中央研究院
資訊科學研究所
Institute of Information Science, Academia Sinica • Taipei, Taiwan, ROC

TR-IIS-05-019

數位典藏國家型科技計畫
數位權利管理技術簡介

Jen-Hao Hsiao, Lee-Feng Chien, Chu-Song Chen

December 2005 || Technical Report No. TR-IIS-05-019

http://www.iis.sinica.edu.tw/LIB/TechReport/tr2005/tr05.html

數位典藏國家型科技計畫

數位權利管理技術簡介

Jen-Hao Hsiao, Lee-Feng Chien, Chu-Song Chen

Institute of Information Science, Academia Sinica, Taiwan,
{jenhao, lfchien, song}@iis.sinica.edu.tw

2005 年 3 月

目次

1. 簡介

隨著資訊科技的快速發展及資訊的數位化、電子數位產品不斷的出現，與網際網路無遠弗屆的便利性，使得所有數位資料得以快速簡便的複製與傳遞，大量的文字，繪畫與傳統媒體等均轉換成數位檔案作儲存，電子化社會（e-society）已經儼然成型！『數位典藏國家型科技計畫』在民國 91 年 1 月 1 日正式成立，是承襲行政院國家科學委員會『數位博物館計畫』、『國家典藏數位化計畫』、『國際數位圖書館合作計畫』三個計畫的經驗，依據國家整體發展，重新規劃而成。在數位典藏計畫中，各典藏單位將其珍貴的歷史文物轉換成數位檔案進行儲存與典藏，也因此產出了大量的數位內容。

數位內容在形式上有別於傳統有形著作，必須面臨許多不可避免的問題與挑戰。其以檔案形式存在，各類影音、文件出版品與錄音著作的儲存媒介與電腦的儲存媒介相互整合，使用者不僅可以輕易地在電腦上播放各類影音及錄音檔案，更可以毫不受限地重製受到著作權保護的著作，如此則容易導致使用者有意無意中去觸犯到智慧財產權擁有者的權利，造成了著作權人利益的損害。國家典藏的數位化，可以有效提升知識的累積、傳承與運用，是知識經濟的重要基礎環節，要如何享受國家典藏數位化後為我們帶來的便利，而同時又能兼顧著作權人之權利，也因此為成一門相當重要的課題。

數位權利管理（Digital Rights Management）技術近年來引起了廣泛的討論與注意，其所提出之數位物件保護架構，提供了著作權人一個可靠的數位智財保護方案。在其架構概念下將可以達到：

- 避免數位智財未經授權的複製濫用

藉由數位權利管理可以有效的減低數位智財被複製濫用的情形，因為不論原始的數位內容被複製多少份，還是只有擁有相關數位權限的使用者得以使用，也因此讓數位內容的安全性多了一份保障。

- 有效的數位智財控管

數位智財的擁有者可以利用數位權利管理系統來管控流通在外的數位智財之使用情形，也可以動態決定所有使用者的存取權限，以確保正確的人員以合適的方法使用正確的資訊。

- 侵權行為的偵測與追蹤

數位權利管理系統除了對數位內容進行加密外，同時也會加入可供日後追蹤用的訊息在其內，如：數位指紋(Fingerprint)或生物資訊…等。如果數位內容的保護機制遭到破解，數位智財的所有權人可以憑著這些可供追蹤的資訊來進行侵權行為的追蹤，使侵權行為得以控制在一定範圍內，以降低傷害。

DRM 技術小組，隸屬於數位典藏技術分項之下，專職於發展及導入適用於數位典藏計畫之數位權利管理技術，並負責推廣與建置相關系統。為了協助典藏單位以更有系統的方式了解目前數位權利管理技術發展現況與未來之趨勢，特別製作本件，文中並分析當前之數位權利管理技術工具應用於數位典藏計畫之可行性，並以多媒體中心(Multimedia Center)為例，建置一套整合數位權利管理技術之示範網站 (DRM Demo Site , http://nddemo.iis.sinica.edu.tw/ndmmc2/)，以供典藏單位做為技術導入之參考。

2. 數位權利管理技術概觀

2.1. 定義

數位權利管理技術 (Digital Rights Management，簡稱 DRM)，國際數據資訊中心 IDC(Internet Data Center)為數位權利管理技術下定義為[7]：結合硬體與軟體的存取機制，將數位內容設定存取權限，並與儲存媒體聯結，使得數位內容在其生命週期內 — 從產生到消失，都會受到保護。不管在其使用過程中是否有複製行為發生，仍然可以持續追蹤與管理數位內容之使用狀況。簡而言之，在數位內容生命週期內，能提供完善保護數位內容、權利之管理技術，則稱為數位權利管理技術。

2.2. 數位權利管理技術典型架構

數位權利管理技術運作的過程中，通常會涉及到以下四個不同的實體[14]：內容提供者(Content Provider)、數位內容經銷者 (Distributor)、交易與權限控管中心(Clearinghouse)與消費者(Consumer)。 圖 1 描繪出了一個典型的數位權利管理技術模型概念，而每個實體所代表的意義為：

(1) 內容提供者(Content Provider)

數位內容的提供者，擁有數位內容的權利。

(2) 數位內容經銷者(Distributor)

數位內容經銷者為內容提供者和消費者之間的媒介，並擁有數位內容銷售或散佈的管道及通路。他們從內容提供者接收取數位內容後，再利用其通路交給消費者。

(3) 交易與權限控管中心(Clearinghouse)

負責管控數位內容的權限與交易等事宜，並負責核發數位權限(digital rights)，所有消費者的相關執行權限與交易記錄都會被記錄在此。

(4) 消費者(Consumer)

有意願取得及利用數位內容的末端使用者。

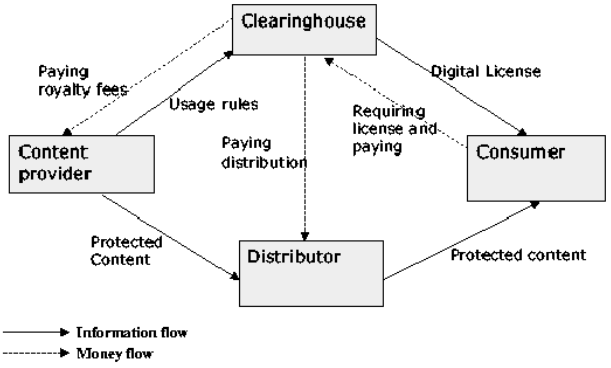


圖 1 (資料來源：[14])

模型的運作流程如下。首先內容提供者利用加解密技術封裝原始的數位內容，並加入代表其所有權的浮水印及其願意開放的數位權限。封裝完成的數位內容將會傳遞給擁有通路的『數位內容經銷者』，而其相對應的數位權限則交由『交易與權限控管中心』進行保存。消費者可以透過數位內容經銷者取得經過封裝的數位內容，並向『交易與權限控管中心』要求相關授權，或進行數位權利之購買。『交易與權限控管中心』收到消費者的請求後，再依據其提出之要求審核其資格是否符合，確認後再給予其要求之數位權利。最後消費者則可以依據此數位權利所允許執行之項目，來解開封裝的數位內容，並進行利用。值得注意的是，消費者仍然可以任意的散佈從數位內容散佈者所下載的封裝數位內容，但是其它使用者將因沒有『交易與權限控管中心』所核發的數位權限，而無法對該數位內容進行應用。

2.3. 商業數位權利管理系統

根據不同的保護需求及用途，數位權利管理技術系統的架構也不盡相同，因此廠商也推出了各種不同保護標的之數位權利管理技術系統。這些系統可以粗略分為：

- 多媒體影音的保護
  保護的標的物為 MP3、DVD、VCD 等多媒體方面，用來防止影音內容遭到盜拷。在技術上多採用 stream 的方式將媒體從伺服器端送給客戶端，並對傳送的封包進行加解密的動作，以進一步達到控管的目地。

- 機密文件的保護
  主要用於保護機密資訊免於未經授權的使用，並管理其在允許權限內合理範圍的使用，並紀錄其使用時間及方式，這類數位權利管理技術系統通常用於企業環境或電子書的使用上。

由於目前各典藏單位對於數位權利管理技術的需求較為傾向對於機密文件(影像)的保護，因此在本節中，將主要針對此一類型的數位權利管理技術開發廠商進行現狀評估，以了解目前市場上之數位權利管理技術發展情形。

