ECP-2007-DILI-517005

ATHENA

Overview of collective licensing models and of DRM systems and technologies used for IPR protection and management

Deliverable number	*D6.2*
Dissemination level	*Public*
Delivery date	*31 October 2009*
Status	*Final*
Author(s)	*Barbara Dierickx (PACKED) & Dimitrios Tsolis (University of Patras)*

e*Content*plus

This project is funded under the eContentplus programme1,
a multiannual Community programme to make digital content in Europe more accessible, usable and exploitable.

[1] OJ L 79, 24.3.2005, p. 1.

Table of Contents

Executive summary

This report, created by the WP6 on Intellectual Property Rights of the ATHENA-project, is divided into two main parts; one on collective licensing and one on the use of Digital Rights Management (DRM) techniques.

Part one: overview of collective licensing models

The goal of this part is to present an overview of collective licensing models in relation to the digitisation and disclosure of cultural heritage content. It should be noted that the general scope of copyright will not be discussed in this report since it already featured extensively in the ATHENA D.6.1. Overview of IPR legislation in relation to the objectives of Europeana.

The first section of the report situates current trends in unlocking cultural heritage content by making it digitally available on the internet. Some specific issues on copyright to which collective licensing might provide an answer are presented here as well. We take a look at the current copyright discussions within the European policy field as well as regulatory initiatives by Europeana.

The following chapter gives an overview of the actual collective licensing mechanisms. It starts off by presenting what the collective management of rights is and why it can be useful to the cultural heritage sector. Different collective licensing models are then illustrated, as well as some country-specific regimes.

This is followed by a chapter on new and emerging licensing models. Collective licensing may be one option but we should also look at others. Open content licenses and Creative Commons licenses in particular will be discussed here. Their application in the field of cultural heritage, as well as some cases and best pratices, illustrate the theory.

A general conclusion summarizes this first part of the report.

Part two: overview of DRM techniques

The issues of wide access to cultural and scientific content and in parallel protection and management of copyright create the next digital dilemma and considerable scepticism to Web 2.0 users and content providers: do we consider creations as human kind advances and in some way patrimony of the humanity freely accessible and reusable by anyone or do we consider wiser to protect it as the result of ‘personal’ investments and efforts?
How intellectual property laws could embrace the apparently paradoxical goals of motivating individual creation and preserving the ultimate benefits of that creation for the common good, is a major question. As a result the necessity of using systems which allow broad exchange of the creations while at the same time use copyright protection methodologies and tools during this exchange is important. Digital Rights Management systems have the objective to fulfil this goal, thus to protect and manage rights and copyrights and in parallel support the distribution and publication of priceless digital creations in the form of digital content.
A technical study presents the main aspects of Digital Rights Management Systems and is structured in the following main sections:

- Digital Rights Management Systems – An Overview. The DRMS is being defined and certain technological aspects are presented.
- Digital Watermarking in-Depth. The state of the art, new trends and the uses regarding digital watermarking for image and video files are presented.
- Digital Rights Management and Transactions – On-line Rights Clearance. The DRMS uses for transactions between users and content and new on-line clearance strategies are being analysed.
- Digital Rights Management – A European Law Perspective. A specialised review of legislation referring to Digital Rights Management systems is included.
- Best Practice for DRM & IPR Protection in Europeana. This chapter is concluding on what is the best practice for implementing a Digital Rights Management System which applies IPR protection and management for digital cultural content which is being published through websites and/or Europeana’s portal.

This technical study could be proved useful to organisations and people who might not know what a DRM system is, while at the same time and in certain aspects reaches depths useful for experienced scientists and experts active in the scientific field of DRM and copyright protection/management.

PART ONE – OVERVIEW OF COLLECTIVE LICENSING MODELS

1. General introduction

1.1. Introduction

The 21st century marked the birth of the 'information society' as we know it today. The availability of technology and infrastructure for digitisation and disclosure of cultural material increased drastically, and made it possible to disseminate a vast array of cultural information (including digital cultural heritage) over the internet. This possibility opened up the physical boundaries of collecting institutions have existed for a long time. Digital representations of cultural objects can now be shared with a worldwide audience at an unseen speed. But for some of these objects and the institutions that manage them, this idea will just stay what it is – a concept, and one that can not be realised. After all, a considerable amount of cultural works that institutions would want to digitise are protected by authors' rights and may not be digitised or made available to the public over the internet without a proper agreement that regulates the copyright(s).[2]

This issue and the recurrence of similar reactions from copyright owners has caused some internet users to associate the notion of 'authors' rights' with negative feelings. Internet users experience authors' rights often as a restriction of the freedom of information. On the other hand, the content industry sees (and treats) copyright as a key component in the development of an economic (culture) market.[3]

The protection of intellectual property rights, and authors' rights in particular, has therefore led to a paradoxical effect. The power of the internet to offer on demand services and numerous other applications has given rise to a boom in creative digital content creation and the distribution thereof. It offers content providers unseen ways of exploiting their content by reaching a global audience. At the same time, copyright protected works become more exposed to piracy, illegal copying and shady forms of distribution. Very recently the founders of the Bittorrent website 'The Pirate Bay' were convicted to a one year prison sentence and had to pay 2.7 million euros worth of damages for violating Swedish copyright.[4] Not only were they sentenced; their denunciation of the current copyright system led them to set up a political party; the Pirate Party[5] (or Piratpartiet in Swedish). Their mission can be upheld in one sentence: *"The Pirate Party wants to fundamentally reform copyright law, get rid of the patent system, and ensure that citizens' rights to privacy are respected."* [6] By the end of December 2009 their commitment and active engagement resulted in two seats in the European Parliament on behalf of Sweden.[7]

> *"It's almost a truism in the tech world that copyright owners reflexively oppose new inventions that do (or might) disrupt existing business models. Most of it turned out to be absurd hyperbole, but it's interesting to see just how consistent the words and the fears remain across more than a century of innovation and a host of very different devices."* – Nate Anderson[8]

---

2 E. Werkers, R. Kerremans, T. Robrechts, J. Dumortier, Auteursrecht in de digitale samenleving, 2009, pp. 9. Available online (only in Dutch) http://www.cjsm.vlaanderen.be/e-cultuur/downloads/onderzoeksrapport_auteursrecht_in_de_digitale_samenleving.pdf

3 P.B. Hugenholtz, Toegang tot de bron: het auteursrecht en het internet, in: Ars Aequi, July/August 2008, p. 581. Available online (only in Dutch) http://www.ivir.nl/Publicaties/hugenholtz/AA_jul_aug_2008_Toegang_tot_de_bron_het_auteursrecht_en_het_internet.pdf

4 E. Werkers, R. Kerremans, T. Robrechts, J. Dumortier, Op. Cit., pp. 9.

5 For more information on the Piratpartiet, see their website: http://www.piratpartiet.se/international/english

6 http://www.piratpartiet.se/international/english

7 http://en.wikipedia.org/wiki/Pirate_Party_%28Sweden%29

8 N. Anderson, 100 years of Big Content fearing technology - in its own words, 2009, s.p. Available online http://arstechnica.com/tech-policy/news/2009/10/100-years-of-big-content-fearing-technologyin-its-own-words.ars

Technological developments that facilitate a nearly perfect reproduction of an object often make right holders believe in a doom scenario. Throughout history, these kinds of visions of the future were heard at the arrival of the photocopying machine *("The day may not be far off when no one need purchase books")*[9], the VCR *("I say to you that the VCR is to the American film producer and the American public as the Boston strangler is to the woman home alone")*[10], the audio cassette *("Home taping is killing music")*[11], mp3 players, and so on. The internet and world wide web allows for an even faster distribution and copying of cultural works[12]. This has led to the fact that right holders are pleading for a stronger legal position (one they have up to now received in many legal cases). For quite some time now, they have also begun to use technology (so-called DRM techniques[13]) as a weapon in their battle against counterfeits, net piracy and their cultural contents being digitally stolen.[14]

Technological developments have not only empowered right holders, but also creators and users of cultural content in a way that some of them have become user-creators. Uploading your own film clip or audio work onto an internet platform to share it with millions of visitors has never been easier. At the same time these creators also build on the past by re-using existing cultural material that they find online. These remixes of existing content are in their turn added to the vast web-based global cultural collection.

But while cultural heritage institutions may for example attract a much larger audience due to the online disclosure of digital reproductions of their holdings, these visitors might also 'take' some of these reproductions and transform them into new, remixed content. This may not be authorised by the right holder and/or cultural heritage organisation, but such phenomenon is very hard to control in an online environment. The freedom of distribution of cultural content to European citizens comes in these cases face to face with the safeguarding of the cultural heritage organisation's business model.

And in placing content online, they might also have to bear in mind the rights of third parties (who may, for example, press charges when copyrighted content that belongs to them is placed online by museums, in case rights have not been cleared). So out of fear for claims by these third parties, materials remain in their analog status or are only digitally available within the museum. Locking up cultural content might just be the effect that this debate provokes, instead of working towards solutions that benefit right holders (artists, heirs) as well as intermediary parties (museums, galleries) and end-users (the general public).

In addition, copyright regulations are still often perceived as 'unclear' or 'difficult' and need practical translation for a layman audience. Many cultural heritage institutions do not benefit from an in-house lawyer or legal service[15], so they have to struggle themselves through pages of directives, laws and sometimes case-specific provisions. Not unlocking collections through the internet may therefore also be caused by an ignorance as far as knowledge and understanding of legal provisions goes. But also the fact that contemporary European legal provisions at this moment do not allow for some kind of 'fair use' in dealing with online cultural heritage (which is in se not-for-profit) increases the reluctance against copyright in general.

---

9 N. Anderson, 100 years of Big Content fearing technology - in its own words, 2009, s.p. Available online http://arstechnica.com/tech-policy/news/2009/10/100-years-of-big-content-fearing-technologyin-its-own-words.ars

10 IBIDEM

11 IBIDEM

12 Instead of analog copies, digital ones retain their quality perfectly and can stand up to wear and tear.

13 Digital Rights Management (DRM) is a technique to manage digital rights of right holders. Through digital security techniques, that can be connected to DRM, the right holder can restrict the legal rights of users. DRM-systems therefore have to be connected to usage agreements, in which is stated what kind of use of the material is allowed or not without the permission of the right holder *(will be referred to here in the second part of this deliverable on DRM techniques).*

14 E. Werkers, R. Kerremans, T. Robrechts, J. Dumortier, Auteursrecht in de digitale samenleving, 2009, pp. 9. Available online (only in Dutch) http://www.cjsm.vlaanderen.be/e-cultuur/downloads/onderzoeksrapport_auteursrecht_in_de_digitale_samenleving.pdf

15 See paragraph *4.3. The use of open content licenses in the field of cultural heritage* for exact figures.

Cory Doctorow, author and open content[16] activist, summarizes the reigning feeling:

> *"A law that no one understands and no one abides by is no law at all. Parts of copyright -- the right to regulate how commercial licenses with industrial entities work -- are really important to me and to all working artists. But if we continue to try to expand copyright to cover everything, every interaction that involves a copy (which is every interaction these days), then the broad consensus that copyright is nonsense will continue to grow, and we'll lose the good stuff as well as the ridiculous stuff."* – Cory Doctorow[17]

1.2. Cultural heritage in an online environment

Cultural heritage institutions such as museums, libraries and archives are often confronted with both sides of the copyright coin.[18] Digitisation of collections provides great opportunities for widening access to their collections and especially to unique, rare and fragile material because a digital surrogate gets created, reducing handling of originals which was still necessary in the analog world. However, the lawfulness of digitising an object for this kind of purpose remains unclear. In cases in which works are out of copyright, digitisation and preservation may prove quite a simple task; just some technical procedures to go through and the digital version is there. But for in copyright works, the situation is very different.[19] It causes difficulties for the digitisation of cultural content for the purpose of preservation and disclosure.

A lot of the current material acquired by cultural heritage institutions is still copyright protected. This is especially the case for contemporary paintings, literature, musical works, and so on. In order to digitise this kind of item, one may have to scan the analog material, take digital photographs, use software to create digital files and attach contextual information to the digital object in the form of metadata. All these acts can not be performed without any limitation: they are restricted acts under copyright law. Checking the rights status of the analog object, as well as what is possible with regards to digitisation will be a process one needs to invest in, but one that's necessary before one can start with any digitisation at all. In order to avoid the time and expense needed to address these issues (especially personnel costs), many institutions avoid digitising material that is copyright protected.[20]

In order to know which acts may definitely not be performed without the permission of the right holder, it is necessary to be aware of the exact scope of the rights involved and to know who manages these rights. The actual type of rights, the duration of their term of protection and who should be seen as the right holder can differ according to the nature of the work and/or the creators involved. Depending on the use of the work that a cultural heritage institution envisages, it will be necessary to obtain one or more permission(s), or to address a central rights management body.[21]

---

[16] See paragraph *4.2. Open Content Licenses: Creative Commons as an example* for more information about 'open content'.

[17] C. Doctorow, Lily Allen's copyright problem, 2009, s.p. Available online http://www.boingboing.net/2009/09/23/lily-allens-copyrigh.html

[18] E. Werkers, R. Kerremans, T. Robrechts, J. Dumortier, Auteursrecht in de digitale samenleving, 2009, pp. 10. Available online (only in Dutch) http://www.cjsm.vlaanderen.be/e-cultuur/downloads/onderzoeksrapport_auteursrecht_in_de_digitale_samenleving.pdf

[19] A. Muir, Preservation, access and intellectual property rights challenges for libraries in the digital environment, 2006, p. 5. Available online http://www.ippr.org.uk/members/download.asp?f=/ecomm/files/preservation_access_ip.pdf&a=skip

[20] A. Muir, Preservation, Op. Cit., pp. 6-7.

[21] E. Werkers, R. Kerremans, T. Robrechts, J. Dumortier, Op. Cit., 2009, pp. 11. More information on central rights management bodies can be found in paragraph *3.1. The collective management of rights.*

2. The scope of copyright

2.1. Scope and exceptions

In many cases, the cultural content that is offered on the internet is protected by intellectual property rights. As we have seen these works may not be multiplied/reproduced or communicated to the public without the permission of the right holder(s). Fortunately for the freedom of information and the digitisation of heritage collections, not all works are protected by copyright. Authors' rights end 70 years after the death of the creator of the work and in some cases 70 years after publication.[22] Works on which the term of protection has expired, fall into the so-called 'public domain'.[23]

However, cultural heritage institutions have not been left out in the cold by legislators. Legal exceptions exist for this kind of 'user' which they can call upon for certain envisaged uses of cultural content (e.g. for digitisation of objects and the disclosure of the digital material). These exceptions are acknowledged on an international, European and national level but one cannot speak of a harmonised European framework. Apart from some legal provisions, it has been left up to member states to decide which exceptions to implement in the national legislation.[24]

The traditional model of cultural heritage institutions is based on the collection, preservation and exhibition of physical objects, and is hard to translate to a digital environment. Making a copyright protected work available online can only be done with the permission of the rights holder. Because the online disclosure of materials is an act of 'communication to the public', Europe has introduced an exception that allows making collection material digitally available to a user.[25] This is however only possible on-site, through a closed network, and on the premises of the particular institution.

> *Art. 5 (3) (n) Member States may provide for exceptions or limitations to the rights provided for in Articles 2 and 3 in the following cases: use by communication or making available, for the purpose of research or private study, to individual members of the public by dedicated terminals on the premises of establishments referred to in paragraph 2(c) of works and other subject-matter not subject to purchase or licensing terms which are contained in their collections.* [26]

In the majority of European countries this exception has been adopted and such institutions are therefore permitted to make works available from their own collection to the public, for the purpose of research or private study, through dedicated terminals on the premises of the institution. The works that are communicated this way may not be subject to a contractual statement indicating that this action (the act of communication through on-site terminals) is forbidden. The institutions holding the terminals may not earn any direct or indirect economic benefit from making work available.

The services that libraries, museums and archives wish to offer, as well as the nature of the works protected by copyright are changing fast. The exceptions that are provided for libraries, museums, archives and educational institutions in national legislation are often a reflection of a legislative decision that was made in the (sometimes far

---

[22] P.B. Hugenholtz, Toegang tot de bron: het auteursrecht en het internet, in: Ars Aequi, July/August 2008, p. 582. Available online (only in Dutch) http://www.ivir.nl/Publicaties/hugenholtz/AA_jul_aug_2008_Toegang_tot_de_bron_het_auteursrecht_en_het_internet.pdf

[23] More information on the concept of public domain can be found in paragraph *2.3.3. Europeana: The Public Domain Charter*.

[24] E. Werkers, R. Kerremans, T. Robrechts, J. Dumortier, Auteursrecht in de digitale samenleving, 2009, pp. 10-11. Available online (only in Dutch) http://www.cjsm.vlaanderen.be/e-cultuur/downloads/onderzoeksrapport_auteursrecht_in_de_digitale_samenleving.pdf

[25] Other examples of existing copyright exceptions can be found in the ATHENA D.6.1. report, *Overview of relevant IPR legislation in relation to the objectives of Europeana.*

[26] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, Art. 5 (3) (n). Available online http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001L0029:EN:HTML

distant) past. This causes a tension between what institutions would like to do with their material, and what they are allowed to do with it, according to the law.[27]

Making content available online (without exception) still falls under general copyright regulations. The closed network exception is a step in the right direction towards a new generation of services provided by libraries and related institutions, but online digital libraries as anticipated by the European Commission and as shaped by Europeana and its satellite projects[28] cannot benefit from it.

2.2. The European framework

In April 2009, the European Parliament was the stage of a passionate debate on copyright protection. Representatives of the music industry strived for an extension of the term of protection through neighbouring rights for music recordings to 95 years (it used to be fixed at 50 years). This considerable increase caused a lot of negative reactions, especially since one of the Commission's initiatives – Europeana, Europe's digital heritage library - aims at making cultural content as widely accessible as possible. The longer cultural works are copyright protected, the more expensive and difficult it will be to achieve. In the end, a compromise was reached at 70 years; nevertheless members of the European Parliament voted in favour of extending the term of protection for music recordings in the European Union by 20 years.[29]

Copyright is a theme that is still very present within current European communication and policy. The work of the High Level Expert Group on Digital Libraries was illustrated earlier, but Commissioners themselves also draw attention to Europe's position in the global copyright debate, and its influence on the unlocking of Europe's digital cultural heritage. In response to a meeting on the Google Books settlement, Commissioners Reding and McCreevy released a press communication stating that *"[...] Is the present framework still fit for the digital age? Will the current set of rules give consumers across Europe access to digitised books? Will it guarantee fair remuneration for authors? Will it ensure a level playing field for digitisation across Europe, or is there still too much fragmentation following national borders? [...]"* [30] At present day, questions rather than answers still dominate the debate. However, in its recent EU2020 strategy, the Commission states that *"At EU level, the Commission will work to create a true single market for online content and services (i.e. borderless and safe EU web services and digital content markets, with high levels of trust and confidence, a balanced regulatory framework with clear rights regimes, the fostering of multi-territorial licences, adequate protection and remuneration for rights holders and active support for the digitisation of Europe's rich cultural heritage, and to shape the global governance of the internet."* [31] Author's rights and digital cultural heritage were mentioned in the same sentence, indicating the will to tackle the copyright problem. This recent strategy is of course a facilitator for the future development and expansion of Europeana.

2.3. Special points of interest

Works dating from the end of the 19th century, 20th and 21st century, are in many cases still protected by copyright. Libraries and archives wishing to digitise these kinds of works and to offer them in an online environment, are faced

---

[27] K. Crews, Study on Copyright Limitations and Exceptions for Libraries and Archives, 2008, pp. 27-28. Available online http://www.wipo.int/meetings/en/doc_details.jsp?doc_id=109192

[28] Other projects such as the ATHENA project, European Film Gateway (EFG) or EuropeanaLocal all struggle with the same issues as far as the clearing of rights relating to their objects goes.

[29] The proposition to extend the term of protection for musical works has been approved by the European Parliament, but still has to pass the European Council in order to become law. European Parliament press release, 23/04/2009. Available online http://www.europarl.europa.eu/sides/getDoc.do?language=EN&type=IM-PRESS&reference=20090422IPR54191

[30] V. Reding, C. McCreevy, in: MEMO/09/376, Brussels, 07/09/2009. Available online http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/09/376&format=HTML&aged=0&language=EN&guiLanguage=nl

[31] European Commission communication: Europe 2020 - A European strategy for smart, sustainable and inclusive growth, 2010, p. 12. Available online http://ec.europa.eu/eu2020/pdf/COMPLET%20EN%20BARROSO%20%20%20007%20-%20Europe%202020%20-%20EN%20version.pdf

with big copyright problems. Especially in cases where right holders are unknown and/or untraceable. Works of this nature are called 'orphan works' (see below) and are one of the most difficult issues in current copyright.[32] We will look briefly at orphan works and out-of-print works in this paragraph, since some of the suggested models of collective licensing are often quoted as possible solutions to these two specific 'copyright cases'. Another point of interest is the public domain, and how a project like Europeana relates to this collection of 'out-of-copyright' works.

2.3.1. Orphan works

An orphan work is a work that still enjoys copyright protection, but whose right holder cannot be identified (and thus contacted) or can not be located/traced.[33] This may be e.g. due to the fact that the author may be deceased without leaving any heirs[34], or beacause a publisher who holds the rights on the work no longer exists and a register of authors who are being represented by the specific publishing company, has not been kept.[35] Orphan works are problematic for their users; the permission to use or exploit these works cannot be obtained. Since copyright demands that the permission of the right holder has to be obtained prior to the use, a lot of works are threatened with becoming obsolete or lost. They may, for example, not be digitised for preservation purposes by a cultural heritage institution, let alone made available through the internet.[36]

Cultural heritage institutions will often leave orphan materials untouched out of fear of possible consequences. If a right holder eventually shows up after the particular work has been used, the cultural heritage organisation might face juridical procedures and/or the payment of considerable financial compensation. The cost of finding a right holder can be very high. The institution has to invest in staff spending a lot of time to find such a person. They often do not even attempt to undertake such a search, as the effort required is too high. However, in some cases launching a search could pay off: some right holders are pleased to have their work used, especially in a cultural heritage context since it is often non-commercial by nature, and may only require minimal compensation or simply an attribution.

Although it is difficult to estimate the number of orphan works, cultural institutions consider them to be a serious problem. The British Library for instance estimates that *"over 40 percent of all in-copyright works are Orphan Works"*.[37] A survey carried out by the Association des Cinémathèques Européennes (ACE) in 2005 identified 50.000 works within European film archives as 'orphan'[38].

---

[32] P.B. Hugenholtz, Toegang tot de bron: het auteursrecht en het internet, in: Ars Aequi, July/August 2008, p. 582. Available online (only in Dutch) http://www.ivir.nl/Publicaties/hugenholtz/AA_jul_aug_2008_Toegang_tot_de_bron_het_auteursrecht_en_het_internet.pdf. More in-depth information on copyright in general and the legislation in different member states can be found in the ATHENA D.6.1. Overview of relevant IPR legislation in relation to the objectives of Europeana.

[33] MinervaEC Working Group (ed.), Minerva IPR Guide, 2008, pp. 22-23. Available online http://www.minervaeurope.org/IPR/IPR_guide.html

[34] This might only occur in a few cases. In the Netherlands for example, family members or relatives are traced as far as a sixth removed family member.

[35] eIFL-IP, Handbook on copyright and related issues for libraries, 2009, p. 25. Available online http://plip.eifl.net/eifl-ip/issues/handbook/handbook-complete-text/downloadFile/file/handbook2009_en.pdf?nocache=1268692483.68. Some policy gaps or trends in current copyright policy foster the existence of orphan works. The organisation *Electronic Information for Libraries* (eIFL.net) indicates some issues in their 'Handbook on copyright and related issues for libraries' (2009). eILF.net is a not for profit organisation that supports and advocates the wide availability of electronic resources by library users in transitional and developing countries. Its core activities are negotiating affordable subscriptions on a multi-country consortial basis, supporting national library consortia and maintaining a global knowledge sharing and capacity building network in related areas, such as open access publishing, intellectual property rights, open source software for libraries and the creation of institutional repositories of local content. More information can be found on their website: http://www.eifl.net/

[36] MinervaEC Working Group (ed.), Minerva IPR Guide, 2008, pp. 22-23. Available online http://www.minervaeurope.org/IPR/IPR_guide.html

[37] A. Vetulani, The problem of orphan works in the EU – An overview of legislative solutions and main actions in this field, 2008, p. 8. Available online http://ec.europa.eu/information_society/activities/digital_libraries/doc/report_orphan_stagiaire_2/report_orphan_vetulani%20%28corrected%20version%29%20%282%29.pdf

[38] C. Dillmann, Presentation during a day on the European Digital Libraries Initiative: The Stakeholders' Perspectives, Brussels, 14/09/2007. Available online http://ec.europa.eu/information_society/activities/digital_libraries/doc/seminar_14_september_2007/ace_perspective.ppt

The recent UK study 'In From The Cold' indicated that *"[...] Extrapolated across UK museums and galleries, the number of Orphan Works can conservatively be estimated at 25 million, although this figure is likely to be much higher."* [39] This kind of estimation shows that the problem of orphan works in cultural heritage collections is an important reality.

The 'Directive on the harmonisation of certain aspects of copyright and related rights in the information society' (or so-called Copyright Directive)[40] does not provide any explicit mechanism, e.g. a limitation or exception to copyright, aimed at facilitating the use of orphan works. Further in this study we will investigate some collective licensing models that could be seen as 'solutions' to the orphan works problem, but they are still not tailor-made to fit the problem. Apart from legal solutions, the European community is also looking forward to the results of the ARROW-project. ARROW began in November 2008 as a project funded as part of the EC eContent Plus agenda to make cultural content within Europe more accessible, usable and exploitable. One of the means to accomplishing this is the creation of a register of orphan works.[41]

2.3.2. Out-of-print works

Authors sometimes transfer the rights that govern the financial exploitation of their works to a publisher in order to ensure the publication and distribution of their works. Because of this transfer, they lose control over the circulation of their works within the cultural market. After a certain period of time a work can sometimes no longer be available on the market. As a result of poor sales, a publisher can decide to stop reprinting the work. Because of this certain books, films, sound recordings, .. only become available in libraries and similar centres; the work has become 'out-of-print'. Albeit a commercial copy may no longer be available, this does not mean that the work itself is no longer copyright protected. The normal copyright legislation still applies.

A result of this is that a library may for example not digitise it and make it available online as a part of the cultural heritage without explicit permission of the right holder - let alone distribute it. Yet there are cases in which the further distribution of already digitised out-of-print material can be a win-win solution for the multiple parties involved: a right holder may well be prepared to consent to an even wider dissemination of his or her work, beyond the restricted network of public institutions.[42]

The High Level Expert Group (HLEG) has formulated suggestions in order to deal with orphan works and out-of-print works. An important initiative on orphan works has been initiated by the European Union within the i2010 Digital Libraries initiative. The HLEG that was set up in order to investigate the different legal, technological and economic factors in the 'digital libraries' also communicated on orphan works.[43] In the Final Report of this HLEG, out-of-print works are also a point of interest. With this report the HLEG wanted to instigate the wider distribution of digitised out-of-print works, suggesting measures that comply with existing exceptions for digitisation and disclosure. It wanted to stimulate through model licences for example, the creation of agreements between right holders and cultural heritage

---

[39] N. Korn, In from the cold, 2009, p. 6. Available online http://sca.jiscinvolve.org/files/2009/06/sca_colltrust_orphan_works_v1-final.pdf

[40] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, Official Journal L 167 of 22/06/2001, p. 10.

[41] ARROW is a consortium project involving national libraries across Europe as well as publishers and writers' collecting societies supporting the EC's i2010 Digital Library Project. ARROW will enable the identification of rights holders, rights and the right status of works; this will assist users of works, in particular, libraries, which must seek permission to digitise their collections and make them available to user groups. The ARROW project will also facilitate the exchange of information about rights, which is often held by rights holders, collecting societies and others. These solutions are proposed through the establishment of systems for the exchange of rights data, the creation of registries of orphan works, information on or registries of works out of print and a network of rights clearance mechanisms. The project will run until May 2011. More information can be found on the project website http://www.arrow-net.eu/

[42] M. Ricolfi, in: M. Ricolfi, 'Copyright Policy for digital libraries in the context of the i2010 strategy', 2008, pp. 7-8. Available online http://www.communia-project.eu/node/110

[43] MinervaEC Working Group (ed.), Minerva IPR Guide, 2008, pp. 22-23. Available online http://www.minervaeurope.org/IPR/IPR_guide.html

institutions on making digitised out-of-print works available within closed networks.[44] It should be noted that more work on this topic is still needed, since the Internet (and disclosure thereon) is exactly the opposite of a 'closed' network. Finding a solution for the issues of orphan and out-of-print works is crucial for making as much digital cultural heritage objects as possible available online and available through the Europeana-portal.

2.3.3. Europeana: The Public Domain Charter

Europeana[45], the online access point for digital cultural heritage, will release its first version of a fully operational service (the so-called 'Rhine-release') in the summer of 2010. Europeana's goal is to provide all European citizens with access to a broad variety of European digital culture through an online (searchable) portal. In order to fulfill this goal, issues regarding copyright on digital heritage objects need to be tackled.

One of the main focus areas of Europeana in this respect is public domain content. In cases where the term of protection of a work has expired, the work enters the 'public domain'. This means that it can be used by anyone and for any purpose, without remuneration.[46] The public domain has recently also become a point of interest in European copyright research, but has already been a favourite theme of American researchers. Current reflections on the public domain state that in order to be able to innovate and partake in the cultural scene of society, one should be able to draw on an ever growing and vivid public domain. Public domain, the amalgam of works on which there are no restrictions of use and thus the freedom to copy, has long been the rule while intellectual property rights were the exception. Nowadays, the inverse seems true. Copyrights have not always existed but the territory of intellectual property has constantly grown and expanded. Extending terms of protection and expanding the scope of copyright has not helped the evolution of this process. Because of changes in technology, works circulate much more and copyright questions are increasingly raised. As Severine Dusollier points out, *"[...] The intellectual commons, as some have started to dub the contents of the public domain, are increasingly at risk of being commodified, of falling into the private domain of intellectual property rights. [...]"* [47]

Europeana supports the idea of a healthy public domain and asks the cultural heritage institutions to change their mindset, which is often focussed on recouping the digitisation costs of public domain material over maximising the access to public domain material, for the benefit of (the European) citizens and a competitive and innovative society. Europeana has for this purpose launched a soft law initiative: the Public Domain Charter, an instrument that aims to contribute to this larger goal by establishing clear guidelines for working with public content. The Public Domain Charter is a policy statement and not a contract; it does not bind Europeana's content providers to any position. The Charter has not been officially released at the time of this writing. It should be due before Europeana's Rhine-release (summer 2010).

---

[44] The suggestions by the HLEG and their Final Report regarding orphan as well as out-of-print works will not be discussed further here, since more in-depth information on this topic was already included in the ATHENA *D.6.1. Overview of relevant IPR legislation in relation to the objectives of Europeana.*

[45] For more information on Europeana, see http://www.europeana.eu. The different kinds of research that will be carried out within the ATHENA framework will in the end facilitate the delivery of digital museum collections to Europeana.

[46] A remark should be made on the neighbouring rights that are related to the use of a work in the public domain. The text of a theatre play may for example have fallen into the public domain, while the video recording of a performance of the piece could still have neighbouring rights protection.

[47] Séverine Dusollier, in: V.L. Benabou, S. Dusollier, Draw me a public domain, pp. 161-162. In: P. Torremans (ed.), Copyright law : a handbook of contemporary research, 2007, 544p.

3. The collective licensing of rights

3.1. The collective management of rights

The main focus of this report is collective licensing systems. Part of the basic functioning of this kind of system is formed by collective rights management organisations. In exchange for the so-called fiduciary transfer of author's rights and neighbouring rights by the right holder[48], collective rights management organisations (CRMOs) take care of the granting of licenses to users, the management and supervision of the payment of royalties and the collecting and redistribution of them to right holders who are a member of, or gave a mandate to[49], the CRMO.[50]

The entire set of author's rights is comprised of moral rights and economic rights. The set of moral rights remains with the original creator and cannot be transferred to another person. The author may however transfer his or her financial rights, pertaining to the financial exploitation of his or her work, to others.[51] But why would an author want to let a collective rights management organisation manage his or her set of economic rights?

Right holders seem to have become more and more empowered to manage their own rights, e.g. by means of technological developments such as the application of DRM techniques. However, it appears to have become difficult to manage rights by oneself as an individual right holder, due to the fact of the ever increasing globalisation that has also affected the cultural market. Works are being used all over the globe; multiple international creators may have contributed to a work and the kinds of use and formats seem to diversify every minute. Making and closing agreements with every single user of one's work in a networked technological society such as that of the present day is no longer feasible. Therefore right holders (be they literary authors, performers of musical works and others) have united themselves under a collective umbrella. Collective rights management organisations provided an answer to this problem.[52]

By managing the whole chain of rights[53], collective societies liberate right holders from an administrative bureaucracy, they enforce the negotiating position of the right holder compared to financially stronger positioned users and they transfer remunerations for use to their associated right holder members. Also users such as cultural heritage institutions benefit from this kind of system since they only have to address one organisation which can oversee all conditions of permission for their associated right holders and they may grant licenses on their behalf. Collective rights management organisations also bring relief for some types of works held by cultural heritage institutions such as films or multimedia works which can contain multiple rights (and right holders) and may require multiple permissions for their use.[54]

3.1.1.Transparency, a trust issue?

Collective rights management organisations are also the subject of negative criticism. They are often reproached for lack of transparency in their functioning towards the right holders they represent. Users may also be somewhat suspicious of CRMOs since they may not immediately understand where the royalties they pay for certain uses, will

---

[48] In a fiduciary relationship, someone (person or organisation) acts for and on behalf of another person or organisation in a particular matter; crucial to this kind or relationship is trust and confidence.

[49] Authors can also only give a mandate to the CRMO for certain tasks, such as collecting the equitable remuneration that is due in the framework of legal licences.

[50] E. Werkers, R. Kerremans, T. Robrechts, J. Dumortier, Auteursrecht in de digitale samenleving, 2009, pp. 134. Available online (only in Dutch) http://www.cjsm.vlaanderen.be/e-cultuur/downloads/onderzoeksrapport_auteursrecht_in_de_digitale_samenleving.pdf

[51] For more information about the complete set of author's rights, see ATHENA *D.6.1. Overview of relevant IPR legislation in relation to the objectives of Europeana.*

[52] E. Werkers, R. Kerremans, T. Robrechts, J. Dumortier, Op. Cit., pp. 134.

[53] This is not always the case. A crucial point in enabling digital use by third partiers is that CRMOs must acquire the competence to represent the digital rights for their members as well. Not many CRMOs have already managed to do so.

[54] eIFL-IP, Handbook on copyright and related issues for libraries, 2009, pp. 31-32. Available online http://plip.eifl.net/eifl-ip/issues/handbook/handbook-complete-text/downloadFile/file/handbook2009_en.pdf?nocache=1268692483.68

end up. The functioning and communication of CRMOs should be more transparent. High administrative costs, lengthy negotiation terms, a lack of supervision as well as deficiencies in the management and the redistribution of fees are the most common complaints. The monopoly position of certain CRMOs could also be questioned, but national and European economic competition regulation can step in where a situation seems to become 'unhealthy'[55] (and before a shortage or overload of possible representing organisations come into being). Efficient and transparent functioning of CRMOs is necessary to guarantee a successful border crossing trade of cultural goods in and outside the European market.[56]

However, CRMOs are not just exploiters of cultural content. The Belgian and French CRMOs SABAM[57] and SACEM[58] for example also put a lot of effort into promoting the works of their associated authors. They provide promotional material on professional cultural fairs; they provide financial support for the realisation of larger projects; they provide grants to support young authors in the making of new work and so on.

3.1.2. Different types of licenses, uses and user groups

Collective rights management organisations have different ways of granting licenses, based on the intended use of the copyrighted material, or the sector/organisation that applies for a license. Licenses for a specific array of organisations, such as museums, archives and other cultural heritage institutions, can usually be negotiated in terms of tariffs for use.**[59]** It is logical that a publisher who wants to use an image in a commercial publication, should face higher license fee tariffs than a non-profit public sector body (museum, library, archive, ...).

The organisation Electronic Information for Libraries (eIFL) indicates two different types of licenses which may be granted by CRMOs:**[60]**

- An individual licence: regulates the specific uses of a specific work by an individual. This kind of license is fit for one-off situations. Example: a library wants to digitise an article from a print journal for an online course reading list.
- A 'blanket' licence: regulates the use of works by all the right owners in a certain field. Example: a broadcasting company wants to use a certain genre of music for a specified period e.g. rock 'n' roll for a 1960's music documentary.

When a legal licence (or statutory licence) is granted by a public body, the CRMO can also play a role. A statutory license regulates the copying of a specific work and legally the right holder is entitled to a payment. A CRMO can collect the equitable remuneration that is due when such legal licences are used.**[61]**

As with the tariffs, the different types of licensing show that CRMOs do not operate by a 'one fits all' credo. If a cultural heritage organisation wishes to work with a collective rights management organisation it will find that in many cases it will be provided with a specific set of tariffs[62] and contractual statements that will be in line with the (often) non-commercial use and public interest aimed for.

---

55 It should be noted here that it is the task of the right holder him or herself to appeal to a court on matters of economic competition regulation.

56 E. Werkers, R. Kerremans, T. Robrechts, J. Dumortier, Auteursrecht in de digitale samenleving, 2009, pp. 135-137. Available online (only in Dutch) http://www.cjsm.vlaanderen.be/e-cultuur/downloads/onderzoeksrapport_auteursrecht_in_de_digitale_samenleving.pdf

57 For more information on SABAM, see: http://www.sabam.be/nl/getpage.php?i=160

58 For more information on SACEM, see: http://www.sacem.fr/cms/home/

59 eIFL-IP, Handbook on copyright and related issues for libraries, 2009, p. 31. Available online http://plip.eifl.net/eifl-ip/issues/handbook/handbook-complete-text/downloadFile/file/handbook2009_en.pdf?nocache=1268692483.68

60 IBIDEM

61 IBIDEM

62 For example, the tariffs of OLA (see paragraph 3.1.3. for more information) distinguish clearly between profit and non-profit uses. They also explicitly mention use of content by museums:

Web content published by for-profit organisations (e.g. content publishers including press and magazines), as well as any website producing incomes especially but not solely through pay-access pages or pay per view: for an amount of works that is between 101 and 200 -> €438/month.

3.1.3. Territoriality versus online exploitation

The increasingly cross-border exploitation of author's rights and the digital transmission of cultural artefacts over the internet (online services, on-demand services, etc.) are no longer in line with the traditional way of territorial management of rights by collective rights management organisations, whereby only licenses for right holders from the specific country of origin of the CRMO are granted. When a European cultural heritage organisation wants to disclose cultural artefacts on an internet website, this service will be aimed at at least 27 European member states. This implies that licenses will have to be concluded in accordance with 27 national copyright legislations (i.e., in every country, a license would have to be granted by a local rights management organisation).[63] However, one also has to keep in mind that the internet and the dissemination of cultural material over the internet does not stop at national or even European borders. If a license for use of content in an online internet environment has to be obtained, this should therefore cover the use of it in every country around the world.[64]

One can see that the system of territoriality can slowly become unbearable. A 2006 study by the Dutch Institute for Information Law[65], conducted for the European Commission, indicated that this was one of the major obstacles of copyright in a cross-border digital information society. Several networks of copyright associations became aware of this problem and started joint efforts that allowed multi-territorial licenses to be agreed upon, granting certain rights for online services. Every copyright association can still, by means of reciprocity agreements, offer the repertoire of others as they used to do in the past but nowadays they may also grant licenses for the territory of other CRMOs. The supervision of this action happens in one member state, whereby one can take into account the tariffs of the different countries of destination in order to formulate an appropriate fee to be paid.[66]

An initiative in this field of granting licenses also on behalf of other collective licensing organisations is 'OnLineArt'[67]. The organisation describes itself as a one-stop-shop that offers worldwide licenses on works of more than 30.000 authors for the specific purpose of use in an online environment.
The organisation is authorised to grant global licenses for the online use of, for example, images of artworks. So if you would, for example, like to start with a large-scale digitisation project that would involve multiple museum collections, you could just talk to the CRMO in your specific country to create an arrangement within the OnLineArt-structure. This CRMO will then contact the other rights management organisations and will clear all permissions that you will need in one go (instead of you having to contact all CRMOs in the different countries involved in your project).

From their website; *"Rights involved in uses on web sites are regularly the right to scan, digitise and store a reproduction of a work, the right of communication to the public and the right of making available. Besides, moral*

- *Cultural and educational internet contents*

This tariff concerns non-profit or cultural or educational institutions publishing cultural and or educational contents.

Cultural uses means all cultural contents published without commercial or for-profit aims by non-profit- cultural organisations (e.g. museums) in relation to the exhibition or representation of works to the public for cultural purposes. For an amount of works that is between 101 and 200 -> €175/month.

- *Cultural Archives*

This tariff is applied for non-profit archives of non profit- institutions. The works concerned are the works of its own collection as well as the art works of any other touring exhibitions scheduled by the institution and whose images are archived and permanently posted on the site. Works should be displayed on the website in a uniform manner (database). For an amount of works that is between 101 and 200 -> €88/month.

Source: https://www.globalcube.net/clients/onlineart/content/medias/download/OLAInternetTariff2010.pdf

63 E. Werkers, R. Kerremans, T. Robrechts, J. Dumortier, Auteursrecht in de digitale samenleving, 2009, pp. 137-138. Available online (only in Dutch) http://www.cjsm.vlaanderen.be/e-cultuur/downloads/onderzoeksrapport_auteursrecht_in_de_digitale_samenleving.pdf and provided that they are able to issue licenses for digital uses.

64 If the website is not aimed at other countries but still accessible from these countries, one could argue that a licence expanding to these other countries is not necessary. This is however a complex issue.

65 P.B. Hugenholtz e.a., The recasting of copyright and related rights in the knowledge economy, Institute for Information Law (IViR), University of Amsterdam, 2006, 305 p. For more information about the iVIR, see http://www.ivir.nl/index-english.html

66 E. Werkers, R. Kerremans, T. Robrechts, J. Dumortier, Op. Cit., pp. 138.

67 For more information on OnLineArt, see: http://www.onlineart.info/

rights of authors might be affected. In any case, it is OnLineArt's business to provide you with a rights package tailored for your project." [68] Current members of OnLineArt are the USA (ARS), Australia (VISCOPY), France (ADAGP), Germany (BildKunst), Spain (VEGAP), Switzerland (ProLitteris), Italy (SIAE), Sweden (BUS), Norway (BONO), Denmark (Copy-DAN), Belgium (SABAM), United Kingdom (DACS) and The Netherlands (Pictoright). The presence of the USA and Australia in such an organisation illustrates the fact that it is not possible to set up such a cooperative body just for the territory of the European Union. In the internet world, this is just not workable.

3.2. Voluntary collective licensing

Voluntary collective licensing implies that a right holder can decide whether or not he or she authorises a collective management organisation to represent and exercise his or her rights. This means that a right holder can 'opt in' to the system, but it is not obliged to do so. Since it is very likely that not every right holder in a country will opt in on such a system, the catalogue of copyrighted works which a collective rights management organisation is entitled to manage and grant licenses for, will most likely not cover the entire world repertoire. In cases where these CRMOs grant a blanket license, the user who obtains the license can not be guaranteed that a right holder whose repertoire is not represented by this CRMO will not come forward to claim his or her right and ask for a compensation (additional to the blanket license, for which a fee has already been paid to the CRMO).[69] In the IVIR-study[70], an example of this problem is illustrated by the functioning of the French Institut National de l'Audiovisuel:

> *"The French Institut National de l'Audiovisuel (INA) made a deal with five French collective rights management organisations[71], authorising the INA to use the collective management societies' audiovisual and sound catalogue, to the extent that it is available in its archive, for any mode of exploitation (including internet and mobile telephony). Although this agreement greatly facilitates and simplifies the exploitation of INA's archives, it does not cover the repertoire of right holders who are not members of any of the contracting societies. Consequently, the obstacle remains that INA still needs to identify and locate these, perhaps unknown, right holders to clear the rights of the works not covered by the agreement."* [72]

3.2.1. The system of indemnity

Just as we have seen with orphan works, undertaking a search for a right holder or even starting a negotiation with him or her can be very time consuming. Collective rights management organisations try to tackle this problem by granting a blanket licence that also includes an indemnity for the use of works on which the rights are not represented by the specific CRMO. This kind of licensing mostly happens in the cases where a CRMO represents a significant amount of right holders in a certain field (thus holding a considerable repertoire, whereby one may likely assume that the specific right holder one is looking for will be represented). With this kind of licensing, one has to bear in mind that an indemnity does not always provide for the necessary legal safeguards for users.[73]

An example of the use of indemnity clauses is the Dutch Stichting Foto Anoniem[74]. In exchange for the payment of a fee, this organisation grants an indemnity to the user of a photograph of which the right holder is unknown or untraceable. If the right holder of the photograph that has been used contacts the user, e.g. a cultural heritage organisation which has used the photograph to illustrate its website, he or she may contact Foto Anoniem and they will

---

[68] http://www.onlineart.info/

[69] P.B. Hugenholtz e.a., The recasting of copyright and related rights in the knowledge economy, Institute for Information Law (IViR), University of Amsterdam, 2006, p. 182.

[70] P.B. Hugenholtz e.a., The recasting of copyright and related rights in the knowledge economy, Institute for Information Law (IViR), University of Amsterdam, 2006, 305 p. For more information about the iVIR, see http://www.ivir.nl/index-english.html

[71] These were SACEM, SACD, SCAM, SDRM and SESAM.

[72] P.B. Hugenholtz e.a., Op. Cit., p. 182.

[73] P.B. Hugenholtz e.a., The recasting of copyright and related rights in the knowledge economy, Institute for Information Law (IViR), University of Amsterdam, 2006, p. 182.

[74] For more information about Stichting Foto Anoniem, see: http://www.fotoanoniem.nl/

provide him with a correct remuneration for the use. In case the right holder demands a higher remuneration, this surplus will have to be paid for by the user.[75]

The indemnity clause however is in some cases not beneficiary for the user. As a user one has to pay for this added indemnity, even if the use one has envisaged might not ever bother the right holder and he or she might not ever ask for a compensation, and there are risks that indemnity is paid for the use of a work that is actually in the public domain. In case the indemnity is being paid for but no specific claims arise, users might ask where there money went (see also paragraph 3.1.1. on transparency).

3.2.2. A solution for orphan works?

A system of voluntary collective licensing, whereby a right holder can choose to 'opt-in' to the system, does by definition not provide a solid framework for the licensing of orphan works. In this voluntary system, CRMOs will likely not represent every existing author, and some cultural sub sectors may not be able to rely on a CRMO at all. If the right holder you are looking for did not explicitly grant a CRMO the authorisation to act on his or her behalf, a license on the work you envisage may not be granted by them.[76]

As we will see (paragraph 3.4.), the system of extended collective licensing (which is more of an 'opt-out' mechanism) is more suited to tackling the licensing of orphan works.

3.3. Country specific regimes for orphan works

In some countries, licenses for the use of copyrighted works can be granted by a public (state) body. The country specific regimes that will be discussed in this chapter illustrate the way in which this can happen, and what the conditions are in order to receive a license to use the work you have in mind. This does not mean that in these countries CRMOs are not active; the state takes over in the case of unknown and/or unlocatable right holders). Depending on the envisaged use or the conditions set by law, one system may be preferable to another.

3.3.1. Canada

> *"Exceptions to the Copyright Act just don't work. They're not flexible, and in an environment that's evolving as rapidly as the digital realm is, collective licensing is the most responsive solution to meet people's needs, now and in the future."* – Roanie Levy[77]

In Canada, the Copyright Board[78] may grant non-exclusive licences for the use of published works in cases where the right holder cannot be located. This Copyright Board is a public agency body, therefore this system is also known as 'compulsory licensing'.

In a compulsory license, a government forces the holder of a copyright or other exclusive right to grant certain uses. Usually the right holder receives royalties in return, either in an amount determined by law or determined through some form of arbitration.[79] The Canadian Copyright Board is a body with an economic background and is part of the Canadian Ministry of Industry.[80]

The granting of the licenses is based on Art. 77 of the law on authors' rights:[81]

---

[75] M.H. Elferink, A. Ringnalda, Digitale ontsluiting van historische archieven en verweesde werken, 2008, p. 21.

[76] P.B. Hugenholtz e.a., Op. Cit., pp. 182-183.

[77] R. Levy, Director of Legal Services and Government Relations for 'Access Copyright' (Canada), in: News release from Access Copyright, 12/05/2004. Available online http://www.accesscopyright.ca/resources.asp?a=147

[78] More information on the Canadian copyright Board can be found on http://www.cb-cda.gc.ca/home-accueil-e.html

[79] eIFL-IP, Handbook on copyright and related issues for libraries, 2009, p. 27. Available online http://plip.eifl.net/eifl-ip/issues/handbook/handbook-complete-text/downloadFile/file/handbook2009_en.pdf?nocache=1268692483.68

[80] See http://www.cb-cda.gc.ca/unlocatable/licences-f.html

[81] See http://www.cb-cda.gc.ca/unlocatable-introuvables/brochure2-e.html

> *Art. 77 (1) Where, on application to the Board by a person who wishes to obtain a licence to use (a) a published work, (b) a fixation of a performer's performance, (c) a published sound recording, or (d) a fixation of a communication signal; in which copyright subsists, the Board is satisfied that the applicant has made reasonable efforts to locate the owner of the copyright and that the owner cannot be located, the Board may issue to the applicant a licence to do an act mentioned in section 3, 15, 18 or 21*, as the case may be.*
> *(2) A licence issued under subsection (1) is non-exclusive and is subject to such terms and conditions as the Board may establish.*
> *(3) The owner of a copyright may, not later than five years after the expiration of a licence issued pursuant to subsection (1) in respect of the copyright, collect the royalties fixed in the licence or, in default of their payment, commence an action to recover them in a court of competent jurisdiction.*

The Canadian provision is aimed at published works, registrations of performances, published sound recordings or communication signals such as broadcasting. It does not mention any restriction regarding the scope of the reproduction (on the restriction of use within Canada, see below), the carrier of the reproduction or the intended purpose as seen by the interested party (user).
In order to receive a license, the requester must indicate that he or she tried to trace the right holder and thereby describe all efforts he or she undertook in this search. If the Canadian Copyright Board then decides that these efforts qualify as 'reasonable efforts' in the search for the rights holder, it will construct a license based on the envisaged terms of use and an appropriate fee. As we have seen with regards to the modus operandi of CRMOs, the amount of the due fee will likely also be more modest if the requester is a cultural heritage organisation. In case the right holder does not surface to collect this fee within five years, the money will go to the appropriate collecting society.[82]

The 'reasonable effort' as described above, should be documented in order to prove it to the Board.
The requester is advised to contact different collective rights management organisations as well as publishers; to consult the catalogues of national libraries, universities and museums; to check the registration systems of copyright associations; to investigate the registers of inheritances/estates or to simply undertake a search on the internet.

There are some characteristics to this system of licensing which makes it less user-friendly than it would seem. The license is non-exclusive but is limited to the Canadian territory; the Copyright Board does not have the authority to grant licenses outside its own territory. For use of e.g. cultural material on the internet, such a license is useless since it only covers use within Canada and does not allow for global use aimed outside of Canada. The license can also not be granted for all types of work; it is only aimed at already published works. Lastly, the undertaking of this 'reasonable effort' in locating the right holder can be an expensive and time-consuming process in order to come up with a body of evidence.

