digital rights of parties. The current DRM systems are quite primitive as they tie the content to a particular playback device. The content is not allowed to be played on any other device or to be diverted to another device. The DRM system depends on strong encryption schemes and ties the decryption to the device on which it is decrypted [46]. Often these DRM products only support the digital rights of owners, but do not address false implication, fair use, and privacy concerns of consumers. Therefore, these DRM solutions are not widely used. Consequently, not many high valued copyrighted or archival digital contents are available on the Web due to piracy, or recreation and reuse concerns. It must be noted that there are digital delivery channels such as satellite, cable broadcasts etc. other than the Internet. They too need to address piracy and reuse concerns. We discuss various delivery techniques in section (2).

While digital assets fall into various categories such as text, audio, image and video, in this chapter we concentrate on the DRM issues for digital video. The challenges in solving DRM for digital video are multifaceted. Video files are large and they require a lot of storage space. Therefore to reduce the storage requirement, videos are compressed before being stored. For example a typical two hour, 35mm feature

film scanned at a standard high quality resolution of 1920 by 1080 pixels, 1 byte per color and 24 frames per second would, in its uncompressed form, require 120x1920x1080x3x24 = 17,915,904,000 bytes of disk space. Assuming a compression ratio of 30:1 the disk space requirement becomes more manageable. These requirements are going to go up as the high-resolution 4000 by 4000 pixels scanners (Kodak Cineon and Quantel Domino) gain widespread use [56]. Therefore compressed video would be preferred over uncompressed video. Again the large size of the video compels the owners/distributors to broadcast the video to multiple receivers rather than to unicast to individual receivers. Broadcasting reduces the channel bandwidth requirement and also the transmission costs. Therefore the preferred transmission technique for the digital video is broadcast. For DRM, compressed domain processing and broadcast type transmission make matters more complex. Essentially DRM is a one-to-one contract where by rights of both the parties are to be defined, complied, monitored and enforced. But broadcast is a one-to-all transmission scenario where every receiver in the broadcast region receives the video. How to satisfy these seemingly contradictory requirements is a challenging problem for DRM in the broadcasting environment.

Past decades might have seen tremendous achievements in the creation, processing and delivery of multimedia data. But growth of digital commerce of these digital objects over the Internet or other digital delivery mechanisms have been somewhat slow, due to the major concerns regarding DRM.

Sections 2, 3, and 4 concentrate on the environments and requirements for achieving the DRM. Particularly section 2 discusses digital video asset management, section 3 presents digital usage controls and section 4 discusses digital rights requirements. Sections 5, 6, 7, and 8 elaborate on the various components of DRM. Specifically, section 5 discusses the business aspects, section 6 presents social aspects, section 7 describes the legal aspects, and section 8 elaborates on the technical aspects.

2 Digital Video Asset Management

After creating the digital asset, storage and delivery functions need to be addressed as part of digital asset management [37]. We discuss storage and delivery mechanisms in this section.

Storage: Digital video is usually compressed. The open compression standards from ISO/IEC, Moving Pictures Experts Group (MPEG) are MPEG-1, MPEG-2 and MPEG-4 [27]. The MPEG-1 standard is used in Video Compact Disc (VCD). The DVD, digital video broadcasts (digital TV transmissions), and High Definition Television (HDTV) transmissions currently use MPEG-2 standard. The MPEG-4 is newer standard, which is intended for low bit-rate (wireless, mobile video applications) and high bit-rate applications. There are other open standards such as H.261, H.263 from ITU primarily for video conferencing over telephone lines. Apart from the open standards there are proprietary compression standards from Real Networks, Apple, and Microsoft etc. In addition to compression, the digital assets are to be wrapped in metadata to declare the structure and composition of the digital asset, to describe the contents, to identify the contents, and to express the digital rights. We discuss about the declarations, descriptions, and identifiers in section (8.5).

Digital Video Delivery: E-shops in the World Wide Web (WWW) typically offer downloading or streaming modes for delivering the video. The downloading mode employs unicast type of transmission technique whereas the streaming mode can use either unicast or broadcast type of transmission. Digital TV transmissions usually use the broadcast channel. The most popular medium of digital TV transmission is terrestrial digital TV transmission. Other popular mediums are satellite and cable transmissions. Direct to home satellite transmissions are becoming more and more popular these days due to their ease in deployment. Stored media such as DVD and VCD are other means of distributing digital video.

Digital cinema is a system to deliver motion pictures and "cinema-quality" programs to theatres throughout the world using digital technology. The digital cinema system delivers digitized or mastered, compressed, and encrypted motion pictures to theatres using either physical media distribution (such as DVD-ROMs) or electronic transmission methods such as the Internet as well as satellite broadcast methods. Theatres receive digitized programs and store them in hard disk storage while still encrypted and compressed. At each showing, the digitized information is retrieved via a local area network from the hard disk storage, then is decrypted, decompressed and displayed using cinema-quality electronic projectors.

As we can see, digital TV, digital cinema and Internet streaming services use broadcasting technique whereas the Internet downloading service uses the unicast technique for transmission. In all the above delivery methods except in stored media such as DVD, VCD delivery for home segments, a return channel (other than the content and control signal delivery channel from owner or distributor(s) to the consumer) is provided for communication from the consumer to the distributors or the owner for DRM implementation. The return path need not be always on-line as in case of certain prepaid digital pay TVs where the communication is at certain intervals of time.

3 Digital Asset Usage Controls

Owners often want usage controls to be associated with the digital asset. These controls essentially specify the various ways the digital asset can be used. For example, whether the digital asset can be copied or not, and if allowed to copy, the number of times that the digital asset can be copied. Currently DRM systems are being designed with no copy, one time copy and many times copy features [33][34][46]. The controls can specify whether the digital asset is allowed for usage activities such as play, copy, or reuse. If allowed, additional controls based on count, time, time period, and territory can also be placed [37][55].

The count parameter will support the service such as ‘pay-per-usage’ i.e. if the video is allowed to copy once, after making a copy once no further copying of the original video is allowed. A new video needs to be purchased to make another copy. The time period parameter supports ‘pay-per-view-per-time period’ programs i.e., the billing can be for the period of time the video program is viewed. Another application may be to have a differential billing scheme based on the time of the day. The territory parameter may support the differential billing for different geographic regions. The reuse control specifies whether the digital asset can be reused. If reuse is allowed, new digital assets can be created from the digital asset. For example, consider the creation of a home music VCD album where the music is from different VCDs or the creation of a new VCD with new characters replacing the original characters. These controls support new business models.

4 Digital Rights Requirements

The digital asset creation and delivery chain consists of creators, owners, distributors, and consumers. Each of these parties has their own rights and we call these as the digital rights. The DRM system is expected to build the trust among the parties by meeting the digital rights of each party. It must be noted that in this chain, the created digital asset moves from the creator to the consumer through the owner and distributors. And the fee for the digital asset flows from consumer to the creator through owner and distributors. This can be seen from the figure (1). Often the owner already pays the fee for the creation of the digital asset to the creators, as in the case of employee-employer relationship. Therefore, the owner is the one concerned about the loss of revenue due to piracy and unauthorized usage. The owners can directly deliver the digital asset to the consumers or they may use a hierarchy of distributors. This can be seen from figure (1). The hierarchy of distributors is preferred to deal with the business scalability and viability. Each of the distributors may have their own already existing consumer bases and infrastructure, which can easily be tapped in by the owners to deliver their digital asset to the consumers. When there is a hierarchy of distributors, building a trust relationship between the owner and the distributor, distributor and sub-distributor becomes more complex. This is because while the owner is concerned about the revenue loss due to malpractices of the distributors and also of the end consumer, the distributors would be concerned about the false framing by the owners and also would be concerned about the revenue loss due to the malpractices of the sub-distributors and the end-consumer. Since consumer is at the end of the distribution chain, they would be concerned about the digital asset, its quality and integrity and also false framing by the distributor or owner [18]. There should also be a trust relationship built between consumer and the distributor or the owner. We now elaborate on the digital rights requirements of each party for various application scenarios.