(1) Microsoft Windows 版權管理服務

微軟近年來在數位權利管理技術的發展不遺餘力，其所提出的解決方案含蓋多媒體影音及電子文件的保護，尤其以其軟體業龍頭的地位，可以說舉手投足間皆對數位權利管理技術未來的規格及發展皆有相當大的影響。而微軟在 2003 年推出了新一代的數位文件保護技術： WindowsR 版權管理服務 (Rights Management Services，RMS)[27] 架構(如圖 2)，來提供協助保護敏感的 Web 內容、文件、及電子郵件。RMS 架構於 Windows Server 2003 平台上，再搭配可執行於 Windows 用戶端上且具有版權功能的應用程式和檢視器，以? 成其數位文件保護的架構。數位文件的創造者或擁有者可以透過客戶端版權管理程式(Rights Management Services Client Access Licenses)設定文件或電子郵計件訊息相關聯的使用權限，並可指定使用項目，例如：文件是否可被列印、複製、或轉寄…等等。RMS 還提供了持續保護，即無論資料傳到何處，所設計的原則都會一直跟隨著資料。並可搭配現有的參數型解決方案 (如防火牆與存取控制清單)，便可在起始時就限制有那些人具有存取文件或檔案的權限。當一般使用者欲開啟受到 RMS 保護的檔案時，首先他必需先安裝用戶端存取程式 (Windows Server CALs)，之後才可以對該檔案進行利用。而在使用者驗證方面，RMS 使用

Active DirectoryR 來進行使用者身份驗證，並可與其它如智慧卡或生化科技之類的技術整合。

整體而言，微軟提供了一個植基於 Windows 平台之上的數位版權保護機制，並利用其在作業系統上的優勢，結合了 Windows Server 2003 與 Office 2003 來建構出安全的數位文件傳遞環境，也提供了數位權利管理技術一個未來的方向。

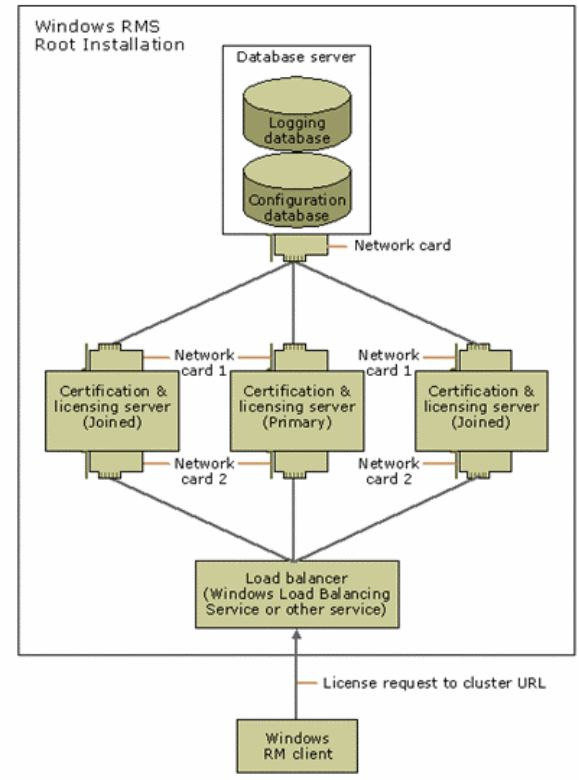


圖 2(資料來源：Microsoft: http:// http://www.microsoft.com/)

(2) InterTrust Rights|System

InterTrust[10]幾乎可以說是第一個以數位版權管理技術為其技術核心的科技研發公司，也因此有著相當卓越的數位權利管理技術，其所開發的 Rights|System 也為數位內容提供了安全封包、散佈及權限管理的技術支援(如圖 3)。Rights|System 的主要系統核心在於『封包程式』與『權限管理伺服器』兩大元件。『封包程式』使用了 AES 加密演算法對數位內容進行加密，並提供 SHA-1(Secure Hash Algorithm)數位簽章演算法來防止數位內容被惡意的竄改。『權限管理伺服器』則完整記錄了使用者端的認證資訊、使用者所擁有的數位權限及數位內容加解密金鑰資訊。

使用者需要安裝 Rights|System 客戶端程式才可以開啟經過『封包程式』封

裝後的數位內容。較特別的是，Rights|System 客戶端程式不只支援一般 PC 版本，還額外支援機上盒(set-top boxes)及數位影音播放裝置(music/video players)，是功能十分完整的數位權利管理技術解決方案。

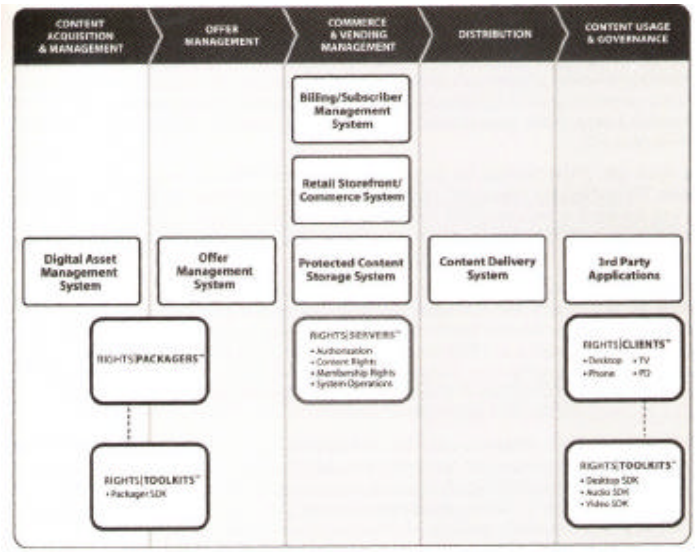


圖 3 (資料來源：InterTrust: http:// http://www.intertrust.com/)

(3) 優碩 TrustView

優碩資訊[25]是國內少數幾家專注於數位權利管理技術的廠商，並為國內第一個擁有 InterLock 技術及專利的公司，在台灣擁有智慧財產局核准之「防止電子文件盜拷之系統及方法」等多項專利。優碩資訊早期為國內電子書交易平台的主要提供者，囊括 95%以上電子書市場，現在並利用原有數位內容數位權利管理核心技術，為機關及企業有效提供文件安全管理之解決方案，有效防堵智慧財產權外洩。其所提出 TrustView 系統（圖 4）可以有效將 Microsoft Office 及 Acrobat PDF 等文件，確實做到文件內容的「加密保護、存取管理、使用權限管理、使用紀錄追蹤」，而在電子郵件、網頁的內容安全管理及多媒體影音的防盜拷部分，優碩資訊也提供了各種相對應的解決方案，茲將其解決方案列表於下：

Product	Description	Status
TrustView for Office	Protect Microsoft Office documents; control read/write, print, copy, save as privileges, provide document effective dates and document usage tracking	Released TrustView for Office v3.0 Enterprise Edition in this October. It has been deployed on several customers including HTC and Foxxcon
TrustView for PDF	Protect Acrobat PDF documents; control read/write, print, copy, save as privileges, provide document effective dates and document usage tracking	Released TrustView for PDF v3.0 Enterprise Edition in this October. It has been deployed on several customers including HTC and Foxxcon
TrustView for Web	Protect web content; control read, print, copy, save as, cache and view source privileges	Release TrustView for Web v2.0 in this September. It has been deployed in AttansIC.