The Canadian system has been operating since 1989, but since that time only a limited number of licenses have been granted; only 242 over a period of 20 years (until October 2009).[83] With an average of 12 licenses per year, one could wonder if the practical implementation of this system is that successful. It seems that also only few Canadian libraries, archives or museums were granted such a license, thus the usability for the cultural heritage sector is still very low.[84]

In addition, the Canadian system only deals with right holders who are known (thus identified), but who cannot be located. This model does not therefore provide a workable solution to the entire orphan works problem, since their right holders are either unknown and/or untraceable/unlocatable.

3.3.2. Luxemburg

A similar system to the one used in Canada can be found in Luxemburg. According to Art. 91 of the law of 18 April 2001 on authors' rights, neighbouring rights and databases, as amended by the law of 18 April 2004[85], a user in

---

[82] eIFL-IP, Op. Cit,, p. 27.

[83] See http://www.cb-cda.gc.ca/unlocatable-introuvables/licences-e.html

[84] A. Vetulani, The problem of orphan works in the EU – An overview of legislative solutions and main actions in this field, 2008, p. 10. Available online http://ec.europa.eu/information_society/activities/digital_libraries/doc/report_orphan_stagiaire_2/report_orphan_vetulani%20%28corrected%20version%29%20%282%29.pdf

[85] Available online http://www.eco.public.lu/documentation/legislation/lois/2004/04/Loi_modifiee_du_18_avril_2001_.pdf

Luxemburg may request the district court to allow him or her to reproduce a work, if he or she did not succeed in locating the right holder, despite the efforts undertaken (see Canadian 'reasonable effort').

According to this provision, the user should also deliver proof of the fact that the author or performing artist is deceased. The court then determines a preliminary amount of remuneration for the rights that has to be established before every use. The user has to pay this amount to a consignation fund. The verdict is made public by the publication in a national newspaper on the initiative and on account of the user. In case the right holder appears afterwards, the user will be summoned to appear in court. The Luxemburg court will then entitle the right holder to claim the determined amount of remuneration for the use of his or her work directly (from this consignation fund). The legal provision in Luxemburg is aimed at works that have already been made accessible to the public in a legitimate way and does not imply any restriction on the envisaged use by the user, the scope of the act of reproduction or the carrier onto which the work will be reproduced.

Some other regimes exist where an authorised public body may grant licenses for the use of works in cases where the right holder can not be found. Such regimes exist in Japan, Fiji, Southern Korea, India and the UK (see paragraph 3.3.3.). The particular rules vary according to application and scope and are based on a case-by-case analysis of the situation. In the UK for example the authority to grant a license is restricted to the creation of a copy of a recorded performance.[86]

3.3.3. The United Kingdom

Nick Poole (Collections Trust's Chief Executive) gives an overview of the UK's copyright strategy regarding digital cultural heritage (and the problem of orphan works) in his presentation on the occasion of a meeting of the European Member States Expert Group (MSEG) of September 2009.[87]

In the United Kingdom, a country-specific regime for the solving of specific copyright issues such as orphan works is not yet in place. Based on the existence of other systems, the UK cultural heritage field suggested solutions to change the current copyright legislation in the UK.

The challenges that cultural heritage institutions are facing at the moment are, amongst others, that there is relatively little legislative weight behind the concept of a 'diligent search', that there is no standard definition of an orphan work and that any proposals to change legal policy on orphan works within the European Union and in any member state would need the support of the European Commission. [88] The 'Gowers Review Report of Intellectual Property'[89] of December 2006 recommended that the UK Patent Office should maintain a voluntary register of copyrighted works (so as to be able to identify and locate right holders) and that the UK government should strive within the EU to find legal provisions concerning orphaned works. [90]

In the UK IPO Consultation[91] of early 2009, three options were investigated. There could be a new exception to copyright; an extension to current UK rules governing unclaimed or ownerless property could be installed and the last

[86] A. Vetulani, Op. Cit., p. 10.

[87] N. Poole, Presentation during a meeting of the European Member States Expert Group, 30/09/2009. Available online 2009 http://ec.europa.eu/information_society/activities/digital_libraries/doc/mseg/meetings/5th/presentations/digital_britain_np3009.pdf

[88] N. Poole, Presentation during a meeting of the European Member States Expert Group, 30/09/2009. Available online 2009 http://ec.europa.eu/information_society/activities/digital_libraries/doc/mseg/meetings/5th/presentations/digital_britain_np3009.pdf

[89] The Gowers Review is an independent 2006 study to prepare a revision of the legislation regarding intellectual property in the United Kingdom. It is available online http://www.mileproject.eu/asset_arena/document/TY/GOWERS_REVIEW_OF_INTELLECTUAL_PROPERTY.PDF

[90] eIFL-IP, Handbook on copyright and related issues for libraries, 2009, p. 27. Available online http://plip.eifl.net/eifl-ip/issues/handbook/handbook-complete-text/downloadFile/file/handbook2009_en.pdf?nocache=1268692483.68

[91] In 2008, a broad consultation was launched in the UK by the Intellectual Property Office on the future direction of copyright. More information can be found at http://www.ipo.gov.uk/pro-types/pro-copy/c-policy/c-policy-consultation.htm

one was the adoption of the US model of limited liability but this was deemed as legally unsatisfactory (see paragraph 3.3.4. for the American model).[92]

The idea of formulating a new exception to the UK copyright law, on the basis of which the re-use of an orphan work could be allowed under certain conditions, seems to be a popular option. This solution was also advocated by the British Screen Advisory Council (BSAC) in a paper[93] that was written as a response to the Gowers Review. The BSAC proposition suggests that in case a person cannot find the right holder of a work after undertaking a diligent search, he or she may use the work on the basis of a suggested new exception to the author's right. The judging of the search and whether it was done at best endeavours should be decided case by case. The proposition includes the obligation to compensate the right holder in case he or she appears at a later date; this last part is quite similar to the Luxemburg model.[94]

In order for this exception to be applicable, the work, when used, should be marked as being used under the conditions that are set in the exception. This way, if a right holder sees this work being used and recognizes the conditions of use (used under the exception), he or she may ask for a reasonable compensation for this use. The amount of this remuneration should be negotiated between the parties. If no accordance can be reached, the UK Copyright Tribunal will intervene and determine the due amount of remuneration in order to have to pay a remuneration that is not in proportion with the envisaged use of the work.

This seems to be a workable approach to the orphan works problem, but it is not that simple to implement a new exception into existing copyright law. Nick Poole acknowledges that it is highly unlikely that anything will happen on this terrain before 2011.[95] The Art. 5 of the EU Copyright Directive indicates a limited list of exceptions; propositions that do not appear in this list cannot be implemented into national legislation. An additional problem is the Berne three-step-test[96], which states that exceptions may only be applied in certain specific cases; provided that it does not conflict with a normal exploitation of the work and that it does not unreasonably prejudice the legitimate interests of the right holder. It is doubtful whether the UK exception proposal would pass this test. It would after all not be exclusively restricted to specific cases, and according to Van Gompel there are insufficient guarantees that the legitimate interests of the right holder will not be damaged unreasonably.[97]

3.3.4. The United States of America

In January 2006, the US Copyright Office issued a 'Report on orphan works' which included a proposition to introduce a 'limitation-on-remedy rule'. The limitation-on-remedy rule means that there is a limitation of liability for those who use an orphan work, after an unsuccessful but reasonable search for the right holder has been undertaken. This solution does not require issuing any licence.
Contrary to the Canadian model, the American solution would apply to all kinds of orphan works, even unpublished ones, without any terms and conditions for the use of the actual orphan works.

According to this model a user is required to prove that he or she has performed a reasonably diligent search in order to provide attribution to the author or right holder of the work. No definition of a 'reasonable diligent search' is provided, but similarly to the Canadian model the user is asked to review information maintained by the Register of Copyright

---

92 N. Poole, Op. Cit.

93 British Screen Advisory Council, Copyright and orphan works, 2006. Available online www.bsac.uk.com/reports/orphanworkspaper.pdf

94 M.H. Elferink, A. Ringnalda, Digitale ontsluiting van historische archieven en verweesde werken, 2008, pp. 45-48.

95 N. Poole, Op. Cit.

96 By means of the conditions set by the international three-step-test, a judge can make a discriminate judgement regarding the balance of interests between the right holders on the one hand, and the users (such as heritage institutions wanting to disclose their material) on the other. The three-step-test states that copyright exceptions are only allowed in certain exceptional cases, provided that such reproduction does not conflict with a normal exploitation of the work, and provided that it does not unreasonably harm the legitimate interests of the author. The conditions of the test are cumulative. More information about the three-step-test can be found in the ATHENA *D.6.1. Overview of relevant IPR legislation in relation to the objectives of Europeana.*

97 S. Van Gompel, Audiovisual archives and the inability to clear rights in orphan works, in: Iris plus, 2007, afl. 4, p. 1-8.

and use expert assistance and the technology that is available to him or her.[98] It would still be up to a court to decide if a search was 'reasonably diligent' in the given circumstances.

In the American system, the user would have to remunerate the right holder if he or she appears, but not in advance as is the case in the indemnity system. In the case of non-commercial use (for a charitable, religious, scholarly or educational purpose), no monetary relief would be required.[99] For cultural heritage institutions in particular this is a huge benefit. The legal proposition also provides a settlement for the future use of the work. If an orphaned work is incorporated in a derivative work (e.g. feature film or documentary), the right holder can not ask the court to oblige the user to stop the exploitation of the derivative work, on condition that the user does pay a reasonable remuneration to the right holder and provides for a proper attribution of the right holder. The further use of the orphan work can however be stopped in case the orphan work is only republished, or placed online (e.g. on a museum's website) without any source references. However, according to the legal proposition, the courts do also have to take into account the interests of the bona fide user who could, through a possible notification to cease (actions), be too hard hit by legal consequences.

After some minor adaptations it was submitted as a legal proposition - the 'Orphan Works Act of 2006' – in the American House of Representatives.[100] The US Copyright Office has stated that *"the public interest may be harmed when works cannot be made available to the public due to the uncertainty over its copyright ownership and status, even when there is no longer any living person or legal entity claiming ownership of the copyright or the owner no longer has any objection to such uses."* It goes on to acknowledge that *"the uncertainty surrounding ownership of such works might needlessly discourage subsequent creators and users from incorporating such works in new creative efforts or making such works available to the public."* [101]

Such a system provides a global solution for the problem of orphan works. The difference with the Canadian system is that the user will only have to pay compensation when a right holder appears at a later stage (and not beforehand). Such a system will not be applauded by right holders since they will fear that users will call upon the statute of orphan works too rapidly (too easily, without undertaking a proper search) and that they will speculate about the fact that a right holder will not necessarily appear. Such a system can also create legal insecurity for users, especially when their search was conducted a long time ago. It could be difficult, for example, to post communicate to the court the proof that they had undertaken a diligent search.[102]

3.4. Extended collective licensing

The system of extended collective licensing is based on the collective management of rights (see paragraph 3.1.) and legally provides for the coverage of (the interests of) 'missing authors'.[103]

An extended collective licence (ECL) covers the use of works of right holders who are not represented by the collective rights management organisation. This provides users with security to legally copy materials without the threat of individual claims from right holders who are not members of the CRMO that granted them a license. The system of

---

98 eIFL-IP, Handbook on copyright and related issues for libraries, 2009, p. 27. Available online http://plip.eifl.net/eifl-ip/issues/handbook/handbook-complete-text/downloadFile/file/handbook2009_en.pdf?nocache=1268692483.68

99 A. Vetulani, The problem of orphan works in the EU – An overview of legislative solutions and main actions in this field, 2008, p. 12. Available online http://ec.europa.eu/information_society/activities/digital_libraries/doc/report_orphan_stagiaire_2/report_orphan_vetulani%20%28corrected%20version%29%20%282%29.pdf

100 Orphan Works Act of 2006, H.R. 5439, introduced in the House of Representatives, 109th Congress, 2nd session, 22/05/2006. Available online http://thomas.loc.gov/cgi-bin/query/z?c109:H.R.5439:.

101 eIFL-IP, Op. Cit., p. 14.

102 It should be noted here that this statement is not just USA-case specific, but is the case for every copyright system in which a diligent search is requested in order to receive a permission for use.

103 UK Intellectual Property Office, The way ahead - A Strategy for Copyright in the Digital Age, 2009, p. 38. Available online http://www.ipo.gov.uk/c-strategy-digitalage.pdf. See paragraph 3.2. Voluntary collective licensing; the INA-example could be facilitated by the use of an extended collective license instead of their current 'opt-in' system.

ECL was originally adopted by Nordic countries in the 1960's as a means for addressing the complexity brought on by mass use and exploitation of numerous rights at the same time.**104**
In cases in which a CRMO is deemed to represent a 'critical mass' of right holders in a certain domain, it is assumed to act for all right holders in that domain. The works of all right holders in this field (whether domestic or foreign) are assumed to be part of the repertoire of the CRMO unless the right holder specifically opted out of this ECL system (by explicitly stating that he or she does not want to be represented under an extended collective license).[105] Rights holders who choose to leave the system will not be covered by the extended collective license any longer.[106] However extended collective licensing can also be beneficiary for right holders: it guarantees remuneration for right holders since their works are assumed to be in the repertoire of the relevant collecting society.[107]

An example of use can be found in broadcasting. In the Scandinavian countries (Denmark, Finland, Iceland, Norway and Sweden)[108] an ECL is applied for the use of musical works in radio- and television broadcast emissions. According to this system, a broadcast organisation receives a license for the broadcasting of all musical works from a CRMO that represents a significant part of musical composers and text writers. The license is legally extended also to those musical composers and text writers who are not represented by the specific CRMO which grants the license for use.

Extended collective licensing can reduce the cost of obtaining a licence; instead of investing time and money on several individual licences, a requester may, under an ECL, obtain one licence for a broad repertoire of works. Extended collective licensing has the potential to be a mechanism for the quick and efficient processing of agreements. An example of this is stated in 'The way ahead: a strategy for copyright in the digital age'[109], a document by the UK Intellectual Property Office: [110]

> *"KOPINOR, an umbrella organisation for Norwegian reprographic collecting societies, recently concluded a complex agreement for making works available on the internet with Norway's National Library. The process took two months. This compares favourably to the five years taken to clear the rights for the BBC's iPlayer service."* [111]

104 eIFL-IP, Handbook on copyright and related issues for libraries, 2009, p. 31. Available online http://plip.eifl.net/eifl-ip/issues/handbook/handbook-complete-text/downloadFile/file/handbook2009_en.pdf?nocache=1268692483.68

105 UK Intellectual Property Office, The way ahead - A Strategy for Copyright in the Digital Age, 2009, p. 38. Available online http://www.ipo.gov.uk/c-strategy-digitalage.pdf

106 P.B. Hugenholtz e.a., The recasting of copyright and related rights in the knowledge economy, Institute for Information Law (IViR), University of Amsterdam, 2006, p. 183.

107 UK Intellectual Property Office, Op. Cit., p. 38. and
http://aix1.uottawa.ca/~dgervais/publications/extended_licensing.pdf

109 UK Intellectual Property Office, The way ahead - A Strategy for Copyright in the Digital Age, 2009. Available online http://www.ipo.gov.uk/c-strategy-digitalage.pdf

110 UK Intellectual Property Office, Op. Cit., p. 38.

111 IBIDEM. The Norwegian agreement only allows for access to library material by Norwegian IP-numbers (BBC's iPlayer is likewise only accessible by British IP-numbers). This once again implicates a territorial limitation and does not provide for a worldwide internet access.

4. Open and new licensing models

4.1. Introduction

> *"The notion of providing access to content in an open way is a core part of what has been labelled 'Web 2.0'. Although this term has become part of the ecosystem in which we now work, the subtleties have in many areas yet to be worked out. For many people (and in many contexts), 'Open Content = Free Content'. For organisations such as museums where exploitation of IPR is a core part of their business, this is understandably very hard to come to terms with."* – Kelly, Ellis & Gardler[112]

In their 2008 article, Brian Kelly (UKOLN), Mike Ellis (Eduserv) and Ross Gardler (JISC OSS Watch) question 'What does openness mean to the museum community?'.[113] The statement above summarizes the principal response within the museum community; first of all 'openness' is seen as a threat, only later is it seen as an opportunity.

In a fully operational Web 2.0 environment, users govern content. To allow these users to become active content providers as well as content users, openness[114] is needed. Opening up one's collections in an internet environment makes cultural heritage institutions rethink their 'authority' concept. Is it possible to find a balance between the museum as a curator with an authorised voice (as it has been in the past), and the user as a curator? Museums (but also other cultural heritage organisations) have relied heavily on the concept of scarcity in the past. It was all about limiting access to collections since this could earn them money (from physical visitors entering). When one decides to disclose (parts of) a collection of cultural heritage material through the internet, access to it becomes 'free' and museums tend to think that they will lose physical visitors at first – and fear for digital copying of their objects. As the above quoted authors state: *"Text and image content that is published on the Web is available to all; technologies that attempt to prevent or limit usage (watermarking for example) have met with limited success."* [115]

The question that should really be posed is whether limiting access in a digital environment is still something worth attaining (since users will be clever enough to 'steal' digital online content anyway if they want to), or should we increase access to our collections and encourage this (more people will have access to the material and consequently also pay an 'analog' visit to it)?[116]

4.2. Open Content Licenses: Creative Commons as an example

4.2.1. Creative Commons?

A Creative Commons license is an open content license, which means that it differs from a classic copyright license which requires financial compensation for the author. Open content licenses cover a family of licences that explicitly allow for access at no cost, copying and re-use. 'Open content' is a concept used to describe content that is licensed in such a way that users are given permissions that are normally covered by exclusive copyrights[117] - at no cost to the

1 [112] M. Ellis, R. Gardler, B. Kelly, What Does Openness Mean To The Museum Community?, 2008, s.p. Available online http://www.archimuse.com/mw2008/papers/kelly/kelly.html

[113] IBIDEM

[114] As the authors point out, the concept of 'openness' appears in many contexts. You've got open standards, open source software, open content and open services. The meaning of this 'open' in the different contexts is basically one of giving easy access to content, giving access to more and more content, let people share information and collaborate on enriching this information. Source: M. Ellis, R. Gardler, B. Kelly, Op. Cit., 2008 and L. Regebro, The benefits of openness, a modern example. 2008, s.p. Available online http://theopensociety.wordpress.com/2008/08/17/the-benefits-of-openness-a-modern-example/

[115] M. Ellis, R. Gardler, B. Kelly, Op. Cit, 2008, s.p.

[116] IBIDEM

[117] Open content offers the right to make more kinds of uses of this content than those normally permitted by copyright law. It might for example be that you may use an open-licensed image in a non-commercial publication for free (against no royalty payment), as long as you credit the author of the image.

user. The fact that they're royalty-free is a feature characteristic to this kind of license. The fewer copyright restrictions are placed on the user of a piece of content, the more open the content is.[118]

This does not mean that any author who chooses to apply an open content license to his or her work, automatically relinquishes all his or her author's rights.[119]

Some common restrictions of open content licenses are described in the Minerva IPR guide[120]:

- Attribution of the source of the content must be attached to the content, and retained in derivate works;
- No warranty is provided – the work is provided on an 'as is' basis;
- The license cannot be modified or repealed once it has been issued.[121]

Further more, some additional restriction can be present, depending on the chosen licence:

- Some licences do not allow the modification of the work;
- Some licences provide that works that are based on previous work should in turn be released under an open content license – this prevents a third party from making a "property" product on the basis of open content;
- The open content shall not be used in a commercial application;

(These lists do not imply that every open content license contains these elements, they are just exemplary).

Creative Commons (CC)[122] for example is a non-profit organisation that was founded in 2001 in the USA. The organisation offers an easy way for authors and other cultural creators to choose how they wish to make their work available. They choose the conditions of use and the standardised Creative Commons licenses are an easy way for users to identify the conditions under which a work may be used.[123]

A Creative Commons license typically contains several options from which an author may choose to apply to his or her work. These options indicate under which conditions the work may be used. They are:

- Attribution: the work may be copied, distributed, displayed and performed (including derivative works), but only if due credit is given to the author of the work;
- Non-commercial: the work may be copied, distributed, displayed and performed (including derivative works), but only for non-commercial purposes;
- No derivative works: the work may be copied, distributed, displayed and performed, but does not allow the creation of derivative works based upon it.
- Share alike: derivative works based on this work are allowed and may be distributed but only under a licence identical to the licence that governs the original work.

Through the combination of these options, six main types of licence are created:

- Attribution alone (CC-BY)
- Attribution + Noncommercial (CC-BY-NC)
- Attribution + NoDerivs (CC-BY-ND)
- Attribution + ShareAlike (CC-BY-SA)
- Attribution + Noncommercial + NoDerivs (CC-BY-NC-ND)
- Attribution + Noncommercial + ShareAlike (CC-BY-NC-SA)

---

118 See http://opencontent.org/definition/

119 eIFL-IP, Handbook on copyright and related issues for libraries, 2009, p. 43. Available online http://plip.eifl.net/eifl-ip/issues/handbook/handbook-complete-text/downloadFile/file/handbook2009_en.pdf?nocache=1268692483.68

120 MinervaEC Working Group (ed.), Minerva IPR Guide, 2008. Available online http://www.minervaeurope.org/IPR/IPR_guide.html

121 MinervaEC Working Group (ed.), Minerva IPR Guide, 2008, pp. 31-32. Available online http://www.minervaeurope.org/IPR/IPR_guide.html. A website providing general information on Open Content is at http://opencontent.org

122 For more information on Creative Commons, see http://creativecommons.org/

123 eIFL-IP, Op. Cit., 2009, p. 30.

Each licence type has three operational versions:[124]

- a 'Commons Deed' that explains in simple terms what is permitted under the licence and uses symbols that are easy to recognise;
- a 'Legal Code' aimed at lawyers which is the full text of the licence;
- a machine-readable version containing RDF/XML metadata that describes the licence, enabling CC-licensed works to be located by search engines on the web.

How cultural heritage institutions relate to the use of CC-licenses and examples of web content on which Creative Commons licenses are featured will be discussed further in this document, see paragraphs 4.3. and 4.4..

4.2.2. Creative Commons and collective rights management organisations

Creative Commons licences are translated in many languages and compatible with national copyright systems. Yet there are still some players who seem reluctant to give CC a try. Collective rights management organisations are not willing to let associated authors or right holders issue their work under a CC license, when they are already represented by a CRMO (the role and functioning of collective rights management organisations has been discussed earlier, see paragraph 3.1).[125]

On the basis of their copyright, authors have the right to decide how to exercise their rights and through whom they want to do so (e.g. CRMO). But in any case it should be possible for an author to negotiate about applying a CC license to his work, in combination with a CRMO representative. Indeed, every author can decide for him or herself which rights he or she will transfer to a CRMO (only certain rights or the entirety), making it possible to manage the remaining rights him or herself.[126] This is an opportunity for new modes of exploitation, certain genres or certain territories that can be taken out of the collective management of rights.[127]

In the Netherlands, a pilot project between the largest collective rights management organisation for music authors, the BUMA/STEMRA[128], and Creative Commons was launched in 2007. Until then authors had been unable to make available part of their repertoire for non-commercial use on the internet and at the same time have BUMA/STEMRA collect and redistribute their royalties for commercial use of those works.[129] Paul Keller, Public Project Lead of Creative Commons Netherlands, says, *"We are pleased that this pilot brings to an end the all-or-nothing scenario. This way the Creative Commons Licenses can complement the existing collective management system."* [130]

A project such as this offers possibilities for cultural heritage organisations as well, in cases in which a museum wants to make a person's work digitally available when it has been licensed under the CC-regime. Since the nature of the use

---

[124] eIFL-IP, Op. Cit., pp. 30-31 and H. Hietanen, V. Oksanen, Legal metadata, open content distribution and collecting societies, s.d., s.p. Available online http://fr.creativecommons.org/articles/finland.htm

[125] H. Hietanen, V. Oksanen, Op. Cit.,, s.d., s.p.

[126] CRMOs themselves argue against this. They state that it renders the global management of works very difficult. If authors keep some works, or parts of their rights on some works, outside of the repertoire, this will quickly become unworkable according.

[127] R. Kerremans, T. Robrechts, Juridische denkpistes voor de opslag en ontsluiting van multimediale data, 2009, p. 42. Available online (only in Dutch) http://biblio.ugent.be/input/download?func=downloadFile&fileOId=764218&recordOId=764214

[128] See http://www.bumastemra.nl/en-US/OverBumaStemra/Overzicht.htm

[129] See http://www.bumastemra.nl/nl-NL/MuziekrechtenVastleggen/Pilot+Creative+Commons/CreativeCommonspilot.htm, http://www.creativecommons.nl/bumapilot/ and http://www.bumastemra.nl/en-US/Pers/Persberichten/pilot+CC.htm. From the press release: *"This pilot will give members of Buma/Stemra the opportunity to publish their music works under a non-commercial Creative Commons license. Composers and lyricists, who to date have only been able to publish their work under a Creative Commons license, may now opt to join Buma/Stemra and have this organisation collect their royalties for commercial use of their work. With this pilot Buma/Stemra and Creative Commons Netherlands seek to provide Dutch musicians with more opportunities to promote their own repertoire."*

[130] See http://www.bumastemra.nl/en-US/Pers/Persberichten/pilot+CC.htm

of the work will most likely be non-commercial[131], the museum could use it without paying any remuneration. It should be noted that this will mostly only apply to recent works which have been given a CC-license by their author, and the amount of such works will be rather limited. In case a license is requested for commercial use of the work, the right holder may refer the institution to the CRMO who will then discuss tariffs for the license fee.

4.3. The application of open content licenses by cultural heritage institutions

It is generally accepted that the current copyright system, as opposed to open content licenses, offers little flexibility when it comes to making cultural heritage collections available online. Thanks to the use of, for example, Creative Commons, the (re)use of copyrighted works on the internet has been simplified, because it provides a standardised, well recognised way of giving others the right to re-use and remix content for free.
However, these licenses can only be applied by cultural heritage institutions themselves if they are the only right holders on the content they would want to (re-)use or exploit. However, museums and other cultural heritage institutions are not only 'users' of another's content; they also create their own cultural content. They may have taken pictures to make their website more attractive, there are exhibition catalogues which have been created by the museum, there could be conference posters, papers and presentations made by museum staff. When the cultural heritage institution holds the rights to these artefacts, it is very easy to give them a CC license[132] and make these contextual resources available online. They often provide a valuable source of additional information about the context of the collection (both historically as well as from an institutional perspective) and are in many cases forgotten about if they are not disclosed to the public.

The use of CC can benefit museums and other cultural heritage organisations in two ways:

- Instead of having to add extensive rights statements for the online content on the organisation's website[133], the CC-license is self-explanatory.
- If a user wants to use the content that has been put on one's website, he or she will just have to look at the CC-license to see what he or she is allowed to do with the content.

It should be kept in mind that CC-licenses are often difficult to implement (even if the will is there) because they require that the licensor, e.g. the museum, has the (full) copyright of the object(s).[134]

This implies that the knowledge and awareness about what rights are applicable to the collection, who the right holder is, and which exploitation rights the institution holds, are crucial for the application of open content licenses (and on a broader scale, facilitating the distribution of collections).[135]

In 2007, a survey on the use of open content licenses in the UK cultural heritage sector was conducted. This survey targeted UK cultural heritage organisations — primarily museums, libraries, galleries, archives, and those in the media community that conduct heritage activities (such as TV and radio broadcasters and film societies).[136] A similar survey was held in Belgium, one year later. The Belgian survey showed that only 20% of surveyed institutions could rely on

---

131 For instance a museum might want to use CC-licensed images to put them onto its website for illustration purposes (to make it look more attractive) or they might want to provide free online access to publications that have been made by museum staff under a CC-license.

132 However easy it may be, a cultural heritage organisation should still be aware of acting 'too straightforward', for instance when it licenses a work that is actually in the public domain. For every application/use of an open source/open content licence, one must first deterring the copyright on the object before releasing it under the licence of choice.

133 Providing every single work with a separate CC license also takes time and work. An alternative could be to provide a general statement, indicating that all content on a particular website is licensed under one type of CC license. The problem here is that in many cases such a general statement is not valid for literally every piece of content on the website (to which perhaps also third parties hold the rights).

134 T. Evens, Het gebruik van open content licenties in het culturele veld, 2008, p. 14. In cases where the museum does not hold the full copyright, they might want to contact the right holder and ask them about terms of use of the work. At the same time they can ask if he/she is willing to license his/her work under CC-conditions for use by the museum.

135 T. Evens, Op. Cit., 2008, p. 14.

136 J.S. Hatcher, Snapshot study on the use of open content licences in the UK cultural heritage sector, 2007, p. 3.

an in-house legal advisor (or legal department), whereas in the UK this was the case in 36.9% of surveyed institutions.[137] This is still less than half, leaving copyright issues in cultural heritage institutions often 'untreated' or silenced.[138]

The overall awareness of the existence and working of Creative Commons seems to be relatively good. Approximately 30% of the surveyed institutions in Belgium indicated to have considered using CC licenses for the disclosure of materials on the internet.[139]

The way Creative Commons works is largely by means of a trust relationship. Technological applications such as DRM (digital rights management) techniques often enforce the user to only use the content in a specific way. CC in contrast relies on the trust that users will use the work according to licence conditions. Therefore it is fit for individual authors who want to license their work under specific conditions, but this is sometimes perceived as less trustful by cultural heritage institutions. Museums for example value their digital images highly, since they are a source of income to them and they would rather put small thumbnails online or images that have been watermarked, instead of also licensing full-size images under Creative Commons conditions and making them available through the internet.[140] Museums are therefore reluctant to license any content under the CC system.

A final remark on the use of CC-licenses in the cultural heritage sector was made by Esther Hoorn in her 2006 study on the use of CC licenses within cultural heritage organisations[141]. She concluded that although the Creative Commons (CC) licences do not offer a solution for orphan works, cultural heritage institutions can stimulate the use of CC Licences as a strategy to prevent future orphan works (by e.g. convincing and stimulating right holders to license their works under such a license).[142]

4.4. Examples & cases of best practice

A number of cultural heritage institutions have over the past year embraced the 'open' approach to the collections they hold[143]. Not only do they make their content available on line, for example on their own website, but they strive to make it available on a scale that's as broad as possible. Co-operations are set up between large, high-trafficked websites and the cultural heritage organisation, often under a CC-related licensing basis. Some examples of how cultural heritage organisations could benefit from new online display platforms at their disposal, in combination with a free licensing of content, are presented below.

4.4.1. Wiki Loves Art

One of the most popular platforms for the inclusion of digital cultural heritage (mostly images) outside the 'regular' distribution pool (such as museum websites, national aggregator portals, educational project websites, etc.) is

---

137 IBIDEM

138 T. Evens, Het gebruik van open content licenties in het culturele veld, 2008, p. 16.

139 T. Evens, Op. Cit., p. 17.

140 M. Ellis, R. Gardler, B. Kelly, What Does Openness Mean To The Museum Community?, 2008, s.p. Available online http://www.archimuse.com/mw2008/papers/kelly/kelly.html

141 Esther Hoorn, Creative Commons Licences for cultural heritage institutions - A Dutch perspective, 2006, 72 p. Available online http://www.ivir.nl/creativecommons/CC_for_cultural_heritage_institutions.pdf

142 Esther Hoorn, Creative Commons Licences for cultural heritage institutions - A Dutch perspective, 2006, p. 12-13. Available online http://www.ivir.nl/creativecommons/CC_for_cultural_heritage_institutions.pdf, and A. Vetulani, The problem of orphan works in the EU – An overview of legislative solutions and main actions in this field, 2008, p. 13. Available online http://ec.europa.eu/information_society/activities/digital_libraries/doc/report_orphan_stagiaire_2/report_orphan_vetulani%20%28corrected%20version%29%20%282%29.pdf

143 It should be noted that the extent to which 'openness' can be put into practice mainly depends on the rights status of the objects that form the collection of a cultural heritage organisation.

Wikipedia. This open content-licensed encyclopedia was started in 2001 and now contains over 15.300.000 articles in more than 270 languages.[144]
The entire content of the encyclopedia is written by an active community of volunteers, using a wiki content management system. Wikipedia itself has inspired some projects that are linked to the actual encyclopedia, such as Wikimedia Commons[145]. This project hosts a media repository for freely licensed works: CC-BY-SA, CC-BY, GFDL and public domain files are accepted. It contains mostly images, but also sound and video clips are accepted. The link between Wikipedia and Wikimedia Commons is that files at Wikimedia Commons can be directly integrated into Wikipedia articles for illustration purposes.[146]

The fact that Wikipedia is such a highly trafficked website makes it attractive for cultural heritage institutions to be part of that success. Several projects have been set up between Wikipedia and/or Wikimedia and the cultural heritage field. One of these projects is 'Wiki Loves Art'[147]. This project started off in the United States but has been picked up in other countries as well; in 2009, Wikimedia the Netherlands (in cooperation with some other partners such as CC NL and Erfgoed Nederland) organised a Dutch version of the project[148]. Just recently a similar initiative called 'Britain Loves Wikipedia' was launched in Britain[149].

> *"We need to win back the right to photograph our human heritage in museums and galleries, and we need to beat back the snitch-cams rent-a-cops use to make our cameras stay in our pockets."* – Cory Doctorow[150]

The idea of Wiki Loves Art was that museums open their doors to photographers during a one month period. Visitors of all kinds could take pictures of objects displayed in the museum. Every participating museum could determine a list of objects of which pictures could be taken; sometimes there were no restrictions and the entire collection could become part of the project, other times due to copyright restrictions only a set of objects could be photographed. Restrictions mostly had consequences for contemporary works of art on which the term of protection had not yet ended. These pictures taken ended up on Wikimedia Commons to enrich articles with them, but were first uploaded to Flickr, licensed as CC-BY-SA. A photography contest was also linked to the project; the 'best' pictures were awarded with prizes.

144 See http://meta.wikimedia.org/wiki/List_of_Wikipedias#Grand_Total

145 See http://commons.wikimedia.org

146 M. Schindler, presentation at the 5th COMMUNIA Workshop 'Accessing, Using, Reusing Public Sector Content and Data', 26-27/03/2009.

147 See http://en.wikipedia.org/wiki/Wikipedia:Wikipedia_Loves_Art

148 See http://www.wikilovesart.nl/

149 See http://www.britainloveswikipedia.org/wiki/Main_Page

150 C. Doctorow, Content, 2008, p. 210. Available online http://craphound.com/content/

Image: by 23 dingen voor musea[151]. Taken during a Wiki Loves Art photoshoot at the Dutch ceramic museum Princessehof.

4.4.2. Bundesarchiv + Wikimedia Germany

Another successful example of a cooperation between a cultural heritage institution and Wikipedia/Wikimedia Commons is the release of some 100.000 images under an open content license to Wikimedia Germany by the German Federal Archive (Bundesarchiv) in December 2008.[152] This cooperation serves as an example that can be repeated with other archives.

The German Bundesarchiv[153] is a federal authority that permanently collects and keeps archive material and makes it available for scientific purposes. At the time it contributed to Wikimedia, the archive owned about 10 million images, most of them not yet digitised. In 2007 they started an online image repository was started, in which the public could look at thumbnails for free and pay for access to higher resolution images. Wikimedia Germany contacted them to ask if a cooperation would be possible and they responded positively; a contract between the Bundesarchiv and Wikimedia Germany was signed just a year later. This cooperation was based on the idea that media files created with public funding should be released to the public under an open content license.[154]

Of course nothing is really 'for free'; in return for the Bundesarchiv providing its images, the Wikimedia community is conducting a matching process between the authority files of the Bundesarchiv, the German National Library and Wikipedia persondata-templates. The images that are provided by the Bundesarchiv are licensed as CC-BY-SA and a minority as CC-BY, to ensure that media files remain freely available to the public. The release of files with slightly reduced resolution (800px on the larger side) can be an acceptable temporary solution to preserve traditional sources of

151 See http://commons.wikimedia.org/wiki/File:WLANL_-_23dingenvoormusea_-_wiki_loves_art_@_Princessehof.jpg

152 See http://commons.wikimedia.org/wiki/Commons:Bundesarchiv

153 See http://www.bundesarchiv.de

154 M. Schindler, presentation at the 5th COMMUNIA Workshop 'Accessing, Using, Reusing Public Sector Content and Data', 26-27/03/2009.

income for archives. Thanks to the integration of images into the Wikipedia articles, the number of visits to the Bundesarchiv website has never been greater.[155]

Image: screenshot of a Wikipedia article on the life of Helmut Kohl[156], containing an image of Kohl by the German Bundesarchiv.

4.4.3. GLAM-WIKI Recommendations

In August 2009 a conference[157] was held in Australia on the correlation between the Wikimedia Foundation and 'GLAMs'; galleries, libraries, archives and museums. This conference resulted in a set of recommendations, in order for every party to benefit optimally from the cooperation.

170 representatives of the Australian and New Zealand cultural sector were also present at the conference, in various professional capacities as well as Wikimedians from all Australian states, Wikimedia Germany and the Wikimedia Foundation in San Francisco. Also represented were several peak body organisations, relevant government departments, arts funding organisations and politicians from all major parties.[158]

The recommendations are divided into four sections (Legal, Technological, Education and Business) and are addressed to the GLAM sector, the Wikimedia community and the government. They are not binding in any way but their purpose is to encourage sustainable collaboration between institutions in the cultural sector and the Wikimedia community - so that they may be easier to set up, maintain and be more productivel.[159]

On the 'Law' aspect of cooperation, the following suggestions were (amongst others), made to the cultural heritage institutions:[160]

- Use a 'free-culture' Creative Commons license (either CC-BY or CC-BY-SA) for content on GLAM websites which is owned/controlled by the institution e.g. fact sheets, inventory files, photos of objects, statements of object significance and educational materials.
- Pro-actively publish the copyright status of specific content in the online collection rather than blanket access statements for the whole collection. Give guidelines for users to make their own copyright assessment.

---

155 M. Schindler, presentation at the 5th COMMUNIA Workshop 'Accessing, Using, Reusing Public Sector Content and Data', 26-27/03/2009.

156 See http://en.wikipedia.org/wiki/Helmut_Kohl

157 See GLAM-WIKI: Finding the common ground

158 See http://meta.wikimedia.org/wiki/GLAM-WIKI_Recommendations

159 See http://meta.wikimedia.org/wiki/GLAM-WIKI_Recommendations. Basically this is a similar way of working as the Europeana Public Domain Charter.

160 See http://meta.wikimedia.org/wiki/GLAM-WIKI_Recommendations

- Remove claim of copyright over scans/photographs of Public Domain content as per the 'originality' principle.

The following requests were (a.o.) made to Wikimedia:[161]

- Take pro-active care of the moral rights of content creators as these are not waived even with free-licensing.
- Publish donor/acquisition information as an integral part of the attribution statement.

The following requests were (a.o.) made to the Government:[162]

- Provide definitive statement on the applicability of Bridgeman v. Corel corp. principles as they apply to Australia i.e. whether 'sweat of the brow' is enough to create new copyright or whether "originality" is required as in the USA (see below).
- Extend archival copyright exceptions to allow for format/time-shifting for preservation and to allow for archival copying before deterioration/obsolescence.

A verdict in an American court case against the Bridgeman Art Library in 1999 determined that technically perfect pictures (reproductions) of two-dimensional objects that are in the public domain (e.g. a painting by Rubens or Breughel) can not be subject to copyright protection. Such a verdict states that it is prohibited to take a picture of a two-dimensional object out of the public domain by marking it as 'all rights reserved' and thus bringing it into the realm of copyright protected works. On the contrary, in the United Kingdom there exists a concept called 'sweat of the brow'. This implies that when the reproduction, the picture, is only a mere exact depiction of the original work (and therefore does not involve any creative input by the photographer), copyright may still be claimed on the picture because the person who made the reproduction invested in creating it (his or her 'labour').[163] In other European countries – and we see the same in Australia – there has not yet been a court case or verdict that explicitly favours one interpretation or the other, leaving this entire issue in a grey zone as far as copyright protection goes. [164]

4.4.4. Flickr The Commons

Flickr is a six year old online photo sharing community. Before January 2008, it primarily held 'user-generated content'; photographs and stories from individuals from all around the globe. 'The Commons'[165] is a project that was developed to add publicly-held photography collections to this online photo collection.[166] The idea was not only to give more publicity to these images by adding them to Flickr. The vast user base of the platform could add context to

---

[161] See http://meta.wikimedia.org/wiki/GLAM-WIKI_Recommendations

[162] See http://meta.wikimedia.org/wiki/GLAM-WIKI_Recommendations

[163] In the European Directive 2006/116/EG, the concept of what a photograph, eligible for copyright protection is, was harmonised. But in the text, it is additionally stated that *(16) The protection of photographs in the Member States is the subject of varying regimes. A photographic work within the meaning of the Berne Convention is to be considered original if it is the author's own intellectual creation reflecting his personality, no other criteria such as merit or purpose being taken into account. The protection of other photographs should be left to national law.*

There are arguments against the acceptance of copyright on photographs who are mere reproductions, because monopolies could be created on the reproduction and depiction of certain art works, even though they might be hundreds of years old. Such an infinite right of reproduction is according to Chavannes unnecessary and not desirable in a context of (maximum) freedom of information. This does not mean however that reproduction photographs can never be protected by copyright, but in order to enjoy copyright protection they must have some kind of extra feature (e.g. non-neutral backgrounds or special lighting, a well-thought staging of objects, an original framing …). Source: R. Chavannes, De kunst van het onzichtbaar blijven: het auteursrecht van de reproductiefotograaf, in: N. van Eijk, P.B. Hugenholtz, Dommering-bundel, 2008, pp. 40-41.

[164] For more information on this case, see http://en.wikipedia.org/wiki/Bridgeman_Art_Library_v._Corel_Corp.

[165] The Flickr the Commons website contains a rights statement section. This contains a.o. the following: *"By asserting 'no known copyright restrictions', participating institutions are sharing the benefit of their research without providing an expressed or implied warranty to others who would like to use or reproduce the photograph. If you make use of a photo from the commons, you are reminded to conduct an independent analysis of applicable law before proceeding with a particular new use."* Source: http://www.flickr.com/commons/usage

[166] G. Oates, The Commons on Flickr: A Primer. In: J. Trant and D. Bearman (eds.). *Museums and the Web 2008: Proceedings*, Toronto: Archives & Museum Informatics, 2008, s.p. Available online http://www.archimuse.com/mw2008/papers/oates/oates.html

the images by tagging and describing them, they could link images to each other and this way the contributing cultural heritage organisations could re-use this information to enrich their own databases.[167]

As George Oates points out, it is the mandate of museums and libraries around the world to increase access to their collections. An online sharing community such as Flickr is an ideal platform for opening holdings up to millions of interested users. Flickr set up a pilot project with the American Library of Congress, presenting their Prints & Photographs Catalog to a global audience. The LOC is the worlds' largest library and manages an enormous (digitised) photographic collection. However, a lot of descriptions of the photographs are missing. As part of the images of this collection are already in the public domain, the LOC hoped that by putting them online, users would want to become involved and improve the description of the photographic collections.[168]

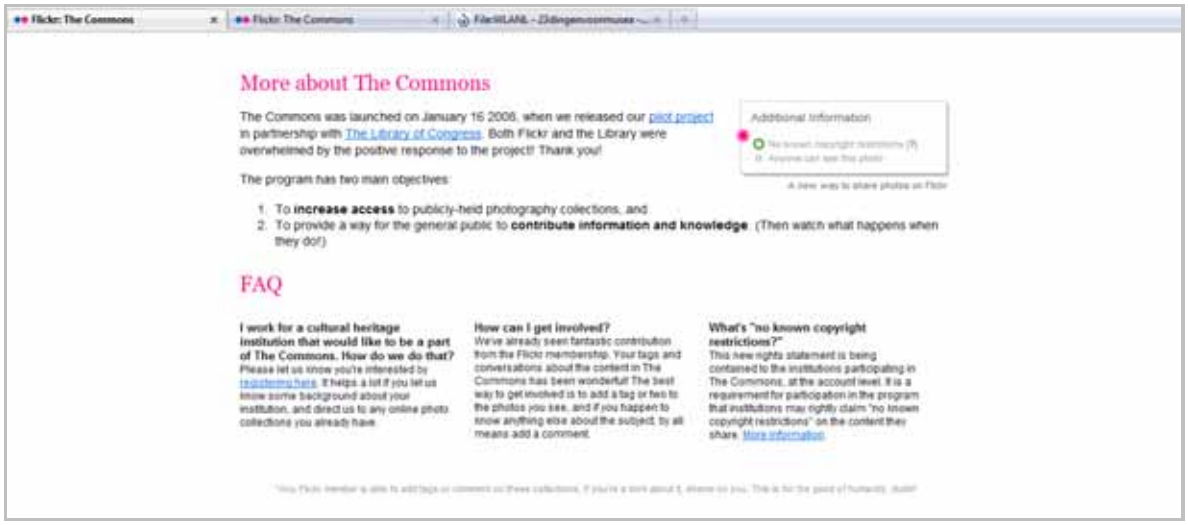

Image: screenshot of http://www.flickr.com/commons

Other participating institutions in the Flickr The Commons project have been, amongst others, Powerhouse Museum Collection, Brooklyn Museum, Smithsonian Institution, Bibliothèque de Toulouse, George Eastman House, National Maritime Museum, The Library of Virgini, Australian War Memorial collection, New York Public Library, National Galleries of Scotland Commons, State Library of Queensland, Australia, Swedish National Heritage Board, The National Archives UK and the Dutch Nationaal Archief.

The Dutch Nationaal Archief[169] also made a part of its photo collection worldwide available through Flickr The Commons. After a period of six months, they evaluated the participation in this project. The Nationaal Archief went to look for the stories behind the photographs and called upon the visitors of the Flickr website to add comments: does anyone recognise his or her (grand)parents in a picture? Can someone tell something more about the activity that is depicted in the photograph? Does anyone recognise his or her own street or village? After the six months of the pilot, the Flickr account of the Nationaal Archief contained nearly 800 photographs which resulted in over 1.000.000 pageviews, nearly 2.000 comments and over 6.800 tags added.[170]

---

167 G. Oates, The Commons on Flickr: A Primer. In: J. Trant and D. Bearman (eds.). *Museums and the Web 2008: Proceedings*, Toronto: Archives & Museum Informatics, 2008, s.p. Available online http://www.archimuse.com/mw2008/papers/oates/oates.html

168 J. Moortgat, Taking pictures to the public – Evaluatieverslag Nationaal Archief & spaarnestad Photo op Flickr The Commons, 2009, p.4. Available online http://www.nationaalarchief.nl/images/3_16370.pdf (Dutch only)

169 See http://www.flickr.com/photos/nationaalarchief/

170 J. Moortgat, Op. Cit., p.4.

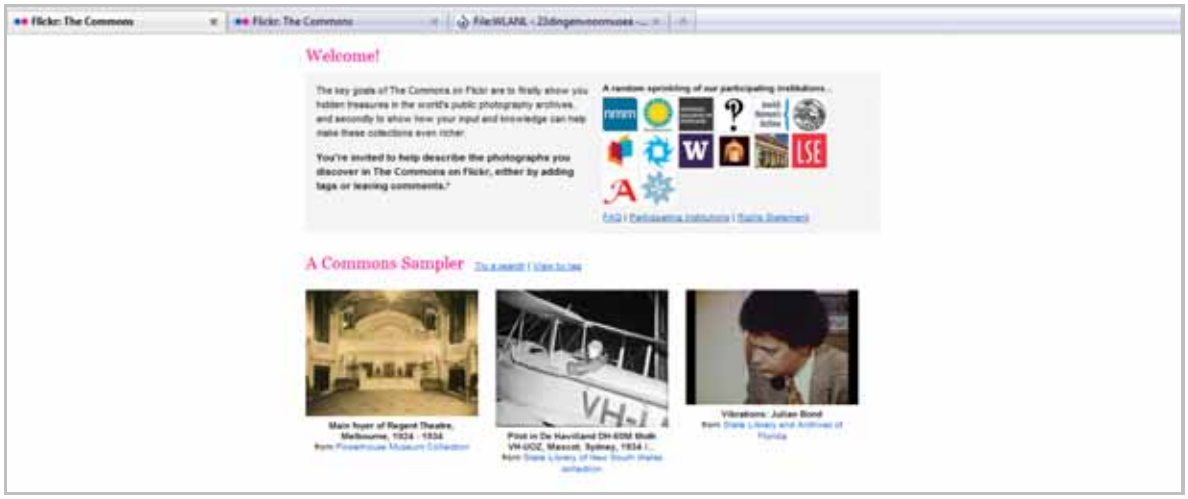

Image: screenshot of http://www.flickr.com/commons

4.4.5. Open Images

Open Images[171] is a Dutch open new media platform that offers access to a selection of archival materials for creative re-use. Footage from audiovisual collections may be downloaded and remixed into new works on the website. Users of Open Images also have the opportunity to add their own material to the platform and expand the existing collection.

Access to the material on Open Images is provided under the Creative Commons licensing model (CC-BY-SA). The policy of the project is, as they put it, 'open-open-open': the content is available under open content licenses, an open source media platform is being used (MMBase), it uses an open video codec (OGG-theora) and has an open API.[172]

Open Images is an initiative of the Netherlands Institute for Sound and Vision in collaboration with Knowledgeland. Since the end of 2009 Open Images offers access to over 450 Polygoon items from the Sound and Vision archives (on which Sound and Vision holds the rights). The collection will grow substantially over the coming years, as new items will be uploaded continuously and audiovisual items have, thanks to the CC license, been uploaded to Wikipedia to illustrate articles.[173]

171 See http://openimages.eu/.en

172 J. Oomen, P. Keller, Presentation on Open Images during Europeana v1.0 plenary meeting, The Hague, 15/19/2009.

173 See http://openimages.eu/about.en

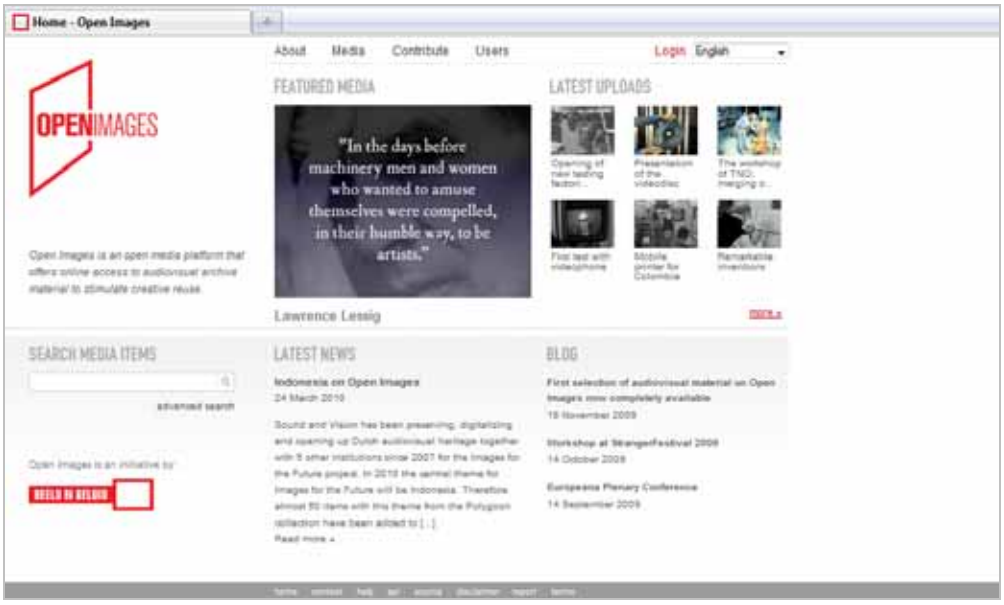

Image: screenshot of http://www.openimages.eu/.en

4.4.6. The Biodiversity Heritage Library

The Biodiversity Heritage Library (BHL) is a consortium of 12 natural history museum libraries, botanical libraries, and research institutions organised to digitise, serve, and preserve the legacy literature of biodiversity. The consortium aims to establish a corpus of digitised publications concerning biodiversity in the internet. The digitised material is made available in an open access way and forms part of a global 'Biodiversity Commons'. In doing so, they started a dialogue with right holders, the online community interested in the field and other interested parties in order to ensure that this literature can be made available online. The BHL slogan therefore is 'Science has no borders'.[174]

Image: screenshot of a search result on the BHL website http://www.biodiversitylibrary.org/item/90982#10

All of the images on the BHL website BiodiversityLibrary.org are free to use as long as this use is non-commercial and the user follows the conditions as set in the CC-BY-NC license under which the images are licensed. In the future, as the online library is likely to expand, more licensing models will be investigated and made possible. Following the

[174] See http://biodivlib.wikispaces.com/Open+Access and http://biodivlib.wikispaces.com/About

spirit of Europeana, BHL states on its website that *"[…] The Biodiversity Heritage Library is committed to keeping public domain materials in the public domain."* [175]

4.4.7. Points of interest

There are different degrees of public interaction that a cultural heritage institution may strive for in making their content available online. One could for example make users use the content by just providing them with a search or browse function which only enables them to look at the content. However, in case one, as an institution would want to get some feedback on the actual content of the material you've placed online, a technical infrastructure should be provided.