Digital rights of creators: A digital asset may be jointly created by one or more creators. All those participating creators would expect that their participation be provable to any party. This requires that a jointly created mark be placed on the digital asset or individually created marks be individually placed on the digital asset. In either case the idea is to establish the right of creatorship. The mark(s) should be robust

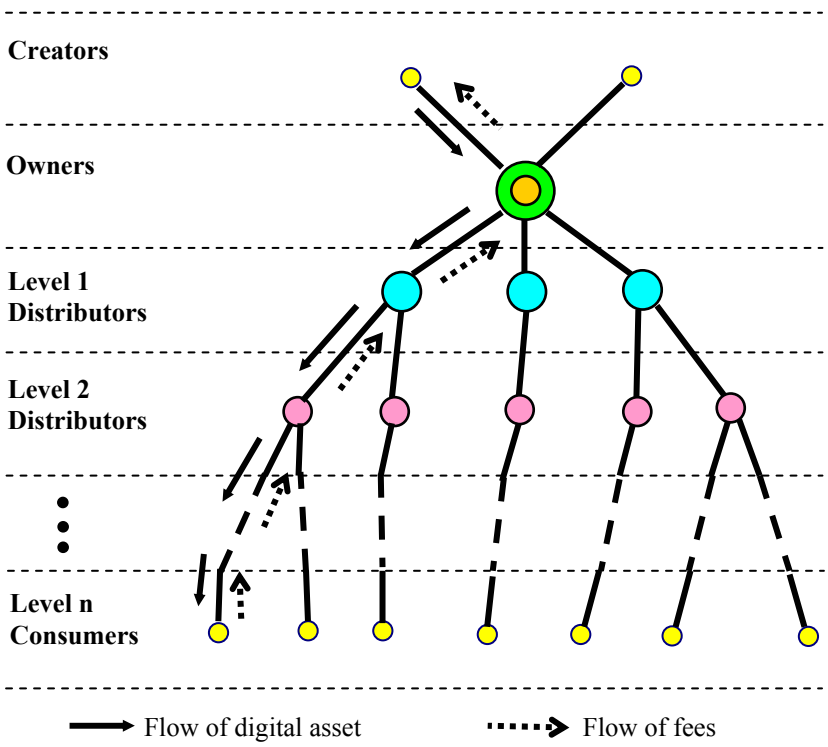

Figure 1 Digital asset creation and delivery chain

so that no one can remove the mark(s) except the concerned creator himself. The mark also should be robust against collusion removal attacks. For example few creators may collude and remove the creatorship information of another creator from the digital asset, which should not be allowed. Only few researchers have addressed this problem. The marking technique should be scalable with increase in number of creators and the marks should not cause considerable perceptual degradation of the digital asset.

The creators may be paid royalty by the owner for every copy of the digital asset made as in the case of publishing books. In this case the creators would need to track the number of copies made. The typical scenario in a digital movie/video creation is that the creators are the employees of the production house and hence no such tracking of number of copies is needed.

Digital rights of owners: Video distribution can either be subscription-based distribution or free. In both these cases, the owner would like to specify how the distributors and consumers should use the digital asset. This is primarily specified through the usage controls. Often the copyright protected videos are

distributed using the subscription-based schemes. In these subscription-based schemes the owners may want to associate various usage controls on viewing, copying, play back device in use, and reuse. The usage control can vary from one time view to many times view, no copy to many times copy, play back on dedicated device to any device, and conditional to unconditional reuse.

The free distribution mode can fall into two categories - one that can be reused as well as modified and the other in which the asset cannot be tampered with. An example of free distribution that cannot be tampered is archival material with historical importance. In this case, usage control needs to specify whether the digital video can be reused or not. And the other usage control parameters are of little importance since the distribution is free. These usage controls essentially constrain the usage of digital asset by consumers and distributors.

We list the owner's requirements for a subscription-based distribution:

- Needs to specify the usage controls
- Needs the consumer/distributor to be authenticated
- Needs the ability to trace the consumer/distributor who has violated the DRM contract
- Needs to declare the ownership of the digital asset
- Needs to distinguish consumers from non-consumers
- Needs a payment protocol to handle the fees

Authentication of consumers/distributors is needed to reliably identify the consumer/distributor. In the event of DRM contract violation, the violating consumer/distributor can be identified. This can be implemented using authentication protocols. In order to trace the DRM contract violating consumer/distributor, and also to declare the ownership of the digital asset, digital watermarking techniques can be used. The digital watermarking technique should be robust against attacks and also non-invertible to prove the ownership of the digital asset. Since the distribution is subscription based, only the consumers (who have paid the subscription fee) should get a clear video for viewing where as the non-consumers

should not get a clear video for viewing. This requirement is the confidentiality requirement and can be implemented using encryption techniques.

Next we list the owner's requirements of free distribution with archival importance:

- Needs to specify the reuse policy (essentially no tampering allowed)
- Needs the consumer/distributor be authenticated
- Needs to detect any tampering of the content
- Needs the ability to trace the consumer/distributor who has tampered the video
- Needs to declare the ownership of the video

For tamper detection one can employ fragile watermarks. For tracing the consumer/distributor who has tampered the video and also to declare the ownership of the video, non-invertible robust watermarking techniques can be used. Authentication can be implemented using authentication protocols.

For free distribution with no archival importance, there need not be any rights associated as the digital asset is free to use in whichever way the consumer desires.

Digital rights of distributors: It can be seen from the digital asset delivery chain that the distributors act as middlemen. The owners fall at the upper end, the distributors are at the middle part, and the consumers fall at the lower end of the delivery chain. To the owners/upstream distributors, the downstream distributors are consumers with same or less restrictions on usage compared to end consumers. For example, usage control on viewing/playing on any device may be unimportant, whereas usage control on copying and reuse would be important. As far as trust building measures between the downstream distributor and the owner/upstream distributor, the downstream distributor will have the following concerns for both subscription-based and free distribution with archival importance, which need to be addressed:

- Needs to address false implication by the owner/upstream distributor
- Needs the owner/upstream distributor be authenticated
- Needs proof of ownership/distributorship of the video
- Needs the integrity of video to be proved

- Needs a payment protocol to handle the subscription fee (for subscription-based schemes only)

The above requirements apply for both subscription-based and free distributions with archival importance. The false implication concern is that, often the fingerprinting marks for tracing the copyright violator is placed by the owner/upstream distributor alone [18]. And it is possible that the owner/upstream distributor may knowingly or unknowingly creates a second fingerprinted copy with the same mark, which had been already used for someone else and distributes the second copy to a second party. Later the owner/upstream distributor can sue the first legal recipient for the copy seen with the second recipient. This false implication by sellers is a major concern for the downstream distributors and end consumers. As a trust building measure between upstream distributor and downstream distributor or end consumer the following requirements of upstream distributors are to be addressed:

- Needs to specify the usage controls (this can be a subset of what the owner has specified)
- Needs the consumer/downstream distributor be authenticated
- Needs to trace the consumer/downstream distributor who has violated the DRM contract
- Needs to distinguish consumers/downstream distributors from non-consumers/non-downstream distributors (for subscription-based schemes only)
- Needs to detect the tampering (for free distribution with archival importance only)
- Needs a payment protocol to handle the subscription fee (for subscription-based schemes only)

