Digital Rights Management in the Cultural Heritage Arena: A true or a Myth?

by Andrea de Polo
Fratelli Alinari SpA
www.alinari.com
andrea@alinari.it

SUMMARY:

Digital Rights Management (DRM) describes a set of functionalities which control access to, and the use of, copyright material. In particular, they focus on the acquisition of revenue from copyright material, and the prevention of its re-use and misuse in the online environment.

This document describes the DRM system in the cultural heritage sector. The value of the DRMS to the content repositories and also to the end users is described.

Managing digital rights is a focal point for any content provider.

DRM is the necessary building block on which to build online content-trading processes. Every day a vast amount of material is distributed online, through the Internet and private networks. Owners of digital material need to protect their digitized goods without inhibiting their trade. In economic terms, the contribution made by (digital and non-digital) copyright-based goods and services to the Community's GDP is significant and rising (around 6% of GDP).

The aim of a reliable and trusted DRM system should be as follow:

1. A trusted photographic licensing and IPR solution
2. Third party content providers
3. A "trusted" network of providers and users. Trusted because the access will be through a subscription fee and because the end user will have to agree to certain IPR and image usage regulations before entering into the site. A specific IPR image licensing model will be available for download, through the content provider site
4. The "standard" DRMS solution described here is related to the "Standard" IPR image licensing form
5. The images are watermarked (statically and-or dynamically, on the fly) and by carry on a small visible copyright logo
6. The system is monitored remotely by the content provider personnel in order to assure the most reliable usage of the system
7. A web crawler monitor the download of the images and their possible (not legal) usage, after words, on the web.

The future of internet based solutions for content delivery are further enhanced, beside still jpeg images also by MPEG audio and video through greater choice in the content with which the user can choose to interact. In structured audio books, for example, a specific chapter from a text book can be provided in a specific form.

Business solutions can also be incorporated through the use of DRM, allowing several user types or profiles to co-exist in one revenue stream. At a consumption level, the common user can then specify how that content is delivered and save these preferences for their particular user scenario.

The aim of this document is to define the rule that governs the usage of the images and video shared by content providers. This IPR guideline document is meant to encourage also to use text and other content.

Definition of “DRM”:
a system, comprising technological tools and a usage policy, that is designed to securely manage access to and use of digital information.
By “technological tools,” we refer to both hardware-based and software-based measures. In the copyright context, these tools are often called “technological protection measures” (“TPMs”) or, simply, “technical measures.” In this report, we distinguish between DRM systems and TPMs: DRM systems often utilize TPMs – the “technological tools” of our definition – as component parts.
The term “TPM” typically refers to technologies that control access to or use of information, or both. A TPM that controls access to information might be as simple as a password protection. More complex access-control TPMs use encryption to regulate access to information by encrypting it and permitting decryption and access only by authorized individuals or devices.
Use-control TPMs control the uses that can be made of a work after an individual accesses it. The most common type of use-control TPM is a copy-control mechanismwhich regulates or prevents duplication of all or part of a work. Macrovisiontechnology, for example, is a copy-control technology which prevents or distortscopying of Macrovision-protected DVDs.

1. THE DRMS AND THE CONTENT REPOSITORIES

The digital rights management system embedded in cultural heritage online sites (mainly stock agencies, galleries, photo archives and content providers) is an important element of the value proposition to content repositories. By protecting the rights of the content owners, it provides the platform whereby revenue can be derived from online virtual access to their important material. Without such a system, the value of having online material is greatly decreased, and is reduced to merely advertising for 'real' visits to the institutions which host the source material, or to sell physical prints and copies of images.

Having a strong DRMS makes cultural sites attractive as a business partner to those institutions which host the content. By utilizing the DRMS, the memory institution or image repository gains the benefits of a DRMS, without having to implement its own.

1.1 THE DRMS AND LARGE REPOSITORIES

Large content providers should adopt a DRMS policy in order to be sure to place their valuable content into a trusted repository, even through a shared network. This means increased web traffic, more visibility and better chances for selling content.

The unity and standardization of the tools used within the DRMS system are some of the main reasons why large archives should license their content to large online repositories.