In cases such as the co-operation with Flickr, users were allowed to publicly comment on online images (a similar feature has been applied by multiple museums also on their own institutional website). The institution should be aware of the fact that not only highly valuable comments could end up there, but also inappropriate statements. The more 'freedom' of interaction you grant to a user, the more you should keep an eye on moderating user actions. A similar problem might also arise on web platforms where users can download content, remix it and upload their versions of it. There is no guarantee that they will not incorporate unsuitable material; this kind of feature therefore also requires moderation.

[175] See http://biodivlib.wikispaces.com/Licensing+and+Copyright. The term 'public domain' in this sentence should be interpreted as 'not subject to copyright protection', because of the nature of the work or the fact that the term of protection has expired. Members of the public without a background in legal affairs sometimes interpret the concept of public domain as 'everything that is part of a public collection (e.g. museum collection) and has been acquired with public funding'. This is also a correct interpretation, but it is no the one aimed at in this context.

5. General conclusion

While the availability of technology to help us digitise cultural material and make it available (and re-usable) online increases, copyright regulation still restricts the playing field. Because the creation of a 'safe' online environment for digital collections of cultural heritage organisations and the surveying of copyright status of the (analog) work are tasks that demand increased personnel, time and technological knowledge from the institutions, they do not start a process to open up their collections overnight. Unlocking cultural holdings is also no longer just a matter of technology; it has become one of politics. Lawmakers have been paving the way, but making content available online still falls under general copyright regulations – despite the copyright exceptions that have been launched. There are steps taken in the direction of the new online path of cultural heritage institutions (such as the creation of copyright exceptions, the increased attention for works in the public domain ...) but initiatives like Europeana cannot benefit from it.

Under current copyright law, any time a cultural heritage institution wants to make a work from their collection available online, this should happen with the full consent of the right holder of this work, which is a problem for orphan works. Collective rights management organisations make it easier for cultural heritage organisations to get hold of licenses on the material in their collections; in some cases there is only one organisation to address, which might even grant licenses for a global repertoire of works. But use of this content is often still linked to the payment of a remuneration – despite the often non-commercial nature of the act of making this content available online.

We've seen that in some cases a payment to these collective rights management organisations is due anyway, even if the right holder does not claim it in the end. In other cases still a lot of time and money has to be invested in licensing systems which require the proof of a diligent search for a right holder. Extended collective licensing may have the potential to be a mechanism for the quick and efficient processing of agreements.

Within the European Commission the copyright debate is a crucial one, and an active point of interest in the EU2020-policy. However, unless some legal decisions are made on this European level, the chances of law changes in any of the member states are slim (since exceptions cannot be implemented if they have not been approved on a EU level). Some collective licensing models may prove to be beneficial also for cultural heritage organisations but they should be taken out of their country-specific regimes. Further research is necessary and crucial in order to pick the best parts of collective licensing policies (e.g. limiting of liability, providing for exceptions ...), blend them together and make them applicable on a European (and national) level.

In the cases in which a cultural heritage institution is the only right holder on the content it would want to (re-)use or exploit, the content can be 'opened up'. Licensing mechanisms such as Creative Commons are fit for the job in such a non-commercial framework. A number of cultural heritage institutions have over the past year embraced this 'open' approach to the collections they hold. Not only do they make their content available on line, for example on their own website, but they strive to make it available on a scale that's as wide as possible. Co-operations are set up between large, high-trafficked websites and the cultural heritage organisation, often under a CC-related licensing basis.

Some examples of how cultural heritage organisations could benefit from new online display platforms, in combination with a free licensing of content, were presented. Yes, increasing the amount of user-interaction on one's website might require a change of policy (e.g. one might require content moderation), but this could well weigh up against the benefits a cultural heritage organisation might receive from it. Additional contextual information that is delivered by a user which can be incorporated into the museum's database, a link between images or content on the museum's website and others, increased visibility of the institution to a global audience …For more indirect results (e.g. the more people come into contact with the material, the more one could want to pay an 'analog' visit to it) we would have to give these initiatives some more time. Hopefully these examples can be an inspiration to other cultural heritage organisations.

PART TWO – OVERVIEW OF DRM TECHNIQUES

1. General introduction

Creativity is one of the most significant assets of human kind. People may express creativity in different ways with different media and as a result musicians, composers, singers, painters, sculptors, actors, movie directors, architects, industrial designers, writers, engineers, ..., computer scientists and more are producing creations. All of them are able to add something special to a simple mix of common ingredients: lines, notes, colours, words, instructions etc. In such a way creativity is the inner engine of innovation.

Of course creativity does not start usually from *tabula rasa*, it takes into account and is influenced by the cultural background and previous experiences and 'products'. All this happens voluntarily or involuntarily. Painters create their own style, even the most groundbreaking one, starting from the elaboration of existing ones. Composers are frequently influenced by other artists as well as architects and industrial designers.

Obviously speaking about innovation and inventions it is a common understanding that no-one is just going to sit down and think: *"Now I will invent something that does not exist at all!"* Sometimes the recipe includes part or a set of parts of already existent 'objects. In certain cases, the original aim of the invention or research is not exactly or not at all the real one on the market. By trying to optimise the efficiency of water pumps the steam engines were invented, by researching peer-to-peer secure wireless communication a 'bug' was discovered that later on was called 'broadcasting', when trying to help to solve problems of deaf people one of the most significant objects of the twentieth century was invented: the transistor.

Innovation capacity is disclosed to the public as soon as the 'creation' is available to the people. The general disclosure of the artefact inspires other authors or inventors, enabling them to go one step beyond or just to clone it. It happens every day in every field: music, painting, engineering, architecture, industrial design etc. It is a common understanding that creative people (and companies) invest time and resources in order to make some progress. Productivity and return of investment in this field are not easy to estimate. Of course there are differences amongst painters, musicians and scientists.

The issues of wide access to cultural and scientific content and in parallel protection and management of copyright create the next digital dilemma and considerable scepticism to Web 2.0 users and content providers: do we consider creations as human kind advances and in some way patrimony of the humanity freely accessible and reusable by anyone, or do we believe it is wiser to protect it as the result of personal investments and efforts? How intellectual property laws could embrace the apparently paradoxical goals of motivating individual creation and preserving the ultimate benefits of that creation for the common good, is a major issue. As a result the necessity of using systems which allow broad exchange of the creations while at the same time use copyright protection methodologies and tools during this exchange is important. Digital Rights Management systems have the objective to fulfil this goal, thus to protect and manage rights and copyrights and in parallel support the distribution and publication of priceless digital creations in the form of digital content.

This technical study presents the main aspects of Digital Rights Management Systems and is structured in the following main sections:

- Digital Rights Management Systems – An Overview. The DRMS is being defined and certain technological aspects are presented.
- Digital Watermarking in-Depth. The state of the art, new trends and the uses regarding digital watermarking for image and video files are presented.
- Digital Rights Management and Transactions – On-line Rights Clearance. The DRMS uses for transactions between users and content and new on-line clearance strategies are being analysed.
- Digital Rights Management – A European Law Perspective. A specialised review of legislation referring to Digital Rights Management systems is included.

2. Digital Rights Management Systems – an overview

2.1. Introduction

In this chapter the need of using copyright protection tools in our digital transactions is highlighted. The main tools of copyright protection such as cryptography, data hiding and watermarking along with the security framework where these tools can be used are also presented. However, all these tools and methods can be used only inside a specific technological and legal framework. This framework is constituted by developing the Digital Rights Management systems which are presented as a necessary mechanism to provide integrated e-services over the internet. The existing DRM technologies and the future research directions in this field are also included in this chapter.

2.2. The Focus of Digital Rights Management Systems

The spreading of internet and web technologies during the last years has leaded the world to technological infrastructures where creations and information can be exchanged freely and rapidly. The content providers are investing to new ways of making profits and offering new services concerning their digital products. The internet and its evolution was the best vehicle for the content providers to offer their services world wide. However, in contradiction with the traditional ways of copying where each copy of the original work has reduced quality, the digital information can be copied perfectly and every copy will be identical with the original one.[176] Moreover, the services that have been used today over the internet are giving the opportunity to spread these copies in all over the world, without geographical limitations.

Although www has imposed a tremendous change in the way of thinking, reducing the actual value of information, the digital content is still valuable and it should be protected. The protection of intellectual rights of digital content is concerned to be one of the big problems of the digital age.[177] Digital Rights Management Systems (DRM)[178] in addition with security measures[179] is essential for the protection of digital property. DRM systems are already in use to prevent people abusing information that is copyright protected.[180] Most of the current solutions provide external applications to ensure data protection management.[181]

The current trend though, is to provide embedded applications and not external. This can be done in three ways:

- Hardware-embedded Digital Rights Management systems.
- Digital Rights Management tools attached on the operating system.
- Development of Digital Rights Management functionality controllers embedded to the operating system.

---

[176] Lyon, G. (2001). The Internet Marketplace and Digital Rights Management. Report to the U.S. Department of Commerce, USA.

[177] CSTB (1999). The Digital Dilemma: Intellectual Property in the Information Age. Prepublication Copy, Computer Science and Telecommunications Board, US National Research Council, National Academy Press. Crawford, D. (1999). Intellectual Property in the Age of Universal Access. ACM Publications.

[178] Duhl, J., & Kevorkian, S. (2001). Understanding DRM Systems. IDC White Paper.

[179] Cohen, J. (2003). DRM and Privacy. Communications of the ACM, 46(4), 46-49. Ingemar, C., Miller, M., & Bloom, J. (2002). Digital Watermarking. Morgan Kaufmann Publishers. Institute for Information of Law, Study on the Implementation and Effect in Member States' Laws of Directive 2001/29 on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society, University of Amsterdam, February 2001. Wipro Technologies (2001). Digital Watermarking: A Technology Overview. White Paper.

[180] Heng, G. (2001). Digital Rights Management (DRM) using XrML. T-110.501 Seminar on Network Security. Renato, I. (2001). Digital Rights Management (DRM) Architectures. D-Lib Magazine, 7(6). Renato, I. (2001). Open Digital Rights Management. W3C Digital Rights Management Workshop, 22-23 January, Sophia Antipolis, France. DCITA (2003). A Guide to Digital Rights Management. Department of Communications Information Technology and the Arts. Retrieved February 1, 2008 from http://www.dcita.gov.au/drm. Schmidt, A., Tafreschi, O., & Wolf, R. (2004). Interoperability Challenges for DRM Systems. Reviewed Papers about Virtual Goods, Technische Universitat Ilmenau, Germany.

[181] Russ, A. (2001). Digital Rights Management Overview. SANS Institute.

A Digital Right Management mechanism is needed, so as to produce an integrated protection and management framework, able to diminish the possibilities of inappropriate usage and unauthorised copying. That's where Digital Right Management (DRM) systems are focused. Rights management is a necessity, because the term combines all those techniques and methodologies aiming to define and model actions, dealings and violations of intellectual rights.

2.3. Copyright Protection Tools

In the beginning of the third millennium, the use of digital means has become an inseparable piece of everyday life. Digital photography, video, medical images, satellite images, sounds etc. are some indicative examples. In many cases digital objects are intended to be published, either on the internet or in widely used mediums. Cultural heritage organisations such as museums or digital libraries, need to protect their Intellectual Property Rights (IPR) on this kind of media.

In the past, the scientific community along with commercial organisations has invested in order to find reliable methods to protect digital media. During the last decade digital watermarking, based on the idea of information hiding, originally introduced in the 5th century BC, gave a solution to the problem of designing such mechanisms to protect media.[182] This section is providing information about the currently used technologies in order to protect the digital content (documents, images, videos, sound, graphics etc.) from unauthorised use, along with the technologies that detect the unauthorised use.[183] These technologies are considering a variety of tools that related both with software and hardware.

More specifically these tools focused on:

- Security and integrity of operational systems.
- Cryptography.
- Data hiding and digital watermarking techniques.

2.3.1. Security and integrity

In computer security, an *access control list (ACL)* is a list of permissions attached to an object.[184] The list specifies who is allowed to access the object and what operations are allowed to be performed on it. In an ACL-based security model, when a subject requests to perform an operation on an object, the system first checks the list for an applicable entry in order to decide whether or not to proceed with the operation.

Systems that use ACLs can be classified into two categories, discretionary and mandatory. A system is said to have discretionary access control if the creator or owner of an object can fully control access to the object, including, for example, altering the object's ACL to grant access to anyone else. A system is said to have mandatory access control (also known as *"non-discretionary access control"* in the security literature) if it enforces system-wide restrictions that override the permissions stated in the ACL.

Traditional ACL systems assign permissions to individual users, which can become cumbersome in a system with a large number of users. In a more recent approach called role-based access control, permissions are assigned to roles, and roles are assigned to users.

Microsoft Windows Rights Management Services (RMS) is information protection technology that works with RMS-enabled applications to help safeguard digital information from unauthorised use -both online and offline, inside and outside of the firewall.[185] RMS enforces an organisation's security strategy by protecting information through

[182] Katzenbeisser, S., & Petitcolas, F. (2002). Information Hiding – Techniques for Steganography and Digital Watermarking. Atrech House Inc.

[183] Qiong, L., Safavi-Naini, R., & Sheppard, N. (2003). Digital Rights Management for Content Distribution. Australian Information Security Workshop (AISW2003), Adelaide, Australia. Lyon, G. (2001). The Internet Marketplace and Digital Rights Management. Report to the U.S. Department of Commerce, USA.

[184] Microsoft (n.d.). Retrieved February 1, 2008 from http://www.microsoft.com. Wikipedia (n.d.). Wikipedia. Retrieved February 1, 2008 from http://www.wikipedia.com.

[185] Microsoft (n.d.). Retrieved February 1, 2008 from http://www.microsoft.com.

persistent usage policies, which remain with the information, no matter where it goes. Organisations can use RMS to help prevent sensitive information -such as financial reports, product specifications, customer data, and confidential e-mail messages- from intentionally or accidentally getting into the wrong hands.

2.3.2. Cryptography

The cryptographic algorithms and procedures are very old. In Ancient Greece and Rome they used techniques and cryptographic devices in order to encode and decode messages.[186] From that period till today the field of cryptography has made significant improvement. Especially during the Second World War cryptography was the main instrument for secret communication between spies, military, diplomats etc. The development of computers made possible the construction of more complex cryptographic algorithms and more powerful mechanisms for secure communication.

Cryptography is usually linked with two processes, the encryption and decryption process. The encryption process is operated by using a key and a cryptographic algorithm and the original data (plaintext) converted to encrypted data (ciphertext). The key as a secret parameter can be used also during the decryption process (symmetric cryptography) where from encrypted data derived the original data or a second key is used for that purpose (asymmetric cryptography), depending the application. In public-key cryptosystems, the public key may be freely distributed, while its paired private key must remain secret. The *public key* is typically used for encryption, while the *private* or *secret key* is used for decryption. In addition to encryption, public-key cryptography can be used to implement digital signature schemes. A digital signature is reminiscent of an ordinary signature; they both have the characteristic that they are easy for a user to produce, but difficult for anyone else to forge.

The cryptographic technologies can be used to control the copyrighted material and protect the Intellectual Rights of the copyright holders, in DRM systems. In the whole world there are several laws and directives today that prevent the unauthorised use of copyrighted material and set a legislation framework that should be respected from all users or providers of digital content.

2.3.3. Data Hiding and Digital Watermarking Techniques

The digital watermarking technique is a standard tool today for copyright protection of multimedia objects. The different types of watermarks concerning their characteristics (robustness/fragility, capacity, quality of watermarked object, security etc.), their visibility (visible, imperceptible watermarks) and they have a direct impact on DRM systems design.[187]

Digital watermarking of images exploits the fact that digital images contain redundant data that can be used to hide the information of the image owner. The latter information is called digital watermark. The redundancy of the image data is also exploited by image compression techniques in order to reduce the amount of data that represent an image.

The directions that have been followed in the design of a watermarking method are:

a) modification of cover data in the frequency domain;[188]
b) modification of the cover data in the spatial domain.[189]

---

[186] Katzenbeisser, S., & Petitcolas, F. (2002). Information Hiding – Techniques for Steganography and Digital Watermarking. Atrech House Inc. Wikipedia (n.d.). Wikipedia. Retrieved February 1, 2008 from http://www.wikipedia.com.

[187] Ingemar, C., Miller, M., & Bloom, J. (2002). Digital Watermarking. Morgan Kaufmann Publishers.

Institute for Information of Law, Study on the Implementation and Effect in Member States' Laws of Directive 2001/29 on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society, University of Amsterdam, February 2001. Katzenbeisser, S., & Petitcolas, F. Op. Cit.

[188] Cox, I., Kilian, J., Leighton, T., & Shamoon, T. (1996). A Secure, Robust Watermark for Multimedia. First Workshop on Information Hiding, Newton Institute, University of Cambridge. Gilani, S., Kostopoulos, I., & Skodras, A. (2002). Adaptive Color Image Watermarking. 14th IEEE International Conference on Digital Signal Processing, 1-3 July 2002, Santorini, Greece.

[189] Armeni, S., Christodoulakis, D., Kostopoulos, I., Stamatiou, Y., & Xenos, M. (2000). A Transparent Watermarking Method for Color Images. First IEEE Balcan Conference on Signal Processing, Communications, Circuits, and Systems, June, Istanbul, Turkey. Kutter, M., Jordan, F., & Bossen, F. (1997). Digital Signature of Color Images Using Amplitude Modulation. Proceedings of the SPIE, Storage and Retrieval for Image and Video Databases V, 518-526. Van Schyndel, R., Tirkel, A. & Osborne, C. (1994). A Digital Watermark, Proceedings of IEEE International Conference on Image Processing (ICIP-94), 2, 86-90. Yeung, M., & Mintzer, F. (1997). An Invisible Watermarking Technique for Image Verification. Proceedings of ICIP '97, Santa Barbara, California.

Recent advances in watermarking technologies introduce algorithms working in both spatial and frequency domain.[190]

Perceptible Watermarks
The perceptible/visible watermark is usually connected with the embedding process where a pattern or company logo is inserted in the image or video content in a visible way, without altering the content of the original image/video. The watermark intends to protect the original work so as every attempt to remove it or destroy it will be difficult and should result the watermarked work destruction. Therefore the visible watermark can be inserted in whole image/video or in a part of it depending on the owner needs.

Imperceptible Watermarks
The invisible or imperceptible watermarks are digital information that embedded in the original work (image/video/sound) in a way that the human visual or hearing system can not detect it. The detection of the watermark can be achieved algorithmically, by using a watermark detection system (software/hardware).
Depending on the application there are several types of imperceptible watermarks:

a) watermarks that destroyed when the attacker modifies the watermarked object. These watermarks used for content authentication;
b) watermarks that remain intact after several modifications are used for copyright protection of a digital object.

2.4. Digital Rights Management

Unfortunately, there is not a commonly agreed definition for DRM. The term, according to the World Wide Web Consortium[191], covers the description, recognition, protection, control, commerce, monitoring and tracking of all the possible usage types concerning digital content - including the relationship management between the digital object's owners.

According to Katzenbeisser & Petitcolas[192], DRM is a term that is used to describe a range of techniques which collect information for rights and right holders, so as to manage copyrighted material; and the conditions under which these materials will be distributed to the users.

DRM refers to the protection of the intellectual property of digital content by controlling the actions of the authorised end user to the digital content. It gives the digital object's owner the ability to securely distribute valuable content such as books, photos, videos, magazines; at the same time helps the owner manage the content, avoiding unauthorised usage or copying.

The following image represents DRM lifecycle:

[190] Yu, G., Lu, C., & Liao, H. (2003). A Message-based Cocktail Watermarking System. Elsevier, Pattern Recognition, 36, 969-975. Shih, F., & Wu, S. (2003). Combinational Image Watermarking in the Spatial and Frequency Domains. Elsevier, Pattern Recognition, 36, 957-968.

[191] DRM (2000). Digital Rights Management Workshop. Retrieved February 1, 2008 from http://www.w3.org/2000/12/drm-ws/.

[192] Katzenbeisser, S., & Petitcolas, F. (2002). Information Hiding – Techniques for Steganography and Digital Watermarking. Atrech House Inc.

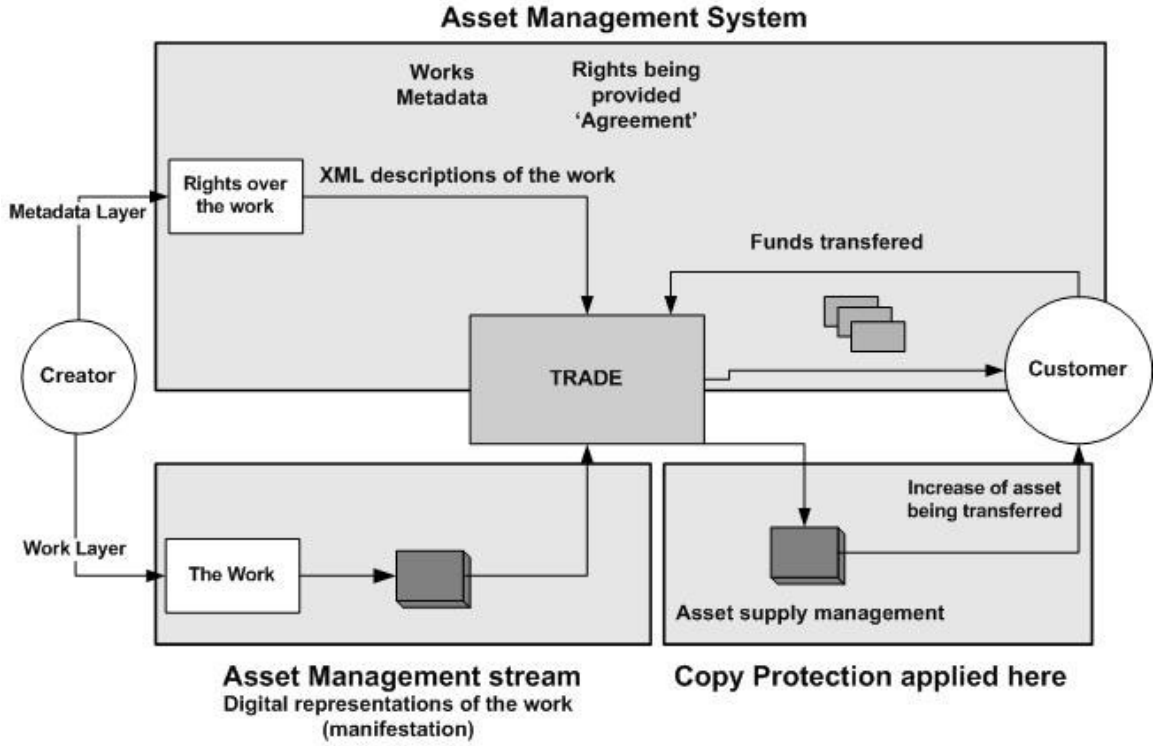

Figure 1: DRM Lifecycle.

2.4.1. DRM systems: an overview

A DRM system is a chain of services and hardware technologies that controls the authenticated usage of digital content; it also manages any actions or results that the aforementioned usage causes throughout the lifecycle of the content.

A typical DRM system may comprise the following elements:

- file and content recognition systems;
- languages for attribute management;
- different file types;
- techniques and methods of digital content distribution;
- metadata.

It can be applied to any business or organisation that deal with sensitive or confidential information and needs to protect valuable digital assets, controlling the distribution and usage of these assets.

A DRM system is essential when the digital content:

- must be accessible to certain groups of people and not available to others;
- should be used in a different way by different user types;
- is tracked and checked according to the flow of the process under which is being used.

Previously, Digital Rights Management (DRM) focused on security and encryption as a means of solving the issue of unauthorised copying, which locks the content and limits its distribution to only those who pay. This was the first-generation of DRM, and it represented a substantial narrowing of the real and broader capabilities of DRM.[193]

The second-generation of DRM covers the description, identification, trading, protection, monitoring and tracking of all forms of rights usages over both tangible and intangible assets including management of rights holders' relationships.

[193] Renato, I. (2001). Digital Rights Management (DRM) Architectures. D-Lib Magazine, 7(6).

Additionally, it is important to note that DRM is the *"digital management of rights"* and not the *"management of digital rights"*. That is, DRM manages *all* rights, not only the rights applicable to permissions over digital content.[194]

In designing and implementing DRM systems, there are two critical architectures to consider. The first is the 'functional architecture', which covers the high-level modules or components of the DRM system that together provide an end-to-end management of rights. The second critical architecture is the 'information architecture', which covers the modelling of the entities within a DRM system as well as their relationships. There are many other architectural layers that also need to be considered, such as the conceptual, module, execution and code layers.[195]

2.4.2. Functional Architecture

The overall DRM framework suited to building digital rights-enabled systems can be modelled in three areas.

- Intellectual Property (IP) Asset Creation and Capture: How to manage the creation of content so it can be easily traded. This includes asserting rights when content is first created (or reused and extended with appropriate rights to do so) by various content creators/providers.
- IP Asset Management: How to manage and enable the trade of content. This includes accepting content from creators into an asset management system. The trading systems need to manage the descriptive metadata and rights metadata (e.g., parties, usages, payments, etc.).
- IP Asset Usage: How to manage the usage of content once it has been traded. This includes supporting constraints over traded content in specific desktop systems/software.

While the above models comprise the broad areas required for DRM, the models need to be complemented by the Functional Architecture that provides the framework for the modules to implement DRM functionality (figure 2).

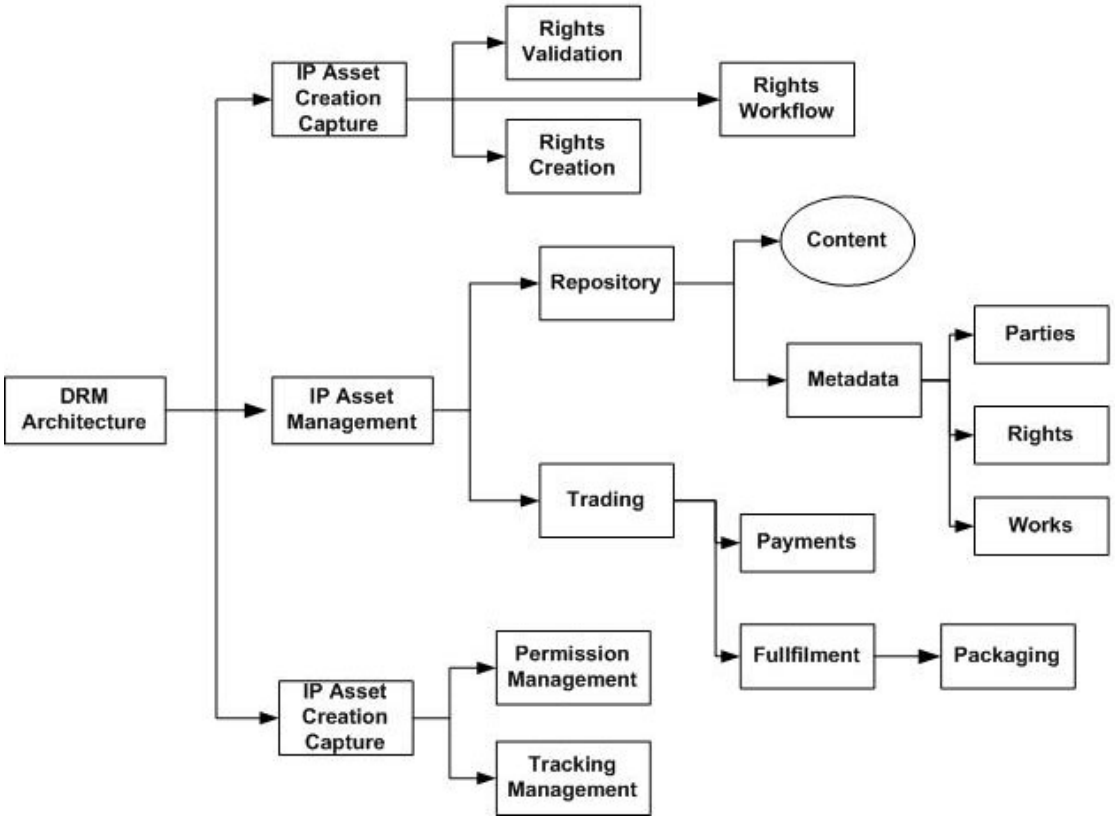

Figure 2: DRM Functional Architecture.

The Functional Architecture stipulates the roles and behaviour of a number of cooperating and interoperating modules under the three areas of Intellectual Property (IP): asset creation, management and usage.

[194] Renato, I. (2001). Digital Rights Management (DRM) Architectures. D-Lib Magazine, 7(6).

[195] Hofmeister, C., Nord, R., & Soni, D. (2000). Applied Software Architectures. Addison-Wesley.

The IP Asset Creation and Capture module supports:

- rights validation - to ensure that content being created from existing content includes the rights to do so;
- rights creation - to allow rights to be assigned to new content, such as specifying the rights owners and allowable usage permissions;
- rights workflow - to allow for content to be processed through a series of workflow steps for review and/or approval of rights (and content).

The IP Asset Management module supports:

- repository functions - to enable the access/retrieval of content in potentially distributed databases and the access/retrieval of metadata. The metadata covers parties, rights and descriptions of the works;
- trading functions - to enable the assignment of licenses to parties who have traded agreements for rights over content, including payments from licensees to rights holders (e.g., royalty payments). In some cases, the content may need to go through fulfilment operations to satisfy the license agreement. For example, the content may be encrypted/protected or packaged for a particular type of desktop usage environment.

The IP Asset Usage module supports:

- permissions management - to enable the usage environment to honour the rights associated with the content. For example, if the user only has the right to view the document, then printing will not be allowed;
- tracking management - to enable the monitoring of the usage of content where such tracking is part of the agreed to license conditions (e.g., the user has a license to play a video ten times). This module may also need to interoperate with the trading system to track usage or to record transactions if there is payment due for each usage.

Together, these three modules provide the core functionality for DRM systems. These modules need to operate within other, existing e-business modules (such as shopping carts, consumer personalisation, etc.) and digital asset management modules (such as version control, updates, etc.).
Additionally, the modules would support interoperability, trust, standard formats, openness and other principles.[196]

Ideally, these modules would be engineered as components to enable systems to be built in a modular fashion. However, this implies a set of common and standard interfaces/protocols between the modules. As DRM matures, the industry will move towards such standardisation.

The functional architecture is only part of the solution to the challenges of DRM. Rights Management can become complex remarkably quickly. As a result, DRM systems must support the most flexible information model possible to provide for these complex and layered relationships. The information architecture provides this.[197]

2.4.3. Information Architecture

The information architecture deals with how the entities are modelled in the overall DRM framework and their relationships. The main issues that require addressing in the development of a DRM Information model include:

- modeling the entities;
- identifying and describing the entities;
- expressing the rights statements.

Modelling the Entities

It is important to adopt a clear and extensible model for the DRM entities and their relationship with other entities. Existing work in this area includes the <indecs> project.[198] The basic principle of the <indecs> model is to clearly separate and identify the three core entities: users, content, and rights as shown in figure 3. Users can be any type of user, from a rights holder to an end-consumer. Content is any type of content at any level of aggregation. The rights entity is an expression of the permissions, constraints, and obligations between the users and the content. The primary reason for this model is that it provides the greatest flexibility when assigning rights to any combination or layering of

[196] Erickson, J. (2001). Information Objects and Rights Management. D-Lib Magazine, 7(4). Retrieved February 1, 2008 from http://www.dlib.org/dlib/april01/erickson/04erickson.html.

[197] Renato, I. (2001a). Digital Rights Management (DRM) Architectures. D-Lib Magazine, 7(6).

[198] INDECS (2002). Interoperability of Data in E-commerce Systems. Retrieved February 1, 2008 from http://www.indecs.org.

users and content. The core entities model also does not constrain content from being used in new and evolving business models.

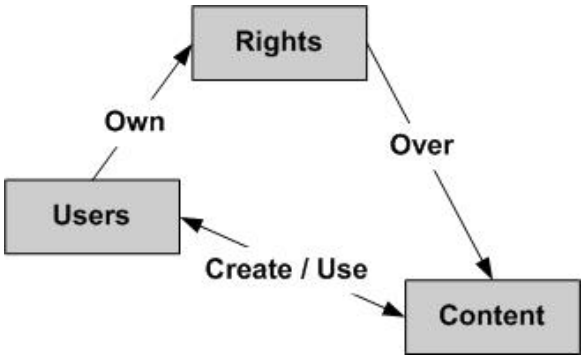

Figure 3: Information Architecture – Core Entities Model.

This model implies that any metadata about the three entities needs to include a mechanism to relate the entities to each other.

Identifying and Describing the Entities
All entities need to be both identified and described. Identification should be accomplished via open and standard mechanisms for each entity in the model. Both the entities and the metadata records about the entities must be identifiable. Open standards such as Uniform Resource Identifiers[199] and Digital Object Identifiers[200] and the ISO International Standard Textual Work Code[201] are typical schemes useful for Rights identification.

Content should be described using the most appropriate metadata standard for that genre (for example, the EDItEUR ONIX standard[202] for books and the IMS Learning Resource Meta-data Information Model[203] for educational learning objects). It is also critical that such metadata standards do not themselves try to include metadata elements that attempt to address rights management information, as this will lead to confusion regarding where to describe such rights expressions. For example, the ONIX standard has elements for a number of rights holders (e.g., authors and publishers) and territories for rights and single price information (the latter poses a problem in setting multiple prices depending on what rights are traded). In such cases, following the <indecs> model should take precedence.

To describe users, vCard[204] is the most well-known metadata standard for describing people and (to some extent) organisations. An additional and important part of the rights model is to articulate the role that the user has undertaken with respect to content. A comprehensive list of roles can be found in the MARC Relators code list.[205]

Expressing Rights Statements
The rights entity allows expressions to be made about the allowable permissions, constraints, obligations, and any other rights-related information about users and content. Hence, the rights entity is critical because it represents the expressiveness of the language that will be used to inform the rights metadata.

---

[199] URI (n.d.). Uniform Resource Identifiers (URI): Generic Syntax. IETF RFC2396. Retrieved February 1, 2008 from http://www.ietf.org/rfc/rfc2396.txt.

[200] DOI (2007). Digital Object Identifier – DOI. Retrieved February 1, 2008 from http://www.doi.org.

[201] ISO (n.d.). ISO International Standard Textual Work Code. Retrieved February 1, 2008 from http://www.nlc-bnc.ca/iso/tc46sc9/istc.htm.

[202] EDItEUR ONIX (n.d.). EDItEUR ONIX International Standard. Retrieved February 1, 2008 from http://www.editeur.org/onix.html.

[203] IMS (n.d.). IMS Learning Resource Meta-data Information Model (Version 1.1). Retrieved February 1, 2008 from http://www.imsproject.org/metadata/mdinfov1p1.pdf.

[204] RFC (n.d.). RFC 2426 vCard Profile. Retrieved February 1, 2008 from http://www.ietf.org/rfc/rfc2426.txt.

[205] MARC (n.d.). MARC Code List for Relators. Retrieved February 1, 2008 from http://lcweb.loc.gov/marc/relators/re0003r2.html.

Rights expressions can become complex quite quickly. Because of that, they are also modelled to understand the relationships within the rights expressions. This has been evidenced in the Open Digital Rights Language[206] and a paper by Gunter et al. (2001).[207]

Rights expressions should consist of:
- permissions (i.e., usages) - what you are allowed to do;
- constraints - restrictions on the permissions;
- obligations - what you have to do/provide/accept;
- rights Holders - who is entitled to what.

2.5. Technological Prototypes – Standards

DRM technology standards initiatives have to fulfill a number of challenges. Some standards are created to confront relatively narrow and specific problems while others are more broad and general. Furthermore, there are many organisations with an interest in the area, many of which are not standards bodies in the usual sense. In this section, we overview the prototypes, standards and metadata used in DRM systems.

2.5.1. DOI

Digital Object Identifier (DOI)[208] is an identification system for intellectual property in the digital environment. It has evolved as an effort of the Association of American Publishers (AAP)[209] in 1996. In 1998, International DOI Foundation (IDF) was created to advance development and promotion of DOI concept. Its goals are to provide a framework for managing intellectual content, link customers with publishers, facilitate electronic commerce, and enable automated copyright management not only for the publishing industry but for many others industries (for example, music).

DOI names are assigned to any entity (documents, publications and other resources) for use on digital networks. These names are unique, persistent (i.e. they do not become invalid) and have high availability (i.e. they do not depend on a single Web server being up and running) for use over their lifetime (like bar codes), while standard Web URLs can change over time.[210] Other information about the digital object may change over time, including where to find it, but its DOI name will not change. DOIs actually are in line with the Internet Engineering Task Force's preliminary specifications for Uniform Resource Names (URNs), a more general standard than URLs. This standard would facilitate interoperability between DRM and non-DRM systems such as content management and electronic commerce systems.

DOIs have a simple syntax, which is depicted in figure 4. The general DOI structure has two components, a prefix and a suffix, separated by a forward slash (/). The combination of a prefix for the Registrant and unique suffix provided by the Registrant avoids any necessity for the centralised allocation of DOI numbers. The two components together form the DOI.

---

206 ODRL (n.d.). Open Digital Rights Language. Retrieved February 1, 2008 from http://odrl.net/.

207 Gunter, C., Weeks, S., & Wright, A. (2001). Models and Languages for Digital Rights. InterTrust Star Lab Technical Report STAR-TR-01-04. Retrieved February 1, 2008 from http://www.star-lab.com/tr/star-tr-01-04.pdf.

208 DOI (2007). Digital Object Identifier – DOI. Retrieved February 1, 2008 from http://www.doi.org.

209 AAP (2007). Association of American Publishers – AAP. Retrieved February 1, 2008 from http://www.publishers.org.

210 Rosenblatt, R. (1997). Solving the Dilemma of Copyright Protection Online. The Journal of Electronic Publishing (JEP), 3(2). Retrieved February 1, 2008 from http://www.press.umich.edu/jep/03-02/doi.html.

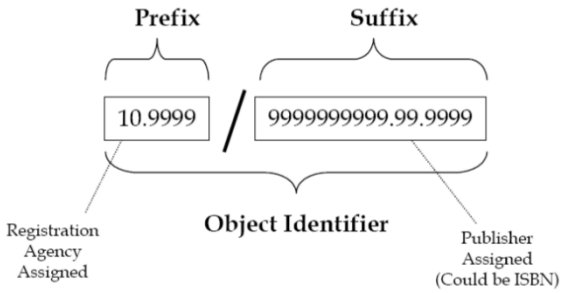

Figure 4: DOI Structure.

The prefix of all DOIs starts with "10", which distinguishes them from any other implementations. The next component of the prefix is a number (string) that corresponds to the publisher (or other intellectual property owner) that assigns the DOI.

The DOI suffix identifies the entity and may be any alphanumeric string chosen by the Registrant (e.g. sequential number, legacy identifier, etc.). It could be comprised of multiple nodes (figure 5) that are separated by a dot (.). Node 1 is the whole work and legacy identifier node (highest structural level). In reflecting that, the full ISBN or other standard identifier should be used in the first node of the DOI suffix. Nodes 2 and following are the component nodes. The addition of a node creates a new DOI, which will need to be registered.[211]

10.0011 / 0999999991
10.0011 / 0999999991.1
10.0011 / 0999999991.01.0001
10.0011 / 0999999991.0.1.01

Figure 5: Examples of valid DOIs.

2.5.2. XrML

Extensible Rights Markup Language (XrML) is an XML-based language for digital rights management. It provides a universal method for securely specifying and managing rights and issuing conditions associated with the use and protection of all kinds of resources including digital content, as well as services.[212] It was developed by Content Guard, a subsidiary of Xerox, and supported by Microsoft. Other backers are Adobe, Audible.com, Hewlett-Packard, OverDrive, Portal Software and Xerox. XrML stem from Digital Property Rights Language (DPRL)[213] that was first introduced in 1996. DPRL became XrML when the meta-language (used to define the language) was changed from a Lisp-style meta-language to XML in 1999.

Contrary to DOI, which is simple conceptually and syntactically, XrML is a rich language of specifications. Its purpose is to expand the usefulness of digital content, resources, and web services to rights holders, technology developers, service providers and users by providing a flexible, extensible, and interoperable industry standard language that is platform, media, format and business independent. It supports an open architecture and can be integrated with both existing and new DRM systems.[214]

The XrML data model consists of four entities: *principal*, *resource*, *right*, and *condition* and the relationship between them. These determine the full context of the rights that are specified. A principal encapsulates the identification of a

---

[211] AAP (2000). Association of American Publishers – AAP, Numbering Standards for Ebooks, Version 1.0. Retrieved February 1, 2008 from http://www.publishers.org/digital/numbering.pdf.

[212] XrML (2007). Extensible Rights Markup Language – XrML, 2.0 Specification. Retrieved February 1, 2008 from http://www.xrml.org.

[213] DPRL (1998). Digital Property Rights Language – DPRL, Manual and Tutorial - XML Edition, Version 2.00. Retrieved February 1, 2008 from http://xml.coverpages.org/DPRLmanual-XML2.html.

[214] Heng, G. (2001). Digital Rights Management (DRM) using XrML. T-110.501 Seminar on Network Security.

party to whom rights are granted. A resource is the 'object' to which a principal can be granted a right (e.g. e-book, audio file, video file, image, email service, B2B transaction service, or even a piece of information). A right is the 'verb' that a principal can be granted to exercise against some resource under some condition. Finally, a condition specifies the terms, conditions, and obligations under which rights can be exercised.[215]

Its latest release, XrML 2.0, expands the capabilities of a digital rights language to enable developers to establish the rights and conditions needed to access web services in addition to digital content. It also contains additional capabilities in the areas of extensibility, security, and life cycle management. Recent actions in several standards bodies, most notably MPEG, OeBF and OASIS, have positioned XrML to become the world wide industry standard for a digital rights language.

2.5.3. ICE

Information and Content Exchange (ICE)[216] is an XML-based protocol used for electronic business-to-business (B2B) content management. It was originally developed in 1998 by industry content providers and software vendors. ICE specification provides businesses with a common language and an architecture to facilitate automated Web content syndication (information exchange, sharing and reuse between Web sites) for traditional publishing contexts and e-commerce uses and relationships.

By using XML, both syndicators and their subscribers (a syndicator produces content that is consumed by subscribers) have an agreed-upon language in which to communicate. The protocol defines the roles and responsibilities of syndicators and subscribers, specifies the format and method of content exchange, and provides support for management and control of syndication relationships. The system uses a client-server architecture.

The protocol covers four general types of operations: (a) subscription establishment and management, (b) data delivery, (c) event logs and (d) miscellaneous.[217] A relationship starts with the subscription establishment. The subscriber obtains a catalog of possible subscriptions offers (including terms such as delivery policy, usage reporting, presentation constraints, etc.) from the syndicator and then subscribes to particular ones. The primary message exchanges center on data delivery. The protocol is able to manage special situations and conditions and to diagnose problems by event logs that automatically exchanged between subscribers and syndicators. Finally, a significant number of mechanisms for supporting miscellaneous operations (protocol parameters renegotiation, unsolicited ad-hoc notifications, queries, etc.) is supported.

With the latest release, ICE 2.0, robust content syndication is supported in a web services environment for the first time. It is defined as a W3C XML Schema, replaces the ICE 1.1 messaging structure with SOAP messaging protocol, and provides WSDL scripts to facilitate syndication as a Web service. ICE is considered as the best solution for those editors that want to build their own syndication architecture. It facilitates the building of flexible and reliable services and allows them to keep the profits of the transactions. ICE comprises an important protocol in DRM standardisation field.

2.5.4. SDMI

Secure Digital Music Initiative (SDMI) was an initiative of music industry that formed in late 1998. Its purpose was to develop technology specifications to protect the playing, storing and distributing of digital music and consequently prevent music piracy. SDMI was a direct response to MP3 file format booming, which allowed digital music of good quality to be distributed via the Internet and forced the music industry to take new measures. In this way, consumers were provided with a convenient access to online music and new digital distributions systems to enable copyright protection.

---

[215] Wang, X., Lao, G., DeMartini, T., Reddy, H., Nguyen, M., & Valenzuela, E. (2002). XrML – eXtensible Rights Markup Language. Proceedings of the ACM Workshop on XML Security, ACM Press, NY USA, 71-79.

[216] Hunt, B. (2000). Information and Content Exchange (ICE) Reference Version. Retrieved February 1, 2008 from http://www.infoloom.com/gcaconfs/WEB/paris2000/S21-04.HTM.

[217] ICE (1998). Information and Content Exchange Protocol – ICE. W3C. Retrieved February 1, 2008 from http://www.w3.org/TR/NOTE-ice.

In June, 1999, they defined a standard for manufacturing portable devices that can play both unprotected and protected music formats.[218] The audio files contained a digital watermark, an inaudible message hidden in music to provide copyright information to devices like MP3 players and recorders.

In September 2000, SDMI announced a public challenge with an 'Open Letter to the Digital Community', invited interested parties to attempt to crack their proposed digital watermarking schemes. The protection scheme was cracked by a team at Princeton led by Professor Edward Felton.[219] So, any device implementing an algorithm based on the same reasoning would inevitably be cracked too.

The last press release from SDMI.org dated May 18, 2001. SDMI admitted that there was no consensus for adoption of any combination of the proposed technologies, although the digital watermark remains in widespread use.

2.5.5. XMCL

Extensible Media Commerce Language (XMCL), a rights specification language, was announced in June 2001 by RealNetworks Inc and is supported by 27 companies (e.g. Adobe, America Online, IBM, InterTrust Technologies, EMI, Sony Pictures Digital Entertainment and Sun). XMCL, as XrML and ICE, is an interchange format for the specification of content copyright information based on XML language. It describes usage rules that apply to multi-media content and is designed to communicate these rules in an implementation independent manner for interchange between business systems (e.g. web store fronts, customer tracking and management) and trusted delivery and playback systems (e.g. DRM implementations responsible for enforcing the rules described in the language).[220]

XMCL describes the minimum, self-complete set of business rules under which digital media is licensed for consumer use.[221] These business rules support multiple business models including rental, subscription, ownership, and video on demand/pay-per-view. When a business system authorises a customer transaction for digital media, it generates a XMCL document that is then acted upon and enforced by a specific trusted system. The generated XMCL document is submitted to the trusted system through the APIs of the trusted system (e.g. HTTP POST, RPC call, API call).

2.5.6. ODRL

Open Digital Rights Language (ODRL) initiative aimed at developing and promoting an open standard for rights expressions. ODRL is intended to provide flexible and interoperable mechanisms to support transparent and innovative use of digital resources in publishing, distributing and consuming of electronic publications, digital images, audio and movies, learning objects, computer software and other creations in digital form.[222] It is an open source language without license requirements.

ODRL is based on an extensible model for rights expressions which involves a number of core entities and their relationships. Three are the core entities of the model: *assets*, *rights* and *parties*. The first include any physical or digital content, should be uniquely identified, may consists of many subparts, may be in many different formats and may also be encrypted to enable secure distribution of content. The second entity includes *permissions* which can then contain *constraints*, *requirements*, and *conditions*. Finally, *parties* include end users and rights holders. With these three core entities, the model can then express or revoke *offers* (proposals from rights holders for specific rights over their assets) and *agreements* (when parties enter into contracts or deals with specific offers).

---

218 SDMI (n.d.). Secure Digital Music Initiative – SDMI, Protection through Encryption. Retrieved February 1, 2008 from http://www.benedict.com/Digital/Internet/SDMI.aspx.

219 SDMI (2001). Reading Between the Lines: Lessons from the SDMI Challenge. Princeton University. Retrieved February 1, 2008 from http://www.cs.princeton.edu/sip/sdmi.

220 Ayars, J. (2002). XMCL – eXtensible Media Commerce Language. RealNetworks, Inc., W3C. Retrieved February 1, 2008 from http://www.w3.org/TR/xmcl.

221 XMCL (2001). XMCL – eXtensible Media Commerce Language. Retrieved February 1, 2008 from http://www.xmcl.org/index.html.

222 Renato, I. (2002). Open Digital Rights Language (ODRL), Version 1.1. IPR Systems, W3C. Retrieved February 1, 2008 from http://www.w3.org/TR/odrl.

ODRL is more comprehensible in modeling the rights than XMCL. Its current version is 1.1, based on XML and provides a standardisation mechanism that is independent from the content and the way of transport. It presents some resemblances with the XrML but also enough differences. ODRL has major application in media sector transactions and books publications and sales, while XrML is of general aim.

2.6. The Future of DRM Systems

DRM technology faces several issues that have to be addressed. In the future, DRM enabled business models will grow dramatically. DRM technology will certainly improve over time and enhance new features, supporting business models that are endorsed by content providers.

The adoption of a DRM system is not easy; they are costly, complex and not fully secure. The success of Digital Right Management systems will be based in a number of other factors, including the balance between protection of intellectual rights and privacy.

A balanced, successful DRM system must be a combination of technological, business and legal concerns in a functional, open and acceptable framework. Digital Right Management is inevitably one of the greatest challenges for content communities. But, what is it going to happen from now on?

First of all, the business models that need DRM will dramatically increase. Successful DRM business models will represent a gradual composition of traditional business models and models which are based on information technology and internet. The only concrete assumption is that different business models will succeed in different business areas.

DRM technology will be improving constantly. A major success factor is to be incorporated at the Computers' core technology and not provided as an additional software product. They are three possible ways that this can happen:

- Build DRM into the PC's Hardware. This is the most effective way to do it with respect to security.
- Bundle the Software into the Operating System Distribution. With this method, every PC that comes with an operating system may include a DRM controller that applies to all content types.
- Build DRM Controller Functions Directly into the Operation System. The system call to open files, as a built-in DRM controller, should determine whether the user has the rights to the file and then make the file available, possibly decrypting it in the process.

Another important factor that must be addressed is the open-standard issue. For instance, the Digital Object Identifier is vitally important. It is almost a no-barrier choice as a standard content identifier that also allows online reference. Yet DOI risks being pigeonholed as a standard that applies only to book and journal publishing.

DRM can be used as the vehicle, for content providers, to run and catch up with the easy spread of their proprietary information. This battle will certainly go on – but there is a great possibility to be able to control and manage a great amount of this information. There are several issues that have to be solved but yet DRM can lead the way.

2.7. Future Research Directions

DRM technology constantly faces new challenges. As the business models that need to incorporate digital right management mechanisms multiply, the research community must constantly address new ideas, models and variations of a typical DRM system. The goal must be the provision of different solutions to each and every alternative case (business model).