Digital rights of consumers: The consumers are at the lower end of the delivery chain. The following concerns of the consumers are to be addressed:

- Needs to address false implication by the owner/distributor
- Needs the owner/distributor be authenticated
- Needs proof of ownership/distributorship of the video
- Needs the integrity of video to be proved
- Needs a payment protocol to handle the subscription fee (for subscription-based schemes only)
- Needs to address fair use and privacy concerns

The digital rights requirements such as authentication of parties, confidentiality against the non-consumers and non-distributors, proving the integrity, ownership/ distributorship of the video, and payment protocols can be implemented using cryptographic and watermarking techniques in the DRM system. But incorporating techniques to deal with false implication concerns, DRM contract violator tracing, fair use [20][21], and privacy management [10][16][41] into the designed DRM is a challenging one. Some of the requirements are seemingly contradictory for example authentication and privacy management. In a broadcasting environment how to implement DRM contract violator tracing is another problem. False implication concern can be dealt using non-repudiation techniques and how to integrate this into the DRM system is another challenging problem. How to support fair use requirement is a major concern. How to design invisible multiple watermarking technique for tracing DRM contract violator in a multilevel delivery chain is another challenge.

Next we discuss various components of DRM such as business aspects, social aspects, legal aspects, and technical aspects of DRM.

5. Business Aspect of DRM

The Internet, and broadcast channels (such as satellite, cable, and terrestrial) act as low cost (compared to hardcopy transport) and quick transmission channels for the distribution of video data. These channels often transcend geographic and national boundaries connecting owners, distributors, and consumers. Various new business models leverage on the anywhere connectivity, quickness, and low cost properties of these channels [35][47][63].

Some of the new business models are:

- Preview and purchase – The preview is through quick and low cost channels, the purchased version can be a hard copy or soft copy with fewer constraints on the usage compared to the preview version.

- Pay-per-usage – The usage can be viewing, copying, or reusing. As an example the pay-per-view programs of TV channels belong to this category. In the pay-per-view TV program the payment is for a single program feature as desired, which could be pre-booked or impulsive.
- Pay-per-usage-per-usage constrained – The usage constraints can be count, time, time period, territory, device etc. The constraint time is for supporting differential pricing scheme based on peak hour, non-peak hour etc.
- Subscription-based – An example for this business model is pay TV.

Some of the business models make use of dedicated transmission channels (cable, satellite link etc.) and end rendering hardware (set top box etc.) and software. Some other business models make use of open networks such as Internet and general rendering software (Microsoft's media player, Apple's quick time etc.) and general hardware such as computers.

Designing DRM solution for the dedicated set-up is easier compared to the open/general set-up, since the owner/distributor is connected to the consumer through a dedicated transmission channel, and rendering hardware and software. Designing DRM solutions for this open/general set-up is challenging due to the following reasons. The Internet service providers (ISPs) do not belong to the owner or distributor category. ISPs merely provide bit pipes and switching mechanisms for transferring the data from one party to the other. But they often implement caching and other temporary storages, which can cause stale or multiple copies to reach the consumers. In the DRM solutions, if we use DRM aware general-purpose third party rendering software/hardware, the third party who is providing the software/hardware also should be part of the DRM agreements. This is because the third party can act as an intruder. For example the third party software/hardware can keep track of the transactions between the owner/distributor and customer (may be for market analysis). This problem is especially important when the client is a corporate entity. Designing a DRM compliant computer would restrict the usefulness of the computer. On the contrary if the copyrighted materials cannot be played/used on the computer, the charm of the computer is lost.

New revenue models are being contemplated to make DRM viable. One is to recover the cost of the copyrighted material by allowing third party advertisers to advertise their wares along with the video. In return, they share the cost of the video. This makes the cost of video that is to be borne by the consumers nominal and which makes the piracy to be unattractive. Another model proposes to make the ISPs as retailers, which make the DRM more implementable [63]. Yet another model proposes some ticket-based system for free/low cost digital videos. Escrow services based systems propose an architecture, which uses economic incentives instead of tamper resistance to motivate users to keep the digital asset within the subscription community [25].

6. Social Aspect of DRM

The social angle of DRM is governed by societal norms of fair use such as institutions which are not for profit may be allowed to use the material free of cost and may make any number of copies, but those institutions/organizations run on a profit basis need to pay for it. Other fair use problems are how does the DRM support the act of giving gifts, loaning a digital video to a friend, making a back-up copy for oneself etc. How to support DRM in a library kind of scenario where loaning is major function, is another problem. Guaranteeing privacy regarding consumer's buying practices is another social aspect of DRM. The social aspect includes also the education of consumers such as to inform them on the risks associated with using the pirated content. Education involves disseminating proper norms on how a copyrighted material is to be used in addition to the information on the penalties associated with the breaking of a copyright agreement.

7. Legal Aspect of DRM

A proper legal framework is necessary for successful implementation of digital rights management (DRM) system [7][8][47][60][61][65]. The framework primarily involves enacting new legislations that support DRM issues such as compliance, investigation, and enforcement. The DRM compliance lays out rules for the hardware and software manufacturers, service providers, owners, distributors, and consumers, what each one of them should do in order to be DRM compliant. In the event of DRM agreement violations, how

do we track the violations and prove the culpability of the violators. How do we enforce the DRM related laws and also what are the penalties/compensations for the DRM agreement violations. These are some of the issues tackled in the legal aspects of DRM. One of the major concerns is how does the legal aspect of DRM work across the national boundaries. Often different countries have their own DRM related laws and the digital asset transactions often take place beyond the national boundaries. Another major concern is how fair use issue is to be tackled in the DRM laws.

USA, European Union, and Australia have already enacted laws to support DRM. The Digital Millennium Copyright Act (DMCA), passed in 1998, is an American law implementing the 1996 World Intellectual Property Organization (WIPO) Copyright Treaty (WCT), and WIPO Performances and Phonograms Treaty (WPPT). European Union enacted in 2001 the European Union Copyright Directive (EUCD), which also implements the WIPO treaties. Both these acts of law make it compulsory to outlaw any attempt of circumventing a technical copyright protection. Both also outlaw the creation and distribution of DRM circumvention tools. While the DMCA allows fair use such as using digital content for research, teaching with the exception of distance learning, the EUCD does not allow fair use. The fair use also allows the consumer to resell what he bought, or make a backup copy for personal use. However, there are no clear rules defining fair use, which is usually decided by a judge on a case-by-case basis. The Australian copyright amendment (digital agenda) act 2000 (DACA) is similar to the DMCA. A new act called Consumer Broadband Digital Television promotion act (CBDTPA) was introduced to US senate in 2002. The CBDTPA mandates that anyone selling, creating, or distributing “digital media devices” must include government-approved security to prevent illegal copying of protected data. The devices include Compact Disc (CD) and DVD devices, and desktop PCs. This act might restrict the deployment of open source products such as Linux and also would limit the usefulness of desktop PC.

8. Technical Aspect of DRM

The technical aspect of DRM includes defining technical standards and infrastructure needed to support DRM in new business models, fair use and privacy issues of the social aspects of DRM, and provability

and traceability requirements of legal aspect of DRM [37][47]. The technical infrastructure consists of the hardware/software protection mechanisms that use cryptographic and watermarking techniques, trading protocols, rights language, and content descriptors and identifiers. We further elaborate on these technical infrastructures in this section. We also discuss the standardization efforts by various bodies such as MPEG, IETF, W3C, SMPTE etc. and also current DRM techniques and tools in digital video broadcasts, stored media such as DVD, and digital cinema.