1.2 THE DRMS AND SMALL REPOSITORIES

The objective of the DRMS is to provide the small content provider with a quality set of legal and technical solutions which securely protect their content. Often, small archives do not have the budget for marketing, promotion or technical security; they can achieve this through financially inexpensive solution.

1.3 THE DRMS AND THE END USER

While protecting the Content Repositories is an essential part of the DRMS, the end users must have a simple and effective method for accessing content – otherwise the commercial offerings of the Repositories will not be attractive.

Essentially, a DRMS is a system which restricts the activities of end users, in terms of re-use of copyright material. However, if the DRMS is seen to be excessively restrictive, or to hamper the activities of the user, this makes the whole solution unattractive. The aim of the DRMS, with regard to end users, is to control their activity in an **unobtrusive** manner.

Four aspects of the DRMS are considered here, with discussion explaining how they serve the end user, and not just the online system and the content repositories :

1. Access Control
2. Use Restrictions
3. Visible Watermarking
4. Invisible Watermarking

1.4 DRM Requirements for Research and Education

DRM is recognized as a complex and critical aspect of the lifecycle of a digital object. In Research and Education (R&E), we are currently witnessing a surge of interest in DRM for several reasons. An obvious reason is the need for DRM to support digital library collections, code and software development, distance education, and networked collaboration, among other applications. Many institutions, for example, have completed the first step in the development of digital collections — the digitization and storage of content, and the development of descriptive metadata schemes for discovery and retrieval of that content. Progressing to the next step of enabling global access to that content will require DRM.

There is also evidence of a growing interest in academia for open publishing models, such as the Budapest Open Access Initiative. These new models are emerging in response to escalating commercial journal costs and restrictive publishing practices, which are perceived as disenfranchising the journal authors from their own intellectual property. Open publishing models require new DRM strategies that emphasize fair use, protection of intellectual property from misuse, and multiple subscription models, which include both fee-based and non-fee based access.

Finally, many in R&E consider that commercial DRM solutions tip the balance between the rights owner and the user too much in favor of the rights owner, undermining fair use and the first sale doctrine in the process — two critical and cherished principles in R&E. There is also concern that some DRM implementations compromise the privacy of the user.

In response to this growing need to support expanding digital collections and new scholarly publishing models, as well as networked collaboration, there is a movement underway to develop DRM solutions to specifically meet R&E requirements. These requirements include: accommodating the highly collaborative and distributed aspect of many R&E activities; supporting fair use of copyrighted materials for educational purposes; supporting granular and differential access to resources; preventing misuse of resources; insuring the integrity of resources; and interoperating with existing and emerging infrastructure.

Two points are worth noting here. The first is that R&E requirements reveal a distinction between conventional definitions of DRM (the e-commercial model, which functions solely to protect the rights of the owner) and the broader definition emerging in the R&E community. The latter includes access management as well as intellectual property rights management, and is as concerned with the rights of the user as with those of the rights owner. Indeed, given this difference in interpretation, it has been suggested that the term "DRM" has been appropriated by the publishing industry and that the goals of the R&E community in this space would be better served using a different term. The second point is that, whether fair use is interpreted as a declarative right or a defense, methods have been proposed to accommodate fair use either in trusted systems or by means of third-party escrow. The notion, therefore, that an accommodation of fair use is beyond the province of DRM technologies is being challenged.

The VidMid Video-on-Demand Working Group is exploring how far middleware (identity management, authentication, authorization, security and metadata) and the establishment of communities of trust might go towards implementing customized, open and interoperable DRM systems. This focus is the theme of an invitational workshop planned for September 2002; the "NSF Middleware Initiative and DRM Workshop is being funded by the NSF NMI program to bring together content management, copyright law, and middleware experts to explore cooperative DRM development to meet R&E needs. The workshop will be facilitated by the authors, and is supported by the Coalition for Networked Information, EDUCAUSE, Internet2, the Southeastern Universities Research Association, and the Video Development Initiative.