A core research direction is inevitably the adoption of concrete privacy models. 'Privacy' and 'security' are often misused as common terms. Technologically, security is easier to be addressed. On the other hand, privacy often is not defined unambiguously. The variation in the way different people understand privacy is an open problem. Thus, a significant issue for researchers is to provide a unique definition of the privacy issues that can be modelled in a way, able to be addressed in such a technological platform.

As already mentioned in this chapter, among the success factors of a Digital Right Management information system is the balance between protection and usability. The latter, usability, should take into account both technical and

functional requirements. As businesses grow in a new internet-oriented environment, technology is also reforming rapidly. New, open standards are continuously brought up and new interoperability needs occur. The need of a fully open and dynamically customisable standard is still a major problem. Researchers must foresee the future of technology in conjunction with the specifications of a Digital Right Management system and integrate technological solutions with new methods of intellectual property safeguarding.

Another vital issue that will be probably the key for the establishment of DRM technology is the level of interconnection between hardware and software modules and the integration methods to a DRM solution that the customer and the companies can trust. The previous generation of DRM solutions was deployed mainly in software and thus was vulnerable to attack. The early DRM solutions were fragmented and attempted to work by themselves being incompatible by design and not having trusted hardware to rely on. They were also designed as static closed devices. Thus, multilevel hardware and software modules must set to work together in a way that the users are able to easily understand (openness) and also the issue of trust as regards as intellectual property is guaranteed.

Finally, although no technical solution can be perfectly designed, the future of DRM systems finally embraces the concepts of system renewability and key revocation. These evolutionary concepts are very important to be addressed providing a very promising research field for the future.

3. Digital Watermarking in-depth

Digital watermarking is one of the most important parts of a DRM system and mainly the tool which provides copyright protection, proof of ownership, content authenticity and the transaction management infrastructure. In this section the most recent trends in digital watermarking for multimedia content are being analysed. Due to the nature of digital watermarking referring to in-detail technological aspects is inevitable and necessary so as to shed light to the objectives and complexity of digital watermarking. This section hosts also an overview of watermarking techniques used in DRM applications, the progress of the field in protecting digital image and video and a new research regarding the protection of JPEG 2000 images.

3.1. Digital Image Watermarking Techniques for DRM applications

The need to safeguard the property rights of multimedia content from an unauthorised copying and the possibility to determine the true owners of the asset can be faced by resorting to efficient digital watermarking systems. This section presents a mathematical formulation to define a digital watermarking system and describes the general requirements to be satisfied by it, with more emphasis given to the aspects of security, robustness and imperceptibility. Finally, the use of watermarking systems in the framework of a DRM is deeply analysed.

3.1.1. Introduction

Data hiding technology, introduced in the early nineties allows to hide a signal or some information into a digital content (an audio file, a still image, a video sequence or a combination of the above), usually named host data.[223] To embed the hidden information in the host data, data hiding techniques apply minor modifications to the host content in an imperceptible manner, where the modifications are related to the embedded information.

The hidden information can be retrieved afterwards from the modified content by detecting the presence of these modifications by means of computing operations.

In general, data hiding technologies allow to provide a communication channel multiplexed into original content, through which it is possible to transmit some information, depending on the application at hand, from a sender to a receiver.[224] In the first years, the research on data hiding was mainly devoted to offer a solution to the problem of copyright protection of digital content.

Copyright protection of multimedia data has been accomplished in the past by means of cryptography algorithms to provide control over data access and to make data unreadable to non-authorised users. However, encryption systems do not completely solve the problem, because once encryption is removed there is no more control on the dissemination of data; a possible solution is given by data hiding of multimedia works to allow their dissemination to be tracked. In this way the number of permitted copies is not limited, but the possibility exists to control the path the original work has been disseminated through.

In this class of application, data hiding was termed digital watermarking, and the hidden information, defined digital watermark, was some code conveying information related to the creator, the distributor, the customer, or licensing terms between them.

According to this design, in the realisation of really effective DRMSs watermarking technologies can undoubtedly play an important role. In fact the need to safeguard the property rights of the multimedia content from an unauthorised copying and the possibility to determine the true owners of the asset can be solved through the use of efficient digital watermarking systems.

---

223 Barni, M., & Bartolini, F., (2004). Watermarking Systems Engineering: Enabling Digital Assets Security and Other Applications. Marcel Dekker (Ed). Cox, I., Miller, M. L. & J. A. Bloom. (2002) Digital watermarking. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc.

224 Kalker, T. (2001). Considerations on watermarking security. In IEEE Multimedia Signal Processing, MMSP'01 Workshop, (pp. 201–206). Cannes, France.

The section is organised as follows. First of all, a mathematical definition and the general requirements of digital watermarking are listed and briefly discussed, with more emphasis given to the aspects of security, robustness and imperceptibility. Next, the use of watermarking systems in the framework of a DRM is analysed. Finally, future trends are discussed and the conclusions are drawn.

3.1.2. Mathematical formulation of the watermarking problem

A digital watermarking system can be modelled as described in Figure .[225] The inputs of the system are certain application dependent information, and the original host content, that could be an audio file, an image or a video sequence, here indicated as *C*. The to-be-hidden information is usually represented as a binary string $\boldsymbol{b} = (b_1,b_2,\ldots,b_k)$, referred as the watermark code. The watermark embedder hides the watermark code ***b*** into the host asset **C** to produce a watermarked content **Cw**, usually making use of a secret information *K* needed to tune some parameters of the embedding process and to allow the recovery of the watermark only to authorised users having access to that secret information.

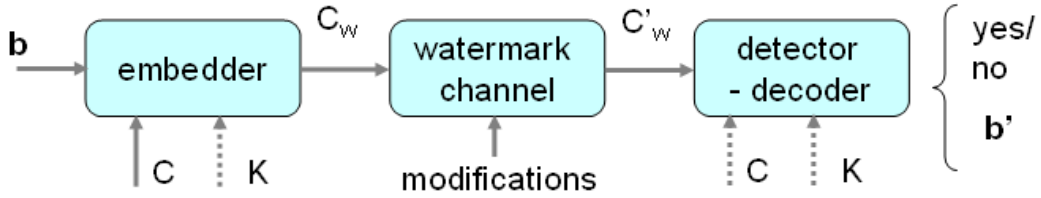

Figure 6: The proposed model describing a digital watermarking system.

The functionalities of the watermark embedding process can be further split into three main tasks: information coding; data embedding; watermark concealment, as indicated in Figure .
With *information coding*, the information message ***b*** is transformed into a watermark signal $\boldsymbol{w} = (w_1,w_2,\ldots,w_n)$ which is more suitable for embedding in the content. As it happens in a digital communication system, the watermark code ***b*** may be used to modulate a much longer spread-spectrum sequence, or it may be transformed into a bipolar signal, or it may be mapped into the relative position of two or more pseudo-random signals in the case of position-encoded-watermarking.

Eventually, ***b*** may be left as it is, thus leading to a scheme in which the watermark code is directly inserted within the host. In this case the watermark signal ***w*** coincides with the watermark code ***b***.
Moreover, before coding, the watermark code may be channel-coded to increase robustness against possible attacks. As a matter of fact, it turns out that channel coding greatly improves the performance of any watermarking system.

In *data embedding*, given the host asset *C*, the watermark signal ***w***, and, possibly, a key K, the watermarked content is generated by an embedding function. To embed the watermark code into the original content, watermarking techniques apply minor modifications to the host data in a perceptually invisible manner, where the modifications are related to the to-be-hidden data. In general, embedding is achieved by modifying a set of features $\boldsymbol{f} = (f_1, f_2, \ldots, f_n)$ extracted by the host content, with the watermark signal ***w***, according to a proper embedding rule that depends on the particular watermarking scheme, obtaining a set of watermarked features $\boldsymbol{f_w} = (f_{w1}, f_{w2}, \ldots, f_{wn})$. The modified features are then reinserted into the content on behalf of the original ones, thus obtaining the watermarked content.

The main concern of the embedding part of any data hiding system is to make the hidden data imperceptible. This requirement is satisfied through the *watermark concealment* procedure, that can be achieved either implicitly, by properly choosing the set of host features to be modified and the embedding rule, or explicitly, by introducing a concealment step after watermark embedding; in this case, the original content *C* is usually required. To accomplish this task, the properties of the human senses must be carefully taken into account, since imperceptibility ultimately relies on the exploitation of the imperfections of such senses. Thereby, still image and video watermarking will rely on the characteristics of the Human Visual System (HVS), whereas audio watermarking will exploit the properties of the Human Auditory System (HAS).

[225] Barni, M., & Bartolini, F., (2004). Watermarking Systems Engineering: Enabling Digital Assets Security and Other Applications. Marcel Dekker (Ed).

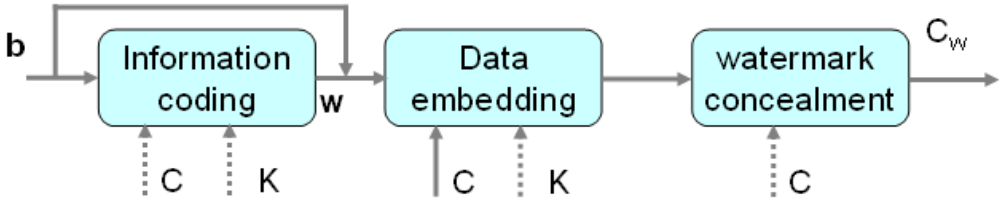

Figure 7: The watermark embedding process can be divided into 3 steps.

The second element of the model represented in Figure , the *watermark channel,* takes into account for all the processing operations and manipulations, both intentional and non-intentional, the watermarked content may undergo during its distribution and fruition, so that consequently the watermarked content can be modified into a new version $\mathbf{C'}_w$.

The third element of the model is the tool for the recovery of the hidden information from $\mathbf{C'}_w$: the extraction of the hidden data may follow two different approaches: the detector can look for the presence of a specific message given to it as input, thus only answering yes or no, or the system (now called decoder) reads the sequence of bits hidden into the watermarked content without knowing it in advance. These two approaches lead to a distinction between *readable* watermarking algorithms, embedding a message that can be read, and *detectable* watermarking algorithms, inserting a code that can only be detected. In the former case, the bits contained in the watermark can be read without knowing them in advance; in the latter case, one can only verify if a given code is present in the document, i.e. the watermark can only be revealed if its content is known in advance. Detectable watermarking is also known as 1-bit watermarking since, given a watermark, the output of the detector is just *yes* or *no*. Note that in readable watermarking, the decoding process always results in a decoded bit stream, however, if the asset is not marked, decoded bits are meaningless.

An additional distinction may be made between systems that need to know the original content *C* in order to retrieve the hidden information, and those that do not require it. In the latter case we say that the system is *blind*, whereas in the former case it is said to be *non-blind*.

Another distinction of the algorithms can be done on the basis of the key *K* used in the decoding/detection process. If the secret key for the detection/decoding process is the same used for embedding, we refer to *symmetric* watermarking schemes. These techniques present an intrinsic lack of security, since the knowledge of *K* is likely to give attackers information sensitive for the removal of the watermark from the watermarked content. In order to overcome the above problems, increasing attention has been given to the development of *asymmetric* methods.[226] In such schemes two keys are present, a private key, K_s, used to embed the information within the host signal, and a public key, K_p, used to detect/decode the watermark (often K_p is just a subset of K_s). Knowing the public key, it should be neither possible to deduce the private key nor to remove the watermark (unlike in asymmetric cryptography, knowledge of K_s may be sufficient to derive K_p; additionally, the roles of the private key and the public key can not be exchanged). More details about the importance of asymmetric watermarking in security oriented applications may be found in the work of Barni.[227]

3.1.3. Requirements

The requirements which the watermarking techniques have to fulfil are briefly described in this chapter. Whereas the three most important ones, that is *security*, *robustness* and *imperceptibility* will be described in the next three subsections, in the sequel the others will be briefly discussed.

Depending on the application at hand, the watermarking algorithm should allow a predefined number of bits to be hidden (defined *payload* or watermark *capacity*). General rules do no exist here, however, system designers should keep well in mind that the number of bits which can be hidden into data is not unlimited, nay very often is fairly small.

[226] Furon, T., Venturini, I., & Duhamel, P., (2001). An unified approach of asymmetric watermarking schemes. In E.J. Delp and P.W. Wong (Ed.), Security and Watermarking of Multimedia Contents III, Proc. SPIE, Vol. 4314 (pp. 269-279). San Jose, CA.

[227] Barni, M., Bartolini, F., De Rosa, A., & Piva, A., (2003). Optimum decoding and detection of multiplicative watermarks. IEEE Transactions on Signal Processing 51 (4), 1118-1123. Barni, M., Bartolini, F., & Furon, T., (2003). A general framework for robust watermarking security. Signal Processing 83 (10), 2069–2084.

Even in the absence of attacks or signal distortions, the probability of failing to detect the embedded watermark (false-negative error probability) and of detecting a watermark when, in fact, one does not exist (false- positive error probability), must be very small (*trustworthy detection*). Usually, statistically-based algorithms have no problem in satisfying this requirement, however such an ability must be demonstrated if watermarking is to be legally credible.

It should be possible to embed a set of different watermarks in the same image, in such a way that each code can be detected by the authorised user (*multiple embedding*). This feature is useful in fingerprinting applications, where the copyright property is transferred from the content owner to other customers. Moreover, we can not prevent someone from watermarking an already watermarked work.

Great attention should be given to watermark invertibility as well. Craver et al.[228] stated that for a watermarking scheme to be successfully used to demonstrate rights ownership, non-invertibility of the watermark has to be granted. Furthermore, this is only a necessary condition to be satisfied, since, more generally, non-quasi-invertibility is needed. Without going into much details, we can say that a watermark is invertible if it is possible to generate a false watermark and a fake original document which is perceptually equal to the true one, such that by embedding the false watermark in it a document which is equal (*invertibility*) or perceptually equal (*quasi invertibility*) to the true marked one is obtained.

Security

At dawn of watermarking systems, performances were measured by proving them with respect to different issues such as payload, perceivability and robustness. In particular, this last one was felt as mandatory to grant algorithm resistance against a possible attacker who acted by means of various image processing tools such as filtering, colour changing, compression, geometric transformations and so on. Anyway, not too much consideration has been paid to analyse problems related to system security, that is to determine if there was one or more weak links to permit an attacker to circumvent the whole system or to use it in illegal manner. In fact, with the term *attacks to security* has to be intended all those strategies that a hacker can put in practice, on the basis of what he knows and he does not, to fake the response of the watermarking algorithm. Only recently, it has been started to give relevance to this kind of problem and to reconsider most of the design approach from this new point of view. This is mainly due to the fact that when watermarking systems, apparently robust, have been tested in an actual insecure environment they have miserably failed. Open challenges like the one recently proposed in the BOWS (Break Our Watermarking System) contest has to be considered on this line.[229]

Before starting the discussion it would be interesting to give a basic definition of what is intended with the term security talking about watermarking. In literature many celebrate phrases which deal with security exist. In particular we would like to cite one that is maybe the eldest and that focuses on a message to be kept in mind when debating on security, not only of watermarking systems. This is the *Kerchoffs* law[230] that establishes that *security cannot be based on algorithm secrecy but on one or more secret keys used by the algorithm itself*. After having reported this important paradigm, let us try to propose a general definition for security in watermarking framework among the various that can be found in literature and that will be adopted as reference: *security refers to the inability of unauthorised users to access the additional channel created with watermarking.*[231] The main difficult when talking about security in watermarking is the lack of a defined general framework in which globally analyse all the elements involved in security aspects and, almost always, it is necessary to refer, time to time, to a specific application case; usually, in fact, it is the application at hand which determines ad-hoc requirements and levels of security.

Sometimes, anyway, there are some important issues to be taken into account and that can constitute a sort of a “best practice” to follow when a watermarking algorithm is called to operate:

---

228 Craver, S., Yeo, B., & Yeung, M., (1998). Technical Trials and Legal Tribulations. Communications of the ACM 41 (7), 44-54.

229 BOWS-2: Break Our Watermarking System 2nd Ed., (2007). From http://bows2.gipsa-lab.inpg.fr.

230 Kerckhoffs, A. (1883). La cryptographie militaire. Journal des sciences militaires, IX, 5–83.

231 Kalker, T. (2001). Considerations on watermarking security. In IEEE Multimedia Signal Processing, MMSP’01 Workshop, (pp. 201–206). Cannes, France.

- what is available to the attacker to help his illegal action;
- which kind of attack procedure the attacker can put in practice;
- what the attacker wishes to do.

What is available to the attacker to help his illegal action

The first issue regards the definition of what the hacker knows and/or owns to succeed in making a successful action. The greater the information the easier the attack to security: the effort to be done by the attacker in terms of resources (e.g. computational time, number of attempts, etc.) is reduced by any availability he has. First of all, it has to be considered if the attacker can benefit of the knowledge of the watermarking algorithm (public algorithm) to perform, for instance, a reverse engineering operation by selecting the watermarked features. He also could have at his disposal the decoding/detection system, and on the basis of which software/hardware devices he has access to, being helped in performing his action. In such a situation he could read the embedded code or on the contrary he could have access only to the detector, in this case he can realise if a watermark is present or not, but not which information has been encoded. Similar considerations can be made for the eventuality that the attacker has the knowledge of one or more secret keys used by the algorithm during the watermark embedding and/or the watermark extraction phases. Another crucial issue to be analysed concerns the possibility that the hacker owns multiple watermarked copies so he can check more than one copy of the same watermarked asset or different documents watermarked with the same system and try, by means of a certain analysis (e.g. making a collusion attack), to understand something more on the watermarking algorithm he is cracking or make it fails.[232]

Which kind of attack procedure the attacker can put in practice

Another issue to be considered basically concerns the manner the attacker performs his action, in fact in the "game" between him and the watermarking system designer, he can play *fairly* or *unfairly*. In the first case, the attacker only uses the means and the knowledge he has got and tries to carry out diverse kinds of attack that are feasible according to the application at hand and to the specific characteristics of that system; he can analyse the algorithm to understand if there exists one or more trojan horses to fool the system. Many are the attacks that have been proposed in literature depending on the application such as sensitivity attack, Holliman&Memon attack, collage attack, etc. In the second case, the hacker tries to illegally discover some secret information (e.g. secret keys, watermarking parameters), he does not possess, to use them to crack the system and does it in every possible way. It is obvious to comprehend that in a real application framework the hacker will be always an unfair player and this is the less favourable situation for the watermark designer.

What the attacker wishes to do

The third issue to be evaluated concerns what the hacker could wish to achieve through his illegal action and how much sophisticated is the result he wants to obtain. It also depends on the kind of watermark, if it is robust or fragile, and partially if this watermark is adopted for an application such as authentication or copyright protection. A common malevolent activity performed could be to decode the hidden bits; in this case the attacker wishes to read the information encoded within the digital object to possibly re-encode it into a fake document. Other actions might be to destroy hidden bits (the attacker only wants to erase the message the watermark carries, obviously this action is simpler), to alter the hidden bits (the attacker tries to modify the hidden bits to insert a proper information for creating a fake document) or to make undetected modifications, in this circumstance the attacker is not interested in making the watermark unreadable or undetectable but he wants to perform some small modifications that are not revealed by the decoder, this is the

[232] Doerr, G., & Dugelay, J. L., (2003). New intra-video collusion attack using mosaicing. In IEEE International Conference Multimedia Expo., Vol. II (pp. 505-508). Baltimora, USA. Caldelli, R., Piva, A., Barni, M., & Carboni, A., (2005). Effectiveness of ST-DM watermarking against intra-video collusion. In 4th International Workshop on Digital Watermarking, IWDW 2005, LNCS Vol. 3710 (pp. 158–170). Siena, Italy.

specific case of digital asset integrity. Sometimes the pirate could want to leak some information to perform a successive unauthorised action against the watermarking system, for instance, trying to understand which are the secret keys.

After having introduced which are the basic rules to be attended to improve security of a watermarking system, it is also proper to point out that a substantial help could come from the integration of watermarking algorithms with cryptography tools, at the protocol level. As compared with watermarking, in fact, cryptography allows to establish the security level of a technique more formally, and many secure tools have been developed and largely used today. Starting from this, some interesting solutions have been recently proposed in the field of Zero-Knowledge Watermarking (ZKW).[233] With the use of such techniques, it is possible to reduce the amount of sensible information that is exchanged among the untrustworthy players (e.g. during a transaction within a DRM system).

Robustness

One of the merits of watermarking technology is to embed directly the informative data in the content without resorting to an attached header, but, on the other side, this can lead to a loss of information each time the host data are undergone to any transformation or processing. W*atermark robustness* refers to the capability of the hidden message to survive possible host signal manipulations. It is important to point out what is intended with the term "host signal manipulations" to better differentiate the case of robustness by that of security, treated in the previous section. Usually manipulations are divided into two categories: *non-malicious* which do not explicitly aim at removing the watermark or at making it unreadable, and *malicious* manipulations, which precisely aims at damaging the hidden information.[234]

Roughly speaking we could say that the first class deals with robustness of the watermark, that is the watermark algorithm must tolerate those attacks that can occur during the normal use of the asset. Their nature and strength is strongly dependent on the application for which the watermarking system is devised; among these we have lossy compression, geometric and temporal manipulations, digital to analogue conversion, extraction of asset fragments (cropping), processing aimed at enhancing asset quality (e.g. noise reduction), etc.

Consequently, we can asses that the second class (malicious) refers to watermark security, that is the watermarking technique must be invulnerable with respect to an attack (e.g. collusion, sensitivity) whose main goal is just to remove or make the watermark unrecoverable. Sometimes, within this category of attacks, there is a further subdivision between *blind* (do not exploit any knowledge on the algorithm) and *informed* (exploit some knowledge on the algorithm). It is quite immediate to understand that the border between robustness and security is not well drawn, in fact it can happen that normal non-malicious transformations such as filtering can be adopted by themselves or together with other security attacks, for malevolent purposes.

Anyway, after this distinction, it is worth trying to propose a qualitative evaluation of the level of required robustness the hidden data must guarantee by referring to four general cases, usually considered in literature, in fact it would not be possible to establish a precise degree of robustness without fixing a specific application in which the watermarking algorithm is called to work.

Let us see these four cases:

- Secure watermarking: this case encompasses copyright protection, ownership verification or other security-oriented applications and the watermark must survive both non-malicious and malicious manipulations. In secure watermarking, the loss of the hidden data should be achievable at the expense of a significant degradation of the quality of the host signal and consequently a depreciation of the digital asset. When considering malicious manipulations it has to be assumed that the attackers know the watermarking algorithm and thereby they can conceive ad-hoc watermark removal strategies. As to non-malicious manipulations, they include a huge variety of digital and analogue processing tools, including lossy compression (e.g. JPEG/JPEG-2000), linear and non-linear filtering, cropping, editing, scaling, D/A and A/D conversion, analog duplication, noise addition, and many others that apply only to a particular type of media. Thus, in the image case, we must consider zooming and shrinking, rotation, contrast enhancement, histogram manipulations, row/column removal or exchange; in the case of video we must take into account frame removal, frame exchange, temporal filtering, temporal resampling; finally,

[233] Adelsbach, A., Katzenbeisser, S., & Sadeghi, A.-R., (2002). Crytpography meets watermarking: detecting watermarks with minimal or zero knowledge disclosure. In XI European Signal Processing Conference, EUSIPCO' 02, Vol. I (pp. 446–449). Toulouse, France.

[234] Barni, M., & Bartolini, F., (2004). Watermarking Systems Engineering: Enabling Digital Assets Security and Other Applications. Marcel Dekker (Ed).

robustness of an audio watermark may imply robustness against echo addition, multirate processing, reverb, wow-and-flutter, time and pitch scaling. It is, though, important to point out that even the most secure system does not need to be perfect, on the contrary, it is only needed that a high enough degree of security is reached. In other words, watermark breaking does not need to be impossible (which probably will never be the case), but only difficult enough.

- Robust watermarking: in this case it is required that the watermark be resistant only against non-malicious manipulations. Of course, robust watermarking is less demanding than secure watermarking. Application fields of robust watermarking include all the situations in which it is unlikely that someone purposely manipulates the host data with the intention to remove the watermark. At the same time, the application scenario is such that the, so to say, normal use of data comprises several kinds of manipulations which must not damage the hidden data. Even in copyright protection applications, the adoption of robust watermarking instead than secure watermarking may be allowed due to the use of a copyright protection protocol in which all the involved actors are not interested in removing the watermark.
- Semi-fragile watermarking: this is the case of applications in which robustness is not a basic requirement, mainly because the host signal is not intended to undergo any manipulations, but a very limited number of minor modifications such as moderate lossy compression, or quality enhancement. This is the case, for example, of data labelling for improved archival retrieval, in which the hidden data is only needed to retrieve the host data from an archive, and thereby it can be discarded once the data has been correctly accessed. It is likely, though, that data is archived in compressed format, and that the watermark is embedded prior to compression. In this case, the watermark needs to be robust against lossy coding. In general, a watermark is considered as semi-fragile if it survives only a limited, well-specified, set of manipulations leaving the quality of the host document virtually intact.
- Fragile watermarking: a watermark is said to be fragile, if the information hidden within the host data is lost or irremediably altered as soon as any modification is applied to the host signal. Such a loss of information may be global, i.e. no part of the watermark can be recovered or local, i.e. only part of the watermark is damaged. The main application of fragile watermarking is data authentication, where watermark loss or alteration is taken as evidence that data has been tampered with, whereas the recovery of the information contained within the data is used to demonstrate data origin.

Furthermore, after this classification for the diverse degrees of robustness, we can generally say that robustness against signal distortion is better achieved if the watermark is placed in perceptually significant parts of the signal. This is particularly evident if we consider the case of lossy compression algorithms, which operate by discarding perceptually insignificant data not to affect the quality of the compressed image, audio or video. Consequently, watermarks hidden within perceptually insignificant data are likely not to survive compression. Achieving watermark robustness, and, to a major extent, watermark security, is one of the main challenges watermarking researchers are facing with, nevertheless its importance has sometimes been overestimated at the expense of other very important issues such as watermark capacity and protocol-level analysis.

Imperceptibility

As stated in the previous sections one of the main requirements a watermarking system must satisfy is the possibility of making the embedded watermark imperceptible to a human observer. Such a requirement has two main reasons: one concerning a quality point of view, i.e. the watermarked content should not be degraded by the watermark insertion, but on the contrary it should be perceptually identical to the original content; the other reason is from a security point of view, i.e. possible hackers should be prevented from locating if and where the hidden information has been embedded within the original data. Since in most of the cases the end users of the watermarked content are human observers or listeners (e.g. an exception occurs when watermarking is used for remote sensing multispectral images, for which invisibility should be granted with respect to classification tools), the importance of having a good knowledge of the characteristics of the *Human Visual System* (HVS) and *Human Auditory System* (HAS) appears with evidence. In fact, having a clear idea of the mechanisms underlying the perception of visual and auditory stimuli can help in fine tuning the watermark embedding phase for making the embedded signal imperceptible; in particular it is important to know how the user is able to perceive or not perceive certain stimuli. In the following we describe the main principles characterising the HVS (firstly) and the HAS (secondly).[235]

[235] Barni, M., & Bartolini, F., (2004). Watermarking Systems Engineering: Enabling Digital Assets Security and Other Applications. Marcel Dekker (Ed).

Even if the *Human Visual System* is certainly one of the most complex biological devices far from being exactly described, each person has daily experience of the main phenomena which influence the ability of the HVS to perceive (or not to perceive) certain stimuli.

By observing two copies of the same image, one being a disturbed version of the other, it is readily seen where the noise is more or less visible, thus letting to derive some very general rules:

- disturbs are less visible in highly textured regions than in uniform areas;
- noise is more easily perceived around edges than in textured areas, but less easily than in flat regions;
- the human eye is less sensitive to disturbs in dark and bright regions.

In the last decades, several mathematical models have been developed to describe the above basic mechanisms. Basically, a model describing the human visual perception is based on two main concepts: the *contrast sensitivity function* and the *contrast masking model*.

The first concept is concerned with the sensitivity of the human eye to a sine grating stimulus; as the sensitivity of the eye depends strongly on display background luminance and spatial frequency of the stimulus (as evidenced by the general rules reported above), these two parameters have to be taken into account in the mathematical description of human sensitivity. The second concept considers the effect of one stimulus on the detectability of another, where the stimuli can be coincident (*iso-frequency masking*), or non coincident (*non iso-frequency masking*) in frequency and orientation; specifically the masking effect indicates the visibility reduction of one image component due to the presence of other components. A mathematical model which considers all the recalled phenomena should result in an equation that provides the minimum level of contrast (i.e. the *Just Noticeable Contrast - JNC*) necessary to just detect a sine wave of a given frequency and orientation superimposed to another stimulus (the masking one) at a given frequency and orientation.

Regarding the *Human Audio System*, it is still possible to give a mathematical formula that indicates the minimum level sound (i.e. the *Sound Pressure Level - SPL*) necessary to a young listener with acute hearing to perceive, in a quiet environment, a pure tone stimulus at a given frequency. In addition it has to be taken into account the *masking effect*, that is the phenomenon by which a sound stimulus is not perceived by the HAS if it is near in frequency to another higher level stimulus. Such a masking effect depends on the characteristics of the two considered sound stimuli: specifically, if the stimulus is a pure tone or a narrow band stimulus (also called noise sound). It is convenient to distinguish three cases: 1) a noise sound masking a pure tone sound; 2) a pure tone sound masking a noise sound; 3) a noise sound masking a noise sound. The first case is the more effective one and the pure tone is easily masked by the noise sound (we suppose that the pure tone signal has frequency equal to the central frequency of the band of the noise sound): if the masking signal has a SPL around 5 *dB* higher than the SPL of the pure tone, it completely masks the pure tone. In the other two cases, the SPL of the masking signal must exceed the SPL of the stimulus to be masked more than 20 dB. Of course, when the frequencies of the two considered sound stimuli do not correspond, the detection threshold is reduced, proportionally to the distance between the frequencies.

After the analysis of the models of human perception, let us see how such concepts can be exploited for better hiding information into host content. Basically, we distinguish two different approaches for considering HVS / HAS characteristics during the data embedding process. The former approach considers the selection of appropriate features that are most suitable to be modified, without dramatically affecting perceptual content quality; in other words, the idea is to locate which features can better mask the embedded data. By following the second approach, the inserted data, embedded into the host content without a particular care for the selection of the most suitable features, are adapted to the local content for better reducing their perceptibility.

Let us first consider the concealment process through *feature selection*. In this case a set of features belonging to the host content has to be properly selected for the watermark embedding. But there is the binding requirement that, for a correct recovery of the watermark, the same set of features are identified for the detection/decoding phase, thus imposing an a-priori fixed choice. To be more explicit, let us make an example concerning the choice of the features in the *host content domain*. By taking into account that disturbs are less visible in highly textured regions than in uniform areas, one can choose to watermark those blocks of the content that have a large degree of texture: a simple function can measure the variance of the block and based on this value classifies it as suitable or not suitable for embedding. During the recovery phase, any processing applied to the watermarked content, could modify the classification produced by the same function, thus making the selection of the blocks really unpredictable.

The situation is different in the case of the *transformed domain* techniques. In general we have in fact seen that both the HVS and the HAS are less sensitive to disturb having high or very low frequencies; it is then common to partition the

frequency range into two regions, one of which used for the embedding step. Since this partition is fixed, and not estimated time by time during the embedding phase, the problem outlined for the host content domain case does not raise now. In particular, the choice of the frequency range to be watermarked is a compromise between the imperceptibility and the robustness requirement, since the high frequencies will be the first to disappear due to many common attacks such as compression, low-pass filtering, etc..

Similar considerations are valid for the *hybrid techniques*. In particular the situation for block-based transforms is identical as for the transform domain case, high frequency coefficient are usually preferred for watermark embedding, in order to reduce watermark perceptibility. The same objective can be reached in the DWT (Discrete Wavelet Transform) case by performing embedding in the finest sub-bands.

We can conclude that perceptual data hiding through feature selection is not very easy to be performed. In particular, if it is desired that watermark recovery has to be achieved also after possible attacks, that can make the selected features no longer available or identifiable, the sole possibility is to select the features on a fixed basis. This choice, nevertheless, implies that the embedded data are not always inserted into the most suitable image features.

The other possibility for perceptual watermarking is to perform concealment through *signal adaptation*: in the following we briefly describe two possible approaches for adapting the watermark signal to the local host content.

In the first case we make use of *perceptual masks* giving a measure of the insensitivity to disturbs for each sample of the host content. Let us suppose to have a copy of the content $\mathbf{C_W}$ watermarked without taking care about perceptibility issues (e.g. uniformly) and the original host content $\mathbf{C}$. If the perceptual mask $\mathbf{M}$ taking values in [0,1] has the same dimensions of the content, we can obtained a perceptual watermarked content $\mathbf{C'_W}$ by mixing $\mathbf{C}$ and $\mathbf{C_W}$ through $\mathbf{M}$:

$$\mathbf{C}'_{\mathbf{w}} = \overline{\mathbf{M}} \otimes \mathbf{C} + \mathbf{M} \otimes \mathbf{C}_{\mathbf{W}},$$

where $\otimes$ is the sample by sample product, and $\overline{\mathbf{M}}$ is the masking function whose elements are the complement to 1 of the elements of $\mathbf{M}$. Let us note that such an approach is valid apart from the domain where watermark embedding has been performed and the embedding rule. An example of a watermarking system based on signal adaptation through perceptual masks is given in the following when the scheme proposed by Piva et al. is described.[236]

Following the second approach for concealment through *signal adaptation*, we make use of a criterion establishing the maximum amount of modification that can be sustained by the host data: this can be defined both in the host content domain (independently on the features used for embedding) or directly in the embedding features domain. It is defined an imperceptibility region around the host data: if watermark embedding brings the host data outside this region, hence the applied modifications will be perceptible, otherwise no. When the imperceptibility region is not defined in the same domain where embedding is performed, it is possible to use optimisation techniques for tuning the strength of the watermark signal in the embedding domain in such a way to satisfy the imperceptibility constraint in the domain where this is defined. An example of this approach has been described by Pereira et al.[237], where the perceptibility constraint is defined in the spatial domain, while the embedding is performed in the block DCT domain. In the case in which the imperceptibility constraint is given in the same domain where the embedding is performed, the simplest imperceptibility region is defined component wise, i.e. a maximum possible modification is given for each component of the host feature set. As an example, for an image watermarking scheme working in the hybrid block DCT domain, for each frequency coefficient of the block a perceptual threshold imposing a limit on the watermarked coefficients is fixed by referring to the default quantisation matrices defined in the compression algorithm (e.g. JPEG). A more refined model defining the imperceptibility threshold for each frequency coefficient in the DCT blocks, has been proposed by Watson and takes into account the iso-frequency masking effect.[238]

3.1.4. Watermarking based DRM

[236] Piva, A., Barni, M., Bartolini, F., Cappellini, V., De Rosa, A., & Orlandi, M., (1999). Improving DFT Watermarking robustness through optimum detection and synchronisation. In GMD Report 85, Multimedia and Security Workshop at ACM Multimedia '99 (pp. 65-69). Orlando, Florida.

[237] Perreira, S., Voloshynovskiy, S. & Pun, T. (2000) Optimised wavelet domain watermark embedding strategy using linear programming. SPIE AeroSence 2000: Wavelet Applications VII, H. H. Szu, (Ed.), (April 2000, Orlando, FL).

[238] Watson, A.B., (1993). DCT quantisation matrices visually optimised for individual images. In Human Vision, Visual Processing and Digital Display IV, Proc. SPIE, Vol. 1913 (pp. 202-216). Bellingham, WA.

The problem of digital content piracy is one of the major problem to be solved in the world of ICT and technical instruments are to be provided to avoid that major content producers risk seeing their business being drastically reduced because of the ease by which digital contents can be copied and redistributed for instance in P2P infrastructures. This is the reason why digital rights management systems (DRMS) have been indicated, in the last years, like a possible answer to such a claim and much attention both from industry and from research has been dedicated to these systems.[239]

Among the various technologies that can contribute to set up a reliable DRM system, digital watermarking has gathered much approval, basically thanks to its potentiality of persistently attaching some additional information to the content itself. Many potential applications such as ownership proofing, copy control, user tracking and so on, could be implemented by resorting to a DRMS based on data hiding techniques. DRM technology could benefit from digital watermarking in several ways, as it is evident by the variety of watermarking- based systems addressing DRM problems proposed in the literature.

Trying to give a general definition of what a DRM system is seems to be quite arduous, anyway a *DRMS can be considered as an ensemble of services, connected through a network environment, co-operating together, to allow the protection of the IPR of multimedia data, on the basis of terms and conditions agreed among the involved parties, and to control their delivery and usage.*

DRM can make possible for commercial publishers to distribute valuable content electronically, without destroying the copyright holder's revenue stream. DRM can also be used in other settings to enable safe distribution of digital content including, for example, document management within and between corporations, protected email, medical patient records handling, and government service access.

At a minimum, a well-designed DRM system should provide:

- *Governance*: DRM is different from classical security and protection technologies. Conventional media distribution systems based on conditional access techniques protect media during transmission using a control model based on direct cryptographic key exchange. DRM systems, on the other hand, implement control, or governance, via the use of programming language methods executed in a secure environment.
- *Secure Association of Usage Rules with Information*: DRM systems securely associate rules with content. These rules determine usage of the content throughout its lifecycle. Rules can be attached to content, embedded within content (e.g., via watermarking), or rules can be delivered independently of content.
- *Persistent Protection*: DRM systems are designed to protect and govern information on a persistent basis throughout the content's commercial lifecycle. Protection is frequently provided using cryptographic techniques. Encrypted content is protected even as it travels outside of protected distribution channels.

According to the previous classification and to better highlight the different composing parts, a complete technological scheme which incorporates all possible means for rights management and protection can be treated as composed by two separated functional units:

- Digital Property Management (DPM): that is a system concerned with the management of intellectual property related to the contents. As described in the following, DRMS should include a set of services and solutions:
    - Identification Systems;
    - Metadata for IPR management;
    - Rights management programming languages;
    - Data Format definitions;
    - Delivery methods and technologies.
- Technical Protection Means (TPMs) or Digital Rights Enforcement (DRE): that is a set of technologies to secure and protect multimedia contents from an unauthorised use, and to enforce usage policies so that the content is used only for the terms and the conditions agreed during purchase. TPMs can include:
    - Security and integrity of OS and computer networks
    - Encryption of transferred data
    - *Watermarking of multimedia content*
    - Tracking the use of the protected content

[239] Kundur, D., Lin, C.-Y., Macq, B., & Yu, H., (2004). Special Issue on Enabling Security Technologies for Digital Rights Management. Proceedings of the IEEE, Vol.92 (6), 879-882.

These TPMs are called to work together within a DRM infrastructure and their action is usually complementary. In fact, for example, once the DRM system has identified the intellectual property of a given data, and has set the rules for its usage, it is necessary to grant that such rules are enforced, through a so called *persistent* content protection, that is the content protection has to stay with the content itself along all its life, from delivery to the users enjoyment. A digital content can be transferred securely to an user through Internet by means of cryptographic algorithms. However, cryptography systems do not solve the problem of unauthorised copying. Once an authorised user decrypts the work, there is no more control on his/her possible illegal actions: for example, the recipient could save and copy the content in an unprotected format and redistribute the digital copy to many other users without reduction in quality. Therefore, the protection problem in DRM systems goes beyond simply granting the access to the content only to authorised users, but concerns also the support of restrictions of the content usage rights also after the digital asset is delivered to the end user. All these problems are faced by the Technical Protection Means.

It is important to note that the security model where TPMs have to work is different from the common cryptographic model where there are two trusted parties trying to exchange a message in a way that an attacker sitting in between is unable to recover the information. In this case, it is not possible to separate honest and dishonest users. A malicious user (cracker), once the protected content is delivered to his/her device, may try to break the security system with unlimited time and resource. Since Internet is an open distribution channel, the attacker can publish his breaking tool on Internet, so that anyone can download it and crack the protection scheme.

In the light of these considerations, it is easy to understand that techniques such as *digital watermarking* can be particularly appreciated due to fact that they provide the chance to attach a code to a multimedia document in such a way that the code is persistent with respect to the possible changes of format the document may undergo. The digital insertion of marks to individualise, trace, and control usage of a digital copy, even when it is transformed into analog signals, will be one of the pillars of future DRM systems. To fully exploit the potentiality of this peculiar characteristic, the concept of persistent association has been developed during the past few years. The basic idea is to associate a unique identifier (UI) to each multimedia creation. The UI is embedded inside the document itself by means of a watermarking primitive and is used for indexing a database where more detailed information (not only related to IPR) can be retrieved (see Figure 8).

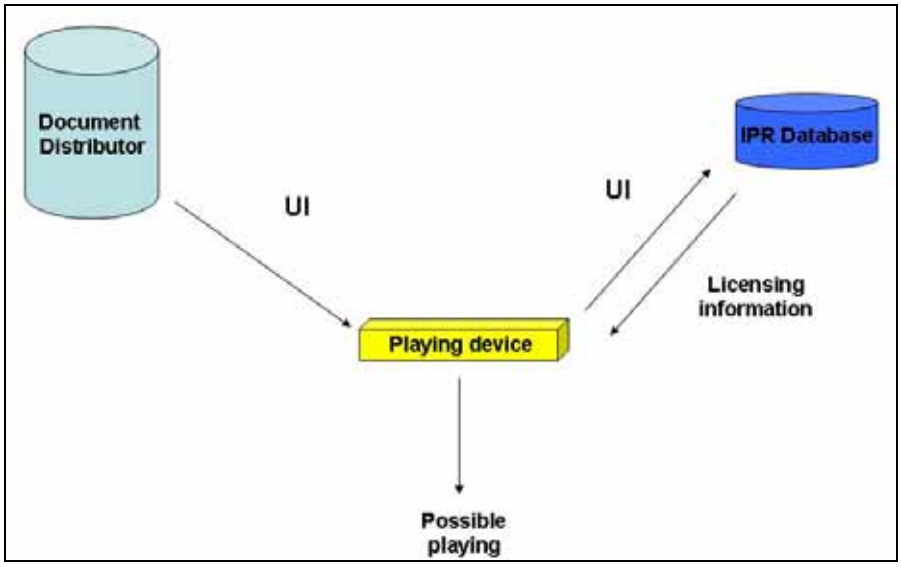

Figure 8: Persistent association of an UI to a multimedia document

In Figure 8 it is presented that a player can request the licensing information from an IPR database and, as a consequence, apply the corresponding copyright policy to the document.

The use of watermarking for tightly attaching a UI to a document has been widely proposed in diverse occasions such as the Content ID Forum Specification, in the framework of the MPEG-21 standardisation process and so on.[240]

[240] MPEG21, MPEG-21 Overview v5, Last checked: 11 October 2007, http://www.chiariglione.org/mpeg/standards/mpeg-21/mpeg-21.htm

Watermarking has been indicated as a basic tool to permit the implementation of several application scenarios mainly related to image/video distribution. On of these ones it is surely the digital cinema distribution in which the content exhibited in a theatre room is rescanned by a camera during the exhibition.. In this circumstance, watermarking allows to trace the room identification and time of a projection, In this kind of scenario, the retrieval of the parameters of an unauthorised copy can be helped by using the original version of the content. Another one could be the broadcast scenario, in which a specific content is broadcasted to set-top decoders; watermarking has to allow to trace the content and to control the copy. Another possible application might be the publication over the Internet of digital images/videos.

Each scenario has specific requirements regarding the watermarking technology to be deployed. First of all, the watermark should be able to survive the types of transformations typically encountered in the life of a document, including conversions to and from the analogue domain (i.e., the watermark should be robust). It is also required that the association created by means of watermarking is secure (i.e., it should resist transformations deliberately performed for removing it). Authorised users should be able to remove or at least change the status of the watermark, but when this is done without authorisation, it should be possible to obtain sufficient evidence of the former presence of a watermark to be used in forensic examinations. A DRM protocol based on the persistent identification of the multimedia document to be enjoyed should work by querying an IPR database with the UI extracted from the document and by analysing the returned licensing rules (MPEG-21 has been also investigating the standardisation of languages for the description of the rights associated with a multimedia document (MPEG-REL, 2003)) to decide if and how the document can be used. Such an approach allows a much higher flexibility than the simple protocols of ownership verification, copy control, or infringement tracking that we have seen above. The cost of this is a major complexity of the verification process that requires a trusted archive to be queried.

Finally, it is worth mentioning that the concept of persistent association, as approached by MPEG-21, can also have a wider scope: it is, in fact, foreseen that the persistent association could regard not only an UI but also transactions identifiers (thus implementing a generalised fingerprinting service), users, and temporal information (i.e., a time stamp).

Anyway, as we have previously seen, data hiding techniques can endure many types of attacks, and up to today no technique has exhibited enough resilience against all of them. These considerations urged researchers to find novel approaches to the problem of DRM, and there have been some proposals in which watermarking can still be helpful. The main assumption is that it is (at least today) almost impossible to design a secure watermarking technique, but it is really feasible to get a robust one. The main approach thus consists of trying to motivate users neither to attempt to remove the watermark nor to distribute the legally acquired and watermarked document for free. This could be obtained by assigning the function of enhancing the host data content to the watermark: as an example, the watermark could give access to discounts on other documents or to update services to a more sophisticated version of the document or to other added-value services (trials on other products, bonus programs, etc.).[241] In this way, the users would not be motivated to remove the watermark as this would deprive them of the associated advantages; they are not motivated to distribute the watermarked document as well since this would mean giving that advantages to others. Similarly, users would be not motivated to illegally acquire non-watermarked documents as this would not offer them the enhanced values associated with the watermark. This approach mainly requires that the watermark is resistant to the copy attack to avoid dishonest users transferring the advantages associated with a given document to another. Furthermore, the integration with effective cryptography protocols is required in order to avoid misuses. The use of a watermark associated with the added-value information, instead of the simpler format-header based approaches, is still motivated by the characteristic of persistence of the watermark. Indeed, this approach does not appear to be very effective: it would be really successful only if the added value services associated with the watermark were really of high value. On the contrary, what is of most interest for the widest part of the users is the document itself and not the possibly associated added values.

DRM in the Bricks Project: an example

The European project BRICKS (Building Resources for Integrated Cultural Knowledge Services)[242] has researched and implemented advanced open source software solutions for the sharing and the exploitation of digital cultural resources and can be an example of how transactions of digital items could be managed. The BRICKS Community is a worldwide federation of cultural heritage institutions, research organisations, technological providers, and other players

[241] Kalker, T., Depovere, G., Haitsma, J., & Maes, M., (1999). A video watermarking system for broadcast monitoring. In E.J. Delp and P.W. Wong (Ed.), Security and Watermarking of Multimedia Contents, Proc. SPIE, Vol. 3657 (pp. 103-112). San Jose, CA.

[242] Bricks Project, (2007). From http://www.brickscommunity.org/

in the field of digital libraries services. The BRICKS Cultural Heritage Network provides access to and fosters, through its architecture based on the B-Nodes, the European digital memory. In each B-Node a DRM module is implemented to deal with security issues. The role of the DRM module inside the BRICKS Security Architecture is basically that of defining and enforcing digital rights on content and services. The direct integration of a DRM component into the Security Architecture brings this functionality directly into the core of the BRICKS framework, ready to be leveraged by all the other services. In order to provide IPR protection, the following functionality is required.

Digital rights definition: the DRM Layer uses the MPEG 21 Rights Expression Language (REL) to define rights and conditions associated with the use and protection of digital content and services. The REL is defined as an XML based grammar. Its main functionality is to define rights, in term of which parties are allowed to use a resource, which rights they have and the terms and conditions that have to be fulfilled in order to be able to use those rights. MPEG-REL model provides the ability to map existing licenses such as Creative Commons, ROMEO, JORUM+, etc.

Digital rights enforcement: there is obviously no utility to define rights if they aren't enforced in any way. The DRM Layer cooperates with the Security Management Layer to block every user operation that can violate rights defined using the DRM tools.

Digital rights protection: once outside the BRICKS environment, the digital content must still be protected and its usage be traced. This kind of protection is implemented into the DRM module as a Watermarking and Data Encryption Service, that provides among other means to embed a reference to the license acquired to obtain a content and the ability to check if a content (an image in particular) has been downloaded from the BRICKS environment.

3.1.5. Future Trends

In the next future, DRM systems will probably continue to evolve in order to provide infrastructures for media distribution which can grant a higher level of interoperability and security, having to deal with heterogeneous consumer devices, media formats, communication protocols and security mechanisms. This effort, which also regards watermarking technologies, is mainly a technical effort and this is not enough to overcome the existing hurdles to achieve an interoperable and secure architecture for multimedia services. A standardisation process could help, but, as well-known, standards are rarely applied on a world-wide basis.

It is worth pointing out that given the social nature of DRMS, technologists must take into account the involved sensitive legal aspects to be able to design broadly accepted technologies.
So it is clear that DRM is a field of growing activity in which innovation interacts with emerging business models, legal policy and social norms. Due to this is easy to understand that an integrated action which involves technical aspects, legal issues, business policies and standards could lead to a feasible solution or, at least, to widely accepted models.

Strictly speaking from the point of view of watermarking technologies, it can be seen that scientific community has been researching, in the last years, much more in the field of security; in fact the requirement that a watermarking algorithm has to operate in a hostile environment (e.g. a component of a DRM system) in which a possible hacker might try to crack the process has become the new frontier for watermarkers. Open contests such as BOWS (Break Our Watermarking System)[243] and BOWS-2[244] that has been launched on the internet go in this direction. In each of these contests some images marked with an unknown watermarking algorithm have to be “unmarked” trying to maintain the better final perceptual quality; the participants could obviously use any approach they preferred to achieve the aim: exactly what happens when a DRM system, based on watermarking, is working in un-trusted scenario. Such a new trend in watermarking techniques design will probably better satisfy most of the needs that business models and media providers had in the past and surely still have nowadays, but that state-of-the-art solutions could not definitely match.

3.1.6. Conclusions

The conversion from analogue media to digital media has doubtless led to a large amount of benefits: in order to capitalise the digital content distribution and fruition, all the actors involved in such a digital chain must be assured in their own rights, e.g. the owner of a digital content wants to receive proceeds for selling it, whereas the buyer wants to make use, without restriction, of the content he bought. In the last years, Digital Rights Management Systems (DRMS) have been indicated as a possible solution for the promotion and the large diffusion of digital media distribution

[243] BOWS: Break Our Watermarking System, (2006). From http://lci.det.unifi.it/BOWS.

[244] BOWS-2: Break Our Watermarking System 2nd Ed., (2007). From http://bows2.gipsa-lab.inpg.fr.

environments. A DRM system can be considered as an ensemble of services, connected through a network environment, co-operating together, to allow the protection of the IPR of multimedia data, on the basis of terms and conditions agreed among the involved parties, and to control their delivery and usage. Several technologies, usually complementary, are requested to work together for achieving a reliable DRM system; among them, digital watermarking has gathered much approval, basically thanks to its potentiality of persistently attaching some additional information to the content itself. DRM technology could benefit from digital watermarking in several ways, due to the different functionalities a watermarking system can realise such as ownership proofing, copy control, user tracking and so on, that can be exploited in a DRM chain.

By starting from such considerations, this chapter has been mainly devoted to the presentation and discussion of digital watermarking technology, letting the last part of the chapter to the analysis of DRMS based on watermarking techniques. Basing on the particular purpose the watermarking technology serves, different requirements must be satisfied: during the chapter the fundamental requirements have been discussed, with particular reference to security, robustness and imperceptibility issues. Furthermore, the two main approach for watermark embedding (namely the Spread-Spectrum and the Side-Informed) has been presented and analysed. An image watermarking system, previously proposed by the authors, has been also described, for giving an example of a practical implementation of a watermarking scheme.