圖 4(資料來源：優碩資訊 http://www.trustview.com.tw)

以下我們將國內外數位權利管理技術相關開發廠商列表(以字母筆劃排序)，並比較其間之異同與特色：

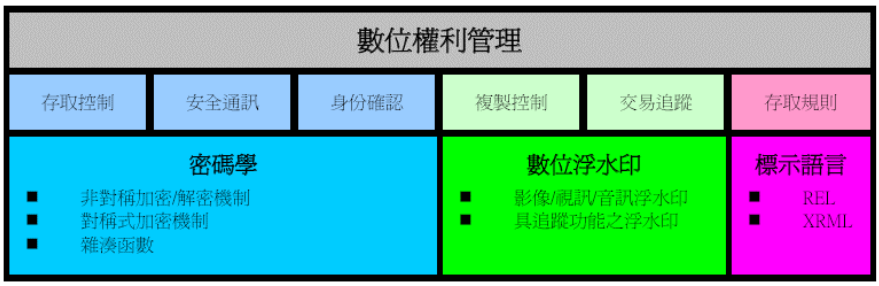
廠商名稱	產品	功能
國外廠商		
Alpha-Tec LTD (www.alphatecltd.com)	數位浮水印系列相關產品	● EIKONAmark 提供? 性數位浮水印的嵌入。 ● Authentication Check 提供數位影像的竄改偵測。 ● AlphaCrawler 網路機器人，負責在網路上收集資訊，並偵測有違法侵權數位內容的網站，以協助使用者進行犯罪追蹤。

Digimarc (www.digimarc.com)	數位浮水印系列相關產品 (該技術為 Corbis 採用)	● Digimarc watermarking 提供? 性數位浮水印的嵌入。 ● Digimarc MarcSpider™ 網路機器人，負責在網路上收集資訊，並偵測有違法侵權數位內容的網站，以協助使用者進行犯罪追蹤。
LTU (www.ltutech.com)	Image Seeker (該技術為 Corbis 採用)	提供以影像內容為基礎的影像比對技術，可以用來找出相似的影像。
PicScout (www.picscout.com)	PicScout	PicScout 提供客戶一個完整的版權保護執行環境，他使用其獨特的網路搜尋引擎，來偵測網路上是否有受其技術保護的違法使用影像，藉以達到數位智財保護。
國內廠商		
永豐紙業 (www.oiprint.com.tw)	數位版權保護家	● 利用 USB Key，讓閱讀時的版權管理型成一可隨身攜帶的載體。 ● 對同一份電子書內容，根據不同之讀者進行個人化的加密。 ● 這將使得不同使用者間，在 USB Key 不借用之條件下，將無法解開其加密內容。 ● 消費者使用特製的 Reader 閱讀，閱讀程式根據《個人私鑰》，將電子書解密後，開啟閱讀。 (註. 節錄自永豐紙業官方網站)
欣領航網路科技 (www.esecure.com.tw)	eGATE 系列產品	提供客戶利用網際網路的科技，在電子商務的領域，不論在任何時間、地點，均能透過尖端網路安全技術的運用，進而達到在電子商務交易過程中，認証性(Authentication)、完整性 (Integrity)、機密性 (Confidentiality)、不可否認性(Non-Repudiation) 的功能，讓商業交易或資訊交換的過程都能安心使用，進而

		創造客戶更大的商機與效益。 (註. 節錄自欣領航網路科技官方網站)
凌網科技 (www.hyweb.com.tw)	版權管理技術解決方案	● 採用之國際標準版權描述語言（XrML） ● 數位物件加解密模組 ● 數位物件保護機制模組 ● 支援版權交易金流服務模組 ● 數位物件批次管理模組 (註. 節錄自凌網科技官方網站)
優碩資訊科技 (www.trustview.com.tw)	TrustServer TrustView	● 採用標準 256-bit 的 AES(Advanced Encryption Standard)加密技術，PKI 認證、X.509 certificates 數位權證。 ● TrustView Client 為 Plugin 形式，可支援 Microsoft Office 與 Adobe PDF。 ● 使用者用合法帳號登入 Server 通過認證並得到作者的同意權限，才能開啟這份文件。 ● 提供事件記錄與查詢，記錄用戶的每一個動作，以方便日後的文件管理及追蹤。 (註. 節錄自優碩資訊科技官方網站)

3. 數位權利管理技術組成元件

一般而言，一個完整的數位權利管理技術架構由密碼學、數位浮水印及權利語言三大技術建構而成[9] (如圖 5)。密碼學技術用來限制數位內容的存取，數位浮水印技術用來嵌入隱藏的版權資訊，權利語言則用來傳遞使用者相對應於數位內容的使用權利範圍。以下章節將就這三大技術進行說明。



數位權利管理架構的必要技術，可依其需求約略區分為密碼學，數位浮水印，利語言等基礎。

圖 5 (資料來源: Communication and Multimedia Lab, CSIE, National Taiwan University)

3.1. 數位浮水印

- 何謂數位浮水印 (Digital Watermark)

將代表原創作者的資料或是一組特別的資訊，嵌入到數位多媒體資訊中，將來若發生版權爭議時，就可以透過此一技術，將嵌入在數位多媒體中的認證資訊取出，作為版權認證的依據。這一種技術就稱之為數位浮水印。當所嵌入之資料或資訊在視覺上是無法察覺的，稱為「隱性浮水印」；如果加入的資料是可察覺的，稱為「顯性浮水印」。一般而言，當提到數位浮水印技術時，絕大部分的情況所指的都是隱性浮水印。數位浮水印在設計上常需考慮下列因素：[12][26]

(1) 透明度 (Transparency)：
浮水印加入影像後，不能影響原始影像在視覺上的品質，此為浮水印的基本要求。

(2) 安全性 (Security)：
所藏入的浮水印必須具有不可偵測的特性。即使知道了浮水印的架構，使用者仍必須擁其對相應之秘鑰 (secrete key) 才可以取出浮水印。

(3) 明確性(Unambiguous)
所藏入之浮水印應該清楚確認版權所有人。

(4) 強健性 (Robustness)：
含有浮水印之影像在經過攻擊後，是否仍能存在於影像之中。

(4) 容量 (Capacity)：

在原始影像中，能加入最多不同的浮水印長度或個數。一個好的浮水印技術必須能使原始影像盡可能容納更多的資訊，但這個條件通常和透明度的要求背道而馳。

(5) 是否需要來源的比對 (Blindness)：
在抽取浮水印時，是否需要原始來源資料或相關資訊。

- 數位浮水印的應用分類

根據不同的需求，數位浮水印可以區分以下不同類別的應用[11]：

(1) Copyright Protection

版權保護是最常見的數位浮水印應用類型。為了辨識所有權，在影像在散佈前事先加入一組可以代表所有權人資訊的數位浮水印到其中，以便將來發生版權上的爭議時，可以用來驗明影像的所有權。

(2) Authentication

數位浮水印也可以拿來當成數位資料真確性驗證及竄改偵測。在此種應用模式中，數位資料會被加入一組強韌性較低的脆弱浮水印(fragile watermark)[27]。在進行數位資料的傳遞時，如果數位資料遭到第三者的截取並進行修改，則隱藏在其中的浮水印將因遭到破壞而無法抽取，也因此數位資料的接受方得以驗證資料之真確性，與查覺是否數位資料已遭到第三者的竄改。

(3) Tracking / Traitor Tracing

為了追蹤數位內容非法使用情況及來源，賣方在釋出數位內容之前可以事先嵌入一組數位指紋（ Fingerprint ）至其中。數位指紋為一個獨一無二的識別碼，就像指紋一樣，當為了追蹤使用者或購買者非法地將產品轉賣或移做其它用途時，則通常會在數位資料交給使用者之前，就在每個釋出的版本中放入數位指紋，以供日後辨別。當日後發覺了非法的散播產品時，就可以取出數位指紋，以查明是誰將數位資料做了非法的用途。

- 小結

由於數位智財議題近幾年來發燒發熱，數位浮水印技術的發展也如火如荼的展開[13]，從以展頻通訊觀念來嵌入浮水印 (Spread Spectrum Watermark)[6][15]， 到

利用向量投影概念的 Quantization Watermarking[1][24]，從抽取浮水印需要原始數位內容資訊到 Blind Detection[29]，浮水印的技術日進千里！

數位浮水印在過去曾被視為數位智財保護的完整解決方案，但在今日各種不同的需求與應用中，單純的數位浮水印技術在數位內容的保護上顯的力有未逮[8]，也被許多專家評論為承擔過高期待的新技術。浮水印技術僅為數位內容安全機制的一部份，具財產權宣示作用，但現有技術強健性不足，不能絕對保障加入浮水印的典藏品不受非法利用。使用單位採行浮水印時，宜同時建立資訊安全及數位產權管理等機制，朝向由數位內容製造的起始端即開始進行保護，包含其間的傳遞、使用存取與行為紀錄，使用者驗證等。強調完整流程的保護，與資訊安全相關技術的整合，以建構起完整的數位智財保護環境。除此之外，浮水印也並非證明智財權擁有者的唯一證據，相關的數位智財法律配套措施更為重要，唯有結合技術與法律層面的保護，才能使數位典藏品得到有效保護。