8.1 Cryptographic Techniques

Cryptographic techniques provide confidentiality, authentication, data integrity, and non-repudiation functions. They are also designed for traitor tracing. However in the DRM world, cryptographic techniques are primarily used for providing media confidentiality, trading party authentication, trading protocol non-repudiation. There are well-established party authentication protocols such as Kerberos, X.509 etc. Some of these are based on symmetric key cryptosystem while as others are based on public key infrastructure. They authenticate the parties involved and also, if necessary, hand over secrets such as keys for confidential communication. The confidential communication may be intended to transfer payment information and also may be the media in transaction. Free video with tracing requirement and pay video need confidentiality to be implemented. Conditional access (CA) systems, which implement confidentiality through scrambling technique, are used in most of the subscription-based video systems [52][67]. The non-repudiation function provides for non-repudiation of the trading agreement. It is easy to combine the party authentication, trading agreement non-repudiation, and payment function into a trading protocol as they are usually one to one protocols and take place before the delivery of media.

Confidentiality of media against non-intended receivers is achieved by scrambling the media under the control of a scrambling key. The descrambling key is distributed only to the intended receivers. Various traitor-tracing schemes have been proposed by the researchers in cryptography [2][18]. Some of the works focus on fingerprinting the descrambling key thus each intended receivers possess and use different descrambling key. Therefore, by looking at the descrambling key used in the pirate decoder, the traitor

receiver who has leaked out the descrambling key can be identified. These schemes make certain assumptions such as video being large sized, so it is easy for traitors to hand over the descrambling key, which is small in size in comparison to the descrambled video. Thus in these schemes traitor tracing cannot be performed from the descrambled video since all descrambled videos are identical. With today's distribution networks such as copy and distribute over the Internet or through CDs, the above schemes would not be effective in combating piracy.

There are other cryptographic schemes, which employ fingerprinting the video for traitor tracing. Fingerprinting of video takes place while descrambling. Combining confidentiality and video fingerprinting for traitor tracing is a challenging problem due to the following reasons. Video data being large sized, broadcast transmission techniques are preferred over unicast transmission, which reduces the transmission bandwidth requirement. Thus a single scrambled copy of video is broadcasted to the receivers. Also video data would be compressed before transmission. The compression scheme used is often lossy scheme. And hence the scrambling needs to be performed after the compression and the descrambling needs to be performed before the decompression. But if fingerprinting is done along with descrambling, the fingerprints can be considered as bit errors occurred during transit. Especially in coding schemes, which employ interframe coding techniques, the errors can propagate into other frames and cause drifts. Thus designing a scrambling technique that would simultaneously perform fingerprinting while descrambling with no adverse effects is a challenging problem [19].

While it is desirable to have the fingerprinting and the descrambling processes combined into one atomic process for making the pirate to put more effort to get an unfingerprinted clear video for piracy, they are often implemented as two separate processes. This allows the pirate to turn off the control bits for the fingerprinting process or bypass the fingerprinting process completely and thus obtains an unfingerprinted but descrambled video [18].

Media data integrity can be ensured through digital signature schemes or by using hashing functions. But these techniques may not survive benign processing that might happen while in transit. However for media

data integrity, watermarking is preferred, since watermarking techniques can be designed to survive processing such as compression, transcoding etc. For traitor tracing also, watermarking techniques are preferred due to the fact that the watermarks can survive various benign/hostile operations.

In a multiparty distribution network (such as owner, distributor(s), consumer), implementing trading protocol consisting of party authentication, trading agreement non-repudiation, and payment function is easy as it is essentially one to one protocol (between owner and distributor, distributor and sub-distributor, sub-distributor and consumer etc.). However, in order to trace the traitor along the distribution channel, owner->distributor(s)->consumer, at every level (owner->distributor one level, distributor->sub-distributor another level, and sub-distributor->consumer another level) of the distribution channel in order to differentiate and identify the recipient of the media in that level, the media needs to be fingerprinted. Thus for *n* level distribution channel the end consumer would get a media with *n* fingerprints in it. Multiple fingerprints can cause them to be visible and can lead to the deterioration of video quality. Multiple fingerprinting technique is a challenging problem, which needs to be addressed by the research community.

8.2 Watermarking Techniques

Watermarking techniques are usually preferred for copyright ownership declaration, creator/authorship declaration, copyright violation detection (fingerprinting function), copyright violation deterrence, copy control, media authentication, and media data integrity functions. They are also devised for variety of media viz., text, digital audio, digital image and digital video. A digital watermark is an embedded piece of information either visible or invisible (audible or inaudible, in the case of audio) [23]. In the case of visible watermarking, [5][50] the watermarks are embedded in a way that is perceptible to a human viewer. And hence the watermarks convey an immediate claim of ownership and/or authorship, providing credit to the owner and/or author, and also deter copyright violations. In the case of invisible watermarking, [11][22] the watermarks are embedded in an imperceptible manner. The invisible watermarks can be fragile or robust. Fragile invisible watermarks [43] attempt to achieve data integrity (tamper proofing). The fragile invisible watermarks must be invisible to the human observers, altered by the application of most common image

processing techniques and should be able to be quickly extracted by authorized persons. The extracted watermark indicates where the alterations have taken place. Sometime it is necessary that the marks remain detectable after legitimate tampering and fail to provide content authentication for illegitimate operations. These watermarks are referred as semi-fragile watermarks. The desired properties for robust invisible watermarks are that they must be invisible to a human observer, the watermark should be detectable/extractable by an authorized person even after the media object is subjected to common signal processing techniques or after digital to analog and analog to digital conversions. Robust invisible watermarking technique is suitable for copyright ownership declaration, creator/authorship declaration, copyright violation detection (fingerprinting function), copyright violation deterrence, copy control. Many watermark algorithms have been proposed in the literature [3][59]. Some techniques modify spatial/temporal data samples while others modify transform coefficients [19]. To be robust, the watermark must be placed in the perceptually significant regions [11].

The input to a watermark embedding system is usually original data, watermark information and a secret embedding key and the output of watermark embedding system is watermarked data. The watermarking system can also be classified based on the watermark detection scheme in use. If original data or watermark information is needed along with watermarked data and the secret key the system is called *private watermarking* systems [4][11][58][59][66]. If, neither the original data nor the watermark information is needed for detection, the watermarking scheme is known as *public watermarking* scheme or *blind watermarking* scheme [19][22]. The original data and the watermark information in certain applications are to be kept secret even at the time of detection. Therefore in these applications blind watermarking schemes are preferred. Sometime during dispute the author has to prove the existence of watermark to a third party. But divulging the original data or watermark information or the key may not be desirable. The *zero knowledge watermark detection* schemes [13][1] are designed for this purpose. *Asymmetric watermarking* schemes [17][57] make use of another key for the detection rather than the embedding key.

Various types of attacks on watermarking techniques have been described in references [12][14][23][45]. There are, several software tools available to benchmark watermarking techniques, e.g., Stirmark,

Checkmark, and Optimark. These tools primarily support benchmarking of image watermarking techniques, but Checkmark also supports benchmarking of video watermarking techniques.