Even if no watermarking system proposed so far can completely assure the high level of security and robustness potentially required in a DRM scenario, much interest is still focused on watermarking technology and its powerful application for developing useful DRM systems. To one side, the research for improving watermarking security in a DRM chain is in progress; on the other hand, novel approaches for using watermarking in a DRM system are proposed, taking into account the current watermark weaknesses.

3.1.7. Future Research Directions

It is possible to identify three possible research areas related to the use of watermarking in DRM applications that seem to be open to new research activity, namely distribution models, customer rights protection, and secure watermark detection.

In classical distribution models, the watermark embedding process is carried out by a trusted server before releasing the content to the user. However this approach is not scalable and in large scale distribution systems the server may become overloaded. In addition, since point-to-point communication channels are required, bandwidth requirements could become prohibitive. A proposed solution is to use client-side watermark embedding. Client-side watermark embedding systems transmit the same encrypted version of the original content to all the clients but a client-specific decryption key allows to decrypt the content and at the same time implicitly embed a watermark. When the client uses his key to decrypt the content, he obtains a uniquely watermarked version of the content. The security properties of the embedding scheme usually guarantees that obtaining either the watermark or the original content in the clear is of comparable hardness as removing the watermark from the personalised copy.[245]

The customer's rights problem relates to the intrinsic problem of ambiguity when watermarks are embedded at the distribution server: a customer whose watermark has been found on unauthorised copies can claim that he has been framed by a malicious seller who inserted his identity as watermark in an arbitrary object. Buyer-seller protocols have been designed as a possible solution to this problem. Buyer-Seller Protocols rely on cryptographic primitives to perform watermark embedding ; the protocol assures that the seller does not have access to the watermarked copy carrying the identity of the buyer, hence he cannot distribute or sell these copies. In spite of this, the seller can identify the buyer from whom unauthorised copies originated, and prove it by using a proper dispute resolution protocol.

In the watermark detection process, a system has to prove to a verifier that a watermark is present in certain content. Proving the presence of such a watermark is usually done by revealing the required detection information to the verifying party. All current applications assume that the verifier is a trusted party. However, this is not always true, for instance if the prover is a consumer device. A cheating verifier could exploit the knowledge acquired during watermark detection to break the security of the watermarking system. A possible solution is represented by Zero-knowledge

[245] Kundur, D., Lin, C.-Y., Macq, B., & Yu, H., (2004). Special Issue on Enabling Security Technologies for Digital Rights Management. Proceedings of the IEEE, Vol.92 (6), 879-882. Adelsbach, A., Katzenbeisser, S., & Sadeghi, A.-R., (2002). Crytpography meets watermarking: detecting watermarks with minimal or zero knowledge disclosure. In XI European Signal Processing Conference, EUSIPCO' 02, Vol. I (pp. 446–449). Toulouse, France.

watermark detection (ZKWD) schemes. In general, a zero-knowledge watermark detection algorithm is an interactive proof system where a prover tries to convince a verifier that a digital content is watermarked with a given watermark without disclosing it. In contrast to the standard watermark detector, in ZKWD the verifier is given only properly encoded (or encrypted) versions of security-critical watermark parameters.

Depending on the particular protocol, the watermark code, the watermarked object, a watermark key or even the original unmarked object is only available in encrypted form to the verifier.

The prover runs the zero-knowledge watermark detector to demonstrate to the verifier that the encoded watermark is present in the object in question, without removing the encoding. A protocol run will not leak any information except for the unencoded inputs and the watermark presence detection result.[246]

3.2. Watermarking and Authentication in JPEG2000

3.2.1 Introduction

Since the mid 1980s, ITU (International Telecommunications Union) and ISO (International Organisation for Standardisation) have joined efforts in order to establish a new standard for efficient compression of grayscale and still color images. The result of this process has been named "JPEG" (Joint Photographic Experts Group) and has been established as international standard IS 10918-1 in 1991. Very soon, the JPEG image format (jpg) has become the most commonly used format. New features were soon added. However, some of them required costly licensing, while some of the more than 40 available options were mutually exclusive. Thus, only basic functionalities were adopted from most users. To correct the mistakes of the past, to take account of new trends (e.g. wavelets) and to adapt to the increased needs and requirements of modern multimedia and Internet applications, a new standard was required. Under these circumstances, almost a decade later, JPEG2000 emerged.[247] The new standard provided a unified coding system for different types of still images (bilevel, gray scale, colour, multicomponent) with different characteristics (natural, medical, remote sensing etc.) allowing different imaging models (client/server, real time transmission, image library archival etc.). The system performs superior to older standards by achieving great compression ratios while retaining image quality at the same time. Part I of the standard (ISO/IEC 15444-1, 2007) can be used on a royalty and fee-free basis. All these lead to the conclusion that it is only a matter of time before JPEG2000 will become widely accepted.

Watermarking and authentication for digital images are also new technologies, descendants of the last decade. The main reason for their introduction was the fact that digital images are quite easy to duplicate, forge or misuse. One of the most important applications of watermarking is the protection of the images' copyright while authentication aims to the verification of the content, investigate if an image is tampered or not and if it is, to identify the locations that these alterations have occurred. Both technologies need in order to succeed, the inclusion of side-information into the original image. That is obviously the reason why lossy compression schemes often cause to them great

246 Craver, S., Yeo, B., & Yeung, M., (1998). Technical Trials and Legal Tribulations. Communications of the ACM 41 (7), 44-54. Adelsbach, A., Katzenbeisser, S., & Sadeghi, A.-R., (2002). Crytpography meets watermarking: detecting watermarks with minimal or zero knowledge disclosure. In XI European Signal Processing Conference, EUSIPCO' 02, Vol. I (pp. 446–449). Toulouse, France. Piva, A., Barni, M., Bartolini, F., Cappellini, V., De Rosa, A., & Orlandi, M., (1999). Improving DFT Watermarking robustness through optimum detection and synchronisation. In GMD Report 85, Multimedia and Security Workshop at ACM Multimedia '99 (pp. 65-69). Orlando, Florida.

247 JPEG 2000. (2007). Retrieved August 07, 2007, from http://www.jpeg.org/jpeg2000.html

"Robustness: JPEG 2000 compression". (2007). Retrieved August 22, 2007, from http://www.cosy.sbg.ac.at/~pmeerw/Watermarking/attack_jpeg2000.html

problems. Part of the watermarking or authentication information may be discarded along with insignificant (presumed) parts of the original image's content, as a side effect in order to achieve better compression. Very few techniques have been proposed to cope with this problem and this is the motivation behind this chapter.

3.2.2. JPEG2000: An Overview of the Standard

The new standard has come to serve a wide variety of applications like the Internet, mobile communications, medical imagery, remote sensing, colour facsimile, printing and scanning, digital photography, e-commerce, digital libraries and many more. Of course, each of these areas imposes certain requirements that the new standard should fulfil in the best possible way.

So the implementation of JPEG2000 provides the following:

- Superior low bit-rate performance: The new standard performs superior according to its predecessors for very low bit-rates. It is now possible to compress grayscale images with high detail, under 0.2 bpp. Of course Internet and mobile communications, as well as network applications greatly benefit from this feature.
- Continuous-tone and bilevel compression: Various kinds of images are supported by the new compression system. The algorithm is capable of compressing images of various dynamic ranges (eg. from 1 to 16 bpp for each color component). This turns beneficial for a variety of applications like compound document compression, facsimile, graphics and images with binary and near to binary regions, alpha and transparency planes.
- Lossless and lossy compression: The new standard can provide both kinds of compression within the same codestream. There are applications like medical imaging, digital libraries and prepress imagery, in which image information loss can not be tolerated. In such cases the lossless part of the codestream is used while in the other cases (web browsing, network transmission over client/server applications) the lossy part can be used instead. JPEG2000 also allows progressive lossy to lossless buildup.
- Progressive transmission and decoding: It is possible to transmit images progressively and decode at the receiver with increasing pixel accuracy or spatial resolution. This a valuable feature for web browsing and digital libraries.
- Regions Of Interest: In almost every image, there are regions that contain more important information content than others. In JPEG2000 one can define these regions of interest (ROI) and allocate more bits for their coding than for the rest of the image.
- Open Architecture: JPEG2000 allows optimisation for different image types and applications.
- Error resilience: The new standard provides robustness to bit errors that may cause catastrophic decoding failures. That is essential, especially when images are transmitted over noisy channels (e.g. wireless networks).
- Fixed-rates, fixed-sizes, limited workspace memory: It is possible to specify the exact number of bits allocated for a group of consecutive pixels or for the whole codestream. Except for the profound advantage of this feature, it is also possible for devices of limited memory (like scanners and printers) to function with the new format.
- Security: One of the last parts of the standard that have been approved is JPSEC (Part 8) which deals with security, authentication, data integrity and protection of copyright and intellectual property rights issues.

The standardisation procedure of JPEG2000 is given in the following table. Of the thirteen parts, ten are completed and published, one has been withdrawn and two are in the phase of final draft. Since all of the finished parts are copyrighted material of ISO and ITU-T, thus not freely distributable, interested readers can get the final committee draft (FCD) from the Committee Draft web page of the JPEG2000 website.[248]

Table 1. JPEG2000 standardisation process

Part	Description	CFP[¤]	Current IS version[#]
1	JPEG 2000 Image Coding System: Core Coding System	Mar-97	ISO/IEC 15444-1:2004
2	JPEG 2000 Image Coding System: Extensions	Mar-97	ISO/IEC 15444-2:2004
3	Motion JPEG 2000	Dec-99	ISO/IEC 15444-3:2007
4	Conformance Testing	Dec-99	ISO/IEC 15444-4:2004

[248] "Welcome to JPEG". (2007). Retrieved August 07, 2007, from http://www.jpeg.org/jpeg2000/CDs15444.html

5	Reference Software	Dec-99	ISO/IEC 15444-5:2003
6	Compound Image File Format	Mar-97	ISO/IEC 15444-6:2003
7	Technical Report: Guideline of minimum support function of Part 1	Withdrawn	
8	JPSEC: Secure JPEG 2000	Mar-02	ISO/IEC 15444-8:2007
9	JPIP: Interactivity tools, APIs and protocols	Mar-02	ISO/IEC 15444-9:2005
10	JP3D:3-D and floating point data	Mar-02	FDIS* in March 2007
11	JPWL: Wireless	Jul-02	ISO/IEC 15444-11:2007
12	ISO Base Media File Format	Oct-02	ISO/IEC 15444-12:2005
13	An entry level JPEG 2000 encoder		FDIS* in April 2007

¤ CFP: Call for Papers # IS: International Standard * FDIS: Final Draft for International Standard

3.2.3. Watermarking and JPEG2000

Watermarking against lossy compression has always been an interesting challenge. Many of the existing literature techniques are inefficient against the JPEG standard. But times are changing and now the time has come to face the next generation in image compression standards: JPEG2000. With the new standard, superior quality for the same compression ratio can be achieved or similar quality for higher compression ratio, you can take whichever view suits you best. Since it is easier now to retain quality by achieving smaller file sizes, this is quite desirable. Thus compression ratios of less than 0.5bpp will become common practice. The problem is that although these images will be visually pleasant, watermarking methods have to evolve in order to survive such high compression. Is the watermarking community ready to undertake that challenge?

Very few works directly relate watermarking with JPEG2000. In the majority of the literature, the new standard is considered as yet another attack. Others examine the effects that the various JPEG2000 coding parameters cause to the watermark's detection. There is also a third category that proposes incorporating watermarking into the JPEG2000 coding pipeline or using it as an important factor in the marking/retrieval process. These may be few but they are of great practical interest. Of course there are lots of papers that deal with watermarking in the wavelet domain. Since the heart of the new standard is the wavelet transform, these works may be seen as the pioneers of watermarking in the JPEG2000 domain. All of these categories will be discussed in the following sections.

Wavelet Domain Watermarking

DCT has always been a very popular transform among the image research community. Its computational simplicity combined with great energy compaction, attracted the interest of the JPEG committee which used it in the core of the JPEG standard, a compression scheme which dominated the field for more than a decade. During that time, the Wavelet transform for image applications has also become popular and corresponding interest was increasing rapidly. The use of the wavelet-based *Embedded Block Coding with Optimised Truncation* (EBCOT) in the JPEG2000 standard has established the wavelet transform as the most interesting transform for compression research. So it was highly expected that many watermarkers have used the DWT as an alternative to the DCT for their schemes. Wavelet based schemes are mainly classified according to the type of watermark (pseudorandom noise sequence, logo or other), the coefficients' selection strategy (approximation, details or mixed) and the detection method (blind, semi-blind, non-blind). Of course other classifications are possible based on the application target or other factors.

First wavelet based watermarking schemes appear around 1995 and for the embedding, the approximation image is selected. For a 3-level wavelet decomposition, this band of coefficients is actually a miniature of the original image (dimensions are 1/8 of the originals). In that way traditional spread spectrum and spatial techniques can be easily used since these methods do not exploit the special features that the wavelet decomposition provides. Examples of these works can be found in numerous publications.[249]

Detail based methods as in Kim, Kwon & Park (1999), Kim & Moon (1999), Barni, Bartolini, Cappellini, Lippi & Piva (1999), Xia, Boncelet & Arce (1998), Kundur (1999), are a bit different. The coefficients distribution in the detail bands is different compared to the approximation. There are only a few coefficients large enough to carry the

[249] Liang, Xu, & Tran (2000), Ohnishi & Matsui (1998), Tzovaras, Karagiannis, & Strintzis (1998), Corvi & Nicchiotti (1997), Nicchiotti & Ottaviano (1998), Perreira, Voloshynovskiy & Pun (2000), Xie & Arce (1998).

watermark and a careful selection strategy is required. To define a selection threshold, the level of decomposition, orientation and subband energy can be utilised. Since the number of appropriate coefficients in each band is small, usually contribution is gathered from all the detail bands in all decomposition levels. An advantage coming out of this practice is that if the watermark is found in one of them, there's no need to search the others, reducing the detection's computational cost. This characteristic makes such methods appealing for real time applications. There are also techniques that use all of the bands, approximation and details for additional robustness.[250]

Built-In Approaches

There's no better way to confront a situation, than being part of it. If someone wants to make code that is JPEG2000 robust, the best way is to put his/her mark inside the coding pipeline. In any other cases, the results will be suboptimal. The next logical question is "in which exact part of the encoder, should I intervene by putting my mark?". One option is to put the mark right after the DWT. In that case though, the scheme wouldn't make any difference to conventional wavelet based methods. Of course an interesting variation would be to insert the mark into the intermediate coefficients from the lifting stages as Seo et al. (2001).[251] Using Daubechies 9-7 filter banks involves four lifting stages and a final scaling stage. In that case, authors propose to insert an extra lifting scheme between the second and third lifting stage (raising the number of lifting stages to five) in which only half of the coefficients are different from those of the previous stage. The whole alteration is based on a tuning parameter ω which selects the frequency characteristics of the desired coefficients. Actually the resulting coefficients correspond to the filtering of the input sequence with a high pass filter; the impulse response of this filter is tuned by the ω variable. If ω=0, the transform is the same as the original DWT (the extra stage is redundant). Authors' experiments show that using values of ±0.1, ±0.2, for ω leads to improved robustness comparing to final stage DWT based methods, while the quality of the image and transparency of the mark are preserved. The scheme can be easily integrated into the JPEG2000 coding and consequently benefit real-time applications like watermarking for digital still cameras, video monitoring etc. The ω parameter, except from selecting the coefficients' characteristics, can also be used as an auxiliary secret key.

One may argue that embedding directly into, or right after the DWT, would cause many problems. In the case of JPEG2000 coding, this can be true. Problems lie in the fact that the DWT is followed by quantisation and bitstream truncation in order to achieve the bit rate constraint. Before the end of the coding process, the mark will be already weakened. As an alternative, Su & Kuo propose to bypass the quantisation procedure and hide data in the coding stage.[252] Their intention is to hide a large number of bits rather than doing it in a robust way, so their primary goal is to achieve high payloads.

However, the bitstream optimisation is quite a hard challenge for their goal. So their method works only for high bit rate with lazy mode coding. The coding stage (right after quantisation) is a 2-tier structure. The first tier consists of three passes: significance propagation, magnitude refinement and cleanup. The authors take advantage of the fact that in lazy mode, during the magnitude refinement passes, except for the four most significant bit-planes, the rest of the passes are raw coded. Thus, a large number of bits can easily be changed at this place in order to conceal the secret information. The goal of high payload is achieved in that way (smaller images can easily be embedded into the cover image), there's no problem with the decoding process (since only raw data are altered, not arithmetic coded) while the information can be progressively retrieved during decoding. Progressive retrieval is possible because during the first of the raw coded passes, the last part of the info is hidden. That means that the first part is hidden at the last pass. Since decoding is exactly the

[250] Davoine, F. (2000). Comparison of two wavelet based image watermarking schemes. Proceedings of the IEEE International Conference on Image Processing ICIP 2000, (September 2000, Vancouver, Canada).

[251] Seo, Y., Kim, M., Park, H., Jung, H., Chung, H., Huh, Y. & Lee, J. (2001). A Secure Watermarking for JPEG2000. Proceedings of the IEEE International Conference on Image Processing ICIP 2001, (October 2001, Thessaloniki, Greece), 530-533.

[252] Su, P. & Kuo, C. (2003). Information Embedding in JPEG-2000 Compressed Images. ISCAS 2003, (May 25-28, 2003, Bangkok, Thailand).

reverse procedure, the parts of the hidden data are backwards retrieved thus achieving progressive extraction.

Although great discussion exists about where is it most appropriate to put the mark, before or after the quantisation of the coefficients, there's also a third view; using the quantisation to engrave the mark. Meerwald[253] uses a method proposed by Chen & Wornell[254] and further analysed by Eggers & Girod[255] called *Quantisation Index Modulation*. In this technique, the watermark bit determines which quantiser should be used from a set of available quantisers. The watermark sequence is a binary sequence with a size of a few hundred bits. The author recognizes the problem that conventional techniques have with the number of suitable coefficients for embedding. To circumvent that, he uses coefficients from both the details and approximation subbands to support his scheme. The distribution of the mark's energy is adjusted so that more energy is placed in those coefficients that the human eye is less sensitive to their changes.[256] JPEG and JPEG2000, blurring and sharpening are used for testing purposes and results are quite satisfactory.

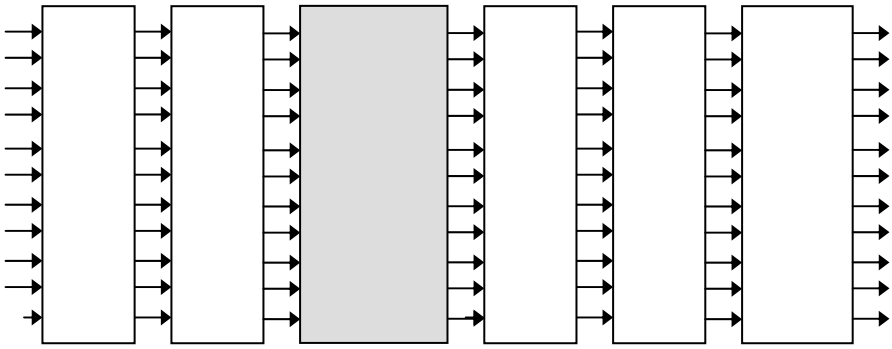

Figure 9: Adding an extra lifting stage for watermarking purposes

JPEG2000 as an Attack

In this category of works, JPEG2000 is simply considered as yet another attack. No special care is taken during the algorithm's design which is simply tested against compression with various bit rates. One of the two publicly available versions of the encoder is usually used, JJ2000 or Jasper. Testing is always based on the bit rate parameter. The lowest the bit rate, the worst the detectors perform. It seems that 0.3-0.1 bpp is the range in which the watermarks start finding great difficulties to survive and under 0.1 bpp the majority of the methods easily fail (speaking of blind detection algorithms). By far, the most complete comparative study of various schemes for different bit rates can be found in Meerwald's webpage.[257]

3.2.4. Authentication and JPEG2000

An alternative application of watermarking technologies in JPEG2000 domain is image authentication. While one of the major directions of digital watermarking aims to protect the ownership of digital images, the safeguarding of the image content is essential. The research community has been activated during the last years to construct effective

---

253 Meerwald, P. (2001). Quantisation Watermarking in the JPEG2000 Coding Pipeline. Communications and Multimedia Security Issues of the New Century, IFIP TC6/TC11, Fifth Joint Working Conference on Communications and Multimedia Security, CMS'01 (May 2001, Darmstadt, Germany), 69-79.

254 Chen, B. & Wornell, G. (2000). Preprocessed and postprocessed quantisation index modulation methods for digital watermarking. Proceedings of SPIE: Security and Watermarking of Multimedia Contents II, Electronic Imaging 2000, (January 2000, San Jose, CA).

255 Eggers, J. & Girod, B. (2000). Quantisation Watermarking. Proceedings of SPIE: Security and Watermarking of Multimedia Contents II, Electronic Imaging 2000, (January 2000, San Jose, CA).

256 Seo, Y., Kim, M., Park, H., Jung, H., Chung, H., Huh, Y. & Lee, J. (2001). A Secure Watermarking for JPEG2000. Proceedings of the IEEE International Conference on Image Processing ICIP 2001, (October 2001, Thessaloniki, Greece), 530-533.

257 "Robustness: JPEG 2000 compression". (2007). Retrieved August 22, 2007, from http://www.cosy.sbg.ac.at/~pmeerw/Watermarking/attack_jpeg2000.html

mechanisms following this direction.[258] Since a lot of work has been done in order to design watermarking mechanisms for image authentication in earlier image formats, the new compression standard meets the research community in a moment that very few attempts have already approached this topic.

Standardisation organisations have adopted the deployment of content authentication mechanisms that can be offered in companion with the digital images or by embedding them in the image data.
The image authentication field is stretched to cover the questions of whether a digital image is altered, whether the content of the image has been tampered, which particular regions, colours or image parts have been altered and finally if these changes can be recovered.

Classification of Image Authentication Techniques
Considering the nature of the watermark and the application that uses an image authentication technique, the image authentication techniques are classified in different categories. The first category of image authentication techniques aims at the integrity check of the image data. Authentication in terms of data integrity originates from cryptography. According to these techniques, if even one bit of the data that compose the image changes, the watermarked image is regarded as non authentic. In these methods, the watermark information is embedded in the original image in a way that it can easily be destroyed after any modification of the data. By this watermark property, in these methods the watermark is called *fragile*.

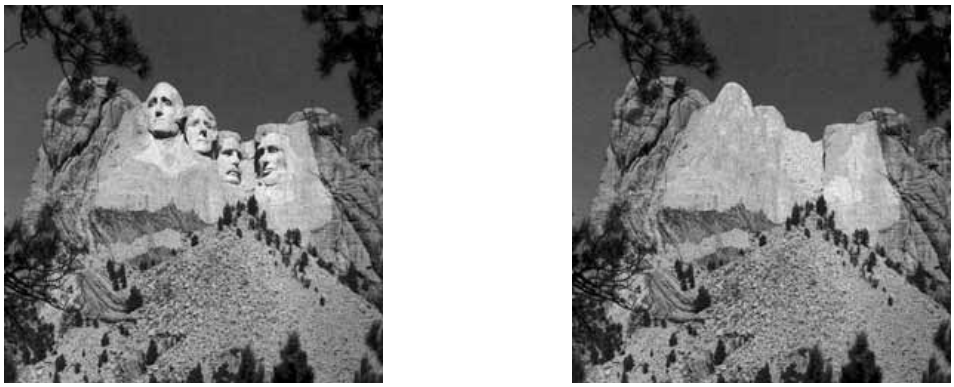

Figure 10: The watermarked image and the altered image

A second category includes the techniques that authenticate the image content. The main idea behind these techniques is that some modifications of the image data do not affect the image content. If for example a watermarked image has to be JPEG compressed (with high quality) then the data of the image will change but the image content will be identical. In these techniques the watermark information must be robust to actions that do not alter the image content and at the same fragile to actions that destroy the image content. The watermark in these techniques is called *semi-fragile*.[259]

Some of the techniques that belong to the previously mentioned categories can also localise the alterations of a watermarked image. This extra characteristic is related with the algorithmic design of those techniques and the nature of the watermark that is embedded in the original image.[260]

Finally the self-embedding techniques have not been appeared yet in JPEG2000 authentication domain. In the past such techniques have been proposed in order to embed a highly compressed version of the original image into itself.[261] This

[258] Eskicioglu, A.M. (2003). Protecting Intellectual Property in Digital Multimedia Networks (Invited Paper). IEEE Computer, Special Issue on Piracy and Privacy, 36(7), 39-45.

[259] Walton, S. (1995). Image Authentication for a Slippery New Age. Dr. Dobb's Journal of Software Tools for Professional Programmers, 20(4), 18-26. Wu, M. & Liu, B. (1998). Watermarking for Image Authentication. IEEE International Conference on Image Processing ICIP'98, vol.2, 437-441.

[260] Bhattacharjee S. & Kutter, M. (1998). Compression Tolerant Image Authentication. International Conference on Image Processing ICIP'98 (October 4-7, 1998, Chicago, IL). Kailasanathan, C., Safavi-Naini, R. & Ogunbona, P. (2001). Image Authentication Surviving Acceptable Modifications. IEEE-EURASIP Workshop on Nonlinear Signal and Image Processing NSIP'01 (June 3-6, 2001).

operation is giving the opportunity next to the watermark detector to localise the alterations and to reconstruct the content of the image that has been destroyed (Fig. 11).

Image authentication techniques can be combined with techniques that protect the copyright ownership in order to have a multipurpose watermarking scheme.[262] Since these schemes have been applied in other image formats with excellent results, similar methods can be expected with application to the new compression standard.

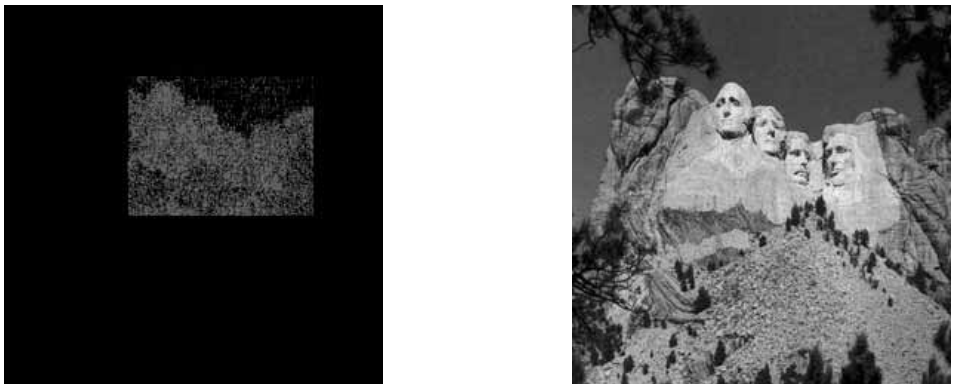

Figure 11: The altered positions and the reconstructed image

Capacity Issues and Suitability of JPEG2000 for Image Authentication

It is necessary for all watermarking applications to contain redundant information in the host data that can be used in order to embed the watermark. This field has been studied well from researchers that work in image compression and image watermarking field. The interest of researchers in image compression field is focused on the existence of redundant data that can be truncated in order to achieve the desirable compression ratio, while the interest of researchers in image watermarking field is focused on the existence of redundant data that can be used in order to embed the watermark information in host data.

It is obvious that in compressed image formats the amount of redundant information has been minimised during the compression procedure. Degrading the image quality by applying an image compression technique, the space for watermark embedding is becoming smaller and smaller.
The data of the image that can be used in order to embed a watermark are considered as a secret channel. The volume of these data can be theoretically estimated and in watermarking terminology, it is called *image capacity*. Depending on the image format, for images with the same dimensions and number of colours, image capacity varies. In general, in compressed image formats the image capacity is lower than non-compressed formats.

Very few attempts have been done to estimate the image capacity in JPEG2000 domain.[263] These estimations are based on the *Human Visual System* (HVS) and more specifically to the *Just Noticeable Difference* (JND) of each Discrete Wavelet Transform coefficient. Authors have adopted the Watson's model (1997) to estimate the JND of transform coefficients. The capacity estimation is achieved by making two basic assumptions. The first assumption is that input and output images are in JPEG2000 format with the same characteristics and the second assumption is that the image dimensions do not change during the watermarking process. The purpose of the method is to estimate the JND of each wavelet coefficient and by these estimations to measure the noise that can be added to the coefficients without affecting the image quality. Experimental results show that the estimated capacity depends on the compression

---

[261] Barni, M., Bartolini F. & Fridrich, J. (2000). Digital Watermarking for the Authentication of the AVS Data. Eusipco2000 (Sep. 4-8, 2000, Tampere, Finland). Lin, C.-Y. & Chang, S.-F. (2000). Semi-Fragile Watermarking for Authenticating JPEG Visual Content. Proceedings of the SPIE International Conference on Security and Watermarking of Multimedia Content II (Jan 2000, San Jose, CA), vol. 3971, 140-151. Kostopoulos, I., Gilani, S.A.M. & Skodras, A.N. (2002). Color Image Authentication Using a Self-embedding Technique. Proceedings of the 14th Int. Conf. on Digital Signal Processing DSP 2002 (July 1-3, 2002, Santorini, Greece).

[262] Lu, C. S., Liao, H.Y.M. (2001). Multipurpose Watermarking for Image Authentication and Protection. IEEE Transactions on Image Processing, 10(10), 1579-1592.

[263] Wong, P.H.W., Yeung, G.Y.M. & Au, O.C. (2003). Capacity for JPEG2000-To-JPEG2000 Images Watermarking. Proceedings of 2003 IEEE International Conference on Multimedia & Expo ICME'03 (2003, Baltimore), vol. 2, 485-488.

bit rate. For compression of 1 bpp the capacity of a typical image (Lena 512x512) is estimated to 25 kbits, while for compression of 2 bpp the estimated capacity exceeds 150 kbits.

The capacity of the watermarking algorithm has also been estimated from Meerwald, where for different window sizes and sub-block sizes the image capacity has been calculated and for images with dimensions 512x512, achieved capacities were 85, 194 and 383 bits, while respective PSNRs were 32.05, 31.45 and 32.09 dB.[264]

Nature of the Watermark Information

Authentication techniques are divided in different categories depending on the volume and nature of the watermark. Therefore, there are watermarking systems that embed watermarks in order to decide about the image alterations, systems that embed watermarks in order to localise these alterations and finally systems that localise the alterations and reconstruct the image content that have been destroyed.

The watermark represents either a reference pattern that if destroyed the detector of the watermarking system responds that the watermarked image is altered, either a hash value of the image content or an approximation of the image content. Some methods are using cryptographic hash functions (SHA, MD2, MD4 etc.) in order to generate digests of the whole image or image code-blocks.[265] The products of these functions are digital signatures with a fixed length (e.g. 160 bits). For extra security, the hash value can be encrypted before the embedding process. The encryption applied in order to avoid the hash value replacement after an attack, an action that disorients the watermark detector. The hash value encryption can be achieved by using a typical public-key cryptosystem (DES, RSA, etc.).[266]

Since JPEG2000 is a more complicated image format, researchers have followed different approaches in order to authenticate the image content. Such an approach is presented from Peng, Deng, Wu & Shao where the authentication mechanism is used to authenticate the sub-images transcoded by a single original image codestream.[267] These sub-images can have different qualities, resolutions, components and special regions.

As described in the beginning of the chapter, the packet generation process consists of five distinct steps. These steps are tile decomposition in tile-components, tile component transformation into resolution levels, resolution level partition into several precincts, precinct partition into several layers and finally packet formation from the bit stream corresponding to a given tile component, resolution level, precinct and layer.

The overall authentication process is based on a Merkle hash tree construction[268], using the source of a JPEG2000 codestream. The usage of this structure is giving the opportunity to the end user to authenticate any subset of the data values in combination with auxiliary information. Along with the Merkle hash tree a signature of the root value of the tree is computed.

The end user on a second step, requests the sub-image with its characteristics (resolution and quality) and the provider sends the corresponding packets. The provider sends also to the end user the signature of the root value accompanied with the auxiliary information that will be used in order to authenticate the sub-image.

---

[264] Meerwald, P. (2001). Quantisation Watermarking in the JPEG2000 Coding Pipeline. Communications and Multimedia Security Issues of the New Century, IFIP TC6/TC11, Fifth Joint Working Conference on Communications and Multimedia Security, CMS'01 (May 2001, Darmstadt, Germany), 69-79.

[265] Zhishou, Z., Gang, Q., Qibin, S., Xiao, L., Zhicheng, N. & Shi, Y.Q. (2004). A Unified Authentication Framework for JPEG2000. Proceedings of 2004 IEEE International Conference on Multimedia & Expo ICME'04 (June 2004, Taipei, Taiwan), vol. 2, 915-918. Grosbois, R., Gerbelot, P. & Ebrahimi, T. (2001). Authentication and access control in the JPEG 2000 compressed domain. Proceedings of the SPIE 46th Annual Meeting, Applications of Digital Image Processing XXIV (July 29th- August 3rd, 2001, San Diego, CA).

[266] Schneier, B. (1995). Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition. New York: John Wiley & Sons.

[267] Peng, C., Deng, H.J.R., Wu, Y.D., Shao, W. (2003). A Flexible and Scalable Authentication Scheme for JPEG2000 codestreams. Proceedings of the eleventh ACM international conference on Multimedia MULTIMEDIA '03, 433-441.

[268] Merkle, R.C. (1989). A Certified Digital Signature. In Gilles Brassard (Ed.), Advances in Cryptology - Crypto '89, Lecture Notes in Computer Science, vol 435, 218-238, Berlin: Springer-Verlag.

A different approach is followed by Meerwald.[269] He has designed a technique that is able to localise the image alterations by using a semi-fragile watermark. The watermark in this case is consisted of coefficients in the approximation image of the wavelet domain. In order to construct an algorithm that will be able to authenticate pixel blocks of size 8x8 the author has selected to apply the Wavelet Transform (three decomposition steps). This technique is differentiated from the others while it is able to localise particular areas (blocks) of the image that could be altered. At the same time the watermark is embedded with semi fragile way in the host data.

JPSEC : Security in JPEG2000 Images

The last parts of the new standard that were left for standardisation were Parts 13 & 8. While the first is currently in the phase of final draft, part 8 has been approved as an international standard in May'07. Known as JPSEC, the intention of part 8 is to define a standard framework for anyone who would like to provide security services e.g. authorised access control, authentication, copyright protection. There are some standard defined template tools as well as provision for future *registration authority* (RA) provided tools. All of these tools should work transparently over the basic functionalities of the standard, meaning that an ordinary Part 1 compliant decoder should have no problem to open and show a j2k image, even if security information content is present in the file. The basic structure of such a file should remain intact. This is performed by the use of security code segments, identified by specific markers in the bitstream that are ignored by non-part 8 compliant decoders.

The two different categories of security code segments are:

- SEC : Marked in the stream as 0xFF65, this code segment is found in the header of the JPEG2000 file. Information provided here, may apply to the whole image or specific parts of it. For these reason, in each tool's syntax, there is a zone of influence field (ZOI) that identifies the tool-affected parts.
- INSEC : Identified in the stream as 0xFF94, this code segment can be found anywhere in the codestream. This marker provides additional security comparing to SEC, as well as alternative implementation schemes.

The forms of the two code segments are given in Figure 12.

One must note here, that for the case of SEC segment, the tool syntax part, may involve the use of several different tools, not only one. Tools are the means by which the RAs provide the aforementioned security services through JPSEC. At the time that part 8 was in final draft form, ten different tools were presented in Annex B.

These tools are:

- A Flexible Access Control Scheme for JPEG 2000 Codestreams
- A Unified Authentication Framework for JPEG 2000 images
- A Simple Packet-based Encryption Method for JPEG 2000 bitstreams
- Encryption tool for JPEG 2000 access control
- Key generation tool for JPEG 2000 access control
- Wavelet and Bitstream Domain Scrambling for Conditional Access Control
- Progressive Access for JPEG 2000 codestream
- Scalable Authenticity of JPEG 2000 Code-streams
- JPEG 2000 Data Confidentiality and Access Control System Based On Data Splitting and Luring
- Secure Scalable Streaming and Secure Transcoding

[269] Meerwald, P. (2001). Quantisation Watermarking in the JPEG2000 Coding Pipeline. Communications and Multimedia Security Issues of the New Century, IFIP TC6/TC11, Fifth Joint Working Conference on Communications and Multimedia Security, CMS'01 (May 2001, Darmstadt, Germany), 69-79.

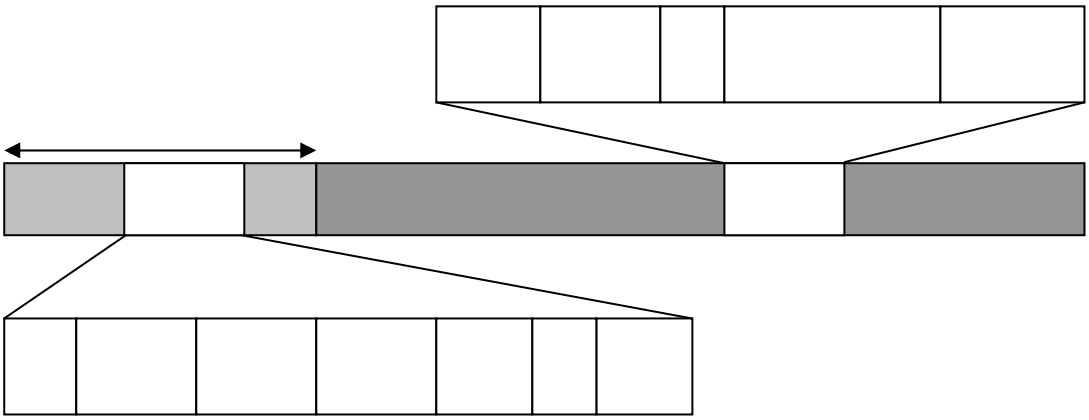

Figure 12: Security code segments inside the JPEG2000 bitstream

This list's tools are indicative. In the future many more, modern and advanced tools may become available. As can be observed, most tools address access control, encryption and authentication issues. Notably, there is not even one watermarking tool (at least at the time of writing of this chapter). This is due to patent restrictions. Most of the companies involved in watermarking, have patented their methods and this is contrary to the openness of the new standard. However, if permission is given for a watermarking tool to be used license free, then there is no problem for the JPSEC framework to include it in the future.

It is not the intention of this chapter to analyse all of these tools. The main targets are watermarking and authentication. Since watermarking is currently absent in JPSEC, a brief discussion will be given on the authentication tools. In the work that led to the second tool of the list, an authentication framework is proposed against unauthorised modifications of digital images in JPEG2000 format.[270] The aim of the authentication framework is to provide a flexible mechanism for different applications and user/provider requirements. The framework is suitable for all kinds of compressed and uncompressed images using the JPEG2000 encoder and it can be used to apply different watermarking techniques to them. A new parameter called Authentication bit Rate is introduced in order to achieve the desirable authentication robustness level.

This parameter is also serving a variety of image authentication applications since it gathers all application's needs in a simple parameter. This mechanism is able to use the traditional digital signatures in case the required robustness of the watermark is to be fragile or robust signatures in case the required robustness of the watermark is to be semi fragile. In the next flowchart (Fig. 13), this general framework is depicted.

[270] Zhishou, Z., Gang, Q., Qibin, S., Xiao, L., Zhicheng, N. & Shi, Y.Q. (2004). A Unified Authentication Framework for JPEG2000. Proceedings of 2004 IEEE International Conference on Multimedia & Expo ICME'04 (June 2004, Taipei, Taiwan), vol. 2, 915-918.

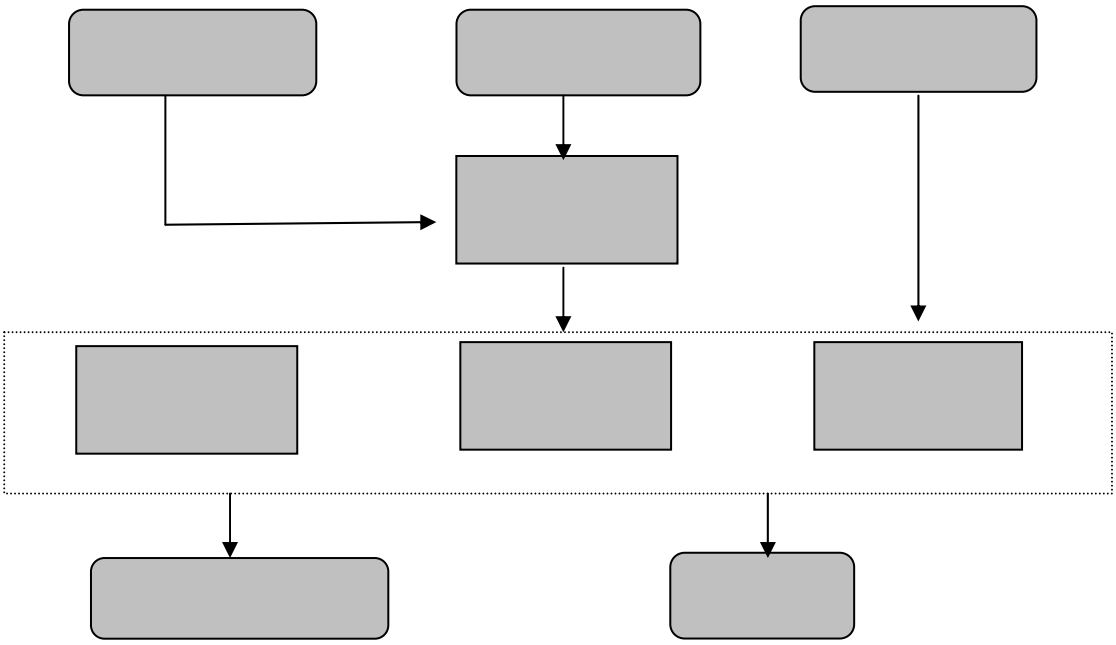

Figure 13: An Authentication framework for JPEG2000 images

In tool number eight a proposal of guarantying the authenticity of the received image data by the end user without trustworthy servers and networks is formulated.[271]

According to this proposal the authentication data on an image code stream and its verification by the end users are performed with three modules. The image provider generates an Integrity Check Value (ICV) of the image using a hash algorithm an then signs on the ICV to generate a digital signature of the image using a public key cryptosystem (e.g. RSA). When the end user requests a portion of the image, the provider sends to him the requested portion along with the Subsidiary Integrity Tokens (SIT) of the unsent portion of the image. Finally the end user verifies the authenticity of the received image portion by using the received digital signature and the SIT's.

3.2.5. Conclusions

In this chapter, a short overview of the new standard has been given. Through this, the possible places for watermarking have been identified. Methods proposed for each place in the coding pipeline (into the transform, after it, in the quantisation stage, in the coding stage) have been presented. Each of these cases has specific advantages and disadvantages. Embedding at the transform coefficients is very compatible with older methods for which great expertise exist. On the other hand, quantisation and coding may lead to significant loss of the watermark's energy. Quantisation methods avoid quantisation errors but haven't been thoroughly tested yet. None of the presented schemes has become part of the standardisation procedure due to patent related issues. The effect of parameters selection for coding has also been discussed. Experiments with levels of decomposition, tile size, regions of interest, filter kernels, compression ratios, prove that the coding strategy is crucial for the survival of the watermark.

As far as authentication is concerned, the complexities of the standard along with the limited bibliography have restrained this activity. Proposed techniques are mostly based on the data integrity check in order to authenticate digital images by using cryptographic hash functions. However, more general frameworks have been proposed that include the application of different watermarking techniques for image authentication, in terms of content authentication. Most work on this field, is coming from the teams that contributed to the standard like Prof. Ebrahimi's team at EPFL, and Infocomm Research, Singapore.

3.2.6. Future Research Directions

[271] Peng, C., Deng, H.J.R., Wu, Y.D., Shao, W. (2003). A Flexible and Scalable Authentication Scheme for JPEG2000 codestreams. Proceedings of the eleventh ACM international conference on Multimedia MULTIMEDIA '03, 433-441.

It is obvious that watermarking in the JPEG2000 domain currently constitutes a promising research area. There are still many places in the coding pipeline in which the watermark can be embedded. There are various arguments about the place of embedding but coding stage embedding seems to be the most promising because no errors are introduced by the previous stages. A good idea could be that a non legitimate user, could decode the image with errors, or inferior quality while the rightful user will have the best quality possible. Quality control watermarking/data hiding is an open issue in JPEG2000 as it is for all lossy image compression formats.

Authentication of digital images in JPEG2000 format is a research field that also attracts the interest of the research community during the last years. Of all techniques, most interesting are the self-correcting ones, those that can partially or fully reverse the tampering. The practical value of such schemes is enormous.

Concluding this section, it seems that in the next years the field of watermarking and authentication of digital images in JPEG2000 format will attract more of the interest of the research community and new powerful protection mechanisms will be provided. The recent release of the JPSEC, will give researchers the opportunity to conform and include their tools in the JPEG2000 codestream. Currently, the number of available tools is very limited, so there's plenty of space for work in this area.

3.3. Protecting the Copyright of Digital Video through Watermarking Technologies

3.3.1. Introduction

Digital video watermarking techniques and algorithms offer a great support to real time digital video applications. These applications include the copy control, the broadcast monitoring, the fingerprinting, the video authentication, the copyright protection as well as the enhanced video coding.

Nowadays, the copying of a digital video is very simple by using a recorder. For this reason, a watermark is embedded to the digital video so that its copying through unauthorised recorders may not be possible. If the recorder is able to read the hidden information comprised into the watermark, then it is authorised to produce copies, otherwise it must not carry out the copying procedure.

As to the broadcast monitoring, the aim of the watermarking is the determination of the identity of the video object transmitted. The owners having the right to create a video want to secure their privileges any time their property is broadcasted. The principal idea here embeds identification information (a unique watermark) into the data, which is identified by a computer. This identification information is obtained directly and with reliability after the decoding process.

In fingerprinting, the aim of the watermark is to show which user created the illegal copies. The problem arises when a 'traitor' shares the protected material without having any sort of permission on behalf of the holder of the right on intellectual property. In order to solve the problem, the basic idea is to be able to identify the identity of the traitor when detecting an illegal copy so that we can prosecute him in court. This can happen by embedding into data an indelible and invisible watermark which determines the client's identity.

The authentication techniques are useful for confirming that a video content is the original. Different methods for the verification of the video content authenticity as well as for the protection against falsification are proposed. Researchers have also studied the use of digital watermarking aiming at verifying the integrity of the digital video content. A basic technique is the typical embodiment of a timestamp into the video frames. The result of the aforementioned technique is that the detection of alterations may be possible.

3.3.2. Requirements of Video Watermarking

A video watermarking technique must fulfil some requirements. We mention below the three most principal requirements for video watermarking. The first is that the technique should be robust to non hostile video processing. The second is that it should be robust to collusions and the third one is that it should be performed in real-time.

The robustness of the digital watermarking is always estimated in regard to the survival of the watermark after the implementation of the attacks. In the environment of digital watermarking the future value of attacks that take place in

the video is multiple. Many different, non hostile attacks in video are in fact likely to happen. The term non-hostile refers to those attacks where for example, the provider of the content processes a bit of information from his digital data for the most efficient handling of his sources. Afterwards, we name any procedures that can lead to non hostile attacks: the addition of noise during the transmission through a wireless network, the conversion of a digital to analog or analog to digital signal, the gamma correction in order to increase the contrast, the changes across display formats (4/3, 16/9, 2.11/1), the changes of spatial resolution (NTSC, PAL, SECAM), the attack by a handheld camera, the changes in frame rate, the video editing process (cut-and-splice or cut-insert-splice) and the overlay with a chart (logos and labels).

Another basic requirement is the robustness against collusions. The term collusion refers to all hostile users who unite information, for example the watermarked data they have in order to produce illegally the non-watermarked ones. There are two types of collusion: the type I collusion and the type II collusion. The same watermark is embedded into different copies of different data. The type I collusion estimates the watermark of every watermarked data. Then, it combines in a linear way the watermarks estimated and provides an exact estimation of it; for example, it measures the mean of various evaluations. Since the collusion obtained a good estimation of the watermark, it removes it from the rest and in this way we have the non-watermarked data. When different watermarks are embedded into different copies of the same data, type II collusion is applied. The only thing that this collusion can do is to apply a linear combination to different watermarked data so as to produce the non-watermarked ones. It can use the average as a linear combination. In general, the average of different watermarks points to zero.

The real-time constitutes the third requirement. It does not have any particular concern in the case of still images. When someone wishes to embed a watermark or to control its presence in an image, then few seconds of delay may be acceptable. However, such a delay is not realistic in a video environment. In fact, the frames are transmitted in a quite fair rate, usually 25 frames per second is a rate that can be achieved for a smooth video stream. The least the embedder or the detector of the watermark or in some cases even both of them can do is to be able to handle such a rate. While monitoring a broadcast, the detector should be capable of detecting an embedded watermark in real-time. In order to fulfil the real-time requirement, the complexity of the watermarking algorithm must be the lower possible.

3.3.3. The Most Important Trends in Video Watermarking

Digital video watermarking is a relatively new area of research which uses the advantages resulting from the conclusions of the digital watermarking in still images. Many algorithms have been proposed and among them we have isolated the three most important trends existing. The simplest and most direct approach considers the video as a sequence consisting of still images and it applies to them one of the existing watermarking shapes for still images. The second approach makes use of the further dimension of time aiming at designing new robust algorithms for video watermarking. Finally, the last trend considers the video stream as compressed data that have been compressed following a specific method of video compression and its characteristics are used in the production of an efficient watermarking shape.

During the very first years, digital watermarking studied to a large extent the case of still images. Many interesting results and algorithms were developed and when new areas, such as the video watermarking, started to become a research issue, the basic idea was to test the reuse of former known results. As a consequence, the community of watermarking considered in the first place the video as a sequence of still images and adopted the existing watermarking shapes for images during video watermarking. A simple way to extend the shape above is to embed the same watermark into the video frames following a typical rate. From the detector's point of view, its presence is controlled for each frame. If the video is watermarked, then a typical vibration can be observed as a response to him. However, such a shape does not have any profitable load. The only thing the detector can do is to say if the watermark given appears or not but he does not extract any secret message. On the other side, host data are much bigger in size than a simple still image. Since it is possible to embed more bits into a larger host signal, we expect that video watermarks have a much more profitable load. This can be easily realised by embedding independent watermarks of many bits into each video frame. However, the benefit as to the profitable load is balanced with the loss of robustness.

The main disadvantage of concerning the video as a sequence of independent still images is that we do not take into great consideration the dimension of time. A number of researchers have studied how it is possible to reduce the visual impact that the watermark has on still images, taking into account the properties of the human visual system as well as the procedures of the frequency mask, the luminance mask and the contrast mask. These studies can be easily extended also in video through a direct frame after frame adaptation. However, the watermark resulting is not the ideal one in terms of visibility since it is not possible to study the sensitivity of the human eye in time. The motion is in fact a very particular characteristic of the video and the new video-based measurements of perceptibility need to be designed so that we will be able to make use of them during digital video watermarking. This simple example shows that the

dimension of time is a crucial point in video and that it should be seriously considered for the creation of effective algorithms.

The last trend considers the video data as compressed ones that have been compressed based on a specific type of compression. In fact, the most of the time, a video is stored in a compressed version to save some space. The watermarking methods have been designed in such a way that the watermark is embedded directly into the compressed video stream. Therefore, we make use of a very specific part of this video compression (run length coding) aiming at hiding information. Alternative watermarking strategies can be used according to the type of frame under watermarking. If we embed the watermark directly into the stream of the compressed video, the real-time video processing is possible. However, the watermark is by nature connected to this compression and it may not survive after a standard video conversion.