雖然浮水印並不能解決數位智財的所有問題，但該技術仍可被定義為數位智財的最後一道防線，除此，若能善用其所帶來之嚇阻作用，對智財權的保護將可發揮莫大之效果。

3.2. 密碼學

在數位權利管理技術系統中常以密碼學技術來限制數位內容的存取，並進一步達到複製保護(Copy Protection)。而依照加解密金鑰設計的不同，我們可以把系統區分為對稱與非對稱式加解密系統。若加密金鑰和解密金鑰是相同的，則稱該系統為對稱式加解密系統，此種系統由於執行速度較非對稱式加解密系統快，因此常被用來保護數位物件本身，常見的對稱式加解密系統包含 DES、AES…等演算法；若加密金鑰和解密金鑰並不同 (區分為公鑰及私鑰)，則稱該系統為非對稱式加解密系統，由於該系統所需計算量較大，因此較適合用來保護重要的小量資料，例如用來保護對稱式加解密系統中的金鑰。最著名的非對稱式加解密系統為 RSA 演算法。整體而言，加解密系統與數位浮水印不同之處在於，數位浮水印將 Metadata 與數位物件結合為一，而加解密系統則否(暫時結合)。並且加密後的數位物件需要經由解密或解譯程式才可以讀取，而受數位浮水印保護的數位物件則與原來的使用方式相同(如 圖 6 所示)。一個同時結合數位浮水印與加解密機制的數位權利管理系統範例如 圖 7 所示[22]。

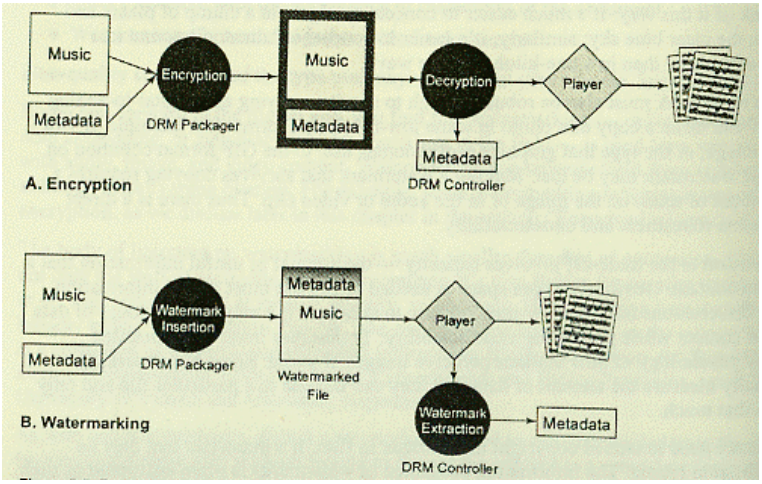


圖 6(資料來源：[22])

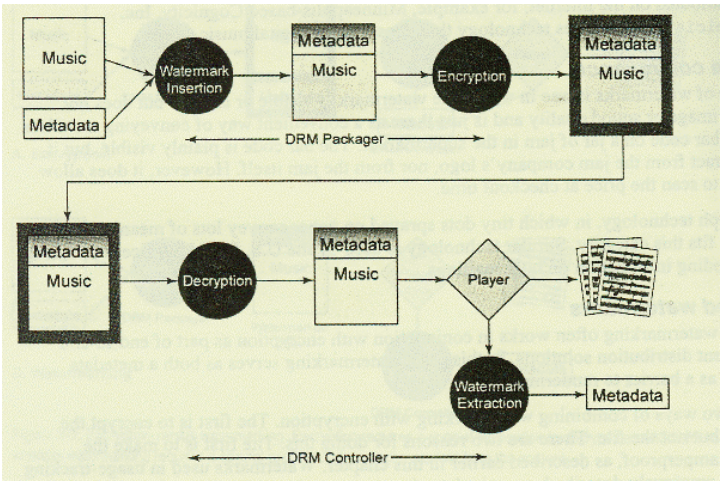


圖 7(資料來源：[22])

3.3. 權利模型與權利描述語言

數位化內容產業包含實體面與權利面，實體面指的是數位內容的部分，包括取得、加值等方面；而權利面即指著作權管理的部分，也是大眾最為關心的，因為它牽涉到數位內容是否有效傳播的關鍵性問題。數位權利管理技術能在數位生命週期內做到「事前防範」的安全管理，其技術不但可以將數位內容加密，並可以設定使用者存取權限(如複製、列印權限、下載次數、到期日設定等)，以及設定追蹤控管使用行為等，讓數位內容在其生命週期內透過數位權利管理機制，並提供較完善的文件存取及使用政策，使得硬體與軟體在最佳狀態下相互結合，進而做到機密資訊內容保密，解決數位內容隨意被洩漏、傳遞、複製、修改，以確

保數位內容受到完整的保護與維護創作人的權利。因此，除了技術面的數位物件保護技術外，權利模型 (Rights Model) 的設計可以說是另一項重點。權利模型包含了權利的種類 (使用者想要對數位內容進行什麼動作)及權利的屬性(允許的次數、允許的時間、授權使用的對象…等)。學者 Mark Stefik [23]曾對權利模型進行了深入的研究，並定義了權利的基本類型(如圖 8)：

(1) 解譯的權利(Render rights)
可以在某個特定的輸出媒介上解譯數位內容的權利，包含有：檢視(View)、列印(Print)、播放(Play)。

(2) 移轉的權利(Transport Rights)
允許移動或複製數位內容的權利，包含有：複製(Copy)、移動(Move)、借出(Loan)

(3) 衍生的權利
允許修改數位內容以取得其衍生物的權利，包含有：擷取部分數位內容(Extract)、修改數位內容(Edit)、擷取部分數位內容並將其用於不同的主題中(Embed)

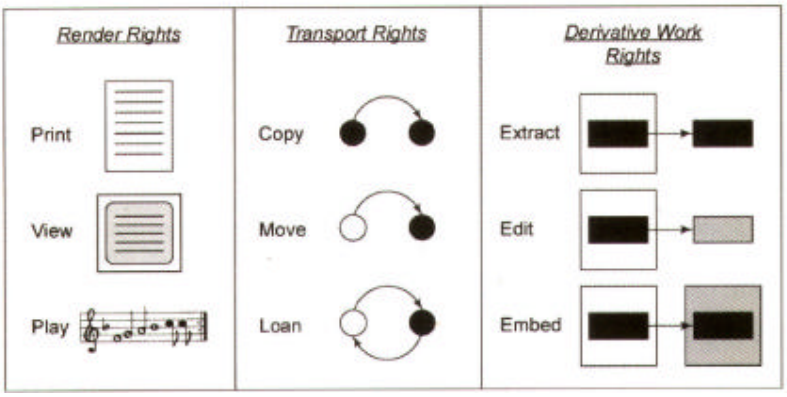
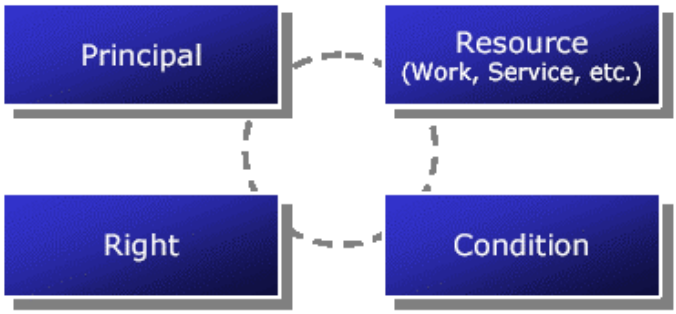


圖 8 (資料來源：[23])

有了權利模型之後，數位物件的存取就可以依照該模型所訂定的規則運作。而權利模型的實作則通常借助權利描述語言 (REL, Rights Expression Language) 工具，目前較常見的權利描述語言包含 XrML 與 ODRL。

由 ContentGuard 所創造的 XrML[2]是一個以 XML 為基礎的權利描述語言 (Rights Expression Language)，目前為 Microsoft 與 MPEG-21 REL 所採用。它希望在數位的世界中，能夠提供一個標準的描述語言，用來描述數位化資料的權限限制，並且也能夠規範在數位世界中的交易行為。

圖 9 顯示了 XrML 所採用的 data model，每一個物件的使用規則由 Principal、Resource、Right 和 Condition 所構成，並由 “grant” 標籤所訂定。Principal 標明了被授權人，Resource 則指定了授權的數位物件；Right 則指定了在某個 Condition 下，所允許開放的行為動作。