An additional and very significant focus for the “NMI and DRM Workshop” is the presentation of a proposal to cooperatively develop a rights metadata core. Equivalent to the Dublin Core for descriptive metadata, the rights core will be cooperatively developed to meet R&E requirements, and will map to existing and future rights languages, as well as interoperating with descriptive metadata schemas. There is a proliferation of rights languages currently, but, for the most part, these support one-to-one e-commercial transactions. A sufficient user base is not yet established to determine whether these languages are flexible and extensible enough for R&E purposes, or whether their use is going to be encumbered by patent claims. The rights core data element set and application schema will be developed by identifying the core DRM needs for R&E, and mapping the data elements required to document and support those needs against existing rights schemas. One of the significant benefits of this process will be the identification of R&E needs that are not currently addressed by existing schemas. The authors expect to propose changes and additions to existing schemas to provide more relevance and utility for R&E among commercial and open source DRM implementations.

A DRM implementation, obviously, entails more than technology. There are complex legal and policy issues implicit in any DRM implementation, as well as a need to support gradations of risk. The FDRM project is a first step for VidMid in testing the hypothesis that it is possible to develop a DRM solution to meet R&E requirements — it does not attempt to address all of these complexities. Our approach to the DRM problem is focused on flexible access management rather than enforcement of rights after the user has legitimately accessed the resource. Our primary goal in this article is to present a reference architecture for FDRM to demonstrate how emerging middleware infrastructure might be leveraged as a foundation and framework for an effective DRM implementation.

a. ACCESS CONTROL

Access to the online repository is available only to the holders of valid passwords. This ensures that all use of the system has been paid for, and thus that the content providers receive revenue from the use of their material.

At the same time, such access control ensures the **highest level of performance** for the end user. With restricted user numbers, system response time are rapid and the use of the system involves the minimum delay and waiting. This is of particular importance when dealing with large image files, which have their own inherent delays.

b. USE RESTRICTIONS AND USER SCENARIO

The DRMS controls the end user by restricting the amount of material which he can view, manipulate or download via the online portal. A counter tracks how many images each subscriber has downloaded or can access, view or download and print. Typically, a user can download a certain number of images per annual subscription. Once no more credits are left, the user can acquire further credits.

The portal makes it clear to the user at all times how many credits he has remaining in his account, and how many credits each operation will cost him. This allows the user to budget his use of the system appropriately, and ensures that he has no unpleasant surprises when he wishes to use the system for research, education, training, etc.

c. VISIBLE WATERMARKING

The use of a visible watermark on the content can be viewed by the end user as a ‘necessary evil’. While the visible watermark does not enhance the value of the image from the user’s point of view, it is an integral part of the system, which is itself of great value to the user. In order to minimize the intrusion and impact on the end user, the visible watermark is translucent and subtle, and is placed non-centrally on the image.

d. INVISIBLE WATERMARKING

The invisible watermark on the images has no impact whatsoever on the legitimate user of the content. This powerful and important element of the DRMS thus serves the user particularly well – it has no impact whatsoever on the user, while being an important enabler of the useful and valuable IPR system.

e. THE VIEW OF THE NEXT GENERATION SERVICES

Gartner view for the future Web 2.0 is “a combination of new technologies, user content and communities that is transforming the Web to a full-fledged computing platform serving Web applications to end users. Retailers have yet to embrace this phenomenon, but they need to do so to protect against threats to their brands.” Consequently the majority of the big enterprises is expected to have the technology to use the new Web 2.0 possibilities but they will be late to apply the most promising aspects of this advance which should respect the social aspect of the new services. The social aspects is evidenced by the following Table 1 where it is clear the user participation to the empowering of the new web contents and services.

Web 1.0	➡	**Web 2.0**
Personal web sites	➡	Blogging
Domains speculation	➡	Optimisation of positioning in web crawlers
Business on page views	➡	Cost per click
Content publication	➡	Content creation in networked partnerships
Content management systems	➡	Wikis (editing the contents)
Taxonomy (top-down and rigid classification of contents)	➡	Folksonomy: the users classify autonomously the contents
Stikiness (try to keep the visiting users as long as possible on the site)	➡	Syndication (portion of the site is made available to other sites that share users and contents)

Table 1: new approach to the Web services

TECHNICAL INVESTIGATION RESULTS

2.1 Introduction

In presenting the results of our technical investigations in this Report, it is helpful to draw a distinction between what we have coined as “autonomous DRM” and “netdependent DRM.” Although useful for presenting the results here, this distinction did not factor into our technical investigations or our *PIPEDA* assessments substantively in any way.