8.3 Trading Protocols

The Internet engineering task force (IETF) trade working group is designing a trading protocol framework for the Internet commerce under the title "Internet Open Trading Protocol (IOTP)" [28]. IOTP provides an interoperable framework for Internet commerce. IOTP tries to provide a virtual capability that safely replicates the real world, the paper based, traditional, understood, accepted methods of trading, buying, selling, value exchanging that has existed for many years. The negotiation of who will be the parties to the trade, how it will be conducted, the presentment of an offer, the method of payment, the provision of a payment receipt, the delivery of goods and the receipt of goods, are the events that would be taken care in the IOTP. IOTP Messages are Extensible Markup Language (XML) documents, which are physically sent between the different organizations that are taking part in a trade. IOTP v2 (Version 2) is intended to extend the IOTP v1 (Version 1). IOTP v2 will provide optional authentication via standards based XML Digital Signatures; however, neither IOTP v1 nor v2 provide any confidentiality mechanism. Both depend on the security mechanisms of payment system (such as Secure Electronic Transaction (SET), CyberCash etc.) used in conjunction with them to secure payments, and require the use of secure channels such as those provided by Secure Sockets Layer and Transport Layer Security (SSL/TLS) or Internet Protocol Security (IPSEC) for confidentiality. Electronic commerce frequently requires a substantial exchange of information in order to complete a purchase or other transaction, especially the first time the parties communicate. Electronic Commerce Modeling Language (ECML) provides a set of hierarchical payment oriented data structures (in an XML syntax) that will enable wallet software to automate the task of supplying and querying the needed information to complete a purchase or other transaction. IOTP is also designed to support the use of ECML, which will enable wallet software to automate the task of supplying and querying the frequently needed information to complete a purchase or other transaction.

The World Wide Web Consortium (W3C), is also developing standards for E-commerce on the web. W3C has actively contributed in developing XML signature, XML encryption, XML protocol, micropayment, and platform for Privacy Preferences Project (P3P) standards [29]. XML signature provides a mechanism for signing documents and metadata in order to establish who made the statement. XML Encryption specifies a process for encrypting/decrypting digital content and an XML syntax used to represent the encrypted content and information that enables an intended recipient to decrypt it. XML protocol is aimed at developing technologies, which allow two or more peers to communicate in a distributed environment, using XML as its encapsulation language, allowing automated negotiations. Platform for privacy preferences project (P3P) provides communication about data privacy practices between consumers and merchant sites on the Web as well as enhanced user control over the use and disclosure of personal information. Micropayment initiative specifies how to provide in a Web page all the information necessary to initialize a micropayment and transfer this information to the wallet for processing.

The IOTP and W3C's standards for E-commerce do not address the DRM issues explicitly. However, there is a proposal for a digital Rights Management System (RMS) that is integrated into IOTP for electronic commerce applications and services [44]. It introduces a rights insertion phase and a rights verification phase for IOTP. In the proposed framework, digital watermarking plays a very important role in facilitating digital rights management.

8.4 Rights Languages

In order to manage the rights of the parties, the rights are to be specified in a machine understandable way [30][31][54][64]. For this purpose, a rights data dictionary of allowed words, and allowed constructs of these words is defined. The allowed constructs are often defined using XML schema, which forms the rights language. One of the rights languages is eXtensible rights Markup Language (XrML) defined by ContentGuard Inc., and another one is Open Digital Rights Language (ODRL) from IPR Systems Pty Ltd. Both of them have their own rights data dictionary/vocabulary for the language. These languages express the terms and conditions over any content including permissions, constraints, obligations, offers and

agreements with rights holders. XrML is designed to be used in either single tier or multi-tier channels of distribution with the downstream rights and conditions assigned at any level. The MPEG-21 Rights Expression Language (REL) is using XrML as the base language. In addition the OASIS (Organization for the Advancement of Structured Information Standards) rights language technical committee, and the Open eBook Forum (OeBF) are using XrML as the base for their rights language specification. Open Mobile Alliance (OMA) accepted the ODRL as the standard rights expression language for mobile content [51].

Table 1 List of identifier codes and the type of content it is intended for

Identifier codes	Type of content
BICI (Book Item and Component Identifier)	Book content
SICI (Serial Item and Contribution Identifier)	Serial content
DOI (Digital Object Identifier)	Any creation
URI (Uniform Resource Identifier)	Any creation
ISAN (International Standard Audiovisual Number)	Audiovisual programs
ISBN (International Standard Book Number)	Books
ISMN (International Standard Music Number)	Printed music
ISRC (International Standard Recording Code)	Sound Recordings
ISSN (International Standard Serial Number)	Serials
ISWC (International Standard Musical Works Number)	Musical works
UMID (Unique Material Identifier)	Audiovisual content

8.5 Content Declarations, Descriptors & Identifiers

A digital content may comprise of many sub-contents. The makeup, structure, and organization of the content/sub-content can be specified using XML based declaration techniques. Metadata can be used to describe the contents/sub-contents (by specifying the media type, playback requirements etc.). In order to

specify the digital rights information associated with the contents/sub-contents, they need to be identifiable. For example in a video, the visual, audio, and text streams, each can be considered as sub-contents. Another example, an audio CD may contain different audio tracks and each track can be considered as individual sub-contents. In the first example, the types of sub-contents are different however for the second example types of the sub-contents are the same. Several identifier codes are already defined and can be seen in table (1). Except the DOI, and URI all the others are content type specific (for example ISBN for books, ISMN for printed music etc.) [29][30]. MPEG-21 uses URIs to identify digital items and their parts.

8.6 MPEG & Digital Rights Management

The MPEG standards MPEG-2, MPEG-4, MPEG-7 and MPEG-21 address the DRM issues. The MPEG's specific term for DRM is "Intellectual Property Management and Protection" (IPMP) [4][24][38][39][40].

The MPEG-2 intellectual property management and protection (IPMP) standard [39] provides place holders for sending the information whether the packet is scrambled, the information about which conditional access system (CAS) is used, control messages such as encryption control message (ECM) and encryption management message (EMM), and copyright identifier of 32 bits, which identifies the type of work (like ISBN, ISSN etc.). The IPMP specification only addresses confidentiality and watermarking. But the IPMP-X (intellectual property management and protection – extension) includes authentication function also along with the confidentiality and watermarking functions. The standard however does not specify the algorithms to be used for confidentiality, watermarking or authentication.

The MPEG-4 IPMP "Hooks" covers identification of content, automated monitoring and tracking of creations, prevention of illegal copying, tracking object manipulation and modification history and supporting transactions between users, media distributors, and rights holders [40]. The more recent call for proposal IPMP-X (extensions) stresses the interoperability of the solution to IPMP, renewability of the security, flexible expression of different business models/rules, protection of user privacy, user rights, and mobility of terminal and content. The IPMP-Descriptors (IPMP-Ds) and IPMP-Elementary Streams (IPMP-

ESs) provide a communication mechanism between IPMP system(s) and MPEG-4 terminal. IPMP-Ds are a part of the MPEG-4 object descriptors that describe how an object can be accessed and decoded. These IPMP-Ds are used to denote which out of the IPMP systems was used to encrypt the object and consequently at the decoder which IPMP system to be used for decrypting the object. IPMP-ESs are special elementary streams that are used to specify IPMP specific data, which can be used to deliver cryptographic keys, key update information and to initiate re-keying protocols. The IPMP-Ds and IPMP-ESs are the inputs to the IPMP system(s) at the MPEG-4 decoder and the IPMP system decides where to apply the IPMP control in the MPEG-4 decoder depending upon the inputs. Watermarking technology is also envisaged for sending the IPMP information. There are mainly three scenarios in which the watermarking technologies are envisaged: broadcast monitoring, watermarking based copy control and fingerprinting. For broadcast monitoring purpose the MPEG-4 decoder need not contain the watermark detectors, as the required monitoring can be done after rendering. The copy control systems require that the IPMP system(s) inside the MPEG-4 decoder implement the watermark retrieval algorithm and for fingerprinting the IPMP system(s) inside the MPEG-4 decoder must implement the watermark embedding algorithm.