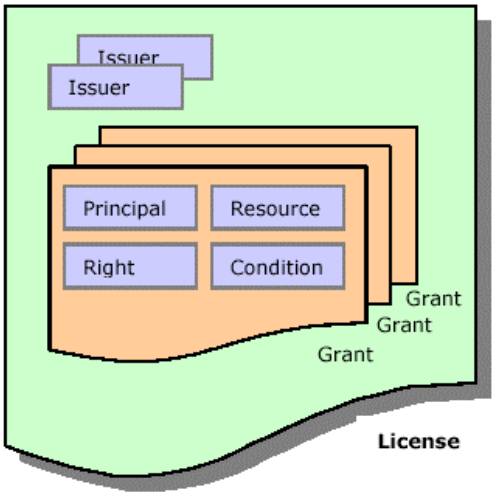


圖 9(資料來源：[2])

一個可能的 XrML 範例文件為：

```
<license>
    <grant>
        <cx: play/>
        <cx: copy/>
        <cx: print/>
        <validityInterval>
            <notAfter> 2004/12/30 </notAfter>
        </validityInterval>
    </grant>
</license>
```

而 ODRL (Open Digital Rights Language) [21]是為了數位權利管理技術所制訂的標準語言，ODRL 傾向於提供有彈性且互通的數位版權宣告，可以應用在電子刊物、數位影像、聲音、電影等各種形式的數位媒體在出版、發行上的應用。與 XrML 不同的是，ODRL 的使用秉持著公開原始碼的精神，所以沒有版權問題。 圖 10 顯示了 ODRL 的整體架構。

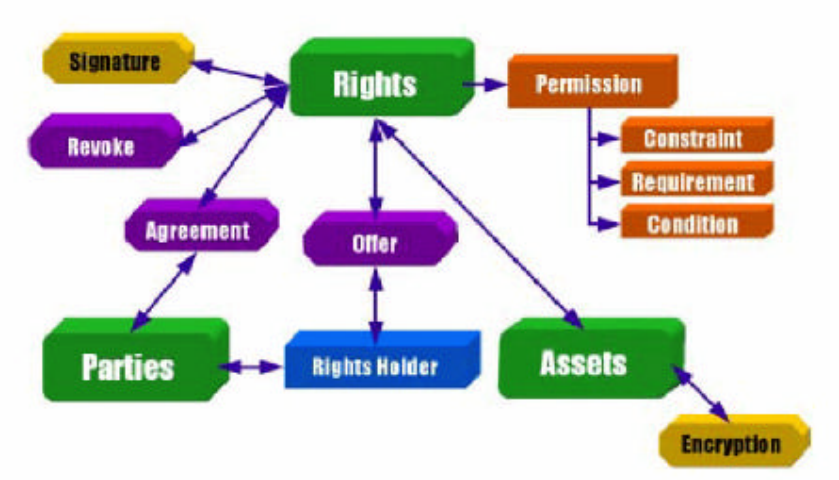


圖 10 (資料來源：[21])

4. 數位權利管理技術相關國際標準

為了讓不同的數位權利管理系統之間可以相容，在國際上也有許多組織提出了數位權利管理技術的標準，只要廠商在實作數位權利管理系統時遵循該標準架構，則不同的數位權利管理系統之間將可以互相溝通！以下我們介紹國際上比較知名的三種數位權利管理技術的標準。

4.1. MPEG-21 Part 4: IPMP

隸屬於 ISO 機構的 MPEG 組織在最新制訂的 MEPG-21 中，也加入了數位內容相關標準[17][18][19]，並強調透通性與交換性，以試圖解決不同的數位權利管理系統之間無法相容的問題。只要遵守 MEPG-21 標準所實作出來的數位

權利管理系統，後此之間將可以互相溝通。

在 MPEG-21 Part 4 中所定義的 IPMP (Intellectual Property Management and Protection) 架構 (如圖 11 [9])，規畫了一個可供不同的數位權利管理系統之間互通的框架。當終端裝置欲存取數位內容時，需使用依照數位內容表頭內所指定的 IPMP Tool，才可以順利讀取；若無法順利取得主要的 IPMP Tool，則根據數位內容表頭依序取得其他或預設的 IPMP Tool。而 MEPG-21 採用了 XrML 權利描述語言，因此，即使是不同的 IPMP 之間仍然可以順利讀取數位內容相關操作權限。

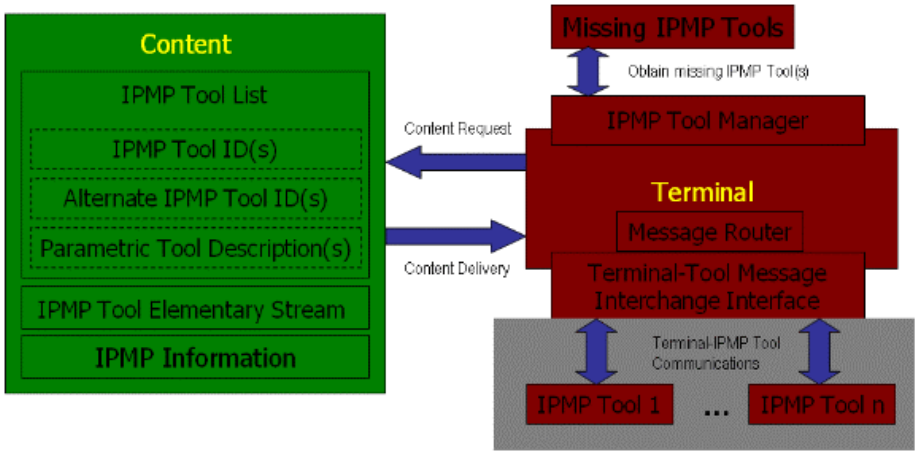


圖 11 (資料來源：[9])

4.2. CPPM / CPRM

CPPM (Content Protection for Prerecorded Media) 與 CPRM (Content Protection for Recordable Media) 是由 4C Entity (IBM, Intel, Matsushita and Mitsubishi) [5]所提出的數位內容保護機制。其中，CPPM 主要是用來保護 已事先錄製好的數位內容 (如: DVD)；而 CPRM 則是針對可以重覆更新的儲存媒介進行保護 (如: SD Memory Cards)。CPPM 和 CPRM 運作的方式相似，主要都是利用密碼學的技術來保護數位內容。數位內容在播放前，必需計算數位內容本身和數位內容播放裝置中所內含的解密資訊，以求得一組解密的金鑰來進行數位內容的解密、播放。若數位內容播放裝置遭到破解，則數位內容擁有者仍可以透過更新數位內容的編碼來防止被破解的機器繼續竊取數位內容。

4.3. DTCP

前面所提到的標準多是在 client 端進行數位內容的保護動作，因此有心人士其實還是可以在傳輸的通道上欄截到解密後的數位內容，如此則數位權利管理保護機制將輕易被破解。因此 5C Entity (Hitachi, Intel, Matsushita, Sony and Toshiba) 也提出了 DTCP (Digital Transmission Content Protection) [6]來保護數位裝置間的傳輸介面 (如: IEEE 1394、USB …等)，讓數位內容由存取、傳輸到播放全程均受到保護。

5. 個案研究

在前面的章節，我們介紹了數位權利管理技術的定義、技術原理及相關技術標準。那麼在現實生活中，是否已經有數位內容機構導入數位權利管理系統，並改善其數位智財保護的例子呢？在本章中，我們從業界與學界各挑選了一個例子，並介紹他們所使用的數位權利管理技術方案，以提供典藏單位參考。

5.1. Corbis

Corbis[3] 為全美最大圖庫授權網站，因此 Corbis 在影像保護機制的做法很值得我們參考。在 Corbis 的網站上，影像可區分為 Thumbnail、Watermarked Web Image 和 Web Image 三種。Thumbnail 為解析度小於 128*128 pixels 的影像縮圖，專為在網路上快速瀏覽而設計；Watermarked Web Image 為解析度小於 640*640 的影像，影像內含顯性 Corbis 版權浮水印，主要提供給未註冊的網站使用者瀏覽用。Web Image 與 Watermarked Web Image 解析度相同，不過移除了浮水印，主要提供給註冊的網站使用者瀏覽觀賞。若使用者想要取得更高解析度的數位作品時，Corbis 的影像授權又可分成二個種類：Rights Managed 和 Royalty-Free。Rights Managed 授權方式會根據你的用途 (如:用於平面廣告、雜誌)、使用區域（如:亞州、美州）、是否為專屬…等等來決定價格，通常需與專人聯絡。Royalty-Free 授權方式則只要依規定付錢，即可取得一次使用權，且使用限制較少。