Autonomous DRM refers to DRM that needs no outside interaction to fulfill its purpose. Software that requires a CD-Key before becoming useable, DVDs that will only work with DVD players in certain regions and software that deactivates after a given number of uses are all examples of autonomous DRM.

Net-dependent DRM refers to a growing trend in DRM schemes that involves either internet authentication, internet surveillance of uses and/or the tying of content to an online platform. Online music subscription services that deploy digital licenses to allow the use of locked content, web-enabled software validation and the tying of content to an online platform are all examples of net-dependent DRM.

In our technical investigations, we found that many, but not all, autonomous DRMs connect to and communicate with external computers during the course of the operation of the DRM. Conversely, *all* of the net-dependent DRM systems that we investigated communicated with external computers. We also found that a number of the DRM products we investigated communicated with the same third parties: Akamai Technologies, Omniture and DoubleClick.

2.2 Autonomous DRM

Six of the products that we investigated used *Autonomous DRM*. Four of these showed no communications. Since autonomous DRM does not appear to need to communicate to fulfill rights management purposes, it is natural to ask questions regarding those that do engage in external communications. Our assessment revealed that these communications appeared in most cases to be linked to advertising and web metrics.

Consider our investigation of Disney's *Pirates of the Caribbean* DVD (disc 2). When we inserted the DVD, a pop-up window appeared asking us to install the Interactual Player, software that plays DVDs on computers. Once we installed the software, a configuration window appeared with a tab marked "Privacy." We deselected all agreements to information transfers. Nonetheless, we captured communications to InterActual servers. Indeed, the software placed a cookie onto our test computer.

The cookie itself can only be read by an InterActual website, but this does mean that InterActual may have collected our IP address, web browser and operating system information through the cookie request from our computer. As the InterActual interface window does not go through a web browser, it is likely that an unsophisticated user would not know that he or she is downloading advertising from the internet or delivering information to InterActual.

2.3 Net-dependent DRM

2.3.1 Products Purchased in Physical Form

Net-dependent DRM systems rely on internet communications to fulfill their rights management purposes.. Whereas *autonomous DRM* authentication usually requires a user to enter a valid identification key as pre-determined by the software, *net-dependant DRM* goes one step further and, for example, cross-references this key with a database to ensure that the key is not already being used by another user.

Our investigation revealed that many store-bought net-dependent DRM-protected products allow users a limited number of uses or limited functionality; others simply will not work until authenticated *via* the internet or sometimes by telephone.

2.3.2 Online Products and Services

Online content subscription services such as the Ottawa Public Library (OPL) and Napster deploy digital licenses to allow the use of locked content. The downloaded content. For example, our investigations revealed that if a user pays for a one-month subscription with Napster and tries to play Napster acquired songs through Windows Media Player while Napster is uninstalled, then the digital license attached to the song will require the reinstallation of Napster. This is not a format issue; songs can be played outside of Napster. If Napster is installed on a user's computer, the user can play Napster-acquired songs through other platforms such as Windows Media Player.

All of our investigations involving online services revealed communications to third party sites belonging to companies such as Akamai Technologies, Omniture and DoubleClick. Although we know something about the general nature of these businesses, we do not know what information was sent to them.

3 CASE DESCRIPTIONS

3.1 ALINARI

- **Fratelli Alinari,** founded in Florence in 1852, is the oldest firm in the world in the field of photography and more in general in that of the image and communication. The birth of photography and the history of the firm go hand in hand in their development and growth, as witnessed by the immense fund of *over 4.000.000* photographs Alinari owns today. The Internet related business can be roughly illustrated by the following descriptive criteria.
  - Number of images on-line: more than 330.000 images
  - format: jpeg, tiff, and soon Microsoft HD-Photo
  - resolution:
    - thumbnails: 128x128 pixels
    - low resolution: 256x256 pixels
    - low-medium resolution: 480x480 pixels
    - medium resolution: 800x800 pixels (internal use only)
    - high resolution: 4000x6000 pixels (on demand)
  - watermarking: watermark on the fly
  - digitised : more than 330.000 images.

- catalogued : more than 330.000 images.