MPEG-7 is a content description standard for content management [27]. The descriptions can be used for searching and retrieval of the content. The description consists of a description scheme (DS), descriptors (Ds) and a binary streamable representation of DSs and Ds called binary format for MPEG-7 (BiM). Since MPEG-7 is for descriptions, the IPMP manages, protects and authenticates these descriptions. MPEG-7 does not manage and protect the contents, however will accommodate and provide a mechanism for pointing to the content rights. MPEG-7 will provide the usage rules, usage history and identification of contents and also identification of contents in descriptions.

The vision of MPEG-21 is to define a multimedia framework to enable transparent and augmented use of multimedia resources across a wide range of networks and devices used by the different sectors [4][38]. MPEG-21 multimedia framework will identify and define the key-elements needed to support the multimedia value and delivery chain, the relation between and the operations supported by these elements. There are seven key elements that have been identified for supporting interoperability and one among them

is IPMP. In the IPMP area, MPEG21's aim is to provide a uniform framework that enables all users to express their rights and interests in, agreements related to digital objects and to have assurance that those rights, interests and agreements will be persistently and reliably managed and protected across a wide range of networks and devices. The MPEG IPMP Extensions are designed so that they can be applied to any MPEG multimedia representation (MPEG-2, 4, 7, 21).

8.7 Digital Video Broadcasts & DRM

There are three popular digital TV broadcasting standards, namely, the American Advanced Television Systems Committee (ATSC) standard, the European Digital Video Broadcasting (DVB) standard, and the Japanese Integrated Services Digital Broadcasting - Terrestrial (ISDB-T) standard. These broadcasting standards use MPEG-2 for video coding. The pay channels of digital video broadcasts require that a confidentiality requirement be implemented against the non-subscribers. Hence, current pay channels employ conditional access system (CAS) for this purpose. Primarily the CAS uses scrambling technique for providing the confidentiality [9][15][18][36][52][67]. The broadcaster scrambles the video data using a control word (*CW*) and broadcasts the scrambled video data. The subscribers use the same *CW* to descramble the received scrambled video data to obtain clear video. The data encryption standard (DES) is used in ATSC and the digital video broadcasting common scrambling algorithm (DVB-CSA) [15] is used in DVB. The DVB supports the simulcrypt and multicrypt standards whereas ATSC supports only simulcrypt standard [15][36]. The simulcrypt standard allows the co-existence of more than one CASs, simultaneously addressing different consumer bases, in one transmission. In case of multicrypt, no program is available through more than one CAS.

The current CAS only supports confidentiality against non-subscribers, but does not implement any fingerprinting technique to trace the copyright violator. Since the broadcasting requires a single copy to be transmitted, and the copyright violator identification requires individual subscribers copy be unique, the fingerprinting for copyright violator identification should be performed at each subscriber end. This means that the current CASs, at the subscriber end has to implement the fingerprinting process for copyright

violator identification in addition to the descrambling process. It is more secure if the fingerprinting and descrambling processes can be combined into a single atomic process. But it is hard to combine the existing descrambling process with fingerprinting process into a single atomic process. It is even more challenging to support confidentiality and copyright violator identification in compressed (MPEG-2) domain broadcast. The challenges are due to the quantization step, which is lossy and interframe coding, which makes use of the motion compensated predictions. Thus, DRM in digital video broadcasts currently implements only the confidentiality requirement against non-subscribers.

8.8 Stored Media (DVD) & DRM

The DVD Copy Control Association (DVD CCA) licenses Content Scrambling System (CSS) to the owners and manufacturers of DVD discs with video contents, manufacturers of DVD Players, DVD recorders, and DVD-ROM drives [33][34][62]. CSS is a data encryption and authentication scheme intended to prevent copying video files directly from prerecorded (read only) DVD-video discs. CSS was developed primarily by Matsushita and Toshiba. The information on DVD-video disc is CSS encrypted. DVD players have CSS circuitry that decrypts the data before it is decoded and displayed. A computer DVD decoder hardware/software would include a CSS decryption module and also the DVD-ROM drive would have extra firmware to exchange authentication and decryption keys with the CSS decryption module in the computer. The CSS license is extremely restrictive in an attempt to keep the CSS algorithm and keys secret. However, this CSS algorithm was broken and posted on the Internet.

Content Protection for Prerecorded Media (CPPM) is for DVD-Audio, which performs the same function as that of CSS . A disc may contain both CSS and CPPM content if it is a hybrid DVD-Video/DVD-Audio disc. Content protection for recordable media (CPRM) protects exchange of entertainment content recorded on portable/removable storage media such as DVD-RAM/-R/-RW, and secure compact flash. The companies responsible for CPPM and CPRM are Intel, IBM, MEI, and Toshiba. The CSS, CPPM, and CPRM are not designed to protect against copying through the analog output port. However, Macrovision's DVD copy protection system supports protection against such analog copying. Macrovision's Copy Generation Management System (CGMS), can accommodate fair use copying by allowing an unlimited

number of first-generation copies, but prohibiting those copies from being recorded again. The CGMS system works by storing two bits of CGMS Copy-Control Information (CCI) in the header of each disc sector. The CGMS can be CGMS-A for analog output, and CGMS-D for digital output. Verance developed a DVD-Audio watermarking technique (which uses CGMS CCI) to guard against the copying through audio analog output. Watermark Review Panel (WaRP) under DVD content protection working group (CPTWG) is working on video watermarking proposals from the Galaxy group (IBM, NEC, Pioneer, Hitachi, and Sony) and the Millennium group (Macrovision, Digimarc, and Philips) to choose one standard technique for DVD content protection. The minimum watermark payload expected is of 3 states (never copy, no more copying, and copy once) and an additional 2 bits for triggering analog protection system.

Digital Transmission Content Protection (DTCP), safeguards data streams transmitted over digital interfaces like IEEE-1394 and USB. DTCP is developed by Intel, Sony, Hitachi, Matsushita, and Toshiba and Digital Transmission Licensing Administrator (DTLA) issues licenses to use DTCP. DTCP can be used to protect DVD content only if it has already been encrypted by CSS, CPRM or CPPM. DTCP also uses two bit CCI to signal "copy one generation", "copy freely", "copy never", and "no more copies".

8.9 Digital Cinema & DRM

Cinemas too are not out of the compulsions of the digital age [6][26][42][49][56]. The digital cinema system delivers motion pictures that have been digitized or mastered, compressed, and encrypted to theatres using either physical media distribution (such as DVD-ROMs) or electronic transmission methods, such as via Internet, and satellite multicast methods. Though today's digital cinema quality is not as good as that of film-based cinema, the digital cinema has many compelling factors in favor of it. One of the advantages is that though the quality is currently not as good, the quality of the digital cinema is preserved over the repeated shows whereas in the film-based cinema, the quality deteriorates after multiple viewings. Another advantage is that the distribution cost is low for digital cinema as they can be transmitted to the cinema halls through electronic transmission methods or through stored media such as DVDs which are much more manageable than the bulkier and heavier film reels. Making copies of film reels for distributing to cinema

halls is an enormous task compared to making copies in digital domain. In addition digital cinema can incorporate advanced theatrical experiences such as moving seats etc. through the use of metadata.