簡單介紹了 Corbis 的商業模式後，接下來我們來看看他的數位影像保護機制。Corbis 主要利用隱性數位浮水印 (Digimarc digital watermarking) 及網路自動偵察機器(Digimarc MarcSpide) 來作為他們的保護機制。首先在每一個釋出的數位影像中，都會加入一組不可視的數位浮水印，以證明版權。之後會再使用網

路自動偵察機器固定在網路上偵察，並偵測是否有未經授權的非法使用者，一經發現，則立刻採取法律行動。據 Corbis 官方說法，每個月平均起訴 50 件商業侵權案件，而每年從侵權案中所獲取的賠償金超過一百萬美元，成果相當驚人！

由上面的概述不難發覺，Corbis 成功的秘訣在於不止善用科技技術來保護其數位資產，同時也採取了相對應的法律配套措施。這點是相當值得我們學習的！

5.2. Greek Orthodox Archdiocese of America

Greek Orthodox Archdiocese of America (以下簡稱 GOA) [20]是美國著名神學教堂，其內收藏了大量珍貴的神學宗教類的器物，包含肖像、照片、信件及其它珍貴的歷史文物。近年來，GOA 致力於將這些典藏品數位化以利於未來的維護及保存，另一方面也可以推廣這些珍貴的文化遺產，讓更多的使用者可以更容易取得與利用。而在他們數位化的過程中，GOA 面臨許多與數位典藏國家型科技計畫相似的挑戰，包含：

- 如何支援琳瑯滿目的多媒體格式
- 如何在典藏物件中加入使用規則與限制，以保護智財權
- 如何設計有效/易懂的典藏品利用流程，以提升民眾使用意願
- 如何提供一個成功的使用者經驗，以鼓勵民眾接受這種新型態的數位利用方式

為了真正有效的保護數位典藏品的智財權，GOA 也決定整合數位權利管理技術到現有的典藏系統中，以杜? 惡意使用者的不當使用。整合數位權利管理技術後的典藏系統架構如 圖 12 所示，其運作的原理類似前面章節所提到的數位權利管理技術模型運作概念，整個系統的設計上採用 client-server 架構。首先由 GOA 的系統管理者為每一個數位典藏品設定相關的數位權限，並將結果存到 Rights Management Database 中。之後使用者可以向 MediaRights ECS (Enterprise Content Server) 發出數位典藏品的使用請求(假設使用者已經獲得館方認證與註冊)，MediaRights ECS 收到請求後，會向 Rights Management Database 確認使用者對於該數位典藏品的可行使權限，確認後，再向 Web publisher 取得數位典藏品的內容，並交由使用者在允許的範圍下進行利用。

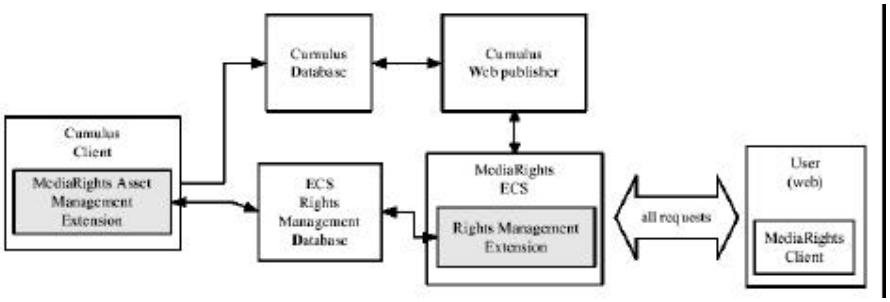


圖 12 (資料來源：[20])

而在數位權利管理技術的權利模型設計上則採用了四個不同的使用權限層級(如圖 13)：

(1) 禁止存取 (No Access)
在此模式下，使用者無法存取及下載數位典藏品，但還是可以在線上透過瀏覽器瀏覽數位典藏品的略圖(thumbnail)。
(2) 只允許線上瀏覽 (View Only)
在此模式下，使用者可以在線上透過瀏覽器瀏覽解析度較低的數位典藏品(大小約為原來的 25%-50%)，但無法下載數位典藏品至使用者的儲存設備中。
(3) 允許線上瀏覽及下載受保護的數位典藏品 (View & Restricted Download)
在此模式下，使用者可以在線上透過瀏覽器瀏覽解析度較低的數位典藏品(大小約為原來的 25%-50%)，也允許下載經過受到保護的數位典藏品至使用者的儲存設備中。受到保護的數位典藏品意指經過加密保護，只能夠在 GOA 所開發的閱覽軟體(MediaRight Client)上使用，而且數位典藏品中加入了時間鎖(time-lock)，使用者只能在某一段期間內得以利用下載的數位典藏品，當時間經過後，則該數位典藏品將自動失效。
(4) 允許對數位典藏品的完整權限 (View & Unrestricted Download)
可以完整瀏覽及下載數位典藏品，通常只開放給系統管理員。

Access Level	View Ability	Download Ability
No Access	not allowed	not allowed
View Only	protected file	not allowed
View & Restricted Download	protected file	time-locked file
View & Unrestricted Download	clearview file	clearview file

圖 13

比較值的討論的是，GOA 所開發的客戶端閱覽軟體：MediaRight Client，使用者必須先下載安裝，然後才能開啟某些數位典藏品的檔案，如此一來，可能會造成使者使用上的不便，甚至造成抗拒而遠離 GOA 網站。這也是數位權利管理

系統有時候較為人所垢病的地方，因過度的保護而造成使用上的不便。在這一方面 GOA 所採取的策略為：並非一定要安裝客戶端的應用程式才可以看到數位典藏品的內容，當客戶端沒有安裝 MediaRight Client 時，仍然可以透過瀏覽器看到數位典藏品的略圖或其較低解析度的版本。但若使用者想要更進一步的瀏覽完整版本的數位典藏品，在享受服務的同時，也需要付出相同的責任義務：安裝客戶端的閱覽軟體！

雖然 GOA 採用的數位權利管理系統並不一定完全符合典藏單位的需求，不過其導入經驗及系統設計架構均是值得我們借鏡及參考的。

6. 數位權利管理技術示範網站

為了讓典藏單位可以以更實務的角度了解數位權利管理技術導入流程，在本節中將以多媒體中心 (Multimedia Center, 簡稱 MMC) 為例，示範如何導入數位權利管理技術進入其中。

多媒體中心的設計概念源起於「數位典藏國家型科技計劃」，其建置目的在於集中所有合作典藏單位的多媒體檔案，以專業的技術和集中且高效能的硬體設備和巨大容量的儲存媒體，提供最有效率的檔案管理機制和多樣化的多媒體處理功能，同時減少各單位因專業技術的欠缺所帶來的多媒體檔案管理之困擾以及高階硬體設備和儲存設備的重複購置造成資源上的浪費。

而多媒體中心中儲存了相當大量且具價值的數位影像，在本節中，將會從最基礎的系統分析設計開始，一步一步將數位權利管理技術元件整合導入多媒體中心內，讓這些數位影像在釋出的同時，仍然可以在數位智財所有人所允許的使用範圍下進行利用。

6.1. 數位智財保護標的

在多媒體中心中，我們主要要保護的數位智財是數位影像，我們將這些數位影像分成以下三種種類 ：

- 低解析度影像：即多媒體中心網站上的 Thumbnail (縮圖)，影像解析度通常為 50*50 pixels 以下。
- 中解析度影像：影像解析度為 500 * 500 pixels 以下之影像檔，用來提供給使用者進行較高解析度的網路瀏覽。

- 高解析度影像：影像解析度為 1024*1024 pixels 以上之高解析度影像檔，在多媒體中心中以 djvu 檔案格式存放。因附加價值高，所以是本示範網站中最主要的保護對象。

6.2. 角色分類

本示範網站假設有以下四種不同的角色會對本系統進行利用，其需求異同如下：

角色名稱	角色描述	角色需求
Content Provider	數位內容的擁有與提供者	能夠有效的管理所擁有之數位內容，並能管控釋出後的數位內容，以保護數位智財權。
Users	一般使用者	可以在網路上瀏覽、使用低解析度之數位內容 。
Advanced User / Researcher	進階使用者 / 研究人員	可以在網路上瀏覽、使用高解析度之數位內容。
System Developer	典藏系統的開發、維護人員	除了提供可正常運行的典藏系統外，還需進一步保護數位內容安全性。因此一套易於整合的數位權利管理技術是其最重要的需求。