The simplest way of watermarking a video is the straight change of pixel values of the video in spatial domain. Another way which has more advantages is embedding the watermark into the frequency domain, by using one of the much known transforms: Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT). Below we briefly describe three important and interesting video watermarking techniques which have satisfying effects during experiments.

An Adaptive Video Watermarking Algorithm

Robustness is the major issue arising in digital watermarking algorithms. An effective method applied for improving the watermark's robustness is that its embodiment is done adaptively to the perceptual property and the characteristics of the signal. Hong-mei Liu, Ji-wu Huang and Zi-mei Xiao suggest an adaptive video watermarking algorithm to the wavelet domain.[272] According to the properties of the 2-D wavelet coefficients, the watermark is inserted into the coefficients of the low frequency sub-band in order to achieve better robustness. If we want to improve the strength of the watermark's components, we perform a classification of the coefficients of the low frequency sub-band based on the motion of the object and the texture complexity of the content in the video sequence. Following the results of this classification, the strength of the components of the watermark is adjusted adaptively. Results from experiments have shown that the watermark generated is robust to video degradation and distortions, while its transparency is guaranteed.

Multiresolution Scene-Based Video Watermarking Using Perceptual Models

The authors Mitchell Swanson, Bin Zhu and Ahmed Tewfik have proposed a watermarking procedure to embed copyright protection into digital video.[273] This procedure makes direct use of spatial masking, frequency masking as well as temporal properties in order to embed an invisible and robust watermark. The last one is composed of static and dynamic temporal components. These components are generated from a temporal wavelet transform which is applied to video scenes. The resulting frames with a wavelet coefficient are modified by a pseudorandom sequence. This one was shaped based on perception and represents the author of the watermark. The noise-like watermark is statistically undetectable and therefore its unauthorised removal is discouraged. Furthermore, the author's representation resolves the deadlock problem. The multiresolution watermark may be detected on single frames, without knowledge of the location of these frames in the video scene. The authors after some experiments have demonstrated that this watermarking procedure is robust to several video degradations and distortions.

A DWT-Based Digital Video Watermarking Scheme with Error Correcting Code

The authors Pik-Wah Chan and Michael Lyu propose a digital video watermarking algorithm.[274] The scheme performs a DWT-based blind digital watermarking with scrambled watermark and error correcting code. This scheme embeds different parts of a single watermark into different video scenes under the wavelet domain. To increase its robustness, the watermark is refined by applying the error correcting code. This last one is embedded as a watermark in audio channel. The video watermarking algorithm is robust against the attacks of frame dropping, averaging and statistical analysis. These attacks were not solved effectively in the past. Furthermore, it allows blind retrieval of the embedded

[272] Hong-mei Liu, Ji-wu Huang, Zi-mei Xiao, "An Adaptive Video Watermarking Algorithm", IEEE International Conference on Multimedia and Expo, pp. 257-260, 2001.

[273] Mitchell D. Swanson, Bin Zhu, Ahmed H. Tewfik, "Multiresolution Scene-based Video Watermarking using Perceptual Models", IEEE Journal on Selected Areas In Communications, Vol. 16, No. 4, pp. 540-549, May 1998.

[274] Pik-Wah Chan, Michael R. Lyu, "A DWT-based Digital Video Watermarking Scheme with Error Correcting Code". Pik-Wah Chan, Michael R. Lyu, Roland T. Chin, "A Novel Scheme for Hybrid Digital Video Watermarking: Approach, Evaluation and Experimentation".

watermark, that is, we do not need the original video for the watermark's retrieval. Finally, the watermark is perceptually invisible.

3.3.4. Future Research Directions

The copyright protection constitutes the principal aim of the digital watermarking applications for digital video in history. The main strategy embeds a watermark into the data of the digital video which indicates the identity of the person holding the right on intellectual property. If an illegal copy is found, this person can prove its authorship due to the embedded watermark and in this way he can sue the illegitimate user.

The video coding process is usually a sequence of two steps. During the source coding, all surplus information is removed so that the compressed representation of data arises, while the authenticity of visual quality is maintained. After that, the compressed representation of the video is subjected to channel coding where further surplus information is added in order to correct all errors. The channel coding is considered obligatory since errors may turn up during transmission. The digital watermarking is initiated as an alternative tactics for the introduction of information concerning the correction of an error after the source coding.

Experiments have shown the feasibility of this approach and following the conclusions it is clear that digital watermarking has more effective performances than the traditional mechanisms and future research direction will focus on this area.

4. Digital Rights Management and Transactions – on-line rights clearance

4.1. Introduction

Rights Clearance has always been an important issue in every transaction that involves copyrighted objects but even in other transactions such as land property acquisition. Typically the owner (seller) has to prove that he possesses the right to make the transaction and the buyer has to be sure of the legitimacy of the transaction that he is going to be part of. The general perspective of this chapter is to address every aspect of rights clearance in e-commerce and DRM transactions mainly from the technical point of view. The major topics that will be addressed in the remaining of this chapter are the investigation of on-line rights clearance background in terms of broad definitions, discussions and contradicting views, the inquire of intellectual property rights as part of a Digital Rights Management system and with respect to a plausible business model, the analysis of the technical components involved in on-line rights clearance, along with the arising flow control and engineering issues as well as the presentation of an operative DRM system integrating on-line rights clearance practices.

4.2. Background

"Rights clearance" is a term often used indiscriminately to describe a set of processes that are followed both in the physical and digital world. As a consequence, the "bad" use of this term and in general the terminology related to rights clearance is usually a source of many ambiguities and misconceptions that prevent readers from acquiring a common understanding on the issue. The goal of this section is to outline the related topics, address controversial issues and eventually formulate a clear basis that will help the reader gain an insightful view of the subject.

4.2.1. Intellectual Property Rights (IPR) & Current Legislation

Current legislation concerning intellectual property primarily aims at protecting artworks that exhibit a considerable level of creativeness and novelty, such as works originating from literature, theatre, music, art etc. Among the large corpora of law proceedings that concern intellectual properties, there is a considerable portion that attempt to address intellectual properties as formulated by digitising and distributing content through computer networks. There is a very strong tradition that seeks to harmonise the activities of all European countries under a common, international action line, with the aim to tackle the problems generating from the misuse of intellectual properties.

The need for common treatment of such issues is considered essential in the context of a European market, mainly due to differences in conception of intellectual property and the obstacles arising by the enforcement of domestic copyright restrictions. If we consider the pace by which digital information is being generated and the practices that are often used for its distribution and sharing, it is evident that individual national legislations are inadequate to guarantee the interests of intellectual property owners, in the light of an emerging and without boundaries digital trade.

The purpose of national legislation is to determine the amount of actions that are considered legitimate within the nation boundaries. However, the study of a national legislation should not be carried out independently from the international status quo. The international state of affairs is constituted by international conventions and directives that act normatively in the establishment of national laws.

The most important international conventions are:

- Berne convention (supervised by World Intellectual Property Organisation) [WIPO]
- The international convention regarding copyright (UCC)
- TRIP's agreement (Trade Related Intellectual Property Rights) under the auspices of World Trade Organisation

The purpose of the aforementioned conventions is to introduce a set of minimum requirements to be adopted by all member states. In this context, the European Commission (EC) envisages the establishment of a European legislation that will be founded on the international conventions and will be adopted by all European countries, in order to facilitate a global, liberal European market where the trade of goods will be conducted in a smooth and unrestricted manner.

Originality is the essential characteristic that an artwork should exhibit in order to allow for its rights to be granted under intellectual property laws. Berne convention does not provide an explicit definition describing which artworks

should be considered copyright protected and which not. However, an artwork should be more than a simple digital representation of a physical object in order to be considered original. Berne convention does not treat the digitised version of an original artwork as a "new original artwork" with completely independent intellectual properties, despite the fact that under certain circumstance such rights can be granted. The copyright holder of an artwork is by default the person who has created it. In the case where the artwork has been generated by more than one creator, intellectual properties are assigned to all participants. Concluding, we can claim that the intellectual properties legislation framework in each European country derives from the combination of Berne convention, European directives and national laws.

4.2.2. Rights Clearance

The term 'Rights Clearance' refers to the overall process of determining the terms and conditions that constrain the use of an artwork, identifying the person or organisation that holds the right to grant its usage permissions and eventually transferring these permissions on the ground of a license agreement.

Although different types of intellectual properties exist such as a) copyright b) database right c) moral rights d) rights bound to patents e) execution right etc, the process of rights clearance can be considered roughly uniform.

The outcome of rights clearance is a set of rules that constrain the use of an artwork, always with respect to a certain agreement. This outcome is described by a license that serves as a contract between the rights owner and the final user. The license is a document that details the terms and conditions under which the content is allowed to be exploited by the end user without committing copyright violation. Hence, as long as the license counterparts obey to the conditions of the agreement, rights violation is not an issue. Nevertheless, this process can either be performed in the digital or the physical world raising important differentiations to its interpretation:

- Rights Clearance in the Physical world is a process quite straightforward since it has been exercised for many decades and its long established practice has set a frame of rules that must be followed. It is usually transacted by attorneys or other professions or organisations with adequate knowledge and access to records describing the rights applied on an object.
- Rights clearance in the Digital world has become an absolute necessity, since e-commerce plays a vital role in modern transactions. After the transition to the Digital world, rights clearance became a more complex procedure and a number of arising issues has to be studied. A key element of this study must be the dissimilarities between the original digital resources and the digitised ones which are bound by different kinds of intellectual property rights. Another important issue introduced by the digital world is the rights on purely digital objects. Such a study will set the foundations on which some standards for on-line rights clearance will be defined.

4.2.3. Digital Rights Management (DRM)

Rights management involves the registration, maintenance, monitoring and administration of the protected content property rights in an efficient and profitable way. Services like tracking the usage of content engaged to a certain license, as well as identifying new rights that bring added value to the content at hand, are considered essential functionalities of a rights management framework. Since rights, as indicated previously, can either refer to physical (i.e., statues, paintings etc) or digital objects (i.e., computer graphics, multimedia content etc), rights management should facilitate both cases. As the number of artworks, digitised or digitally generated, that are being distributed over computer networks rapidly increases, the need for developing advanced digital rights management systems becomes apparent.

Enabling rights management on highly heterogeneous and complex environments as in the case of WWW, requires the extraction and representation of a sufficiently large amount of information in a manner that can be shared among computer systems of the same purpose. Metadata is data about data that aim at describing an object or a resource independently of its nature, physical or digital. Particularly, metadata try to describe sources in a systematic and structured way in order to facilitate their easy sharing and re-use. In this context, intellectual property rights are also information that has to be retained and organised in an interoperable way.

Numerous initiatives, each one with its own advantages and disadvantages, have attempted to establish a set of metadata able to sufficiently capture the information required for managing property rights. Among them, Dublin Core Metadata Initiative [DCMI] has emerged as an international standard that receives considerable support from both industry and academia.

4.2.4. Protecting Digital Rights

Despite the fact that rights clearance, and digital rights management in general, is still in its infancy, numerous technological solutions deriving either from industry or academia have been recorded. The engineering of a holistic rights management system that could meet the requirements of all existing business models seems particularly difficult. However, certain aspects of the problem have been tackled successfully by custom solutions. The aim of this paragraph is to provide an overview of the current state in the field of digital rights protection and identify the areas open to further improvements.

As mentioned previously registration, maintenance, monitoring and administration of intellectual properties are among the most important requirements that a digital rights management system should fulfill. The design and development of technological means that will facilitate the aforementioned operations are considered essential, especially for tracking distributed content. The mechanisms that incorporate technological protection means, work complementary to the digital rights management systems in order to defend the financial interests of content creators.

There are several ways by which technology can be employed to serve the purposes of digital rights protection. The dominant trends can be categorised as follows:

- Distribute digital content of low quality: Constitutes a simple, economical and widely adopted technique for preventing unauthorised actions of content misuse (e.g., printing, replicating etc). For instance, an image resolution of 72 dpi (dots per inch) is high enough to retain the image visual quality for preview purposes but very low to allow exploitation actions such as publishing printed copies.
- Distribute Encrypted Content: A popular method for protecting digital content, adopted by famous DRM systems is the distribution of multimedia content in an encrypted format. In this case only the user having paid a certain fee, obtains a use license which serves as the decryption key.
- Stenography: Protecting digital content using stenographic techniques involves the use of specialised mechanisms that hide encoded messages within the actual content. In this way tracking of content through computer networks is possible, via the transmission of data concerning the content users.
- Digital Watermarking: Digital watermarking constitutes one of the most modern technological solutions for protecting digital content and has been adopted by a number of content providers. Digital watermarking introduces an additional level of protection and has been particularly popular in the field of digital images. Digital watermarks can be either visible or invisible and their purpose is to provide evidence for supporting the copyright holder ownership over the watermarked content.

4.3. Rights Clearance & DRM

The process of rights clearance involves many different players interacting in various modes. The purpose of this section is to describe a case of electronic trade with special focus on rights clearance. The key-entities will be identified and their interrelations will be outlined. This process is motivated by the necessity to trace the slots in the electronic transaction sequence where advanced technologies can be attached and bridge the gap between physical and electronic commerce. Rights clearance can be regarded as part of the general digital rights management objective that has emerged as one of the greatest challenges for content distribution. First-generation DRM systems, used to rely on encryption techniques, limiting content distribution to a very restricted amount of legitimate users. Second-generation DRM systems facilitate the description, identification, trading, protection, monitoring and tracking of all forms of rights usage over both tangible and intangible assets.

4.3.1. Motivating Example

A typical example of a Digital Rights Management system that incorporates rights clearance functionality can be taken from the E-book sector. OzAuthors[275] is a service provided by the Australian society of authors in a joint venture with IPR Systems.[276] Their goal is to provide an easy way for society members (including authors and publishers) to deliver their content to the market place at low cost and with fair royalties for content owners.

[275] OZAUTHORS, OzAuthors Online Ebook Store, Last checked: October 11 2007, http://www.ozauthors.com

[276] Renato, I. (2001). Digital Rights Management (DRM) Architectures. D-Lib Magazine Article, Volume 7, Number 6.

Fig. 14 shows the OzAuthors' interface for collecting rights related information. In this example, the "Usage Rights and Pricing" frame, allows the content provider to specify “Read” and/or “Print” permissions, pricing, and security options for the ebook. Additionally, a number of pages can be specified for free preview. The second frame of the interface allows the content provider to specify all involved rights holders, their roles, and their percentage on the royalty split. Each time the ebook is sold, the rights holders will automatically receive the indicated amount. By inspecting the front end of a DRM system it is evident that there are two critical architectures to consider. The first is the functional architecture, which covers the high-level architectural components of a DRM system. The second critical architecture is the information architecture, which covers the modelling of the key-players within a DRM system as well as their relationships. In the following, indicative diagrams will be used to illustrate an electronic transaction, in terms of the aforementioned architectures, with special focus on the process of removing the constraints on the use of a digital asset by clearing the rights and obtaining on-line licenses for its use.

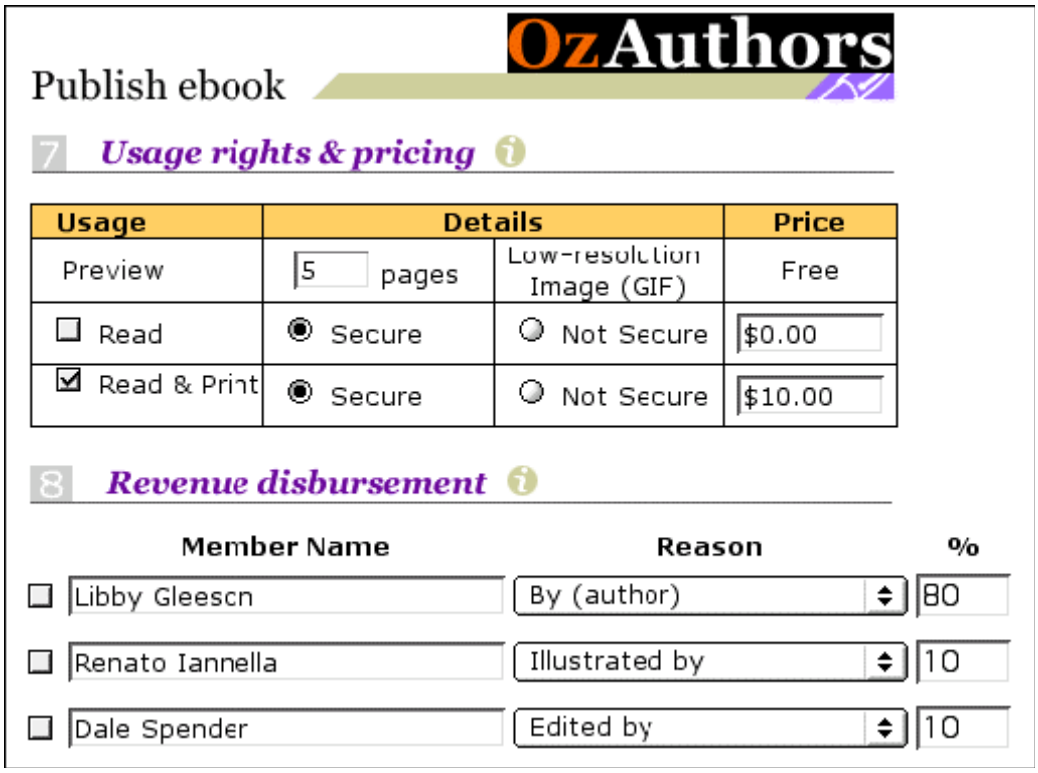

Figure 14: DRM – Front end example application

4.3.2. Functional Architecture

The core functionality of a DRM framework can be separated in the following three main areas.

- Intellectual Property (IP) Asset Creation and Capture: refers to the circumstances under which content is created in order to favor its trade. Asserting rights when content is initially created is one such example, since it reduces the complexity of subsequent rights clearance.
- IP Asset Management: asset management and trade, follows its creation and is carried out by a system that addresses trading requirements, such as descriptive and rights metadata management.
- IP Asset Usage: monitoring of content usage once it has been traded is the primary goal of this component, which involves applying usage rules over traded content.

While the above core components comprise the broad trucks for DRM, these models need to be further extended in order to fully describe the functionality required by a DRM system (see Fig. 15).

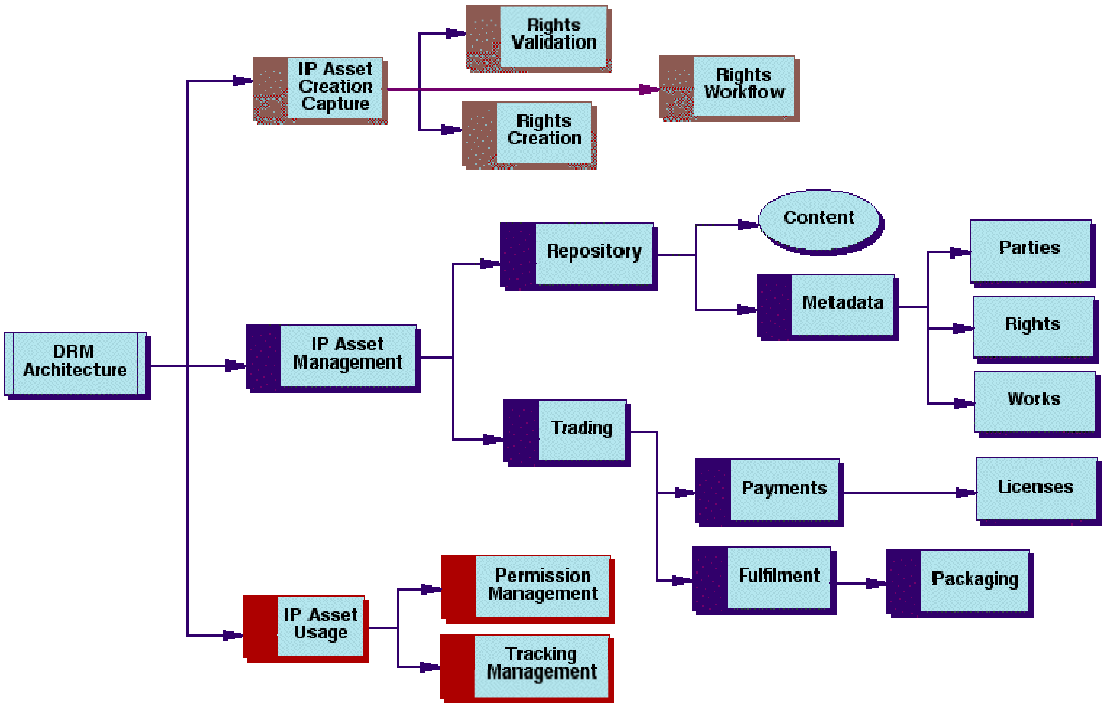

Figure 15: DRM Functional Architecture

The functional architecture stipulates the roles and behavior of a number of cooperating and interoperating modules under the three areas of Intellectual Property (IP): asset creation, management, and usage. Each of these modes is attached with a model hierarchy that provides more detailed description of DRM functionalities. A thorough analysis of the functional architecture can be found.[277] However, functional architecture is only part of the answer to the challenges of DRM, since rights management can become complex remarkably quickly. As a result, DRM systems must follow the, more flexible, information model that addresses these complex and layered relationships.

4.3.3. Information Architecture

Entities and relations are two widely established notions that are used to model certain aspects of the real world. In this context, information architecture is primarily concerned with the entities and relations governing DRM functionality. Modeling all different aspects of DRM functionality requires the following actions:

- model the entities;
- identify and describe the entities, and;
- express the rights statements.

Modeling the entities

A clear and complete model that incorporates all existing entities and relations is useful for identifying the underlying technologies of a DRM framework. The <indecs> project introduces a model where the three core entities: users, content and rights are clearly separated as shown in Fig. 16.[278] The Users entity encompasses any type of user, from a rights holder to an end-consumer. Content can be any type of content that is subject to electronic trade and the rights entity is an expression of the permissions, constraints, and obligations between the users and the content. The main advantage of this model is that it provides the greatest flexibility when assigning rights to any combination or layering of users and content. The core entities model is highly adjustable and can be used to model the needs of new and evolving business models.

[277] Renato, I. (2001). Digital Rights Management (DRM) Architectures. D-Lib Magazine Article, Volume 7, Number 6.

[278] INDECS (2002). Interoperability of Data in E-commerce Systems. Retrieved February 1, 2008 from http://www.indecs.org.

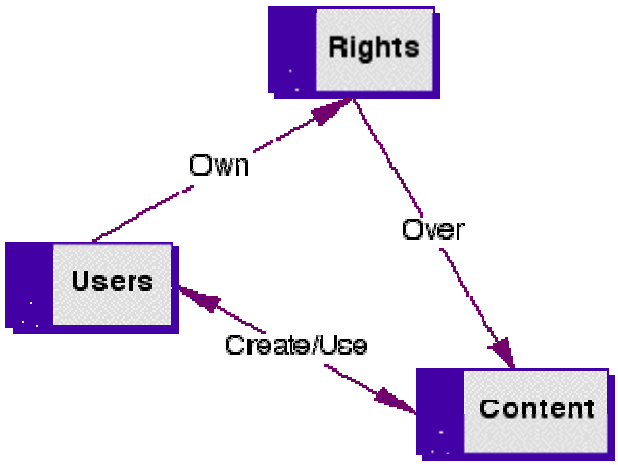

Figure 16: DRM information architecture – core entities model

The core entities diagram depicted above, constitutes a rather abstract modeling of DRM functionality and indicates that all three entities need to incorporate a mechanism for communicating metadata between them. Attempting a more thorough analysis of the model would require the Content and Rights entities to be further extended by more fine grained entities and relations. International Federation of Library Associations (IFLA) has proposed an extended model for Content entity that is based on many "layers" from various intellectual stages or evolution of its development. The goal behind this extended model is to enable clearer (i.e., more explicit and/or appropriate) attribution of rights information. According to this model, content can be identified at the work, expression, manifestation, and item layers, as shown in Fig. 17. At each of these layers, different rights and rights holders may need to be supported. Further explanations of the extended model for Content entity can be found in (Renato 2001).[279]

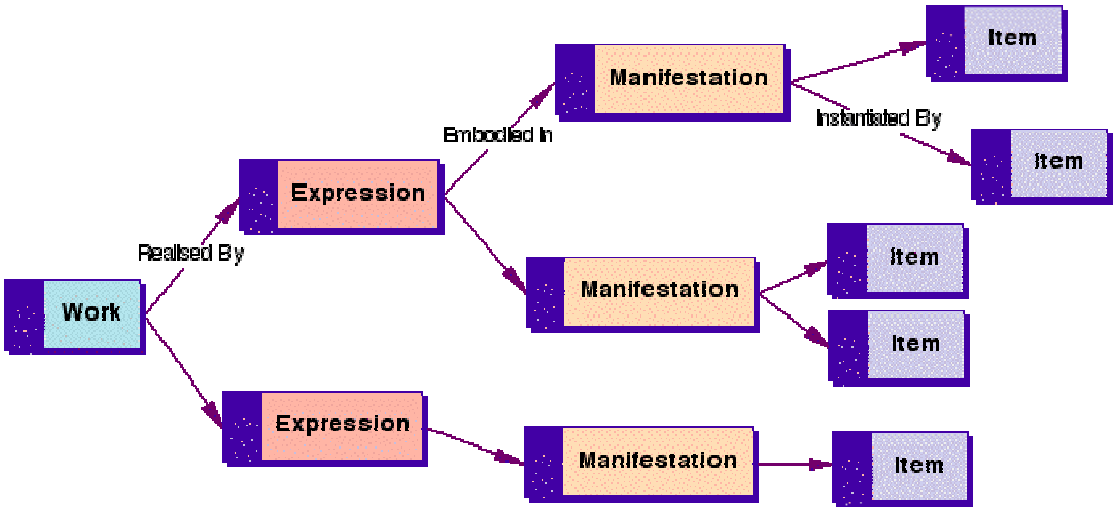

Figure 17: DRM information architecture – content model

Expressing rights statements

The rights entity is dealing with the allowable permissions, constraints, obligations, and any other rights-related information involving users and content and determines the required expressivity power of the language used to represent rights metadata information. Rights expressions can become complex quite quickly, especially in cases where the number of required statements grows large. As shown in Fig. 18, rights expressions should consist of: permissions (i.e., usages) - what you are allowed to do, constraints - restrictions on the permissions, obligations - what you have to do/provide/accept and right holders - who is entitled to what.

[279] Renato, I. (2001). Digital Rights Management (DRM) Architectures. D-Lib Magazine Article, Volume 7, Number 6.

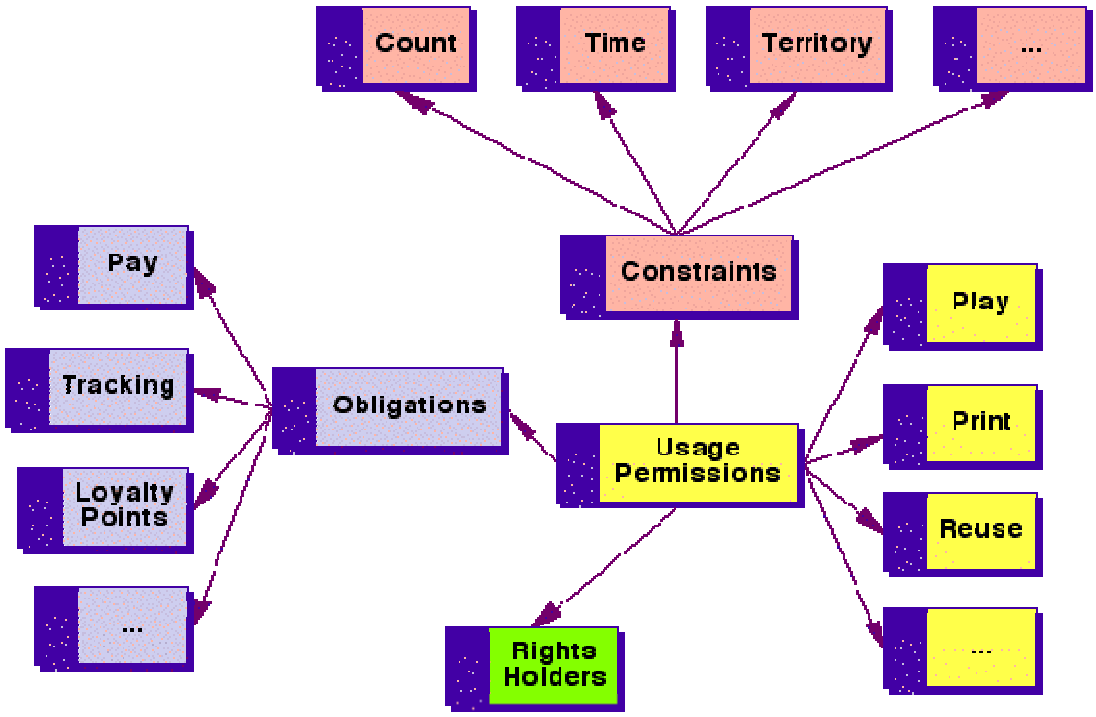

Figure 18: DRM information architecture – rights expression model

For example, as demonstrated by the motivating example, a rights expression may state that a particular ebook can be read and printed (i.e., a usage permission), for a $10 fee (i.e., an obligation to pay) and a maximum of 5 pages can be used for preview purposes (i.e., a count constraint). Additionally, each time the ebook is used, Libby, Renato, and Dale (the right holders) receive a percentage of the fee.

4.4. Rights Clearance & Business Model

After identifying and describing the key-entities and relations of DRM functionality, it is interesting to consider the aforementioned observations in the context of a more general business model. The aim is to investigate inherent weaknesses of on-line rights clearance activities and trace pitfalls that are likely to arise. Eventually, technology potentials will be investigated for tackling these weaknesses.

4.4.1. General Architectural Model

For the purposes of our investigation we will use the business model developed as part of the IMPRIMATUR Project (ESPRIT 20676).[280] The validity of this model was further certified via its subsequent adoption by the TRADEX (TRial Action for Digital object EXchange) Project (IST 21031).[281] For an extensive description of this model in the context of a cultural information system, the interested reader is referred to (Tsolis 2005).[282]

[280] IMPRIMATUR, Intellectual Multimedia Property RIghts Model and Terminology for Universal Reference, Not available, http://www.imprimatur.alcs.co.uk/index.htm

[281] TRADEX, TRial Action for Digital object EXchange, Not available, http://www.iccd.beniculturali.it/download/tradex.pdf

[282] Tsolis, G. K., Nikolopoulos, S. N., Kazantzi, N.V., Tsolis, D. K. & Papatheodorou, T. S. (2005). Re-Engineering digital watermarking of copyright protected images by using xml web services. in Proc. of the Ninth IASTED International Conference on INTERNET & MULTIMEDIA SYSTEMS & APPLICATIONS (IMSA 2005), Honolulu, Hawaii, USA, 15 – 17 August, 2005, pp. 264-270.

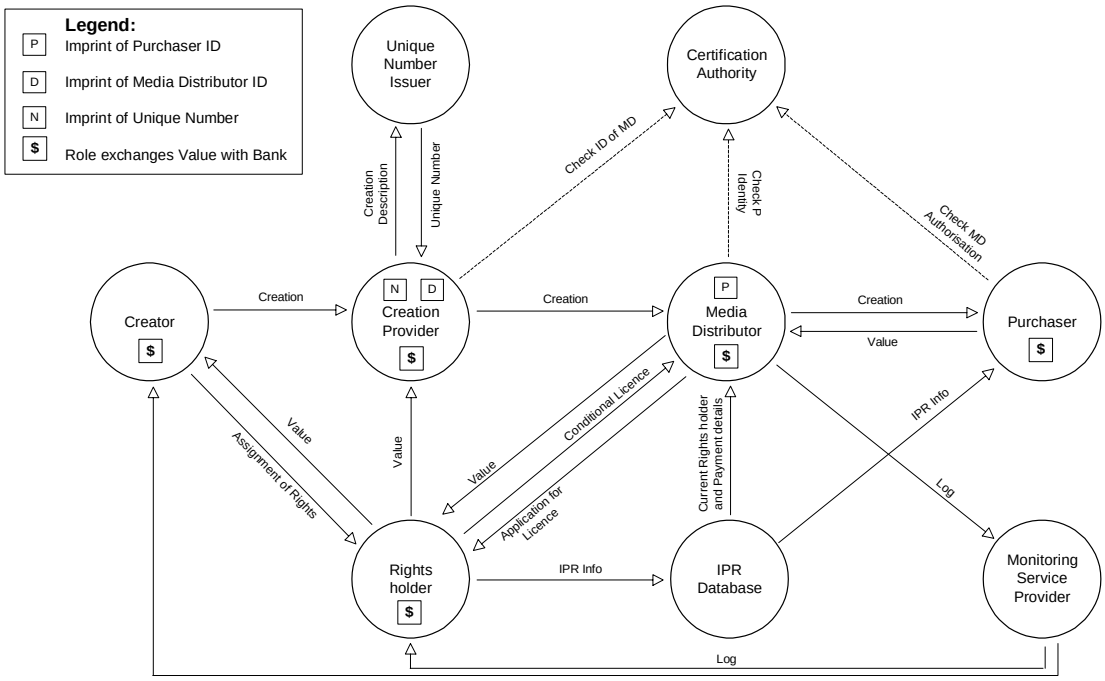

Figure 19: The DRM Business Model

The actors (stakeholders) identified in this model are:

- The creator is the author of the copyrighted work.
- The right holder (or copyright owner), acts of behalf of the creator and is responsible for licensing the use of the creation. Specifically, he defines the conditions of use, records the IPR information at a registry and collects the royalties deriving from trading of the works which he is in charge to administer.
- The content provider (or service producer), is in charge to prepare content for being traded electronically, and thus, for example, to embed into creations those mechanisms that will allow the tracking of copyright (watermarks). This player has to employ the necessary technological means so as to ensure that copyright can always be protected.
- The media distributor (or service provider), who has the responsibility to distribute to purchasers the creations, and thus to satisfy the request of his clients. This involves re-assuring that the IPR on the distributed material is protected and the related fees paid. This actor requires accessing the databases where IPR information is stored and using all the technological means needed to protect the copyright of the creations he trades (watermarking, cryptography, secure protocols). Moreover, he will have to offer the purchasers electronic licenses that determine the permissions, constraints and obligations of content use, as well as provide the authors, right-holders and other authorised actors a set of services to monitor and control the trading of their works.
- The IPR database or register, is the repository of all information related to the intellectual properties of copyright protected works, and has to be accessible at different levels of detail and confidentiality. For instance, the information useful for identifying the creations and detailing the licensing rules is of particular importance and will have to be persistently maintained.
- The unique number issuer, a naming registration authority who will be responsible for assigning a unique identifier to each creation, for facilitating its tracking.
- The monitoring service provider or controller, who will be a trusted third party (TTP) responsible for monitoring that all transactions have been carried out legally.
- The certification authority, which is also a TTP, with the task to authenticate all actors, by means of electronic certification.

It is evident by the aforementioned analysis that besides the need of establishing trusted organisations, there are cases where technological solutions are necessary to facilitate secure and effective electronic trade, without violating intellectual property rights.

4.4.2. Technology Insertion Points

Following the description of the key actors, it is important to outline the technologies necessary to facilitate electronic trade and clearly situate their functionality within the rights clearance framework.

- **Relational databases** can serve as the repository infrastructure that will store all information required by the framework.
- **Communication protocol** will allow different components to seamlessly communicate. As suggested by the diagram depicting the IMPRIMATUR business model, engineering an information system for performing electronic trade, would require the existence of many distributed functional components. Employing a standardised communication protocol would make binding between components more loosely-coupled and greatly benefit the reusability of components and extensibility of the framework.
- **IPR Metadata standards** are essential for representing intellectual property information in an interoperable manner. These standards are particularly important for the **IPR Database** and **Rights holder** actors and its proper use and adjustment will favor the openness of the developed framework.
- **Rights expression language** will try to cope with the increased level of complexity stemming from the number of conditions, restrictions and obligations included in the license documents. The **Rights holder** along with the **Media distributor** will be the main consumers of this technology and is particular important for implementing a valid rights clearance service.
- **Technological Protection Means** such as watermarking, encryption etc, are the key functional component used for the protection and management of intellectual property rights. The DRM framework requires for a means to prevent unauthorised users from violating the intellectual property rights of traded content. In the case of watermarking, copyright information is invisibly embedded inside the image digital content and technological evidence of the image ownership can be obtained by extracting this information.[283] The embedded information typically corresponds to the **Rights holder** copyright notice and according to the aforementioned business model, the player that benefits more from utilising this technology is the **Content provider**.
- **Uniform resource identifiers**, are the cornerstone of services involving transaction tracking, since all entities need to be both identified and described uniformly. Identification should be accomplished via open and standard mechanisms that will facilitate the association of metadata records with creations. Open standards such as Uniform Resource Identifiers (URI) and Digital Object Identifiers (DOI), as well as the emerging ISO International Standard Textual Work Code (ISTC) are typical schemes for producing uniform resource identifiers.

4.5. Rights Clearance Technologies

The purpose of this section is to elaborate on the technologies that are more tightly related to on-line rights clearance and not DRM in general.

4.5.1. Communication Standards

Traditionally, information systems are architected using a component-based approach. Typically, the distinct components of the information system are closely interrelated, in such a way that modifications in any one of them subsequently causes extensive changes to other parts. This fact restricts their maintainability and limits their future expansion. Web Services are a set of open standards and protocols that were introduced to increase the reusability and interoperability of the components, by making the binding between them more loosely-coupled. Further elaboration on the topic of web services is out of the scope of this chapter, but the interested reader can refer to (Tsolis 2005).[284]

4.5.2. IPR Metadata Standards

Independently of the adopted rights protection and management strategy, information is considered of vital importance. It is the information that allows the rights administrator to check the validity of content use, to trace potential usage violations, to grant the copyright of an artwork, etc. Information is also the mean that allows the end user to communicate with the copyright holder in order to file a request for using the copyright protected content or acquire the pricing policy of an artwork available on-line. The data comprising this type of information concerns various aspects of

283 Tsolis, G. K., Tsolis, D. K. & Papatheodorou, T. S. (2001) A watermarking environment and a metadata digital image repository for the protection and management of digital images of the hellenic cultural heritage. Proc. IEEE International Conference on Image Processing 2001, Thessaloniki, Greece, 2001, 566-569.

284 Tsolis, G. K., Nikolopoulos, S. N., Kazantzi, N.V., Tsolis, D. K. & Papatheodorou, T. S. (2005). Re-Engineering digital watermarking of copyright protected images by using xml web services. in Proc. of the Ninth IASTED International Conference on INTERNET & MULTIMEDIA SYSTEMS & APPLICATIONS (IMSA 2005), Honolulu, Hawaii, USA, 15 – 17 August, 2005, pp. 264-270.

object property status such as, a) the intellectual property rights owner b) the intellectual property rights holder in case he is different from the owner c) communication details of the rights holder d) technological means used to protect and manage property rights, etc.

This type of information should accompany the digital artwork and be easily and directly accessible. The amounts of information that is related with a digital object and describe their technical and semantic characteristics are addressed by the term metadata. The set of metadata is intended to capture the information that the content creator chooses to preserve. With regards to the protection and management of intellectual property rights, it is very important that the set of metadata chosen to document the digital artwork, also incorporates data related to intellectual property. These data will formulate the means on which digital rights management systems will base their functionalities. The need for including rights related metadata has been recognised by dominant standardisation bodies and is reflected to some of the most widely accepted metadata standards.

Open standards were established to facilitate the description of digital resources. The introduction of XML (Extensible Markup Language)[285] by W3C has launched numerous resultant languages, protocols and technologies, which are commonly used today by both research projects and commercial applications. XSD (XML Schema Definition)[286] and RDF (Resource Description Framework)[287] have standardised the processes of defining metadata sets and characterising resources. In order to accommodate the requirements of vertical applications, specialised metadata sets were also introduced, such as Dublin Core (DC)[288], DIG35[289] and MPEG-7[290] to name only a few.

Amongst the various metadata standardisation initiatives, Dublin Core (DC) has gained significant visibility and appeal. Dublin Core is a metadata standard that supports the diversity, convergence and interoperability of digital cultural objects and aims at supporting a wide range of business models. The basic schema proposed by Dublin Core is a simple content description model, defined by its 15 elements, out of which four are related with intellectual property rights namely, creator, publisher, contributor, rights.

The Digital Image Group (DIG)[291] is a non-profit cooperation between the industrial players of digital image such as software companies, consumers of digital images, etc. The primary goal of DIG35 is to establish an open framework for the exchange of ideas concerning the investigation, implementation and exploitation of methods and technologies that will boost the market related to digital imaging. This metadata standard is already being widely used in simple end-user devices and even to worldwide networks. DIG35 constitutes a rather extensive metadata set and includes information for a large set of digital image technical and semantic characteristics. Despite the fact that DIG35 is mainly oriented to digital images, the intellectual property related metadata are valid for all different types of multimedia content. The total amount of DIG35 metadata that are directly or indirectly related to intellectual property rights can be divided in 7 categories namely, names, description, dates, exploitation, digital rights management system, identification info and communication info.

4.5.3. Rights Expression Languages

MPEG-REL

MPEG - Rights Expression Language is a machine translatable description language, suitable for defining intellectual property rights, grants and licenses. Its role, in the context of rights clearance, is to provide a flexible and interoperable scheme for large scale consumption of digital objects and facilitate the distribution of digital content while protecting

285 XML, eXtensive Markup Language. Last checked: 11 October 2007, http://www.w3.org/XML/

286 XSD, eXtensible Markup Language Schema, Last checked: 11 October 2007, http://www.w3.org/XML/Schema

287 RDF, Resource Description Framework. Last checked: 11 October 2007, http://www.w3.org/RDF/

288 DCMI, Dublin Core Metadata Initiative, Last checked: October 11 2007, http://www.dublincore.org/

289 DIG35, Digital Image Group - DIG35 Specification – Metadata for Digital Images. Last checked: 11 October 2007, http://www.i3a.org/i_dig35.html

290 MPEG7, ISO/IEC Moving Picture Experts Group. Last checked: 11 October 2007, http://www.chiariglione.org/mpeg/standards/mpeg-7/mpeg-7.htm

291 DIG35, Digital Image Group - DIG35 Specification – Metadata for Digital Images. Last checked: 11 October 2007, http://www.i3a.org/i_dig35.html

its intellectual properties. The rights expression language defines the linguistics for expressing rules through rights statements. License rules can be rather simple such as, *"this content is allowed to be replicated or reproduced"* or more complicated such as, *"this content is allowed to be reproduced on Tuesday on 7 of March and at 6:00 am, under the condition that the reproducing device satisfies a number of criteria"*. Such expressions are likely to be created for every person that has the authority to transfer the copyright of protected content. Rights Expression Language is considered a fundamental part of MPEG-21[292] mainly due to the intention of MPEG group in establishing a protocol that will allow heterogeneous systems to seamlessly communicate. Thus, the existence of a standardised language for incorporating digital content rights into machine understandable licenses is considered very important. The aim of this section is to investigate the REL data model, analyse its structure identify the key-components and summarise the relevant technological platforms.

The REL data model[293] as realised by MPEG-21, incorporates a simple and extensible data model for representing the basic concepts and components. Specifically, it is consisted of four basic entities and the relations among them. The following diagram depicts the fundamental entities and their interrelations.

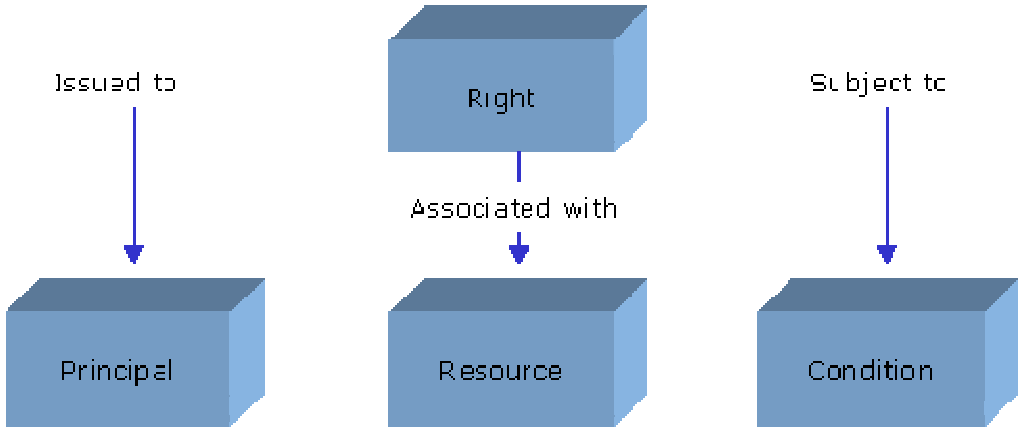

Figure 20: REL Data Model

Principle: The principle entity models the potential users involved in the process of distribution, usage, and content consumption.
Right: Right is the "action" the practice of which is being transferred to the Principle.
Resource: Resource is considered the "object" the rights of which are being transferred to the principle.
Condition: The condition entity determines the terms, restrictions and obligations under which the right is allowed to be exercised.

The four aforementioned entities comprise a grant. By itself, a grant is not a complete rights expression that can be transferred unambiguously from one party to another. A full rights expression is called a license. A typical license consists of one or more grants and an issuer, which identifies the party who issued the license. In case the licence publisher wants to grant distribution rights to an e-shop or DRM, he signs a distribution license. The grant of a distribution license, instead of the right to be transferred, contains a new grant as seen in Fig. 20.

The procedure of implementing the MPEG-21 REL initiated with the establishment of a set consisting of 48 requirements. Experts from heterogeneous sectors agreed that the fulfilment of the aforementioned requirements would suffice to guarantee the success of the initiative. The set of requirements extends to various fields ranging from the language expressivity to security. Eventually, the XrML (eXtensible Rights Markup Language)[294] technological platform was selected to serve as the groundwork of MPEG-21 REL. To promote interoperability, MPEG has developed the Rights Data Dictionary (RDD) to ensure that the semantic interpretation of new verbs is unambiguously

[292] MPEG21, MPEG-21 Overview v5, Last checked: 11 October 2007, http://www.chiariglione.org/mpeg/standards/mpeg-21/mpeg-21.htm

[293] MPEG REL, ISO/IEC FDIS 21000-5: Information Technology - Multimedia Framework - Part 5: Rights Expression Language, (2003).

[294] XrML (2007). Extensible Rights Markup Language – XrML, 2.0 Specification. Retrieved February 1, 2008 from http://www.xrml.org.

understood. The RDD comprises a set of clear, consistent, structured, integrated and uniquely identified Terms to support the MPEG-21 REL. As well as providing definitions of Terms for use in the REL, the RDD specification is designed to support the mapping and transformation of metadata from the terminology of one namespace (or Authority) into that of another namespace (or Authority) in an automated or partially-automated way, with the minimum ambiguity or loss of semantic integrity.

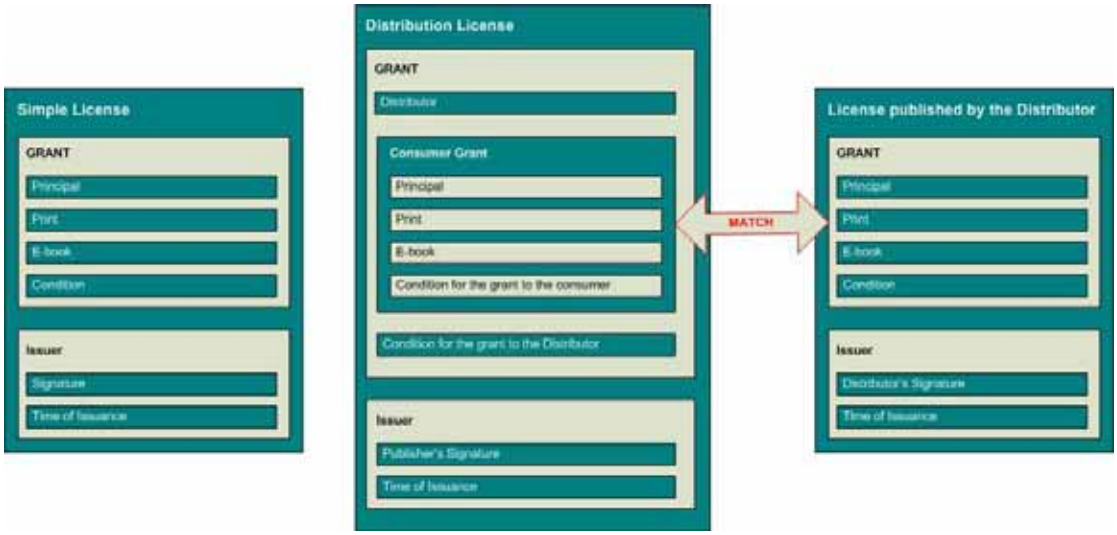

Figure 21: MPEG 21 - REL Data Model

Open Digital Rights Language – ODRL

ODRL complements existing analogue rights management standards by providing digital equivalents, and supports an expandible range of new services that can be afforded by the digital nature of the assets in the Web environment.

ODRL is a standard language and vocabulary for the expression of terms and conditions over assets. It covers a core set of semantics for these purposes including the rights holders and the expression of permissible usages for asset manifestations. Rights can be specified for a specific asset manifestation or could be applied to a range of manifestations of the asset. *ODRL* is focused on the semantics of expressing rights languages and definitions of elements in the data dictionary.

ODRL does not enforce or mandate any policies for DRM, but provides the mechanisms to express such policies. Communities or organisations, that establish such policies based on *ODRL*, do so based on their specific business or public access requirements. *ODRL* depends on the use of unique identification of assets and parties The *ODRL* model is based on an analysis and survey of sector specific requirements (including models and semantics), and as such, aims to be compatible with a broad community base.

ODRL is based on an extensible model for rights expressions which involves a number of core entities and their relationships. This *ODRL* Foundation Model is shown in Fig. 21.

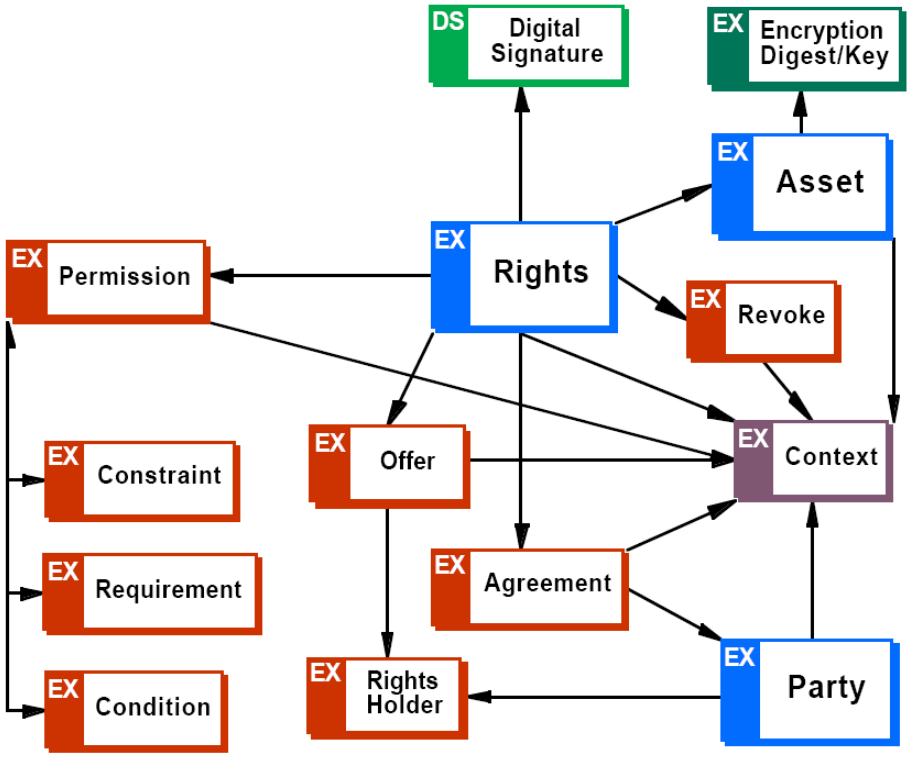

Figure 22: The ODRL Foundation Model

The model, as shown in Fig. 21, consists of the following three core entities: assets, rights and parties. The assets include any physical or digital content. The assets must be uniquely identified and may consist of many subparts and be in many different formats. The rights include permissions which can then contain constraints, requirements, and conditions. Permissions are the actual usages or activities allowed over the assets (e.g., Play a video asset). Constraints are limits to these permissions (e.g., Play the video for a maximum of 5 times). Requirements are the obligations needed to exercise the permission (e.g., Pay $5 each time you play the video). Conditions specify exceptions that, if become true, expire the permissions and renegotiation may be required (e.g., If credit card expires then all permissions are withdrawn to play the video). The parties include end users and right holders. Parties can be humans, organisations, and defined roles. End users are usually the asset consumers. Right holders are usually parties that have played some role in the creation, production, distribution of the Asset and can assert some form of ownership over the asset and/or its permissions. Right holders may also receive royalties.