Usually movies are mastered on a film and are then digitized to obtain the digital version. But with the introduction of high definition digital camcorders, motion pictures are mastered directly in the digital domain. This digital movie is then compressed, encrypted, delivered to the cinema halls. At the cinema hall the digital movie is temporarily stored, decrypted, decompressed, and projected/played back. The cinema halls are equipped with a storage system and a projector system. There are two models for the secure storage and play back of digital cinema content -- the broadcast server model, and the data server model. In the broadcast server model, the storage system provides for temporary storage, decryption, decompression, and local encryption. The projector system implements local decryption, and play back. As far as security is concerned, the storage system and the projector system are to be physically secured and the communication between the projector system and the storage system need to be secured through local encryption. However, in data server model, the storage system implements only temporary storage and the projection system implements decryption, decompression, and play back. In this model only the projector system needs to be physically protected. The audio stream and other advanced feature control streams are routed to the relevant processor and play back after decryption and demultiplexing by the storage/play back system. The producer should employ a strong encryption scheme and the key needs to be transmitted through a secure channel to the security manager in the cinema hall. Usually for enhanced security and control, producers/distributors apply the encryption in such a way that it can be decrypted only in a designated storage/projector system and also can control the play back schedules or revoke the play back if the storage/play back system is found compromised or the exhibitor is found aiding piracy.

In a film-based cinema system, pirates can make pirate copy by taking possession of film reels and digitizing the content. This is possible since the reel content is not encrypted. In case of digital cinema, since the digital cinema content is transferred in an encrypted mode, it would be difficult for the pirates to break the encryption scheme to make a pirate copy. Another technique of making pirate copy is by directly videographing off the screen during the show. In order to trace and control this kind of piracy in digital

cinema systems, digital watermarking techniques can be employed. None of the current digital cinema systems explicitly mention the use of any schemes for tracing piracy. The current systems only provide conditional access using an encryption scheme. Thus, a lot of work remains to be done in this area.

The Society for Motion Picture and Television Engineers (SMPTE) of USA has constituted the DC28 digital cinema technology committee, a working group to discuss the various issues that face the full deployment of digital cinema. DC28 is divided into seven study groups namely, mastering, compression, conditional access, transport and delivery, audio, theatre systems, and projection. The European counterpart of SMPTE is European Digital Cinema Forum (EDCF), where study groups from different European countries share their information on digital cinema and the "technical module" is where all of the security research is being performed.

9 Conclusion

This chapter discusses the rights requirements of each party involved over the life cycle of digital video. It also discusses various requirements to DRM stemming from asset management and usage controls needs. In addition the requirements and constraints to DRM, business, legal, and social aspects of DRM have also presented. The technical aspect of DRM elaborates on the technologies used for obtaining DRM, techniques and tools for obtaining DRM in digital video broadcasts, stored video such as DVDs, and digital cinema, and standardization efforts by bodies such as MPEG, IETF, W3C, SMPTE etc.

Most of the current DRM systems support confidentiality against non-consumers. Some of the systems implement copy protection/control mechanisms. Some envisage the use of fingerprinting mechanisms for tracing piracy. These systems are essentially intended to mitigate the concerns of owners. Though the trading protocols and rights languages are being designed with the intention of supporting consumer concerns, the supporting cryptographic and watermarking techniques and protocols are yet to be designed. A full-fledged DRM system should be capable of supporting the rights of all parties (creators, owners, distributors, and consumers) involved in digital asset creation and transaction. DRM in its broadest sense is

end-to-end management of digital trust Therefore, tremendous research challenges abound in this vital area of information security.

Bibliography

[1] Adelsbach A., and Sadeghi A. R. *Zero-Knowledge Watermark Detection and Proof of Ownership*. Proceedings of Fourth Information Hiding Workshop, IHW2001, Pittsburgh, USA, April 2001.

[2] Anderson R., and Manifavas C. *Chameleon – A New Kind of Stream Cipher*. Encryption in Haifa, Jan. 1997.

[3] Barni M., Bartolini F., Cappellini V., and Piva A. *A DCT Domain System for Robust Image Watermarking*. Signal Processing, European Association for Signal Processing (EURASIP), May 1998, Vol. 66, No. 3, pp. 357—372.

[4] Bormans J., Gelissen J., and Perkis A. *MPEG-21: The 21st Century Multimedia Framework.* IEEE Signal Processing Magazine, Vol. 20, Issue: 2, March 2003, pp 53 – 62.

[5] Braudaway G. W., Magerlein K. A., and Mintzer F. *Protecting Publicly Available Images with a Visible Image Watermark*. International Conference on Image Processing, Vol. 1, 1997, pp 524 –527.

[6] Byers S., Cranor L., Cronin E., Kormann D., and McDaniel P. *Analysis of Security Vulnerabilities in the Movie Production and Distribution Proces*s. Proceedings of ACM Workshop on Digital Rights Management, Oct. 2003.

[7] Camp L.J. *DRM: Doesn't Really Mean Digital Copyright Management.* Proceedings of the 9th ACM Conference on Computer and Communications Security. 2002, pp 78 – 87.

[8] Clark D. *Future of Intellectual Property: How Copyright Became Controversial*. Proceedings of the 12th annual conference on Computers, freedom and privacy, April 2002.

[9] Clayson P.L., and Dallard N.S. *Systems Issues in the Implementation of DVB Simulcrypt Conditional Access*, International Broadcasting Convention, Sep. 1997, pp 470 –475.

[10] Cohen J.E. *DRM and Privacy.* Communications of the ACM, Vol. 46, No. 4, April 2003, pp 47 – 49.

[11] Cox I. J., Killian J., Leighton T., and Shamoon T. *Secured Spread Spectrum Watermarking for Multimedia*. IEEE Trans. on Image Processing, Vol. 6, No. 12, Dec. 1997, pp 1673-1687.

[12] Cox I. J., and Linnartz J. P. *Some General Methods for Tampering with Watermarks*. IEEE Journal on Selected Areas in Communications, Vol. 16, Issue 4, May 1998, pp. 587 -593.

[13] Craver S. *Zero Knowledge Watermark Detection*. Proceedings of the Third International Workshop on Information Hiding, Springer Lecture Notes in Computer Science, vol. 1768, 2000, pp. 101--116.

[14] Craver S., Memon N., Yeo B., and Yeung M.M. *Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks and Implications*. IEEE Journal on Selected Areas in Communications, Vol. 16, No. 4, May 1998, pp 573-586.

[15] Cutts D.J. *DVB Conditional Access,* Electronics & Communication Engineering Journal, Vol. 9 No. 1, Feb. 1997, pp 21 –27.

[16] Durfee G., and Franklin M. *Distribution Chain Security*. 7th ACM Conference on Computer and Communications, pp. 63--70, ACM Press, New York, 2000.

[17] Eggers J.J., Su J. K., and Girod B. *Asymmetric Watermarking Schemes*. Proceedings of Sicherheit in Mediendaten, GMD Jahrestagung, Springer Verlag, 2000.

[18] Emmanuel S., and Kankanhalli M.S. *A Digital Rights Management Scheme for Broadcast Video*. Multimedia Systems, Vol. 8, Issue: 6, April 2003, pp 444-458.

[19] Emmanuel S., and Kankanhalli M.S. *Copyright Protection for MPEG-2 Compressed Broadcast Video*. Proceedings of the IEEE International Conference on Multimedia and Expo (ICME 2001), Tokyo, Aug. 2001.

[20] Erickson J.S. *Fair Use, DRM, And Trusted Computing.* Communications of the ACM, Vol. 46, No. 4, April 2003, pp 34 – 39.

[21] Fox B.L., and LaMacchia B.A. *Encouraging Recognition of Fair Uses in DRM Systems.* Communications of the ACM, Vol. 46, No. 4, April 2003, pp 61 – 63.

[22] Hartung F., and Girod B. *Watermarking of Uncompressed and Compressed Video*. Signal Processing, Vol. 66, No. 3, May 1998, pp. 283-301.