6.3. 系統設計

在本小節中，將針對各個不同的角色進行分析，並描述示範網站如何根據不同角色設計其客製化操作流程及環境，以符合各使用者之需求。

- Content Provider

對於 Content Provider 而言，最重要的事包含：

(1) 有一套方便的數位內容管理工具，使他們可以很輕鬆的與典藏系統溝通。包

含：可以清楚掌控所有數位內容、支援數位內容權限設定...等。

(2) 典藏系統可以有效的保護他們釋出的數位內容。

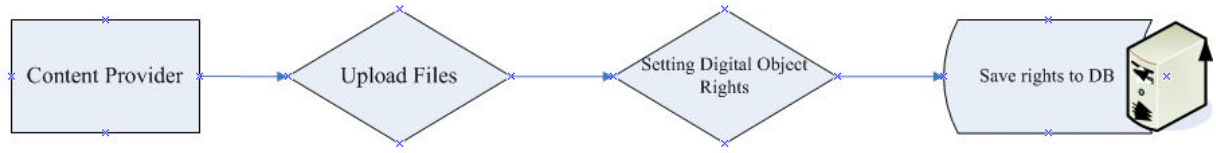


圖 14

圖 14 為本系統為 Content Provider 所設計的數位內容管理流程。Content Provider 可以透過 MMC 或 FTP 軟體上傳 Digital Content，之後再利用 MMC 的視覺化操作環境管理其所上載的 Digital Content，並針對不同的使用者與群組設定數位物件權限，包含：

Rights	Description
Play / View	播放/觀看物數位內容的權利
Print	列印數位內容的權利
Download / Save	儲存數位內容的權利
Valid Date	數位內容被下載後的有效使用期限 當超出 valid date 後，數位內容將無法被存取
Viewable Times	數位內容被下載後的有效使用次數 當超出有效使用次數後，數位內容將無法被存取
Compliant Player	允許取存數位內容的播放器條件限制 (如：只允許在特定的某個 IP Address 上使用)

- System Developer

對典藏系統的開發、維護人員而言，如何在不改變原來的典藏系統架構下的前提下，導入數位權利管理保護機制，是一項極具挑戰性的工作。本架構所提出的 數位權利管理系統，可以讓系統開發人員在不更改原先系統模組的狀況下，進行系統軟體升級。如圖 15 所示，整個典藏系統只需新增一個 DC Packager 模組，讓數位內容在輸出前重新編碼 (加入數位物件權限資訊、數位浮水印) 與加密，因此可以將系統開發人員的負荷減至最低。

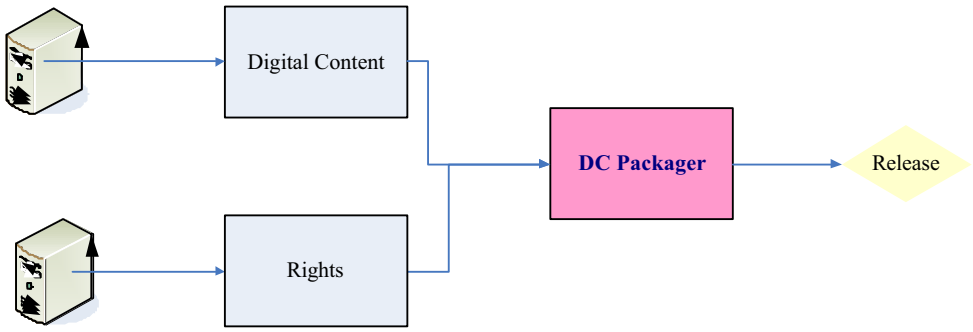


圖 15

- User

在本文中，定義一般使用者為對數位內容品質的需求度較低，通常在 500*500 pixels 以下之數位影像就可以滿足其瀏覽需求。在本架構中，使用者只需要透過 MMC 具親和力的操作介面，在通過基本認證後(username & password)，就可以線上觀賞數位內容(該數位內容具浮水印保護)。整個流程如圖 16 所示

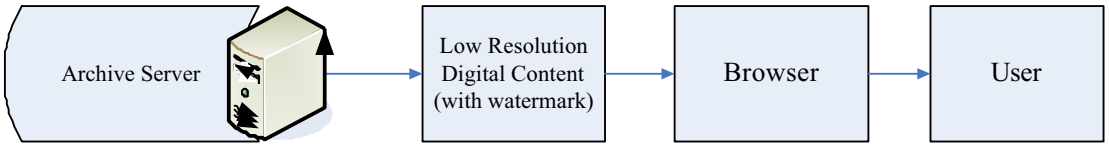


圖 16

- Advanced User / Researcher

(1) 進階使用者 / 研究人員對數位內容的品質有較高的需求，因此提供可以在網路上瀏覽的高解析度影像是基本需求。本架構中，進階使用者的流瀏覽過程和一般使用者相似，但需要事先安裝 Djvu Player、.Net Framework、OpenDreams client side tools，之後就可以透過 MMC 線上存取數位內容，以進行研究。完整的流程如圖 17 所示。

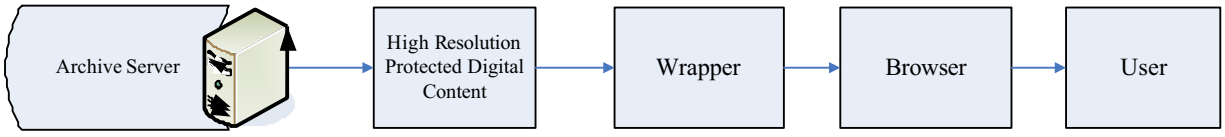


圖 17

6.4. 系統流程

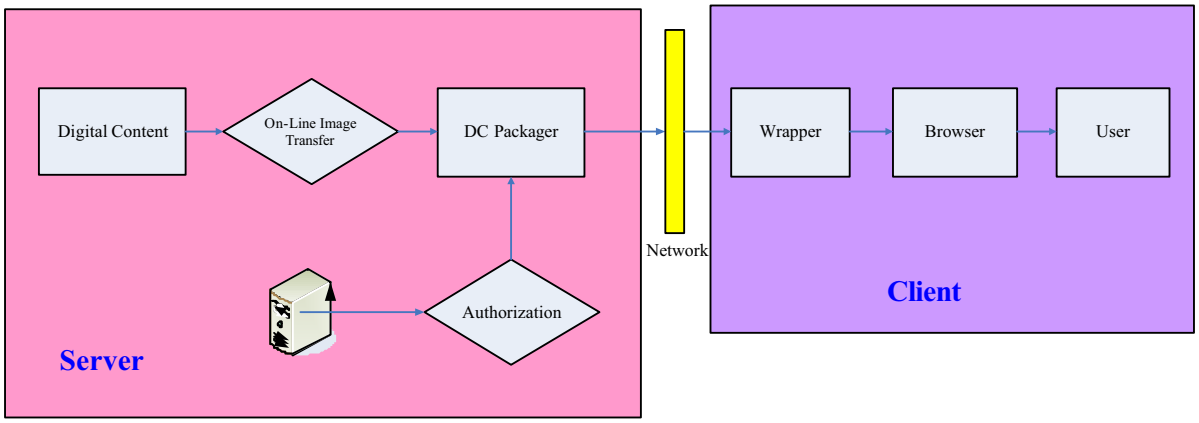


圖 18

圖 18 為 MMC 整合 OpenDream 後的運作流程，功能說明如下：

- Server Side：數位內容封包流程

(1) On-Line ImageTransfer: 當使用者提出數位內容使用需求後，MMC 會線上產生一組原始 djvu 影像檔，並交由 Proxy 進行封包
(2) DC Packager 在取得原始 djvu 影像檔及相關之授權資訊後，會將兩者結成一個新的檔案 (授權資訊寫入 header 中，並嵌入浮水印)，之後並將此物件加密，如此即完成數位內容的封包流程。加密後的數位內容我們稱之為 protected djvu 影像。
(3) Protected djvu 影像開始經由網路釋出給使用者。

- Client Side：播放數位內容流程

(2) 使用者在使用數位內容前，並需確定該系統安裝有 Djvu Player、.Net Framework、OpenDreams client side tools
(3) 使用者透過 browser 送出 digital content 使用需求後 (此時 user 已經通過 user name 與 password 的身份認證)，browser 會再向 wrapper 送出 digital

content 使用需求

(4) wrapper 將被保護的數位內容解密之後，再根據表頭內的權限設定，讓 browser 只能對該解密後的 djvu 影像檔進行權限允許範圍的利用

6.5. 小結

在示範網站中，我們整合了數位權利管理技術的三大元件：數位浮水印、密碼學及權利管理語言，以對多媒體中心內的數位影像進行保護。並提供相對應的管理介面，以方便數位智財擁有者設定並管理其珍貴的數位內容。本示範網站的實作當然只是數位權利管理技術的其中一種可能的實現，但其背後所含的概念 (利用數位權利管理技術來保護數位智財) 才是我們意欲呈現的部分，同時也提供典藏單位一個可能的實作架構參考。