Most entities in the model can support a specific context. A context, which is relative to the entity, can describe further information about that entity or the relationship between entities. For example, the context of an agreement may specify the date of the transaction, the context of a party may specify their role.

The asset entity (sometimes referred to as a work, content, creation, or Intellectual Property), is viewed as a whole entity. If the rights are assigned at the asset's subpart level, then such parts would require to also be uniquely identifiable. However, *ODRL* can specify constraints on subparts of the asset. Additionally, assets can be identified as to their layer of intellectual property as defined by the IFLA model. These include work, expression, manifestation, and item. These features also allow rights to be expressed over non-tangible assets and individual instances.

These core entities together allow for a wide and flexible range of *ODRL* expressions to be declared. Additionally, the expressions can be digitally signed.

4.5.4. Watermarking

Watermarking can be considered as an integrated service, providing protection and assisting management of intellectual property rights. Watermark technology incorporates encryption methods to ensure unambiguous and categorical proof

of ownership, as well as image processing techniques for conveying useful information inside the digital content.[295] The level of functionality that can be achieved by the proposed scheme depends upon the usage policy of the conveyed information. A typical scenario involves an organisation that owns a great collection of digital images and is willing to sale high quality copies of collection objects for a standard price. Prior to delivery, the organisation embeds a digital watermark inside the image content. The watermark serves three different purposes, a) give proof of ownership, b) identify the transaction that took place and c) correlate the transaction description with the specific image copy. All details necessary for describing a transaction are included within the image metadata information maintained within the content provider's database infrastructure.

In this case, the input arguments of watermark embedding mechanism consist of two integer numbers. The first number corresponds to the encryption key while the second to the transaction identification number. The encryption key is used for invoking the core cryptographic module that guarantees for watermark's security. It's a unique private number that constitutes the key of the system's cryptographic attributes and is used by the right's holder for proving his ownership.

Thus, there is a need for universal administration of such numbers in order to avoid conflicts and irresolvable disputes. This role is appointed to uniform resource identifier systems that will be described at a later section. If we consider that a uniform resource identifier is consisted of two distinct numbers, a prefix and a suffix, the watermarking scheme performs the following actions. By using the prefix number as seed for cryptographically encoding the watermark information within the image digital content, the proposed scheme exploit's the handle system administration facilities for resolving ownership disputes. The suffix is an independent number selected by the institution protocol service; it is administered locally and can be regarded as the transaction identification number. This number is encoded inside the digital image content and can be retrieved by the decryption mechanism.

4.5.5. Unique Resource Indentifier

Open object identification systems are deemed very important for distributed environments like the ones encountered in electronic commerce. Global identifiers should allow for unique identification of digital objects in order to facilitate the operations of rights clearance.

Handle System

The Handle System[296] is a distributed information system designed to provide an efficient, extensible and confederated name service that allows any existing local namespace to join the global handle namespace by obtaining a unique Handle System naming authority. Local names and their value-binding(s) remain intact after joining the Handle System. Any handle request to the local namespace may be processed by a service interface speaking the Handle System protocol. Combined with the unique naming authority, any local name is guaranteed unique under the global handle namespace.

It is probably best to view the Handle System as a name-attribute binding service with a specific protocol for securely creating, updating, maintaining, and accessing a distributed database. It is designed to be an enabling service for secured information and resource sharing over networks such as the public Internet. Applications of the Handle System could include metadata services for digital publications, identity management services for virtual identities, or any other applications that require resolution and/or administration of globally unique identifiers.

Handle Namespace

Every handle consists of two parts: its naming authority, otherwise known as its prefix, and a unique local name under the naming authority, otherwise known as its suffix:

<Handle> ::= <Handle Naming Authority> "/" <Handle Local Name>

The naming authority and local name are separated by the ASCII character "/". The collection of local names under a naming authority defines the local handle namespace for that naming authority. Any local name must be unique under its local namespace. The uniqueness of a naming authority and a local name under that authority ensures that any handle is globally unique within the context of the Handle System.

[295] Cox, I., Miller, M. L. & J. A. Bloom. (2002) Digital watermarking. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc.

[296] Kahn, R. & Wilensky, R. (2006). A Framework for Distributed Digital Object Services. International Journal on Digital Libraries, Springer, Volume 6, Number 2, April 2006.

For example, "1082.5000/image1" is a handle for a digital image published on a cultural website. Its naming authority is "1082.5000" and its local name is "image1". The handle namespace can be considered a superset of many local namespaces, with each local namespace having a unique naming authority under the Handle System. The naming authority identifies the administrative unit of creation, although not necessarily continuing administration, of the associated handles. Each naming authority is guaranteed to be globally unique within the Handle System. Any existing local namespace can join the global handle namespace by obtaining a unique naming authority so that any local name under the namespace can be globally referenced as a combination of the naming authority and the local name as shown above.

Naming authorities under the Handle System are defined in a hierarchical fashion resembling a tree structure. Each node and leaf of the tree is given a label that corresponds to a naming authority segment. The parent node notifies the parent naming authority of its child nodes. Unlike DNS, handle naming authorities are constructed left to right, concatenating the labels from the root of the tree to the node that represents the naming authority. Each label is separated by the octet used for ASCII character "." . Each naming authority may have many child naming authorities registered underneath.

Any child naming authority can only be registered by its parent after its parent naming authority has been registered. However, there is no intrinsic administrative relationship between the namespaces represented by the parent and child naming authorities. The parent namespace and its child namespaces may be served by different handle services, and they may or may not share any administration privileges.

Handle System Architecture

The Handle System defines a hierarchical service model. The top level consists of a single handle service, known as the Global Handle Registry (GHR). The lower level consists of all other handle services, generically known as Local Handle Services (LHS).

The Global Handle Registry can be used to manage any handle namespace. It is unique among handle services only in that it provides the service used to manage naming authorities, all of which are managed as handles. The naming authority handle provides information that clients can use to access and utilise the local handle service for handles under the naming authority.

Local Handle Services are intended to be hosted by organisations with administrative responsibility for handles under certain naming authorities. A Local Handle Service may be responsible for any number of local handle namespaces, each identified by a unique naming authority. The Local Handle Service and its responsible set of local handle namespaces must be registered with the Global Handle Registry.

The Global Handle Registry maintains naming authority handles. Each naming authority handle maintains the service information that describes the "home" service of the naming authority. The service information lists the service sites of the given handle service, as well as the interface to each handle server within each site. To find the "home" service for any handle, a client can query the Global Handle Registry for the service information associated with the corresponding naming authority handle. The service information provides the necessary information for clients to communicate with the "home" service.

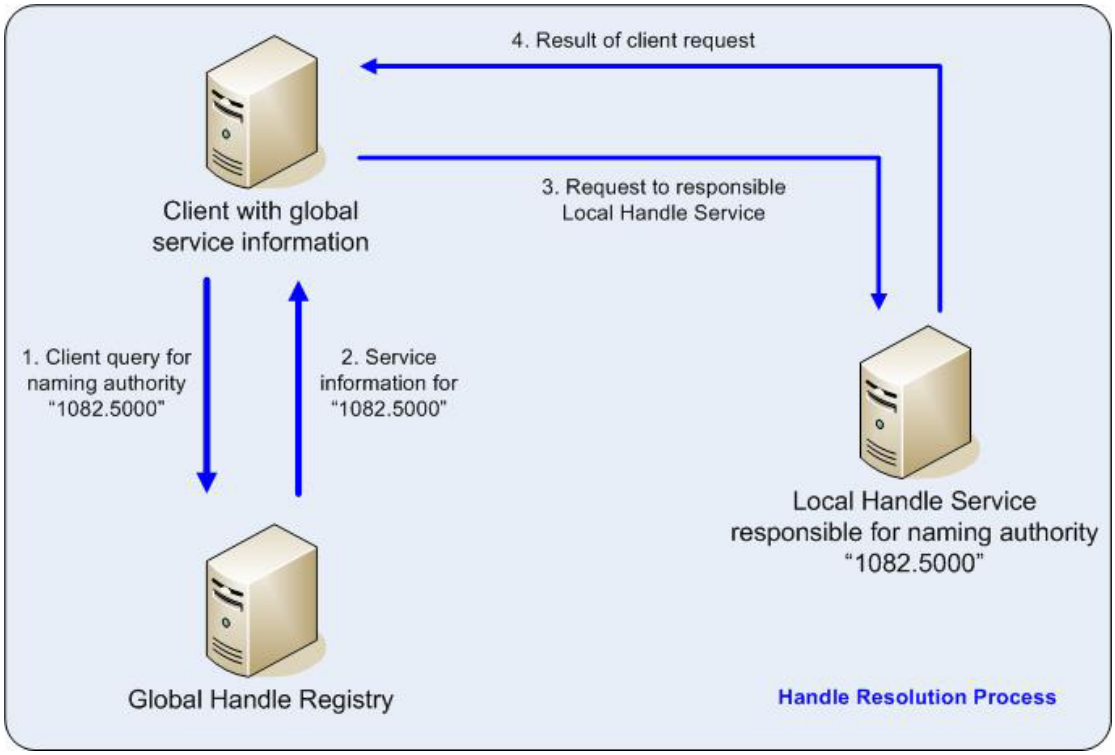

Figure 23: Example of handle resolution process

Fig. 22 shows an example of a typical handle resolution process. In this case, the "home" service is a Local Handle Service. The client is trying to resolve the handle "1082.5000/1" and has to find its "home" service from the Global Handle Registry. The "home" service can be found by sending a query to the Global Handle Registry for the naming authority handle for "1082.5000". The Global Handle Registry returns the service information of the Local Handle Service that is responsible for handles under the naming authority "1082.5000". The service information allows the client to communicate with the Local Handle Service to resolve the handle "1082.5000/1".

To improve resolution performance, any client may choose to cache the service information returned from the Global Handle Registry and use it for subsequent queries. A separate handle caching server, either stand-alone or as a piece of a general caching mechanism, may also be used to provide shared caching within a local community. Given a cached resolution result, subsequent queries of the same handle may be answered locally without contacting any handle service. Given cached service information, clients can send their requests directly to the correct Local Handle Service without contacting the Global Handle Registry.

4.6. Case Study: SilkDRM

SilkDRM is a new Digital Rights Management System that provides on-line Rights Clearance for digital images (or other digital assets). Individuals and/or institutions who own the Intellectual Property Rights of digital images can use SilkDRM in order to ensure the authenticity of their content. Additionally, the system can be authorised by the right holder to issue distribution licenses for the digital resources. This is done by signing a special license which describes the set of rights that can be assigned for a specific resource, as well as the equivalent necessary conditions under which the assignment can be made.

4.6.1. System Functionality

SilkDRM is accessible to internet users through its easy to use web interface. A number of Cultural Institutions who created websites for their digitised content, used the system in order to document their rights on the content and as a mechanism for the production of digital licenses on its use. In practice, the Cultural Institutions registered their content in the system and in parallel, in the webpages presenting the digital assets they provide a hyperlink to SilkDRM. By following that hyperlink, the visitor is directed to the corresponding page from where he can retrieve information about

the intellectual property rights binding the digital resource, as well as the conditions for obtaining a use license. If the rights holder decides to use digital watermarking for protecting his content, he is able to embody the unique code created by SilkDRM in the watermark. In this case, the detection of the watermark can lead one to the corresponding page of the DRM (through the code retrieved).

4.6.2. System Users

The two basic system user types involved in SilkDRM are Content Providers and Content Consumers. Content Providers include single users or members of a Cultural Organisation aiming in registering their digital content in order to authenticate their ownership over the content and pursue its commercial exploitation. A Content Consumer is browsing the DRM webpages, receiving intellectual property information on specific digital resources and potentially apply for a use license. A Content Consumer can be not only an individual but also an e-shop. In this scenario, the rights holder has assigned the distribution of his content to an e-shop. The e-shop contacts the DRM in order to retrieve information concerning the terms and conditions set by the owner for the selling of the digital resource and present them to the potential buyers. In case the item is sold, the DRM is responsible for publishing the corresponding use license and forward it to the e-shop. SilkDRM is able to communicate with various payment services over the web, achieving this way transaction monitoring as well as the validation of published licenses. Beside the aforementioned users, any generic machine, implementing a specific communication protocol based on standard web technologies, is able to connect and transact with the system.

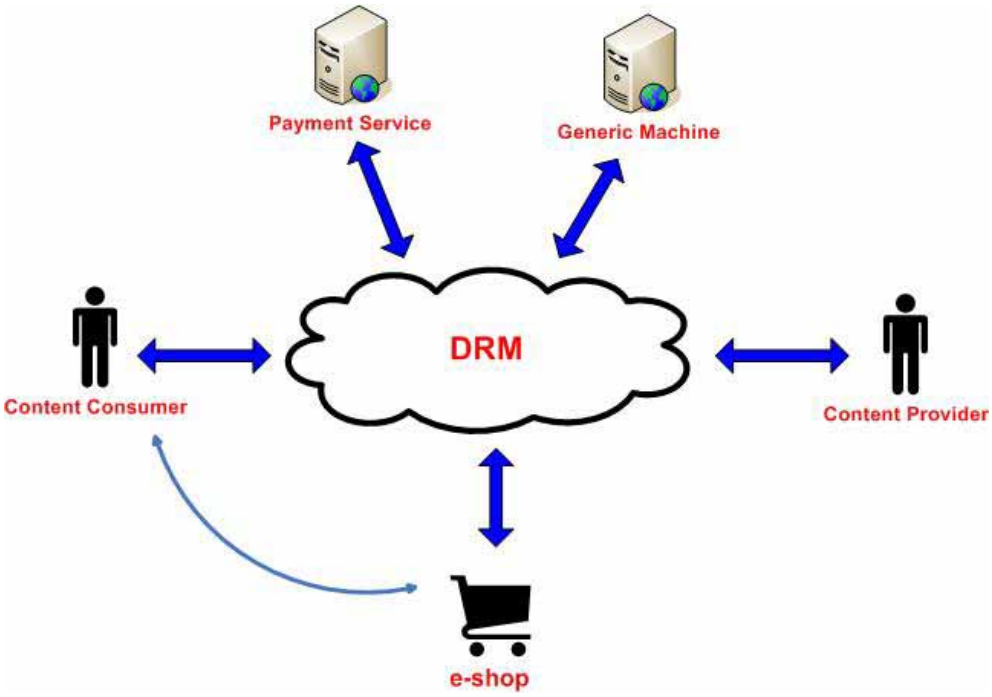

Figure 24: SilkDRM System functionality

4.6.3. Content Providers

When a content provider browses our web pages for the first time, he is prompted to fill in an application form for the creation of an account. This form includes personal and corporate information in case the user acts on behalf of an organisation/institution. SilkDRM administrator processes the application and contacts the applicant in order to retrieve information about the resources that he intends to register in the DRM. The next step includes the preparation of a legal contract, in which the applicant declares that he or the institution that he represents is the intellectual property rights holder of the content that will be registered in SilkDRM. When the contract is signed, a new account is created and the applicant becomes a registered user of the system. The first account created, is an account of the organisation administrator having full rights to all system functionalities.

The administrator can create new accounts and assign user rights to the people he chooses. The “register procedure” for a new digital resource in the DRM, is implemented by filling in some forms containing descriptive information about the resource and its intellectual property. In parallel, a preview picture (eg. thumbnail) can be uploaded. In case the

rights holder has decided to watermark the resource, he can ask the DRM to produce a unique identification number, in order to be embedded in the watermark. SilkDRM can also produce a handle for the resource, in order to facilitate a unique addressing method. The registration of digital assets to the DRM can also be accomplished through a batch process, during which SilkDRM processes a set of xml files (one for each resource), constructed according to a model given to the user. The user can navigate through his collection and edit the registered information. For each digital resource in SilkDRM, the rights holder can authorise the system to publish use licenses, by signing a "distribution license". This procedure is accomplished by selecting the "Create Distribution License" operation for one or more resources. The license to be created will contain the conditions under which the DRM will be able to publish licenses, granting some of the rights "play", "print", "copy", "adapt", "embed", "extract".

The set of conditions, could be one or more of the following:

- The consumer is obliged to pay a certain fee (There is a selection available between payment methods. A payment service can be chosen, or a bank account can be assigned for a deposit to be made);
- Time limit imposition (The right granted can be exercised not before a certain date and not after a certain date);
- Exercise limit (There is a specific number of executions allowed for the right(s) granted);
- Geographical Restrictions (The right granted can be exercised only in a specified country).

When the conditions are selected, the license is published and the DRM acquires the authorisation to create and publish use licenses for specific digital resources, due to the conditions of the distribution license signed. The last service offered to the content provider, is a license management service. The user can browse a list of all the licenses published by SilkDRM for his digital resources. For each license, the system provides information about the principal to whom the rights are granted as well as the potential use of the Validator. The Validator is a subsystem of the SilkDRM which is able to read a license and respond whether it is valid or not. This is accomplished by checking the fulfilment of the conditions set (e.g., fee payment, time limitations). The Validator is not a single "valid" or "not valid". It can indicate the specific terms that are not satisfied.

4.6.4. Content Consumers

The two main services offered to a content consumer, are browsing the collections of registered resources and managing obtained licenses. The resources collections are sorted by rights holder but there is also a search engine available. For each digital resource exists a page demonstrating all available information (e.g., for a digital image elements such as title, legend, description, right holder, creator, digitiser etc. are presented). In case the appropriate distribution license is issued, the choice of obtaining a use license is provided. If the user selects to obtain a license, he will be directed to the license creation page. In this page, the user can see all the rights the DRM is empowered to distribute and select those he wants to receive a license. For each right, the consumer must agree with the conditions set by the rights holder and finally affirm that he wants to obtain the license. Finally the license is published and sent to the user via e-mail. The e-mal, except from the license attached, contains a hyperlink to the Validator, where the obtained license can be validated. The license management service, provides a list of all the licenses granted to the user. The licenses are sorted by date and are accompanied by information about the resource and a link to the Validator.

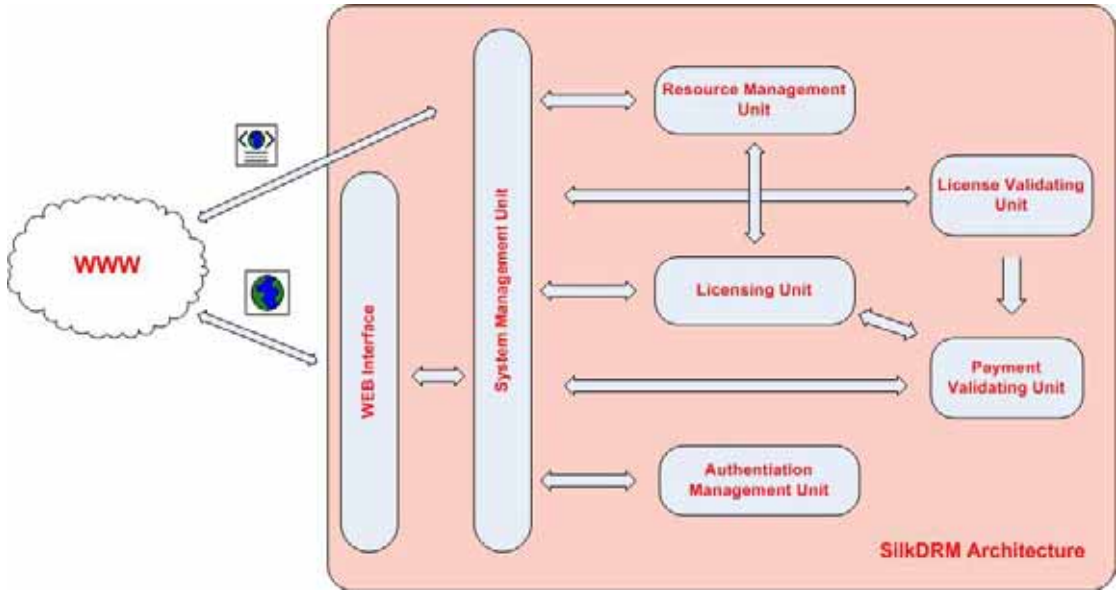

Figure 25: SilkDRM System Architecture

4.6.5. System Architecture

The system comprises of six distinct units, the functionality of which is described in the following paragraphs. These units are designed and constructed independently, as the main goal was the production of a system with the highest possible maintainability and scalability.

System Management Unit

This is the unit that executes the system operation protocol. It receives requests from the web interface or another input (eg. Web service) and orchestrates system units by triggering the appropriate ones at a time, passing messages to them.

Resource Management Unit

This particular unit is responsible for the process of registering and documenting a digital resource. It also undertakes the task of retrieving the documentation and potentially editing and deleting it. Additionally, the Resource Management Unit embraces two distinct sub-units. The Unique Identifier Generator and the Handle Creation Unit which create and register handles for the unequivocal addressing of the digital items.

Licensing Unit

This is the unit responsible for creating and processing licenses for digital resources. For each item, the unit can check whether a distribution license has been published. If such a license is present, the unit is able to read it and dynamically create the terms and conditions a content consumer must agree with, in order to obtain a use license. When a license is published, the unit sends it via e-mail to the holder.

License Validating Unit

This unit receives a license as an input, and checks whether the conditions set in order the grant to be valid, are satisfied. For checking the validity of the payments, the unit is able to communicate with the Payment Validating Unit. Special response messages are produced, according to the results of the validity test. In case a license is not valid, the unit provides detailed information on which of the conditions are not met.

Payment Validating Unit.

Payment Validating Unit's main task is checking whether a fee is paid, according to the conditions set in a specific license. The unit offers the ability of validating a payment, due to the received input by the rights holder or a Payment Service.

Authentication Management Unit

This unit manages the process of creating, editing and deleting user accounts. According to the type of the user logged (content creator or content consumer), it defines the available operations to him on the system. The unit also manages different user rights, offering each user only the services defined by the rights assigned to him by the administrators.

4.6.6. Implementation Details

Registering a digital object

The process followed for registering a digital object in SilkDRM, is described in this paragraph.

1. An application is received by System Management Unit, from a system user wanting to register a digital resource.
2. System Management Unit contacts Authentication Management Unit, to certify that the user is permitted to perform the action.
3. Authentication Management Unit responds whether the user has the right to register the content or not.
4. If the response received is positive, Resource Management Unit is initiated in order to start the registering process.
5. Resource Management Unit provides all necessary data, for the creation of the registering interface. In case of digital images, SilkDRM uses the DIG-35 Intellectual Property Rights Metadata set and when handling other digital resources the Dublin Core Metadata set is used for the registration process.
6. Content Provider fills in the forms with the appropriate data
7. Resource Management Unit receives and stores the data, using a selected format. Relational Database schemes are used for the data storage. The unit is able to export inserted data in xml files. According to the user's

demands, the Unique Identifier Generator and the Handle Creating Unit will be triggered. The Handle Creating Unit includes a Handle Server playing the role of the Local Handle Service responsible for the naming authority "1082.xxxx" Finally the output (the results of the registration process, the unique identification number, the handle etc.) is passed to the content provider (through the System Management Unit).

8. The user wants to create a distribution license for the resource.
9. Licensing Unit is called, for the creation of the license.
10. License Unit provides the necessary data for the production of the license creation interface. For the creation of a license, MPEG – Rights Expression Language is used.
11. The user fills in the form selecting rights and conditions and submits it, thus giving the order for the creation o a license.
12. Licensing Unit receives the data, creates the license, and e-mails it to the content provider. The licenses are created and stored in the xml format specified by the MPEG-REL specifications.

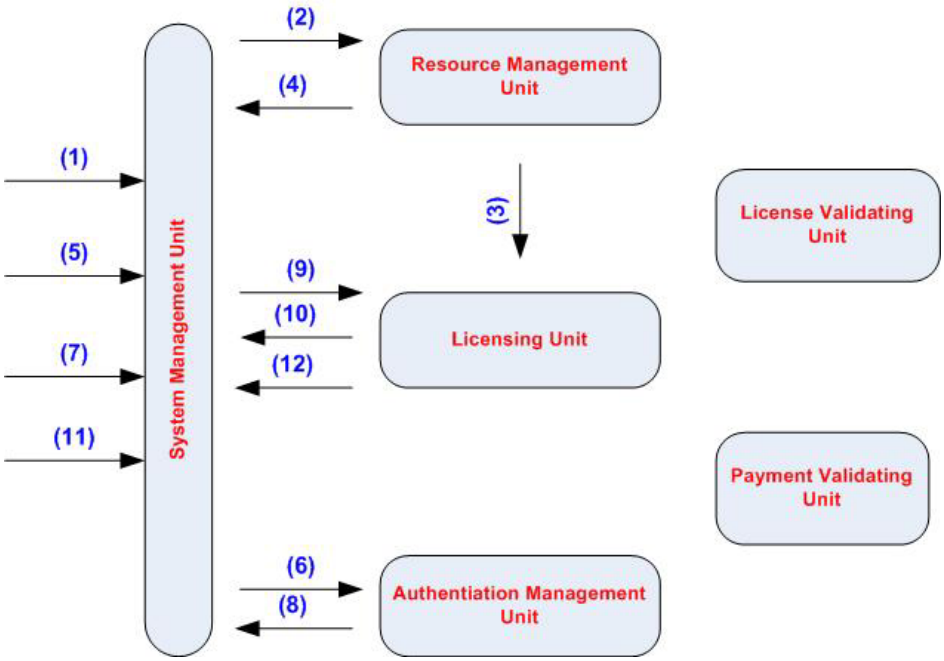

Figure 25. SilkDRM Flow-Chart

The Licensing Process

The next bullets describe the process followed for the creation of a digital license.

1. A system user (content consumer) wants to browse the collections of registered digital items
2. Resource Management Unit is triggered for the presentation of the collection items.
3. Resource Management Unit contacts Licensing Unit to retrieve information about whether a distribution license is published, for each digital resource it will present.
4. Resource Management Unit presents the documentation for the registered items. In case a distribution license is published, the content consumer has the ability to request a silence for the resource.
5. The user makes a license request for a specific digital resource.
6. System Management unit calls Authentication Management Unit to authenticate the user.
7. The user logs on the system if he has an account, or is taken through the steps to create one
8. Authentication Management Unit authenticates the user
9. The request is passed to the Licensing Unit
10. Licensing Unit retrieves and reads the distribution license, in order to produce the forms for the creation of the license.
11. The User accepts the licensing conditions and requests the finalisation of the process.
12. Licensing Unit receives the final data, creates and stores the license and finally sends it to the user via e-mail.

Watermarking

Watermarking functional component incorporates multiple functionalities inside the content provider's operational chain. An Application Protocol Interface (API), was developed to support two basic interfaces for embedding and detecting digital watermarks.

The interface responsible for the embedding operation requires five different arguments from the service user:

- Encryption Key: An integer value that, when used in conjunction with the hash function, produces a secret number appropriate for the invocation of the cryptographic module.
- Transaction Identification Number: An integer value that will be encoded as an imperceptible watermark inside the image digital content.
- Input Image File: The binary data of the original unwatermarked digital image. Output Image File: The binary data of the resulting watermarked digital image.
- Strength Modifier: An integer between 1 and 4 indicating the embedding strength of the watermark procedure. A value of 4 produces more robust watermarks, but introduces more distortion to image quality.

The interface response returns a zero value on success of the watermarking process and a negative value in case of failure.

Respectively, the interface responsible for detecting digital watermarks requires the following input arguments:

- Decryption Key: The integer used during the embedding procedure. With regards to the specific watermarking system, the encryption and decryption keys must be identical in order for the detection to be successful.
- Input Image File: The binary data of the image under detection.

The detector's response, as already mentioned, is consisted of two parts:

- Detection Intensity: Indicating the existence possibility of the watermark inside the image content. If this value is well above a predefined threshold the watermark is considered detected.
- Decrypted Information: An integer value representing the number encoded during the embedding procedure. Normally, this number corresponds to the transaction identification number.

4.7. Conclusion

Rights Clearance has always been an important issue in human transactions. The Internet revolution made the issue a lot more complicated since we passed from the material to the digital substance of an asset. Multiple copies of a digital resource exist over the internet, thus making the monitoring of its use and the identification of its origin an extremely difficult task. Throughout this chapter, we described the rights clearance process in the physical and digital world and the ways it can be accomplished on-line through a Digital Rights Management system. Important issues concerning a DRM system are the definition of key-entities and relations of its functionality, the way a digital resource is represented, protected bound with metadata sets, uniquely identified and the way rights are digitally expressed and assigned. Finally we present an application of all discussed attributes of a DRM system, in an existing system (SilkDRM) that provides on-line Rights Clearance for digital images (or other digital assets).

4.8. Future Research Directions

Future research involves integrating Rights Clearance as a fully functional component of second-generation DRM systems. More specifically, as opposed to first-generation DRM systems where the enforcement of encryption techniques allowed very limited access to content, second generation DRMs introduce more flexible content delivery schemes at the expense of balancing between a set of diverse features such as:

- Uniformly describe and identify an asset (both tangible or intangible).
- Adhere to a globally established protocol for registering rights-holders as well as the set of rights they are allowed to grant.
- Support rights expression languages that are able to describe different types of property rights and facilitate their transfer to a person or an organisation.
- Seamlessly co-operate with technological protecting means both for the tasks of copyright protection and transaction tracking
- Finally, to make all the above work in a unified e-commerce business model.

Each bullet can be considered as a different research field. Although several DRM systems have been developed none of them manages to successfully address all aforementioned aspects. A unified DRM system that operates over the internet is envisaged as the only plausible solution for providing consistent and bullet-proof protection of Intellectual Property Rights.

5. Digital Rights Management – A European Law Perspective

5.1. Introduction

The purpose of this chapter is to provide a brief overview of the legal framework available at EU level that applies to Digital Rights Management (DRM) information and Technological Protection Measures. For this reason, the relevant legal instruments are identified and briefly described, while at the same time an effort has been made to identify the most important points of concern that arise from the interpretation and application of the law. The review concludes by reference to the ongoing discussion over DRM designs in an effort to best combine the requirements of the law into technological solutions and vice-versa.

5.2. EU Copyright Law and DRM

Copyright Law is based on the right of the author or producer of a protected work to forbid unauthorised reproduction. In order to apply this principle in practice, one would have to formulate rules to define (a) what is a protected work, (b) who is the holder of the rights to this work; (c) what are, if any, the exceptions or limitations to those rights and (d) how to enforce those rights and/or exceptions. These rules are defined in law, creating a framework for right holders to exploit their rights when making their works available to third parties and the public in general.

The larger the number or protected works; the wider their distribution and exploitation, the more vital becomes the need for an effective way for authors to manage their rights. In the world of internet, e-commerce, network effects and fast emerging new technologies, legislation often seems inadequate to deal with situations that arise faster than traditional law-making can cope with. This is most evident when considering Intellectual Property rights in the digital world.

Digital Rights Management (DRM) systems are currently the technical means used to facilitate management of rights.[297] "The term DRM refers to the use of technology to describe and identify digital content protected by intellectual property rights, and which enforces usage rules set by right holders or prescribed by law for digital content".[298] Digital rights refer to copyright and related rights in the digital environment, whereas digital content is works created, distributed and/or exploited digitally.

The above definition indicates the two main elements of DRM: (a) identification of protected digital content and (b) enforcement of usage rules. Identification is achieved by digitally marking the protected work so that anyone accessing or using it should be at any time aware of the proprietor of rights and the level of protection of that particular work. Enforcement is achieved technically by limiting the actual uses of a protected work by the rightful user, for example via encryption or watermarking.
The main legal instrument on the functioning and application of DRM technologies at EU level is the Copyright Directive[299] which contains the legal provisions regarding protection of copyright and related rights in the information society and defines the European Commission's policy in the area of Digital Rights Management. The Directive sets the principle goals and the level of protection that Member States must provide for in their national legal systems, yet it leaves Member States to decide on the exact implementing measures in order to achieve the result envisaged in the Directive.[300]

---

[297] See Commission of the European Communities Staff Working Paper, *Digital Rights, Background,* Systems, *Assessment,* Brussels, 14-2-2002, SEC(2002) 197. See also Pamela Samuelson, *DRM {AND, OR, VS.} THE LAW,* Communications of the ACM, April 2003/Vol.46, No.4, at p. 45: "DRM has more than one potential relationship with the law: it can enforce, displace, and override legal rights, while the law can constrain the design of DRM."

[298] Commission Staff Working Paper, supra note 1 at p.6

[299] Directive 2001/29 of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ L167/10, 22.6.2001

[300] This chapter focuses only on legislation at EU level. For an analysis of Member States' implementing legislation see *Study on the Implementation and Effect in Member States' Laws of Directive 2001/29 on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society,* Institute for Information of Law, University of Amsterdam, February 2001, at Part II (Study commissioned by the European Commission's Internal Market Directorate-General), from http://ec.europa.eu/internal_market/copyright/studies/studies_en.htm. See also Urs Gasser and Michael Girsberger, *Transposing the*

DRM technology therefore in Europe must apply and police the provisions of the Directive, safeguarding the rights of IP owners. Right holders identified and protected in the Directive (authors, producers and/or broadcasting organisations) shall be uniquely identified when incorporating DRM technology into protected content; the ownership rights shall also be manifested via marking/registration. Further, the Copyright Directive spells out a number of exceptions to the rights of content owners. DRM technology should allow for certain uses, which the copyright owner must allow on the basis of the rights conferred to him by the Directive. As a result, legislation and its intended effect must be translated into the technological process that will safeguard the proper implementation of the rules. Assuming that this process has been completed in a fair and proportionate way, violation of the provisions of the law should not be possible without tampering with the DRM instrument.

In the digital world, legislation on rights and exceptions is not adequate to safeguard the interests of IP owners against damage incurred by unauthorised acts. Legislation must also allow for the protection of DRM instruments against circumvention and against the production and marketing of circumvention devices. The latter is an indispensable condition for the functioning of electronic commerce and for its acceptance among right holders and commercial users or even for consumers alike.[301] Using those technological measures to achieve control over the uses allowed by law, allows for direct and "real" compensation to content owners for every protected use. In other words, safeguarding business and financial rights of IP owners depends on achieving the technological challenge of enforcement.

The Directive contains an exhaustive list of the rights and exceptions or limitations to those rights. "Fair compensation" is due to copyright owners in specific cases where exceptions or limitations to the exclusive rights of content-owners are imposed in favour of users (articles 2-5 of the Directive). The Directive also contains provisions regarding the legal protection against circumvention of any effective technological measures (chapter III, articles 6-8). In terms of policy orientation, the Directive expressly encourages compatibility and interoperability of the different technical systems of identification of works and protected subject matter in digital format, voting for global standardisation.

As stated in the recital of the Directive, at paragraph 13, "A common search for, and consistent application at European level of, technical measures to protect works and other subject-matter and to provide the necessary information on rights are essential insofar as the ultimate aim of these measures is to give effect to the principles and guarantees laid down in law." Digital Rights Management technologies aim at giving effect to the principles and provisions of the Directive and the implementing legislative measures of the Member States.

5.3. The Provisions of the Copyright Directive 2001/29

The EU Copyright Directive attempted the harmonisation of the laws of the Member States on copyright and related rights, under Articles 47(2), 55 and 95 of the EC Treaty establishing an internal market and safeguarding competition in the internal market,[302] also implementing in the European legal system the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty. The main policy decision behind the harmonisation of copyright law in the EU is to provide for a high level of protection of Intellectual Property, having as ultimate goal to boost investment, innovation and competitiveness of European industry.

The justification behind the introduction of the Directive is that differing Member States' legislations on the level of protection of intellectual property could result in restrictions on the free movement of services and products incorporating, or based on, intellectual property, especially due to the continuous and fast development of technologies and the information society. Furthermore, one of the main benefits of ensuring high level copyright protection, is that the appropriate compensation for creators and authors can be guaranteed, which by itself is a major incentive for copyright owners to continue their creative work. The management of rights in the digital environment helps ensure that all commercial and transactional aspects of distribution, licensing and use of digital content are administered in

---

Copyright Directive: Legal Protection of Technological Measures in EU-Member States, Berkman Publication Series No.2004 -10 November 2004, from http://cyber.law.harvard.edu/publications.

301 Jörg *Reinbothe*, European Commission, submission at the Digital Rights Management Workshop, Brussels, 28 February 2002, "The Legal Framework for Digital Rights Management".

302 For an assessment of the impact of the implementation of the Directive's provisions regarding rights and *limitations* see Study on Directive 2001/29, supra note 4, under 2.4 at p. 73.

such a way that content owners' rights are safeguarded and the agreed remuneration for the licensed act or use of the content is returned to the content owner.

The Directive ensures that maximum protection is offered to copyright owners, save for a number of exhaustively listed exceptions. Once the basic policy line was decisively in place, discretion was left to Member States to decide on certain important aspects on implementation, in order to achieve the Community goal.

The Directive grants to content owners three main rights: (a) the right of *reproduction* (article 2), (b) the right of *communication* to the public including the right of making available (article 3) and (c) the right of *distribution* (article 4). Exceptions or limitations to these rights are listed exhaustively in Article 5 of the Directive. It requires Member States to limit the –otherwise absolute- rights granted to authors and producers, on the basis of *inter alia* public policy, social and cultural considerations as well as use for purposes other than commercial exploitation under circumstances that are explicitly described.

The exceptions and limitations provided for in the Directive are grouped in different categories depending on their purpose and the discretion Member States enjoy in adopting such measures, offering an explicit interface between the protection and exceptions to the rights. In particular:

(a) Member States *have* to provide for exceptions to temporary acts of *reproduction* which are transient or incidental and an integral and essential part of a technological process use to enable transmission in a network or any lawful use of a work or other subject matter, provided they have no independent economic significance.

(b) Member States *may* provide for exceptions or limitations to the *reproduction* right in cases of:

- reproductions on paper or any similar medium, provided that the right-holders receive fair compensation;
- reproductions for private use and, in general, non-commercial purposes, on condition that fair compensation to right holders takes into account the implementation of technological measures, as described below;
- specific acts of reproduction for educational purposes e.g. by libraries, educational institutions and museums, which are not for economic or commercial advantage;
- ephemeral recordings of works by broadcasting organisations by means of their own facilities and for their own broadcasts;
- reproductions of broadcasts made by social institutions pursuing non-commercial purposes, such hospitals and prisons, on condition that the right holders receive fair compensation.

(c) Member States *may*, under specific circumstances, provide for a number of exceptions or limitations to the *reproduction* right and the right of *communication* to the public. From the rather detailed list of article 5 paragraph 3 of the Directive, we distinguish here the following *public* or *social* policy exceptions i.e.:

- teaching or scientific research for non-commercial purposes;
- uses that are necessary for the benefit of people with a disability;
- use for the purposes of public security or to ensure the proper performance or reporting of administrative, parliamentary or judicial proceedings;

In addition to the above, article 5 paragraph 3 of the Directive allows Member States to decide whether to provide for a number of exceptions which mainly relate to everyday commercial uses of protected subject matter for specific uses, where no direct or indirect commercial advantage derives from 'exploitation' of the protected work itself.

All the above exceptions and limitations may be similarly provided with regards to the right of *distribution.* In any case, however, exceptions and limitations must be applied, according to the Directive, only in "certain special cases which do not conflict with a normal exploitation of the work or other subject-matter and do not unreasonably prejudice the legitimate interests of the right holder".
A detailed list of potentially allowed uses avoids at first sight the vagueness in the interpretation of the law, a situation that is most evident in the US where the focus is on courts and their interpretation of the notion of *fair use*.[303] On the other hand, Member States are not obliged to incorporate into their national legislation all of the above exceptions and

[303] For a detailed analysis of the fair use doctrine see Fred Von Lohmann, *Fair Use and Digital Rights Management: Preliminary Thoughts on the (Irreconcilable?) Tension between Them*, Electronic Frontier Foundation, Computers, Freedom & Privacy 2002, 16 April 2002, from http://w2.eff.org/IP/DRM/fair_use_and_drm.html. See also Timothy K. Armstrong, *Digital Rights Management and Process of Fair Use*, Harvard Journal of Law & Technology, Volume 20, Number 1 Fall 2006, from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=885371#PaperDownload.

limitations. In fact, they *may* only provide for any one of those listed, or even *none*, save for those of an obligatory nature. In that respect, especially in jurisdictions where the legislator may have transposed into national law only the minimum level of protection required by the Directive, a policy choice of using 'fair use' notions rather than exhaustive criteria for exempting certain uses would have been much more generous towards protecting user rights.

The specific provisions of the Directive that are of particular relevance regarding DRM technologies are:

- Article 5.2.(b) allows for an exception or limitation to the general reproduction right of authors and producers, "in respect of reproductions on any medium made by a natural person for private use and for ends that are neither directly nor indirectly commercial, on condition that the right holders receive fair compensation which takes account of the application or non-application of technological measures referred to in Article 6 to the work or subject-matter concerned". It is left on Member States to determine the form, detailed arrangements and possible level of such fair compensation, taking into account the particular circumstances of each case.304
- Chapter III of the Directive entitled "Protection of Technological Measures and Rights-Management Information" lists the obligations on Member States to provide for the legal protection of technological measures (Article 6) and rights-management information (Article 7).

The area of law regarding the actual application of DRM technology remains unharmonised and most of these issues are left to Member States. However, the Directive sets the necessary principle for the legal framework to support the use of DRMs which emphasises on (a) the protection of technological measures and (b) taking into account the application of technological measures when providing for fair compensation for the specific uses of content allowed.

The justification behind excluding from harmonisation those areas of law that deal with the development and application of DRM technology, as the Commission recognizes, is that legislation depends largely on the development of technological measures: "*such technology needs to be agreed upon, developed and deployed by the private sector… these criteria should be determined by the market with the risk that possibly divergent or even incompatible standards will emerge*". Digitisation is also transforming the ways content in its different forms is developed, distributed and exploited, with emerging new models such as open source, peer-to-peer, flat rate subscriptions etc. 305.

It seems, therefore, that the move for harmonisation reflects the industry's need to safeguard its proprietary rights over content, by ensuring that the main policy objective of the EU is to remain faithful to traditional copyright protection. The political choice to adopt the principle of protection of technological measures as such was necessary for the industry to invest in resources and effort to develop and implement effective DRM solutions. Thus, the market has been left free to develop its own models of content distribution, licensing and remuneration systems, in a legal environment, however, where the balance leans in favor of right holders and safeguarding IP rights against almost any use, save for a limited number of exceptions that the users, in any event, would have to claim against right holders. In order to encourage uniform technological systems for the management of digital rights, the EU Commission places its entire focus of the Working Paper in listing and describing the available –at the time of the report- DRM Systems and introducing a number of initiatives aiming at promoting such technology and standardisation, through consensus of stakeholders and relevant bodies and organisations.

5.3.1. Protection of Technological Measures under the Copyright Directive[306]

The Directive defines, at article 6 paragraph 3, 'technological measures' as "any technology, device or component that, in the normal course of its operation, is designed to prevent or restrict acts, in respect of works or other subject matter, which are not authorised by the right holder of any copyright or any right related to copyright as provided for by law or the sui generis right provided for in Chapter III of Directive 96/9/EC."

By means of such technological measures, right holders should be in a position to control and enforce digitally their rights, *"as provided for by law"*. The latter refers to any legal provision regarding copyright, any right related to copyright as well as the *sui generis* right on the legal protection of databases. The wording of the law obliges right

304 recital of the Directive, paragraph 35.

305 See Commission Staff Working Paper, supra note 1 p. 9

306 For an overview of the Legal Protection of Technological Measures outside Europe and a comparative remark see Study on Directive 2001/29, supra note 4, under 3.3. at p.81

holders to build their protective mechanisms in such a way so as to prevent acts or uses that would violate their rights but also *to allow* for the statutory exceptions and limitations specifically provided by law.

The Directive considers those technological measures to be 'effective' where "the use of a protected work or other subject-matter is controlled by the right holders through application of an access control or protection process, such as encryption, scrambling or other transformation of the work or other subject-matter or a copy control mechanism, which achieves the protection objective." The level of protection is, as already seen, *provided by law*, i.e. it comprises implementation of the rights as well as their exceptions and limitations.

Protection is twofold and is achieved through the general prohibition (a) against circumvention of technological measures, where the offender acts either in knowledge or with reasonable grounds to know that he is pursuing that objective and (b) against the manufacture, import, distribution, sale, rental, advertisement for sale or rental, or possession for commercial purposes of devices, products or components or the provision of services which in brief promote, advertise, enable or facilitate the circumvention of technological measures.[307] In both situations, it is left to Member States' discretion to decide on what legislation to enact in order to provide for adequate legal enforcement of said prohibitions. Such legal protection must be proportionate, allowing research, development and commercial exploitation of devices implementing such technology (e.g. cryptography) for uses other than to circumvent the technical protection.[308]

Adopting the criterion of *effectiveness* in the Directive meets the necessary requirement of proportionality. It is meant to exclude protection of technological measures that do not achieve the protection objective or offer only very limited protection of copyright and related rights on the subject-matter, in such a way that circumvention would be too easy. It is questionable, however, whether protection should actually extend to those technological measures that prevent *access* to a protected work.[309] It should be accepted that, as the Directive stipulates, control of use of a protected work or other subject-matter *must achieve the protection objective.* If an access control technological measure is implemented by the right holders within the boundaries of protection of subject-matter *as provided by law*, then it should also receive legal protection under article 6 paragraph 3 of the Directive.

Voluntary Measures vs. Legislation
As it is evident from the objective pursued by the technological measures envisaged in the Directive, incorporating into technological measures the exceptions and limitations provided by law could prove to be a rather daunting task. Due to the complexity of the technology and the fact that translating complicated legal notions into technological functions is far from guaranteed, most aspects of the implementation of the provisions of the Directive were left unharmonised.

Therefore, it is not entirely surprising that the Directive encourages *voluntary measures* by right holders, including agreements between them and other parties concerned, allowing legitimate users (beneficiaries) the benefit of an applicable (to electronic communications such as e-commerce) exception or limitation, as provided for by the Directive (at article 6 paragraph 4). Where such voluntary measures or private agreements apply technological measures according to the provisions of the law, they shall enjoy the equivalent legal protection afforded to technological measures by article 6 paragraph 1 of the Directive.

This, in turn, means that either technological measures must be built in such a way so as to identify in each case the use that falls within an exception (on right holder's initiative), or beneficiaries should have recourse, for example on the basis of a separate *voluntary* agreement with the right holder or through national legislation, to some means of claiming their right to a use exempted by law, to the extent necessary to fulfil the purpose of the exception.

Where national legislation incorporates one or more of the specific exceptions or limitations of the Directive (listed above, bulleted items under (b) and (c)), in the absence of voluntary measures, Member States are obliged to take appropriate measures to ensure that right holders make that exception, or the means to benefit from that exception, available to its intended beneficiary and lawful user.

---

[307] At article 6 paragraphs 1 and 2 of the Directive. Member States are allowed to go further and prohibit also the private possession of devices, products or components for the circumvention of technological measures (recital of the Directive, paragraph 49).

[308] recital of the Directive, paragraph 48

[309] See Study on Directive 2001/29, supra note 4, pp. 75-76.

The *private use* exception to the *reproduction* right was not vested with a similar level of protection. In the absence of voluntary agreements, it is left to Member States to decide whether to enforce the private use exception on right holders. Even then, the right of right holders to limit the number of copies to the extent they deem justified and proportionate in order to protect their legitimate interests, cannot be withdrawn or prevented. Moreover, *private use* justifies the imposition of *fair* compensation, for example in the form of royalty payments, which should take into account the application or non-application of technological measures to the work concerned.

This more lenient approach towards the private use exception signifies the expected reduction or phasing out of copyright levies applied in most Member States and their substitution with levies on the basis of the actual use of a protected work, via DRM control measures. This switch will only be possible once technological measures are effectively in operation and are accepted by all stakeholders. Therefore, imposing *ab initio* an obligation on right holders to allow for the *private use* exception without having established that *fair* compensation would be due by legitimate users only once, would create unnecessary excess costs for beneficiaries. As noted by Reinbothe (2002), the issue of private copying may easily be the catalyst for the successful introduction of technological measures.[310]

It follows from the above, that the Directive initially transfers the authority on right holders to safeguard the exceptions and limitations to their rights through technological or other voluntary measures.[311] The requirement is optional on right holders, since failure to provide said voluntary measures shall cause national legislation to intervene in favour of the beneficiary and lawful user. In the absence of voluntary measures or private agreements, Member States are obliged to ensure that beneficiaries enjoy the minimum rights granted to them by the Directive and national implementing legislation against the right holders.

It is not indicated what measures Member States may impose by legislation in order for legitimate users (that is users who already have lawful access) to benefit from the exceptions to the controlled through technological measures use of a copyrighted work. Furthermore, it is not clear how long a Member State must wait, in the absence of voluntary agreements or other voluntary measures before taking action. According to recital 51 of the Directive, this should happen within a "reasonable period of time". As correctly pointed out, "it is unclear under which conditions the mere authority to impose obligations changes to a duty to impose obligations. It is questionable, for example, whether this duty only emerges once an abusive behaviour by a right holder has become apparent."[312]

Since either voluntary or State measures should make possible for the users to exercise an exception to the rights of the content owners, it is widely supported that acts of circumvention needed to exercise a lawful exception are not permitted. The wording of the final text of Article 6 paragraph 1 of the Directive, when compared to the original text of the proposal, has lead to ambiguity as to whether the prohibition of circumvention of technological measures should only be linked to acts of infringement of copyright and related rights over a protected work. Commentaries conclude that the protection afforded under the Information Society Directive can, in principle, be invoked even for acts of circumvention accomplished for purposes that would be lawful under the copyright act.[313]

As it has been generally accepted in literature, "even if article 6(4) creates an obligation to provide the means to exercise a limitation, this obligation is imposed on rights owners and does not give users any authority to perform acts of circumvention themselves. In other words, this provision "does not introduce exceptions to the liability of the circumvention of technological measures in a traditional sense, but rather introduces a unique legislative mechanism which foresees an ultimate responsibility on the right holders to accommodate certain exceptions to copyright or related rights"".[314]

---

[310] See Jörg Reinbothe, supra note 5, p.2

[311] For an analysis of the intricacies of Article 6(4) of the Directive see Séverine Dusollier, *Fair Use By Design in the* European *Copyright Directive of 2001*, Communications of the ACM, April 2003/Vol.46, No.4, p.51

[312] See Study on Directive 2001/29, supra note 4, at p.109 and reference therein to S. Bechtold, "Comment on Directive 2001/29/EC", in T. Dreier P.B. Hugenholtz (ed.), *Concise on European* Copyright *Law*, Alphen aan den Rijn, Kluwer Law International, 2006, p.393

[313] See Study on Directive 2001/29, supra note 4, pp.78-79 and references therein, see also Séverine Dusollier, supra note 14

[314] See Study on Directive 2001/29, supra note 4, p.106 and reference therein to Nora Braun, *The Interface between the Protection of Technological Measures and the Exercise of Exceptions to* Copyright *and Related Rights: Comparing the Situation in the United States and the European Community*, 25 EIRP 11, 499 (2003).