Key words for the search engine: about 8.000 (chosen with the collaboration of the University of Florence). The images are digitised from originals (films, slides, vintage prints, daguerreotypes, collotype, stereotypes…).

- Total Alinari's archive amount of images (owned): over 4.000.000

- Total images (owned plus managed) : about 20.500.000

Areas of interest: Art, Architecture, Travelling, Agriculture, Industry, History, Movie, Fashion, Theatre, Science, Technology,…

Number of photographers **:** 2.500 (from 1852 till nowadays)

Number of artists represented : 5.000 artists (whose works are preserved in more than 200 museums: Gallery of Uffizi, Museum of Louvre, British Museum, National Gallery, Musée D'Orsay, Pinacoteca of Brera, Palatino Gallery of Florence, Vatican Museums, Museum of Egypt in Cairo, Ermitage of Pietroburgo, etc..)

Archives managed or represented by Alinari: Italian Touring Club (about 500.000 images); Ansaldo Industry (about 200.000 images); TEAM Archive (about 50.000); Roger-Violet archive.

*Customers***:** graphic designers, editors, reporters; advertisement; restorers; police; medical; web designers; architects; art buyers; writers; web advertisement; designers; researchers; students; professors

*Transactions via Internet***:** more than 400 transactions/ year

*Number of online-clients***:** more than 8.000 online business clients, more than 7.000 online education clients

Payments: online by credit card, off-line by post or bank

The knowledge presentation in the cultural heritage domain and the basis for an approach towards interoperability must take into account the actual status of the art in the professional context and the on going researches projects that have been set up.

Business

http://business.alinari.it
Educational and multilingual
http://edu.alinari.it
http://www.orpheus-edu.org
http://www.euridice-edu.org
Visual
http://schema.alinari.it
Ontologycal
http://www.acemedia.org
Geographical
http://www.echase.org
Spatial
http://eu.alinari.it/ipix/ecmade/index.htm

Name:	**ALINARI BUSINESS.COM**
Address:	Http://www.business.alinari.com
	ALINARI
Description:	It's a business to business site, developed since 1999, featuring 330.000 images, bilingual. Images can be downloaded at high resolution once the user has registered to the Alinari picture library
Target:	B2B market
Key points:	• This site is used only by professional users (jurnalists, newsagents, editors, etc.)

Name:	**ALINARI EDU.COM**
Address:	Http://www.edu.alinari.com
	ALINARI
Description:	It's a multilingual e-learning photographic site featuring 85.000 images, powered by XLImage zooming technology. It can be accessed through a flat fee subscription business model (30 euros for 1 year for the single student, 10.000 euros for flat fee for a whole university)
Target:	B2B and B2C market in educational area
Key points:	• Difficulties in finding in Europe a proper market to sell easily this kind of services, probably for two main reasons: – a *financial reason*, i.e. universities are often short in money; – a *pragmatic reason*, i.e. universities have often their

	own e-learning system or methodology and joining an independent service can create some problems

Meaning, digital policy enforcement and governance issues

There is a need for digital rights management infrastructure, as a tool for content management (both commercial and noncommercial).

But digital rights management, even in the limited context of the management of “content” on the network, has at least four different components:

· A “policy metadata” layer, which allows for the structured description of policies – what permissions relate to this item of content, under what conditions of use (for example, attribution, period of use, payment), and what is not permitted (for example, adaptation);

· An “authentication, authorization and access” layer – which allows for the structured identification and authorization of different users (or classes of users) and the matching of their privileges with the permissions relating to content;