[23] Hartung F., and Kutter M. *Multimedia Watermarking Techniques*. Proceedings of the IEEE, Vol.87, No. 7, July 1999, pp 1079-1107.

[24] Hartung F., and Ramme F. *Digital Rights Management and Watermarking of Multimedia Content for M-Commerce Applications*. IEEE Communications Magazine, Vol. 38, No. 11, Nov. 2000 pp 78 –84.

[25] Horne B., Pinkas. B., and Sander T. *Escrow Services and Incentives in Peer-to-Peer Networks*. 3rd ACM Conference on Electronic Commerce, 2001.

[26] http://www.mpaa.org/dcinema The Motion Picture Association's Role in Digital Cinema.

[27] http://www.chiariglione.org/mpeg/ The MPEG Home Page.

[28] http://www.ietf.org/html.charters/trade-charter.html Internet Open Trading Protocol (trade).

[29] http://www.w3.org/Help/siteindex The W3C Trading Protocols.

[30] http://www.xrml.org The Extensible rights Markup Language.

[31] http://odrl.net/The Open Digital Rights Language.

[32] http://www.doi.org/The Digital Object Identifiers.

[33] http://www.cptwg.org/ The Copy Protection Technical Working Group.

[34] http://www.dvdcca.org/DVD The DVD Copy Control Association.

[35] http://www.microsoft.com/windows/windowsmedia/wm7/drm/scenarios.aspx DRM Business Models

[36] http://www.atsc.org/standards.html. *ATSC Standard A/70: Conditional Access System for Terrestrial Broadcast with Amendment*.

[37] Iannella R. *Digital Rights Management (DRM) Architectures*. D-Lib Magazine, Vol. 7, No. 6, June 2001.

[38] ISO/IEC TC JTC1/SC 29/WG11/N 6269: Information Technology – Multimedia Framework (MPEG-21) – Part 1: Vision, Technology and Strategy.

[39] ISO/IEC 13818-1: *Generic Coding of Moving Pictures and Associated Audio: Systems.* (MPEG-2 Systems).

[40] ISO/IEC 14496-1: *Coding of Audiovisual Objects: Systems*. (MPEG-4 Systems).

[41] Korba L., and Kenny S. *Towards Meeting the Privacy Challenge: Adapting DRM*. Proceedings of ACM Workshop on Digital Rights Management, Nov. 2002.

[42] Korris, J., and Macedonia M. *The End of Celluloid: Digital Cinema Emerges*. Computer, Vol. 35, Issue: 4, March 2002, pp 96 – 98.

[43] Kundur D., and Hatzinakos D. *Digital Watermarking Using Multiresolution Wavelet Decomposition*. Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Processing, 1998, Vol. 5, pp. 2969—2972.

[44] Kwok S.H., Cheung S.C., Wong K.C., Tsang K.F., Lui S.M., and Tam K.Y. *Integration of Digital Rights Management into Internet Open Trading Protocol (IOTP)*. Decision Support Systems (DSS), 34, 4, (2003), pp 413-425.

[45] Langelaar G.C., Lagendijk R.L., and Biemond J. *Removing Spatial Spread Spectrum Watermarks*. European Signal Processing Conference (EUSIPCO'98), Rodes, Greece, September 1998.

[46] Linnartz J. P., Depovere G., and Kalker T. *Philips Electronics Response to Call for Proposals Issued by the Data Hiding SubGroup Copy Protection Technical Working Group*.

[47] Liu Q., Safavi-Naini R., and Sheppard N.P. *Digital Rights Management for Content Distribution*. Australasian Information Security Workshop, Adelade, 2003.

[48] Löytynoja M, Seppänen T, and Cvejic N. *Experimental DRM Architecture Using Watermarking and PKI*. First International Mobile IPR Workshop: Rights Management of Information Products on the Mobile Internet. Helsinki, August 2003.

[49] Lubell P.D. *A Coming Attraction: Digital Cinema.* IEEE Spectrum, Vol. 37, Issue: 3, March 2000 pp 72 – 78.

[50] Meng J., and Chang S. F. *Embedding Visible Video Watermarks in the Compressed Domain*. International Conference on Image Processing, Vol. 1, 1998, pp 474 –477.

[51] Messerges T.S., and Dabbish E.A. *Digital Rights management in a 3G Mobile Phone and Beyond.* Proiceedings of ACM Workshop on Digital Rights Management, Oct. 2003.

[52] Mooij W. *Advances in Conditional Access Technology*, International Broadcasting Convention, Sep. 1997, pp 461 –464.

[53] Mooney S. *Interoperability: Digital Rights Management and the Emerging EBook Environment*. D-Lib Magazine, January 2001, Volume 7, Number 1.

[54] Mulligan D., and Burstein A. *Implementing Copyright Limitations in Rights Expression*. Languages Proceedings of ACM Workshop on Digital Rights Management, Nov. 2002.

[55] Park J., and Sandhu R. *Towards Usage Control Models: Beyond Traditional Access Control.* Proc. of 7th ACM Symposium on Access Control Models and Technologies, Jun. 2002, pp 57-64.

[56] Peinado M., Petitcolas F.A.P., and Kirovski D. *Digital Rights Management for Digital Cinema.* Multimedia Systems, Vol. 9, 2003, pp 228 – 238.

[57] Pfitzmann B., and Schunter M. *Asymmetric Fingerprinting*. In Advances in Cryptology-EUROCRYPT'96, LNCS 1070. Springer-Verlag, Berlin, 1996, pp. 84-95.

[58] Piva A., Barni M., Bartolini F., Cappellini, V. *DCT-based Watermark Recovering Without Resorting to the Uncorrupted Original Image*. International Conference on Image Processing, 1997. Proceedings, Vol. 1, 1997, pp 520 -523.

[59] Podilchuk C. I., and Zeng W. *Digital Image Watermarking Using Visual Models*. In Human Vision and Electronic Imaging II, Vol. 3016, B. E. Rogowitz and T. N. Pappas, eds. San Jose, IS&T and SPIE, 1997, pp. 100-111.

[60] Rosnay M.D., *Digital Right Management Systems Toward European Law: Between Copyright Protection and Access Control*. Proceedings of the 2nd International Conference on WEB Delivering of Music, 2002.

[61] Samuelson P. *Encoding the Law into Digital Libraries.* Communications of the ACM, Vol. 41, No. 4, April 1998, pp 13 – 18.

[62] Simitopoulos D., Zissis N., Georgiadis P., Emmanouilidis V., and Strintzis M.G. *Encryption and Watermarking for the Secure distribution of Copyrighted MPEG Video on DVD*. Multimedia Systems Volume 9, No. 3, September 2003, pp 217 – 227.

[63] Sobel L. S. DRM as an Enabler of Business Models: ISPs as Digital Retailers, Digital Rights Management Conference, The Berkeley Center for Law and Technology, February, 2003.

[64] Wang X., Lao G., DeMartini T., Reddy H., Nguyen M., and Valenzuela E. *XrML – Extensible rights Markup Language.* Proc. of the 2002 ACM workshop on XML security, Nov. 22, 2002, pp 71 – 79.

[65] Williams J. *IT Architecture Meets the Real (Legal) World*. IEEE IT Pro, Sept/Oct 2001, pp 65 – 68.

[66] Wolfgang. R.B., and Delp E.J. *A Watermarking Technique for Digital Imagery: Further Studies*. Proceedings of IEEE International Conference on Imaging, Systems, and Technology, Las Vegas, June, 1997, pp. 279--287.

[67] Zeng W., and Lei S. *Efficient Frequency Domain Digital Video Scrambling for Content Access Contro*l. ACM Multimedia '99 Proceedings, Orlando, Florida, Nov. 1999.