This approach is justified, assuming that voluntary or State measures actually grant users the right to an exempted use to the effect fully permitted by law and under circumstances that allow the legitimate user to take advantage to the fullest extent possible of his rights. In cases, however, where no voluntary measures or an agreement between the right holder and a legitimate user exist and national legislation measures are either inadequate or too burdensome and time consuming for the legitimate user to invoke, would the legitimate user be held liable for circumventing those technological measures in order to pursue his legitimate right to an exception or limitation?

The general principle behind the provisions of the Directive is that a *fair balance* of rights and interests between right holders and users of protected subject-matter must be safeguarded.[315] Furthermore, the definition of 'technological measures' in the Directive refers to measures designed to prevent or restrict acts "which are not authorised by the right holder of any copyright *as provided for by law*".[316] In effect, right holders do not have *ab initio* the absolute right to prohibit any act with regards to a copyrighted work; rather, their very right is limited in scope at its birth, in a sense that the exceptions and limitations provided by law do not fall within the realm of the exclusive rights of the content owner. In the wording of the Directive, "*they [exceptions] are exempted from the right."*

The way one interprets the Law on this point is of particular importance. Circumvention is not allowed for technological measures built to protect the right holder's right. It is certainly not for the right holder to prevent legitimate uses which have been explicitly identified in law as exempted from the protected right, but rather his duty to allow them. While the wording of the Directive, as already noted above, indicates that one would have committed an unlawful act, in case of circumvention in order to benefit from an exception or limitation,[317] a teleological interpretation of this very provision of the Directive could reach the opposite conclusion. Holding a user liable for claiming his right to an exempted use, where voluntary measures or national legislation in effect preempt his right, as provided for by the Directive, runs against the very principles of fairness and proportionality. An equitable rule-of-reason analysis on a case-by-case basis would probably support the same view. Excluding *a priori* an interpretation of the anti-circumvention rules of the Directive in favor of the rightful user, could lead to situations where although all measures and legislation is in place, the actual benefit of an exception to any legitimate user is limited for merely practical reasons, due to the complexities of the technology involved and the inadequacy of those entrusted to deal with any dispute to promptly react to a request for an exempted use by the rightful user.[318]

Legislation grants authors and producers the right to control the use of their works. Should one wishes to challenge that right, he must refuge to litigation, mediation or other procedures provided by law. Likewise, legislation also grants users the right to use lawfully acquired works for a number or exempted uses, which in turn means that technological protection mechanisms used to restrict access may not be circumvented and should remain unaffected. Nevertheless, it is the rightful user once again who would have to pursue litigation or mediation, as provided for in law, if his right to an exempted use is violated by the right holder. This formulation places unreasonable burden on the user -especially the single not easily identified user[319]- despite the fact that most of the exempted uses have been placed in order to safeguard 'public policy' objectives, which should take precedent over authors' rights. It is the very right of the user to

---

315 recital of the Directive, paragraph 31

316 See Study on Directive 2001/29, supra note 4, at p.48 and references there in: "According to recital 33 of the Directive, a use should be considered lawful "where it is authorized by the right holder or not restricted by law". […] The qualification "not restricted by law" primarily refers to copyright limitations. This expression covers temporary copies that are created to enable uses authorized under existing copyright limitations. The provision ensures that the right of reproduction "cannot be used by rights holders to undermine the copyright limitations listed in Article 5(2) and (3) of the Directive"[…] In principle any limitation of the copyright monopoly may be relevant".

317 This view is further supported by paragraph 5, Article 5 of the Directive according to which "the exceptions and limitations provided for in paragraphs 1, 2, 3 and 4 shall only be applied in certain special cases which do not conflict with a normal exploitation of the work or other subject-matter and do not unreasonably prejudice the legitimate interests of the right holder". Priority is given to the right holder and its legitimate interests which take precedent over legitimate users rights for fair use. See also Gasser and Girsberger, supra note 4, p.17 and reference therein to Nora Braun, 2003,pp. 496, 498 (2003).

318 See in this respect the proposal by Barbara L.Fox and Brian A. LaMacchia, *Encouraging Recognition of Fair Uses in DRM Systems*, Communications of the ACM, April 2003/Vol.46, No.4, pp. 61-63 for the creation of safe harbors for modelling fair use rights in DRM systems, starting from approximating in machine-interpretable form fair use features that are a priori declared non-infringing.

319 See Study on Directive 2001/29, supra note 4, p.108, *"In other sectors of the copyright industry, where users do not belong to easily identifiable groups and where the negotiation of acceptable agreements is more difficult, rights holders appear to ignore the obligation."*

an exempted use that should allow for circumvention of DRM technologies without any sanctions in order for the user to exercise the right to that use.[320]
Adopting that approach is necessary in order to safeguard users' rights and protect the lawful consumer. Relying solely on DRM solutions to ensure that the intended user of the content is not subject to any constraint not provided by law[321] makes lawful use conditional on explicit permission from right holders. If circumvention is in every situation unlawful, then enforcement of users' rights is compromised in favor of absolute –even abusive- enforcement of IP rights. In this respect, the proposal put forward to expressly recognize by law the imperative character of some or all limitations on copyright and related rights is to be welcomed.[322]

On-Demand Services: A Troublesome Provision
Article 6 paragraph 4 of the Directive, fourth subparagraph reads as follows:
"The provisions of the first and second subparagraphs [obligation on MSs to provide necessary means for users to benefit from exceptions] shall not apply to works or other subject-matter made available to the public on agreed *contractual terms in such a way that members of the public may access them from a place and at a time individually chosen by them."*

As indicated at the recital of the Directive at paragraph 53, the above exclusion refers to the provision of interactive on-demand services, as opposed to non-interactive forms of online use, where such services are governed by contractual arrangements. With regards to those services, the obligation to safeguard the exceptions through voluntary or State measures, to ensure that users enjoy the benefits of limitations to the content owners' rights, as described above, does not apply.

At first reading, the wording of this provision is rather alarming, as it seems to remove any obligation or limitation to the basic rights of the Directive in almost every e-commerce activity or relationship. The purpose of the provision is to cover situations were the provision of certain services are tailor-made to individual requests for the provision at a specific place and for a limited duration of time, as per the contractual agreement between the right's owner and the user. In a situation like that, the agreement includes licensing and fee arrangements appropriate and analogous to the use and duration of that use of the transmitted copyrighted content. Furthermore, the provision of the service covers the specific need of a member of the public as requested for a particular point in time, event or situation. Under those circumstances, it is therefore reasonable to assume that the contracting parties have specifically taken into consideration the very specific use of the sought on-demand service, adjusting accordingly the royalties, in a sense that no exceptions to the sought on-demand use should be allowed.

Nevertheless, the concerns expressed against the actual application of this provision in the future, where online on-demand interactive services might become the norm in e-commerce, are valid.[323]

Protection of Rights Management Information under the Copyright Directive
Article 7 of the Directive imposes obligations regarding protection of electronic Rights Management Information analogous to those for protection of technological measures. The Directive defines this term as "any information provided by right holders which identifies the work or other subject-matter referred to in this Directive or covered by the sui generis right provided for in Chapter III of Directive 96/9/EC, the author or any other right holder, or information about the terms and conditions of use of the work or other subject-matter, and any numbers or codes that represent such information." With regards to such information, removal or alteration is strictly forbidden. Accordingly, circulation to the public in any way of works or other subject-matter products without the rights management information initially attached to them, where the offender knows or has reasonable grounds to know that such an act may ultimately lead to infringement of copyright or any related rights (including the *sui generis* right for the protection of databases) is also forbidden. The Directive requires Member States to provide for adequate legal protection against any of those acts.

---

320 See P.Samuelson supra note 1, p.45, on the proposition to reform the US Digital Millenium Copyright Act (DMCA) in order to *"allow lawful acquirers of copyrighted material to circumvent technical measures if necessary to make noninfringing uses of the work if the copyright owner has not made publicly available the necessary means to permit the noninfringing uses without additional cost or burden to users."*

321 See Commission Working Paper, supra note 1, p.13

322 See Study on Directive 2001/29, supra note 4, p. 160-164

323 Séverine Dusollier, supra note 14, p.54

As opposed to Technological Protection Measures, whose purpose is to control access and/or copying of a protected work, it is clear from the definition in the Directive that DRM is used to identify the protected work and the terms and conditions of use of the protected work or subject matter. Enforcement comes as a necessary step and may be effectuated through the implementation of various technological measures, depending on the rules set by right holders or imposed by law, regarding the allowed uses of protected content. The distinction between technological measures and electronic rights management information in the Directive, therefore, is more of a technical nature rather than of substance. The Commission, in effect, recognises that protection of rights in the digital world does not necessary lie on measures that ultimately render a certain use or reproduction of copyrighted material impossible but also the intended protection may be achieved through less restrictive and more flexible approaches, whereby information on the IP rights over a work remain inextricably linked to that particular work and compliance is monitored when accessed by any user.

5.3.2. Sanctions and Remedies under the Copyright Directive

The Directive, at article 8, calls for "effective, proportionate and dissuasive" sanctions and remedies in respect of infringements of the rights and obligations set out in its provisions, as well as all the measures necessary to ensure that these sanctions and remedies are applied.

The absolutely necessary level of protection shall include damages actions as well as injunctions by right holders against infringers and infringing activities and, where appropriate "for the seizure of infringing material as well as of devices, products or components" that facilitate circumvention of technological measures. Intermediary service providers used by a third party to commit an infringement may also face injunction orders.[324]

It is apparent that Member States enjoy wide discretion in deciding what sanctions or measures to introduce against infringers. Hence, implementation has resulted in various approaches in different Member States, most notably regarding imposition of criminal sanctions (especially imprisonment) as opposed to civil sanctions which seem to be most common.[325]

5.4. Other EU Legislation Relevant to Technological Measures and DRM Information

5.4.1. Directive 2000/31 on e-commerce

As already seen, the principle legal basis for the protection of IP rights, technological measures and DRM information in Europe is the Copyright Directive. Protection of copyright liability in the network environment further requires a number of measures to regulate electronic commerce, dealing with issues such as defamation, misleading advertising, infringement of trademarks. These concerns are addressed horizontally in Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market (E-Commerce Directive).[326] The timescale for implementation by Member States of both the Copyright Directive and the E-Commerce Directive has been similar and the need for a coordinated introduction of both measures, as complementary to each other and based on similar principles, has been clearly spelled out in both legal texts.

The objective of the E-Commerce Directive has been to create a legal framework to ensure the free movement of information society services between Member States. The definition of information society services already exists in Community law in Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on information society services[327] and in Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access[328]; this definition

---

[324] Protection of IP rights in terms of enforcement has been significantly enhanced following introduction of Directive 2004/48/EC of the European Parliament and the Council of 29 April 2004 on the enforcement of intellectual property rights (OJ L157, 30 April 2004, p.45-86)

[325] See Gasser and Girsberger, supra note 4, p.28 for a comparative analysis of the applicable regimes in some Member States.

[326] OJ L 178, 17.7.2000, p. 1

[327] OJ L 204, 21.7.1998, p. 37. Directive as amended by Directive 98/48/EC (OJ L 217, 5.8.1998, p. 18).

[328] OJ L 320, 28.11.1998, p. 54.

covers any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service.[329]

The Directive requires Member States to lay down in their legal systems requirements applicable to information society services according to the distinctions provided for by the Directive (coordinated field), which cover on-line activities such as on-line information, on-line advertising, on-line shopping and on-line contracting. Information society services explicitly include on-demand services which are transmitted point to point, such as video-on-demand.[330] Such requirements also concern, under Article 3 of the Directive, the content of the service and the liability of the service provider.

In that respect, service providers have a duty to act, under certain circumstances, with a view to preventing or stopping illegal activities. The Directive encourages the development of rapid and reliable procedures for removing and disabling access to illegal information, primarily by developing such mechanisms on the basis of voluntary agreements between all parties concerned that should be encouraged by Member States. Furthermore, the provisions of the Directive relating to liability in no way precludes the development and effective operation, by the different interested parties, of technical systems of protection and identification and of technical surveillance instruments made possible by digital technology within the limits laid down by Directives 95/46/EC and 97/66/EC on data protection and privacy. To this effect, interoperability and compatibility of electronic means, not only within the EU but also on a global scale, is necessary in order to make laws and procedures compatible.[331] The reference to the technological measures, DRM information and voluntary agreements envisaged in the Copyright Directive is direct and unequivocal.

Liability of service providers is only excluded, under certain circumstances, in cases of ‘mere conduit’, ‘cashing’ and ‘hosting’, as those terms are specifically described in the Directive. A service provider, however, who deliberately collaborates with one of the recipients of his service in order to undertake illegal acts, cannot benefit from the liability exemptions established for these activities. The Directive’s provisions on liability exceptions of service providers in cases of ‘mere conduit’, ‘caching’ and hosting, pinpoint to the major problem posed, for example, by peer-to-peer technology which has to a great extend facilitated copyright violations of massive scale. Effective DRM systems may offer solutions to this problem since protection of content transmitted lies on mechanisms incorporated in the content itself rather than solely at the level of the service provider through which content is disseminated.
Similarly to the Copyright Directive, necessary sanctions against violators must be in place, and especially injunctions of different king should be available, consisting in particular of orders by courts or administrative authorities requiring the termination or prevention of any infringement, including the removal of illegal information or the disabling of access to it.[332]

Under Article 3 of the Directive, Member States may not restrict the freedom to provide information society services from another Member States (for reasons falling within the coordinated field), save for reasons –inter alia- relating to public policy and the protection of consumers. Under the public policy umbrella, the Directive places most emphasis on serious criminal offences, such as those against minors, against human dignity and those on grounds or race, sex, religion or nationality discrimination. Nevertheless, public policy is a wide area and could cover a number of infringements set for the protection of various public policy objectives, when criminal sanctions have been chosen my Member States as means of ensuring compliance.

It is apparent from the provisions of the Directive, when read in conjunction with those of the Copyright Directive, that reliance on private sector initiatives on developing interoperable state-of-the-art technological measures and DRM systems as well as on interested stakeholders (including consumers) to enter into *voluntary agreements* for the exploitation of rights and dissemination of copyrighted material through e-commerce systems, allowing for full application of the law to the benefit of all interested parties, is a policy objective of EU legislation in the area of IP protection and e-commerce systems. The question once again turns to the vital issue of translating legal restrictions into electronic measures, further allowing for negotiation and private contractual solutions, whereas state intervention

[329] recital of the E-Commerce Directive, paragraph 17. Those services referred to in the indicative list in Annex V to Directive 98/34/EC which do not imply data processing and storage, are not covered by this definition.

[330] Ibid. at paragraphs 18 and 21

[331] Ibid. at paragraph 61

[332] Ibid. at paragraph 41

remains the last resort. The balance of rights in favor of IP owners and service providers indicates that State intervention must in any case be available, offering swift and workable solutions to situations where the rights of lawful content users are at stake. State mechanisms to safeguard the legality and proportionality of any *voluntary* measures must also exist, since the balance of powers against the consumer – final user is bound to undermine the creation of a level playing field for all stakeholders.

5.4.2. Data Protection and Privacy

Data about how the protected works are used is of additional economic value. The discussion around application of various DRM designs entails a thorough consideration of issues that could arise in terms of data protection and privacy. It is not within the scope of this chapter to deal with those aspects of law; hence this brief reference is made for informational purposes only.

The protection of individuals with regard to the processing of personal data is governed by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31.) and Directive 97/66 EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector (OJ L 24, 30.1.1998, p. 1.). These two legal instruments establish a Community legal framework in the field of personal data that is fully applicable to information society services.

5.4.3. Legal Protection of Computer Programs

The legal protection of technological measures under the Copyright Directive does not affect the specific provisions on protection provided for by the Directive on the legal protection of Computer Programs[333]. In particular, it does not apply to the protection of technological measures used in connection with computer programs, which is exclusively addressed in that Directive. As stipulated at paragraph 50 of the recital of the Copyright Directive, its provisions should neither inhibit nor prevent the development or use of any means of circumventing a technological measure that is necessary to enable acts to be undertaken in accordance with the terms of Article 5(3) or Article 6 of the Computer Programs Directive.

In particular, article 5(3) of the Computer Programs Directive allows a lawful user of a computer program to observe, study or test the functioning of the program in order to determine the ideas and principles of the program, if he does so while performing any lawful use of the program. Article 6 of same Directive describes the terms and conditions under which a rightful user may perform acts of decompiling of a computer program without the authorisation of the right holder.

On the other hand, article 7 of the Directive contains itself a provision on protection of technological measures, requiring Member States to provide for adequate remedies against a person committing any act of circulating or possessing for commercial purposes of any means intended to facilitate the unauthorised removal or circumvention of any technical device which may have been applied to protect a computer program.

It is apparent that Community law comprises two legal regimes applicable to technological protection measures: on the one hand, a regime that prohibits the business of trafficking in illicit devices, pursuant to the Computer Programs Directive; and, on the other hand, a regime that prohibits both the act of circumvention of TPMs, as well as the business of trafficking in illicit devices or circumventing services.[334]

5.5. Ongoing Discussion on DRM Systems

The discussion over the impact of DRM systems and effective protection of technological measures has for some years now hoped for a shift in online practices and markets. A wide variety of views have been expressed, all stressing the importance of interoperability and flexibility in allowing technology markets to develop the necessary standards for administering IP rights through technological measures.

---

333 Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs, OJ L 122, 17.5.1991, p. 42–46

334 See Study on Directive 2001/29, supra note 4, p. 86 and references therein.

Interoperability is in almost every case presented as indispensable to user acceptance of technological measures and DRM designs. Unavoidably, this principle leads the discussion to Open DRM standards which may guarantee content distribution over a multitude of platforms and user devices.[335] The concern that in a horizontal market, access to services by consumers and access to consumers by providers must remain technology neutral remained as late as in mid-2005 and despite the hopes expressed a couple of years earlier that markets would find their way towards standardisation and interoperability.[336]

The European Commission, in its 2002 Staff Working Paper, expressed the hope that "DRM systems would enable right holders […] to adopt new business models, which would open up new and alternative revenue streams for their content. Ultimately, one solution could be to create an environment where content creators are able to choose whether they wish to protect their rights and receive remuneration or not on a voluntary basis."[337] It goes on to specify an example, drawn from industry interviews, where a single dedicated environment, in the form of a distribution channel, could be used as a platform to ensure compliance with copyright exemptions in favour of beneficiaries.[338] In that case, all content falling within a certain exemption (for example reproduction for educational and public institutions such as libraries, where users could be identified as members of the same group, such as library patrons) would be administered and distributed through a single content platform. This proposal, while it seems viable for a specific content use, it would still require protection of content by DRM systems, in order to prohibit unauthorised copying and redistribution of content from lawful users, for purposes other than their strict intended use. Unauthorised circulation of protected content e.g. in University networks, even were such content is in no way serving an educational cause, is far from limited.

A further passing ascertainment in the Commission Staff Working Paper, is that technological protection measures, in sectors with numerous unidentifiable users such as the music industry, could be applied not by rights holders but rather by an intermediary, like the content or service provider. Lionel S.Sobel has elaborated a similar model in more detail in 2003.[339] Based on a comparative presentation of the available at that time business models for distributing copyrighted content, Sobel proposed that Internet Service Providers (ISPs) could act as Digital Retailers, controlling content distribution through their servers. Content would be identified through watermarking, fingerprinting or other technologies, while technology used to identify protected content would reside on ISP's servers. "ISPs would detect and record those watermarks as files flow through their servers […] and that data would be used to allocate collections proportionately among copyright owners." In that way, Sobel supports, "ISPs would monitor the flow of copyrighted works through their servers, looking for watermarks and recording the recipients of watermarked files. A database would identify the owner of the copyright to each watermarked file, as well as the wholesale price the copyright owner decided to charge for its use." A similar database could be created for fingerprinted files.[340] This model appears to be a realistic proposal that takes advantage of the currently available distribution channels over the internet and exploits the access rights enjoyed by current industry players, such as the ISPs, in order to create a control mechanism of online

---

[335] Remarks by Thomas Curran, Chief Technology Officer, Bertelsmann at the Digital Rights Management Workshop, February 28, 2002, Brussels (from http://ec.europa.eu/information_society/eeurope/2005/all_about/digital_rights_man/index_en.htm). Curran noted however that if by year 2003, the industry were not closer to an open DRM standard, it would be time for the EC and its counterparts in other regions of the world, to switch from a facilitating role to a more activist role. Note in this respect the "Charter of agreement for the development of a legal supply of on-line music, respect for intellectual property and the fight against digital piracy", signed in Paris on 28 July 2004, between the Government of France, access providers, right holders, producers and platforms of on-line distribution, aiming at coordinating efforts, *inter alia*, to develop the availability for all platforms under transparent and non-discriminatory conditions of digitised content, to study filtering solutions in the area of peer-to-peer at the level of access providers and to take the necessary measures to develop compatibility between the formats for encoding and downloading music on the one hand, and the software and equipment for reading music files on the other, while ensuring a secure environment for the contents (from http://ec.europa.eu/information_society/eeurope/2005/all_about/digital_rights_man/doc/drm_workshop_2005/charte_en.pdf).

[336] Presentation by Jean-Pierre Evain, EBU, Towards Reaching Consensus on Digital Rights Management, Brussels 6 April 2005, Open Standards: The path to interoperability: "the answer to the question what can be standardised and how, remains blurred".

[337] See Commission Working Paper, supra note 1, p.16

[338] Ibid. p.108

[339] Lionel S.Sobel, Editor, Entertainment Law Reporter; Distinguished Scholar, Berkeley Center for Law & Technology; Lecturer, Boalt Hall (Spring 2003), paper entitled *DRM as an Enabler of Business Models: ISPs as Digital Retailers*, from https://www.law.berkeley.edu/institutes/bclt/drm/papers/sobel-drm-btlj2003.html

[340] Ibid. pp.5, 13-14

use of protected content. It certainly requires resolving a number of licensing and royalty issues. Also, an immediate reaction would come from advocates of personal data protection and privacy, since ISPs would gain control over all uses of copyright material over the internet. Nevertheless, in most network industries, network administrators and service providers already have access to user data and it is a matter of legislation and proper controls to ensure that privacy rights will be respected.

When elaborating the way DRM mechanisms should be built, the way users may invoke their rights is of critical importance. A proposal that has been put forward involves DRM designs where users would be allowed "to Challenge the Code".[341] Users would be provided with the ability to request authorisation for controlled actions that should be allowed, as stipulated by law, thus challenging the code of a given DRM mechanism. It is not clear, as Armstrong (2006) points out, whether denial of a requested use could be subjected to a further review either outside or inside the DRM system, nevertheless "the proposal hints at a possible opening-up of DRM mechanisms". This notion of giving users the ability to "assert their rights" through the DRM mechanism seems to gain wider consensus in different model proposals to date.[342] The discussion seems to flirt –now stronger that ever- with the long-established and increasingly accepted principles of Open Source technology and Open Source Licensing practices and models. A strong indication of this trend can be found in most relevant literature with presentations of Open Source Licensing examples, most notably by reference to the Creative Commons initiative which strives to balance the two ends between full copyright control and free public works. [343]

5.6. Future Research Directions

The discussion over DRM systems as means of enforcing IP rights and controlling user rights seems to be dependent on the degree of technological development in this area. The requirements as well as the application of the law shall remain blurred for as long as no standardised solutions or generally accepted principles are adopted by the industry. Since the possibility of achieving such a consensus has been on the table for quite a few years now, Open Source principles and technology would inevitably prevail as the most suitable candidate: interoperability and standardisation can be guaranteed from the outset, without however holding back technological progress and development. It is a matter of turning the discussion from the question of how to protect content and enforce proprietary rights effectively to the point of achieving wide dissemination of content to lawful users, to the benefit of both creative producers and consumers.

[341] See Timothy K. Armstrong, supra note 7, p.89-90 with reference to Erickson and Mulligan.

[342] An aspect of this proposal, i.e. the right of users to have recourse to a third party to assert their rights, has to a certain extent been formulated in some Member States' legislation, where mediators (most commonly in a form or government or other administrative body or authority) are entrusted with the task of resolving disputed and intervening by regulating markets where necessary. The introduction of such mechanisms by some Member States was the result of the implementation of their obligation under the Copyright Directive to provide for appropriate measures in the absence of voluntary agreements between right holders and users, see Study p. 124-132. See also summary of Armstrong's proposal, supra note 7, at p. 108, where users would be empowered to assert fair use rights over purchased content, a record of the asserted fair uses in the form of an audit trail would be preserved by the system and user-identifying information would be escrowed with a third party.

[343] See http://creativecommons.org/

6. Best Practice for DRM & IPR Protection in Europeana

6.1. Introduction

This chapter is concluding on what is the best practice for implementing a Digital Rights Management System which applies IPR protection to digital cultural content. Surely, there is not one common solution for all cultural heritage organisations and unfortunately an off-the-shelf solution for DRM does not exist. Each solution is unique per organisation and a DRM should be adjusted and fine-tuned in accordance with the organisation's special needs. Nevertheless, there are certain technological methodologies, standards and tools which could be selected and used by any organisation wishing to achieve a certain level of IPR protection and management. The issue is even more crucial now that organisations are taking certain actions to support Europeana and its deliverables, making their content public through Europeana's online portal. These standards and tools are presented in this chapter.

6.2. Table of existing DRM technologies and associated devices

This table presents nearly all the existing in the market DRM systems and technologies.

Name	Used In	Date of Use	Description
DRM Schemes Currently in Use			
Personal computer DRM			
Windows Media DRM	Many Online Video Distribution Networks	1999+	WMV DRM is designed to provide secure delivery of audio and/or video content over an IP network to a PC or other playback device in such a way that the distributor can control how that content is used.
FairPlay	The iTunes Store, iPod	2003+	Purchased music files were encoded as AAC, then encrypted with an additional format that renders the file exclusively compatible with iTunes and the iPod. On January 6, 2009, Apple announced that the iTunes Store would begin offering all songs DRM-free.[1]
Helix & Harmony	Real Networks services	2003+	A DRM system from Real Networks intended to be interoperable with other DRM schemes, particularly FairPlay. Ultimately used only by Real Networks.
Orion/EasyLicenser	Enterprise, business, networking, financial, telecom and consumer applications	2003+	Restriction for applications written in Java, .Net or C/C++ on Windows, Linux, Solaris and Mac.
Excel Software	Business, educational, government and consumer applications	2006+	Protection for Mac and Windows applications, plugins, DLLs, multimedia and documents with manual and automated activation, trial and perpetual licenses, software subscriptions, floating and dynamic licenses, network floating licenses and user friendly license release, restore, suspend and automated feature delivery.
Adobe Protected Streaming	Flash Video/Audio Streaming	2006+	The Media-Streams are encrypted "on the fly" by the Flash Media Server (the protocol used is rtmpe or rtmps). In addition the client player can be verified via "SWF-Verification", to make sure that only the official client can be used.
PlayReady	Computers, Mobile and Portable Devices	2007+	PlayReady is designed to encrypt WMA, WMV, AAC, AAC+, enhanced AAC+, and H.263 and H.264 codecs files. PlayReady is actually a new version of Windows Media DRM for Silverlight. Silverlight 2-based online content can be restricted using PlayReady and played back via the Silverlight plug-in. PlayReady is promoted by Microsoft.
DRM-X	Computers, Audio/Video Streaming	2007+	A DRM system from Haihaisoft is designed to encrypt both audio/video, swf, and PDF documents. The viewer is based-on Haihaisoft Universal Player and PDF Reader. It restricts play count, expires date, and with Watermarks technology.
ContentGuard	Enterprise, business, networking, financial, telecom and consumer applications	1993+	ContentGuard has a heritage of innovation beginning in the early 1990's in Xerox PARC where our foundational DRM technologies were created and incubated. In 2000, Xerox spun the company out and today Microsoft, Thomson and Time Warner are the three primary shareholders.
SilkDRM	Enterprise, cultural organisations, photographers etc.	2004	DRM solutions for digital images, video and audio files. Unique identification, protection with watermarking tools and other available features.
Portable device DRM			

Janus WMA DRM	All PlaysForSure Devices	2004+	Janus is the codename for a portable version of Windows Media DRM intended portable devices.
OMA DRM	Implemented in over 550 phone models.	2004+	A DRM system invented by the Open Mobile Alliance to control copying of cell phone ring tones. Also used to control access to media files, such as video.
Storage media DRM			
VHS Macrovision	Almost all VHS Video through the end of the 20th Century	1984+	When dubbing a Macrovision-encoded tape, a video stream which has passed through the recording VCR will become dark and then normal again periodically, degrading quality. The picture may also become unstable when darkest.
Content-scrambling system (CSS)	Some DVD Discs	1996+	CSS utilises a weak, 40-bit stream cipher to actively encrypt DVD-Video.
DVD Region Code	Some DVD Discs	1996+	Many DVD-Video discs contain one or more region codes, marking those area[s] of the world in which playback is permitted. This restriction enforces artificial market segmentation.
ARccOS Protection	Some DVD Discs	1997?	Adds corrupt data sectors to the DVD, preventing computer software implementing computer standards from successfully reading the media. DVD players execute the on-disk program which skips the (corrupt) ARccOS sectors.
OpenMG	ATRAC audio devices (e.g., MiniDisc players), Memory Stick based audio players, AnyMusic distribution service	1999+	A proprietary DRM system invented and promoted by Sony.
BD+	Blu-ray Discs	2005+	A virtual machine embedded in authorised Blu-ray players that runs a security check on the playback environment to ensure that it has not been compromised. It also performs necessary descrambling of the audio/video stream on discs, allowing the content to be rendered.
DRM Schemes no Longer in Use			
Extended Copy Protection	Sony and BMG CDs	2005	Also known as the 'Sony Rootkit'. Although not classified as a virus by many anti-virus software producers, it bore many virus-like and trojan-like characteristics, rendering it illegal in some places and dangerous to infected computers in all. After it became publicly known, protests and litigation resulted in withdrawal by Sony. The US litigation was settled by payment by Sony.
DRM Schemes Proposed			
Internal Self Intelligence	CHRISM Software		Internal software unique to each copy of a program is compiled in at the time of purchase. US Patent Office Application Number 11678137. Cracking a compiled version for the right key codes will not result in a redistributable cracked version because the internal algorithms that utilise the key codes also incorporate separate encrypted time of compile and other information, and will prevent installs after, say, 36 hours of compilation.
Marlin (DRM)	Marlin Developer Community (MDC)		Open-standards community initiative, based on the fundamental notion that interoperability and openness are essential to sustainable commercial success. Marlin has a consumer domain approach with emphasis on accessing, using, and sharing content intuitively. Service providers and device markers can create and support innovative content services over open networks using Marlin technology.

The aforementioned existing DRM systems are covering a large range of needs and solutions e.g. for audio and video streaming. For a cultural organisation which has the need to manage and protect digital content, a DRM system should provide some basic features. These are being presented in the next section.

6.3. Building a typical DRM system for a cultural organisation

A typical DRM for a cultural organisation which aims at protecting and managing IPR on its digital content prior making it public through a website or Europeana's portal should include features and technologies mainly for:

1. Unique Identification of digital content;
2. Copyright protection with watermarking technologies;
3. Interoperability between heterogeneous systems using w3c & other standards.

6.3.1. Unique Identification

The digital content which is being transacted through a DRM system (and the internet) should be uniquely identified so that the copyright owner has a means to proof his ownership.

Digital Object Identifier (DOI)[344] (http://www.doi.org) is an identification system for intellectual property in the digital environment. Its goals are to provide a framework for managing intellectual content, link customers with publishers, facilitate electronic commerce and enable automated copyright management not only for the publishing industry but for many others industries as well (for example music).

DOI names are assigned to any entity (documents, publications and other resources) for use in digital networks. These names are unique, persistent (i.e. they do not become invalid) and have high availability (i.e. they do not depend on a single web server being up and running) for use over their lifetime (like bar codes), while standard web URLs can change over time.[345] DOIs have a simple syntax, which is depicted in figure 26. The combination of a prefix for the registrant and unique suffix provided by the registrant avoids any necessity for the centralised allocation of DOI numbers. The two components together form the DOI.

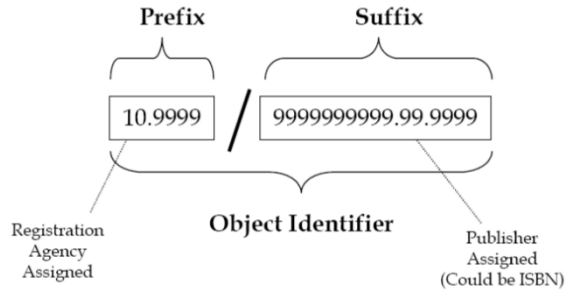

Figure 26: DOI Structure

A DOI could be assigned to digital files so as unique identification to be achieved for the digital content. The most common practice is the DOI to be produced and stored into a database as a metadata item for the digital file. This methodology achieves both unique identification and assignment of a unique number to the digital file. The most efficient way to produce and manage DOIs is the Handle resolution system (http://www.handle.net/). The Handle system is a general purpose distributed information system that provides efficient, extensible, and secure HDL identifier and resolution services for use on networks such as the Internet. It includes an open set of protocols, a namespace, and a reference implementation of the protocols. The protocols enable a distributed computer system to store identifiers, known as handles, of arbitrary resources and resolve those handles into the information necessary to locate, access, contact, authenticate, or otherwise make use of the resources. This information can be changed as needed to reflect the current state of the identified resource without changing its identifier, thus allowing the name of the item to persist over changes of location and other related state information. The original version of the Handle system technology was developed with support from the Defense Advanced Research Projects Agency (DARPA).

6.3.2. Copyright Protection watermarking tools

The copyright of digital content which is being transacted through a DRM system (and the Internet) should be protected with the use of watermarking technologies. There are not commonly agreed standards for digital watermarking but there are commonly identified requirements which the watermarking tools should meet so as to succeed in their purpose. There are many efficient watermarking products which could be purchased from the software market. An indicative table including watermarking tools is shown below.

Tool	Source	Operating System	File Types
Digimarc	Digimarc Corporation http://www.digimarc.com	Win	All image formats
SureSign	Signum Technologies http://www.signumtech.com	Win, Mac	All image formats
EikonaMark	Commercial, Alpha-Tec Ltd	Win	All image formats, video

[344] DOI (2007). Digital Object Identifier – DOI. Retrieved February 1, 2008 from http://www.doi.org

[345] Rosenblatt, R. (1997). Solving the Dilemma of Copyright Protection Online. The Journal of Electronic Publishing (JEP), 3(2). Retrieved February 1, 2008 from http://www.press.umich.edu/jep/03-02/doi.html

	http://www.alphatecltd.com		and audio
SilkMark (in Greek only)	SilkTech SA http://www.silkmark.gr/, http://www.silktech.gr	Win	All image formats

These products have an efficient level of copyright protection. The key issue for an organisation which already maintains its digital content in databases and uses user interfaces for inserting new content into these databases is how to connect the watermarking tools with an already established database or GUI. For this case the organisation should purchase an SDK (Software Development Kit) edition of a watermarking tool. This edition is open and reusable enough so as to connect already built watermarking functions (e.g. watermarking insertion and detection) with already established databases and GUIs. In such a case, a DRM system could be implemented which whenever a new digital image, audio or video file is inserted in the database this is automatically being watermarked. Finally, the digital content which is being published through the Internet or through Europeana's portal is being retrieved by the database and therefore it is protected by watermarking technologies. Nevertheless, in all cases GUI and Database re-engineering costs are necessary so as to achieve the embedment of watermarking functions into the already established Databases and GUIs. All the above watermarking tools are available in SDK versions.

6.3.3. Interoperability using W3C & other standards

Interoperability is crucial for Europeana. The complexity of collecting content by heterogeneous systems is unpredictable. Using technological standards for producing a semantically enabled DRM system is important so as to alleviate this complexity. In the next sections technological standards for producing an interoperable DRM system are being presented. The technologies described bellows are used to develop the web interfaces for a typical DRM system.

XrML

Extensible Rights Markup Language (XrML) is an XML-based language for digital rights management. It provides a universal method for securely specifying and managing rights and issuing conditions associated with the use and protection of all kinds of resources including digital content, as well as services.[346] Contrary to DOI, which is simple conceptually and syntactically, XrML is a rich language of specifications. Its purpose is to expand the usefulness of digital content, resources, and web services to rights holders, technology developers, service providers and users by providing a flexible, extensible, and interoperable industry standard language that is platform, media, format and business independent.[347]

ODRL

Open Digital Rights Language (ODRL) initiative aimed at developing and promoting an open standard for rights expressions. ODRL is intended to provide flexible and interoperable mechanisms to support transparent and innovative use of digital resources in publishing, distribution and consuming of electronic publications, digital images, audio and movies, learning objects, computer software and other creations in digital form.[348] It is an open source language without license requirements.

ODRL is based on an extensible model for rights expressions which involves a number of core entities and their relationships. There are three core entities to the model: assets, rights and parties. The first includes any physical or digital content, should be uniquely identified, may consists of many subparts, may be in many different formats and may also be encrypted to enable secure distribution of content. The second entity includes permissions which can then contain constraints, requirements, and conditions. Finally, parties includes end users and right holders. With these three core entities, the model can then express or revoke offers (proposals from right holders for specific rights over their assets) and agreements (when parties enter into contracts or deals with specific offers).

346 XrML (2007). Extensible Rights Markup Language – XrML, 2.0 Specification. Retrieved February 1, 2008 from http://www.xrml.org

347 Heng, G. (2001). Digital Rights Management (DRM) using XrML. T-110.501 Seminar on Network Security.

348 Renato, I. (2002). Open Digital Rights Language (ODRL), Version 1.1. IPR Systems, W3C. Retrieved February 1, 2008 from http://www.w3.org/TR/odrl

6.4. Conclusion

Based on the above findings, for a cultural organisation the combination of 1) unique identification technologies, 2) watermarking tools connecting to existing databases with the use of SDKs (Software Development Kits) and 3) W3C open standards for the development of web interfaces is a key solution for implementing an efficient, open and interoperable DRM System. Unfortunately an off-the-shelve solution for DRM does not exist. Consequently, the development of a complete DRM System requires time and costly man effort. Nevertheless, a solid database which is structured upon an interoperable metadata standard (e.g. ESE or LIDO) which includes a minimum set of fields for IPR is the basic infrastructure for a future DRM system. Then the specialised IPR services (unique identification, watermarking and GUIs) could be built, based on W3C standards and Open Source software, upon this database extending its capabilities.

7. General Conclusions

The necessity of using web based initiatives and systems which allow broad exchange of the creations while at the same time use copyright protection methodologies and tools during this exchange is important. Digital Rights Management systems have the objective to fulfil this goal, thus to protect and manage rights and copyrights and in parallel support the distribution and publication of priceless digital creations in the form of digital content. Through this study and technological review some key conclusions have been produced.

1. The adoption of a DRM system is not easy; they are costly, complex and not fully secure. The success of Digital Right Management systems is based on a number of other factors, including the balance between protection of intellectual rights and privacy. A balanced, successful DRM system must be a combination of technological, business and legal concerns in a functional, open and acceptable framework. Digital Right Management is inevitably one of the greatest challenges for content communities.

2. Digital watermarking is one of the most important parts of a DRM system and mainly the tool which provides copyright protection, proof of ownership, content authenticity and the transaction management infrastructure.

3. DRM technology faces several issues that have to be addressed. In the future, DRM enabled business models will grow dramatically. DRM technology will certainly improve over time and enhance new features, supporting business models that are endorsed by content providers.

4. Rights clearance has always been an important issue in every transaction that involves copyrighted objects. Typically the owner (seller) has to prove that he possesses the right to make the transaction and the buyer has to be sure of the legitimacy of the transaction that he is going to be part of. This study included:
    a. the on-line rights clearance background in terms of broad definitions, discussions and contradicting views;
    b. the inquire of intellectual property rights as part of a Digital Rights Management system and with respect to a plausible business model;
    c. the analysis of the technical components involved in on-line rights clearance, along with the arising flow control and engineering issues;
    d. the presentation of an operative DRM system integrating on-line rights clearance practices.

5. The discussion over DRM systems as means of enforcing IP rights and controlling user rights seems to be dependent on the degree of technological development in this area. The requirements as well as the application of the law shall remain blurred for as long as no standardised solutions or generally accepted principles are adopted by the industry. Since the possibility of achieving such a consensus has been on the table for quite a few years now, Open Source principles and technology would inevitably prevail as the most suitable candidate: interoperability and standardisation can be guaranteed from the outset, without however holding back technological progress and development. It is a matter of turning the discussion from the question of how to protect content and enforce proprietary rights effectively to the point of achieving wide dissemination of content to lawful users, to the benefit of both creative producers and consumers.

Based on the above conclusions and findings and especially on the fifth point, for a cultural organisation the combination of 1) unique identification technologies, 2) watermarking tools connecting to existing databases with the use of SDKs (Software Development Kits) and 3) W3C and open standards for the development of web interfaces is a key solution for implementing an efficient, open and interoperable DRM System. Unfortunately an off-the-shelf solution for DRM does not exist. Consequently, the development of a complete DRM System requires time and costly man effort. Nevertheless, a solid database which is structured upon an interoperable metadata standard (e.g. ESE or LIDO) which includes a minimum set of fields for IPR is the basic infrastructure for a future DRM system. Then the specialised IPR services (unique identification, watermarking and GUIs) could be built, based on W3C standards and Open Source software, upon this database extending its capabilities.

8. List of Figures

9. Additional Reading

- Acharya, T. & Tsai, P.S. (2004). JPEG2000 Standard for Image Compression: Concepts, Algorithms and VLSI Architectures. Wiley-Interscience
- Adelsbach, A. & Sadeghi, A.-R., (2001). Zero-knowledge watermark detection and proof of ownership. In 4th International Workshop on Information Hiding, IH'01, Springer Lecture Notes in Computer Science, Vol. 2137 (pp. 273-288). Pittsburgh, PA, USA.
- Adelsbach, A., Rohe, M., & Sadeghi, A.-R., (2005). Non-interactive watermark detection for a correlation-based watermarking scheme. In Communications and Multimedia Security, Springer Lecture Notes in Computer Science, Vol. 3677 (pp. 129-139). Salzburg, Austria.
- Adelsbach, A., Huber, U., & Sadeghi, A.-R., (2006). Fingercasting – joint fingerprinting and decryption of broadcast messages. In 11th Australasian Conference on Information Security and Privacy, Springer Lecture Notes in Computer Science, Vol. 4058 (pp 136-147). Melbourne, Australia.
- Ahmed, F., Sattar, F., Siyal, M. Y., & Yu, D., (2006). A secure watermarking scheme for buyer-seller identification and copyright protection. EURASIP Journal on Applied Signal Processing.
- Anderson, R. J., & Manifavas, C., (1997). Chameleon - a new kind of stream cipher. In 4th International Workshop on Fast Software Encryption, FSE '97, Springer-Verlag, (pp. 107-113). London, UK.
- Arnold, M., Schmucker, M. & Wolthusen, S.D. (2003). Techniques and applications of digital watermarking and content protection. Boston, MA : Artech House.
- Braun Nora, The Interface between the Protection of Technological Measures and the Exercise of Exceptions to Copyright and Related Rights: Comparing the Situation in the United States and the European Community, 25 EIRP 11, 499 (2003).
- Byers Simon, Cranor Lorrie, Korman Dave, McDaniel Patrick and Cronin Eric, Analysis of Security Vulnerabilities in the Movie Production and Distribution Process, DRM'03, October 27, 2003, Washington, DC, USA.
- Celik, M., Lemma, A., Katzenbeisser, S., & van der Veen, M., (2007). Secure embedding of spread-spectrum watermarks using look-up tables. In International Conference on Acoustics, Speech and Signal Processing, ICASSP'07, IEEE Press, Vol. 2 (pp. 153-156). Honolulu, Hawaii, USA.
- Cheun Ngen Chong, Yee Wei Law, Sandro Etalle, and Pieter H Hartel, Approximating Fair Use in LicenseScript, Faculty of EEMCS, University of Twente, The Netherlands
- Cox, I., Miller, M., Bloom, J., and Fridrich J., (2007) Digital Watermarking and Steganography, Second Edition (The Morgan Kaufmann Series in Multimedia Information and Systems) Amsterdam Boston : Morgan Kaufmann.
- Craver, S., (1999). Zero knowledge watermark detection. In 3rd International Workshop on Information Hiding, IH'99, Springer Lecture Notes in Computer Science, Vol. 1768 (pp. 101-116). Dresden, Germany.
- Craver, S., & Katzenbeisser, S., (2001). Security analysis of public-key watermarking schemes. In M. S. Schmalz (Ed.) SPIE, Mathematics of Data/Image Coding, Compression and Encryption IV, with Applications, Vol. 4475, (pp 172-182). San Diego, CA.
- Crowcroft, J., Perkins, C., & Brown, I., (2000). A method and apparatus for generating multiple watermarked copies of an information signal. WO Patent No. 00/56059.
- de Rosnay, M.D., Digital rights management systems and European law: between copyright protection and access control**,** Web Delivering of Music, 2002. WEDELMUSIC 2002. Proceedings. Second International Conference on Volume , Issue , 2002 Page(s): 117 - 124
- Dreier T. P.B. Hugenholtz (ed.), Concise on European Copyright Law, Alphen aan den Rijn, Kluwer Law International, 2006, p.393
- Emmanuel, S., & Kankanhalli, M., (2001). Copyright protection for MPEG-2 compressed broadcast video. In IEEE Int. Conf. on Multimedia and Expo, ICME 2001 (pp. 206-209). Tokio, Japan.
- European Commission, First Report on the application of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), Brussels, 21.11.2003, COM(2003) 702 final
- European Commission, Digital Rights Management, High Level Group Documents, at http://ec.europa.eu/information_society/eeurope/2005/all_about/digital_rights_man/documents/index_en.htm
- Gantz, J., & Rochester, J. (2004). Pirates of the Digital Millennium: How the Intellectual Property Wars Damage Our Personal Freedoms, Our Jobs, and the World Economy. FT Prentice Hall.
- GartnerG2, Copyright and Digital Media in a Post-Napster World, Version 2 (Updated January 2005), by GartnerG2 and The Berkman Center for Internet & Society at Harvard Law School.

- Hanjalic, A. (2000). Image and video databases: restoration, watermarking and retrieval. Amsterdam Lausanne : Elsevier.
- Harte, L. (2006). Introduction to Digital Rights Management (DRM); Identifying, Tracking, Authorising and Restricting Access to Digital Media. Althos Publishing.
- Internet Resource For Digital Rights Management: http://www.drmwatch.com/legal/
- Joaquim Filipe, Helder Coelhas, and Monica Saramago, "E-business and Telecommunication Networks: Second International Conference, ICETE 2005", Reading, UK, October 3-7, 2005. Selected Papers (Communications in Computer and Information Science), by (Paperback - Dec 14, 2007)
- Johnson, N.F., Duric, Z. & Jajodia, S. (2001). Information hiding: steganography and watermarking- attacks and countermeasures. Boston : Kluwer Academic Publishers.
- Katzenbeisser, S. and Petitcolas, F. (2000). Information Hiding Techniques for Steganography and Digital Watermarking. Boston, MA : Artech House.
- Kundur, D., (2004). Video fingerprinting and encryption principles for digital rights management. Proceedings of the IEEE, 92(6), 918-932.
- Kuribayashi, M., & Tanaka, H., (2005). Fingerprinting protocol for images based on additive homomorphic property. IEEE Transactions on Image Processing, 14(12), 2129-2139.
- Lei, C.-L., Yu, P.-L., Tsai, P.-L., & Chan, M.-H., (2004). An efficient and anonymous buyer-seller watermarking protocol. IEEE Transactions on Image Processing, 13(12), 1618-1626.
- Lemma, A., Katzenbeisser, S., Celik, M., & van der Veen, M., (2006). Secure watermark embedding through partial encryption. In International Workshop on Digital Watermarking (IWDW 2006), Springer Lecture Notes in Computer Science, Vol. 4283 (pp. 433-445), Jeju Island, Korea.
- Lu, C-S. (Ed.) (2004). Multimedia security: steganography and digital watermarking techniques for protection of intellectual property. Hershey, Pa. ; London : Idea Group.
- Malkin, M. & Kalker, T., (2006). A cryptographic method for secure watermark detection. In 8th International Workshop on Information Hiding, IH'06, Springer Lecture Notes in Computer Science, Vol. 4437 (pp.26-41). Old Town Alexandria, Virginia, USA.
- Memon, N., & Wong, P., (2001). A buyer-seller watermarking protocol. IEEE Transactions on Image Processing, 10(4), 643-649.
- Parviainen, R., & Parnes, P., (2001). Large scale distributed watermarking of multicast media through encryption. In International Federation for Information Processing, Communications and Multimedia Security Joint working conference IFIP TC6/TC11, Vol.192 (pp 149-158). Darmstadt, Germany.
- Picot Arnold and Fielder Marina, Property Rights and Openness as Factors of Innovation, in Bindseil U., Haucap J. and Wey C. Institutions in Perspective, 2006 Mohr Siebeck, Tübingen, Germany
- Piva, A., Cappellini, V., Corazzi, D., De Rosa, A., Orlandi, C., and Barni, M., (2006). Zero-knowledge ST-DM watermarking. In P. W. Wong and E. J. Delp (Ed.), Security, Steganography, and Watermarking of Multimedia Contents VIII, Proc. SPIE, Vol. 6072 (pp. 291-301). San Jose, CA, USA.
- Pik-Wah Chan, "Digital Video Watermarking Techniques for Secure Multimedia Creation and Delivery", July 2004.
- Rosenblatt, B., Trippe, B., & Mooney, S. (2001). Digital Rights Management: Business and Technology. Wiley Publications.
- Safavi-Naini, R., & Yung, M. (2005). Digital Rights Management: Technologies, Issues, Challenges and Systems. Lecture Notes in Computer Science.
- Tassel, J. (2006). Digital Rights Management: Protecting and Monetising Content. Focal Press.
- Taubman, D.S. & Marcellin, M.W. (2002). JPEG2000: Image Compression Fundamentals, Standards and Practice. Boston Dordrecht : Kluwer Academic Publishers.
- Troncoso, J. R., & Perez-Gonzalez, F., (2007). Efficient non-interactive zero-knowledge watermark detector robust to sensitivity attacks. In P. W. Wong and E. J. Delp (Ed.), Security, Steganography, and Watermarking of Multimedia Contents IX, Proc. SPIE Vol. 6505. San Jose, CA, USA.
- Pan, J.S., Huang, H.C., Jain, L., and Fang, W.C. (2007). Intelligent Multimedia Data Hiding: New Directions (Studies in Computational Intelligence) Berlin / Heidelberg : Springer
- Rabbani, M. & Joshi, R. (2002). An Overview of the JPEG2000 Still Image Compression Standard, Signal Processing Image Communication, 17(1).
- Seitz J. (Ed.) (2005). Digital Watermarking for Digital Media. Information Science Publishing.
- Schneider Markus and Henten Anders, DRMS and TCP: Technology and Law, CTI Working Papers, no. 76, Center for Tele-Information, COST A20 Conference Towards, New Media Paradigms, Pamplona 27-28 June 2003

- Wayner P. (2002). Disappearing cryptography: information hiding: steganography and watermarking (2nd Edition). Amsterdam Boston : Morgan Kaufmann.
- Zeng, W., Yu, H., & Lin, C. (2006). Multimedia Security Technologies for Digital Rights Management. Academic Press.
- Zhang, J., Kou, W., & Fan, K., (2006). Secure buyer-seller watermarking protocol. IEE Proceedings on Information Security, 153(1), 15-18.