7. 結論

『數位典藏國家型科技計畫』的意義不僅只侷限於狹義的將資料數位化，也更進一步扮演推廣與教育的角色，透過有系統的規劃與處理，將資訊呈現給大眾。期盼以更快速、便利的機制來吸引更多的民眾，使民眾了解中華文化之博大精深。但在資料數位化或資訊傳播的過程中，卻也延伸出許多的問題，例如智慧財產權的保護、數位典藏品在網路上傳遞可能遭到竊取與典藏資料庫的非法存取...等等問題，種種的攻擊方式都需要依賴於健全的安全機制來加以預防與偵測。

對於數位典藏計畫中的典藏單位而言，是否能夠有效確保數位典藏品的智財權將是數位內容能否釋出最重要的考量。傳統以數位浮水印為基礎而架構起的數位智財保護系統是消極且不周全的！在網路與駭客同樣發達的今天，或許我們可以說，數位浮水印是一種『防君子不防小人』的技術！倘若要求數位浮水印對於目前成千上百種影像攻擊方式都具有強韌性是過於苛求的！關於這個事實我們也不難在 2004 年數位典藏計畫技術分項所舉辦的『浮水印評比競賽』中得到佐證[8]，參賽隊伍的浮水印演算法通常只會對某些攻擊項目具高存活率，而非如我們所想像中般可以抵禦所有的攻擊。數位浮水印的最大作用或許是在於它的嚇阻作用，而非先前我們所期待的樣子：『無論流通在外的數位內容遭遇到何種攻擊或修改，只要發生版權爭議時，我們一定可以將嵌入在數位多媒體中的認證資訊取出，作為版權認證的依據。』那麼為什麼說它只『防君子』呢？因為有動機竊取數位內容的使用者並無法確定數位內容中的浮水印是否已經因為遭受攻擊而被移除(數位浮水印假設使用者並無法得到偵測浮水印是否存在的核心程式)，因此與其冒險違法使用數位智財，還不如安份守己些的好。當然這個論點

對於具有高超技術能力的駭客可能是不成立的，駭客可能可以攻破整個數位浮水印的設計架構，甚至在把原始浮水印移除後，反向加入代表自己的浮水印，如此一來豬羊變色，駭客反客為主，也因此我們說數位浮水印『不防小人』。如果我們從另一個角度來思考，事實上，當等到數位智財發生版權爭議時才來進行補救，這個想法本身對於智財權的保護就已經顯的消極了。人們說：『積極的預防勝過事後的補救！』這句話在數位智財的保護將同樣是最高指導原則。如果我們在數位智財的製作、生產、分佈與流通的過程中，每一個環節都曾留心注意，不予有心人士可趁之機，並佐以法律作為配套保護措施，那麼數位智財才能真正稱為所謂的得到保護！

8. 參考文獻

[1] Chen, B.; Wornell, G.W.; "Quantization index modulation: a class of provably good methods for digital watermarking and information embedding", Information Theory, IEEE Transactions on , Volume: 47 , Issue: 4 , May 2001, Pages:1423 – 1443

[2] ContentGuard, eXtensible Rights Markup Language (XrML) 2.0 Specification, available at http://www.xrml.org/, 2002

[3] Corbis, http://www.corbis.com

[4] Cox, I. J. ,"Secure Spread Spectrum Watermarking for Multimedia," IEEE Trans. IP, vol 6, no.12, pp. 1673-1687, Dec. 1997.

[5] CPPM/CPRM Specification, 4C Entity (IBM, Intel, Matsushita, Mitsubishi), http://www.4centity.com

[6] DTCP Specification, 5C Entity (Hitachi, Intel, Matsushita, Sony and Toshiba), http://www.dtcp.com

[7] Duhl, Joshua; Kevorkian, Susan, "Understanding DRM Systems", An IDC Research White Paper, 2001

[8] Hsiao, Jen-Hao, "2004 Digital Watermark Competition: The Technical Report", Technical Report, IIS Academia Sinica, 2004 April.

[9] Huang, Chun Hsiang; Wu, Ja-Ling, "Information Technologies for Digital Rights Managements: A Survey", Communication and Multimedia Laboratory, Department of Computer Science and Information Engineering, National Taiwan University, Taipei, Taiwan, R. O. C. June, 2004

[10] InterTrust, http://www.intertrust.com/

[11] Katzenbeisser, Stefan; Petitcolas, Fabien A.P., Information hiding techniques for steganography and digital watermarking, Boston : Artech House, 2000

[12] Kutter, M.; Petitcolas, F. A. P. , "A fair benchmark for image watermarking systems", Electronic Imaging '99. Security and Watermarking of Multimedia Contents, vol. 3657, Sans Jose, CA, USA, 25~27 January 1999. The International Society for Optical Engineering.

[13] Lee, Sin-Joo; Jung, Sung-Hwan, "A survey of watermarking techniques applied to multimedia", Industrial Electronics, 2001. Proceedings. ISIE 2001. IEEE International Symposium on , Volume: 1 , 12-16 June 2001, Pages:272 - 277 vol.1

[14] Liu, Qiong; Reihaneh, Safavi-Naini; Sheppard, Nicholas Paul, "Digital rights management for content distribution", Proceedings of the Australasian information security workshop conference on ACSW frontiers 2003 - Volume 2

[15] Lu, Chun-Shien; Huang, Shih-Kun; Chwen-Jye Sze; Hong-Yuan Mark Liao; " Cocktail watermarking for digital image protection", Multimedia, IEEE Transactions, Volume: 2 , Issue: 4 , Dec. 2000, Pages:209 – 224

[16] Memon, N.; Wong, Ping Wah, "A buyer-seller watermarking protocol", Image Processing, IEEE Transactions , Volume: 10 , Issue: 4 , April 2001, Pages:643 – 649

[17] MPEG, ISO/IEC21000-4, MPEG-21 , Part 4: IPMP (Intellectual Property Management and Protection), 2004

[18] MPEG, ISO/IEC21000-4, MPEG-21 Part 5: REL (Rights Expression Language), 2004

[19] MPEG, ISO/IEC21000-4, MPEG-21 Part 6: RDD (Rights Data Dictionary), 2004

[20] Nicolakis, Theo; Pizano, Carlos E.; Prumo, Bianca; Webb, Mitchell, "Protecting Digital Archives at the Greek Orthodox Archdiocese of America", Proceedings of the 2003 ACM workshop on Digital rights management, October 2003

[21] ODRL Initiative, Open Digital Rights Language Version 1.1 (Released 8 August 2002), available at http://odrl.net/

[22] Rosenblatt, William; William Trippe; Stephen Mooney, Digital Rights Management: Business and Technology, M&T Books.

[23] Stefik , Mark, "Letting Loose the Light", Xerox PARC research labs

[24] Swanson, M.D.; Zhu, Bin; Tewfik, A.H., "Data hiding for video-in-video", Image Processing, 1997. Proceedings., International Conference on , Volume: 2 , 26-29 Oct. 1997, Pages:676 - 679 vol.2

[25] Trustview, http://www.trustview.com.tw/

[26] Voloshynovskiy, S.; Pereira, S.; Pun, T.; Eggers, J.J.; Su, J.K.; "Attacks on digital watermarks: classification, estimation based attacks, and benchmarks", Communications Magazine, IEEE , Volume: 39 , Issue: 8 , Aug. 2001, Pages:118 – 126

[27] Windows Rights Management Services, http://www.microsoft.com/

[28] Wu, Min; Liu, Bede, "Watermarking for image authentication", Image Processing, 1998. ICIP 98. Proceedings. 1998 International Conference, Volume: 2 , 4-7 Oct. 1998 , Pages:437 - 441 vol.2

[29] Zeng, Wenjun; Liu, B.; "A statistical watermark detection technique without using original images for resolving rightful ownerships of digital images", Image Processing, IEEE Transactions on , Volume: 8 , Issue: 11 , Nov. 1999, Pages:1534 – 1548