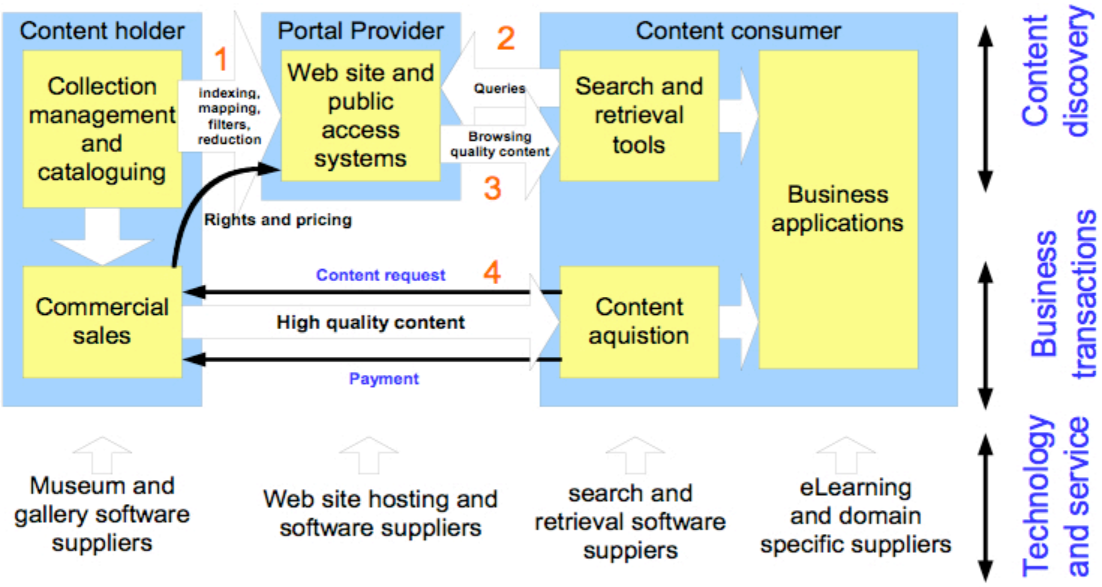
· An “enforcement” layer, which is the technology most commonly associated with the acronym “DRM”
– the technology which allows policies relating to content to be enforced even after content has been
released from a controlled local network into the (uncontrolled) global network;

· An “audit” layer, which allows activities to be recorded and compliance with policies to be monitored.

In essence, a perfect software for the delivery of high quality images should have the following features:

- Allow quick and easy view of even huge (up to gigabytes) image files.
- Not require plugins or special client software.
- Not require proprietary image formats and instead support the most popular ones.
- Allow interactivity with the end user, offering advanced functionalities such as zooming, panning, dragging, comparing of more images, editing of remote images, one-on-one editing sessions.
- Guarantee colour accuracy, enabling the server to deliver image ICC colour profiles and by having the profiles interpreted on the client side, therefore ensuring colour accuracy on user’s display.
- Ensure implicit protection of image by not allowing copy of the whole image file.
- Allow the image to be protected by dynamic digital watermark.
- Enable tracking of the watermarked image and its users.
- Allow easy integration within existing website architecture
- Allow integration with databases.
- Allow full customization for specific functionalities and user interfaces.
- Be browser independent.

- Require minimal hardware power on user's side (low computing power, low RAM, average speed Internet connection)


Content holder
Collection management and cataloguing
Commercial sales
1
indexing, mapping, filters, reduction
Portal Provider
Web site and public access systems
Rights and pricing
2
Queries
Browsing quality content
3
Content consumer
Search and retrieval tools
Business applications
Content aquistion
Content request
4
High quality content
Payment
Content discovery
Business transactions
Technology and service
Museum and gallery software suppliers
Web site hosting and software suppliers
search and retrieval software suppiers
eLearning and domain specific suppliers

Example of DRM standard sign form:
COPYRIGHT RELEASE FORM
I / we agree that the abstract/paper entitled:

____

____

is original work and has not been published in any other publication
I/We give my/our permission for the written paper to be published in the Journal 'Forum' by … if and when the manuscript is accepted for publication.
The author(s) reserve(s) all proprietary rights such as patent rights.
The author(s) retain the right to use all or part of this manuscript in future works of their own, such as lectures, press releases, reviews or text books.
The presenting author is responsible for providing evidence of copyright clearance or authority on any items subject to copyright which are included in the manuscript.

Signed: ____
Date:___________
(presenting author)
Signed: ____
Date:___________
(co-author)
Signed: ____
Date:___________
(co-author)
Signed: ____
Date:___________

Return this signed form together with a hard copy AND electronic version of your paper to:…

Credits and link sources:

1. Federated Digital Rights Management (D-Lib Magazine July/August 2002)
2. Digital Rights Management and Copy Protection Schemes (EFF org)
3. http://en.wikipedia.org/wiki/DRM
4. http://www.drmwatch.com/
5. http://drm.info/