數位版權管理機制實作 - 以數位典藏管理系統為例

陳心渝 李政宏 邱一航 林韋伶
中央研究院 資訊科學研究所
{kwakwai8, chli, yhchiu, winnilin}@iis.sinica.edu.tw

摘要

在現今提倡智慧版權的時代，對公開發行或轉述取用的文或圖都格外注意來源。對數位典藏計畫來說，隨著各類數位典藏系統的持續開發及使用，數位典藏系統對大量圖片有高度的保存需求，需要使用數位版權管理機制將龐大的珍貴圖片等資訊來做完整版權保護及宣告，本研究的主要目的在說明數位版權機制在整個數位典藏系統環境下扮演重要的角色、以及數位版權管理機制的功能與架構，在搭配數位典藏系統的時候，是如何整合應用。

關鍵字

數位版權管理、DRM

1. 前言

由於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，透過網際網路無遠弗屆的便利性，使得所有數位資料得以快速方便的複製與傳遞，大量的文字，繪畫與傳統媒體等均轉換成數位檔案作儲存。

『數位典藏國家型科技計畫』[1]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，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。經由檔案形式存在，可讓各類影音、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，但這樣也可以輕易地從網路上獲得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，同時又能兼顧著作權人之權益，成為一門相當重要的課題。

數位版權管理 (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，主要提出下列三項保護方向：

(1) 避免數位智財未經授權的複製濫用
(2) 有效的數位智財控管
(3) 侵權行為的偵測與追蹤

為因應前述之問題，本研究已實做出一數位典藏系統運用數位版權機制，建置一套整合數位權利管理技術之示範網站。其建置目的在於實際運用以探討過之數位版權機制，有效保護及預防數位內容，以供典藏單位做為技術導入之參考。

本篇論文將於第二節介紹數位版權管理技術的相關技術。第三節詳述數位版權管理技術的架構與運作流程。在第四節將舉出已結合數位版權管理技術的系統應用實例。第五節則提出數位版權管理技術未來可以應用及加強的地方。

2. 相關文獻探討

2.1 數位版權管理技術概觀

2.1.1定義

數位版權管理技術 (Digital Rights Management，簡稱 DRM)，國際數據資訊中心 IDC(Internet Data Center)為數位版權管理技術下定義為[6]：結合硬體與軟體的存取機制，將數位內容設定存取權限，並與儲存媒體連結，使得數位內容在其生命週期內，從產生到消失，都受到保護。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，則稱為數位版權管理技術。

2.1.2 技術架構

數位版權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[2]：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)。 圖一描繪出了一個典型的數位版權管理技術模型概念，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)：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。

(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。

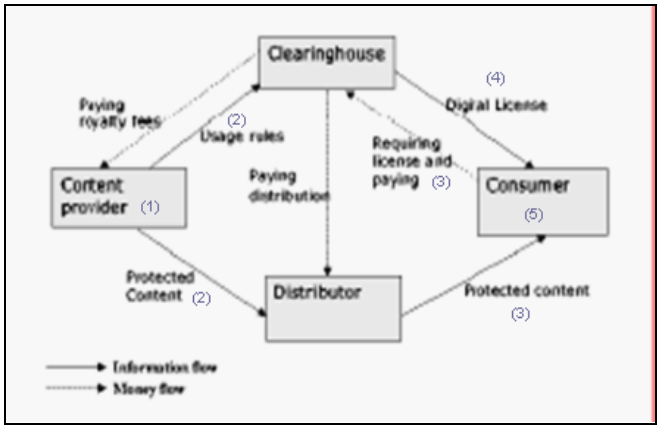

圖1 數位版權管理技術運作圖

模型的運作流程如下：

(1) 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。

(2) 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。

(3) 消費者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，或進行數位版權之購買。

(4) 『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版權。

(5) 最後消費者則可以依據此數位版權所允許執行之項目，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。

2.1.3 商業數位版權管理系統

從功能面來看，商業數位版權管理系統，可大致劃分成兩類：

(1) 多媒體文件的保護

(2) 機密文件的保護

由於目前各典藏單位對於數位版權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版權管理技術開發廠商進行現狀評估，以了解目前市場上數位版權管理技術發展情形。

2.1.3.1 Microsoft Windows 版權管理服務

微軟近年來在數位版權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。微軟在 2003 年推出了新一代的數位文件保護技術： Windows® 版權管理服務 (Rights Management Services，RMS) [3] 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。

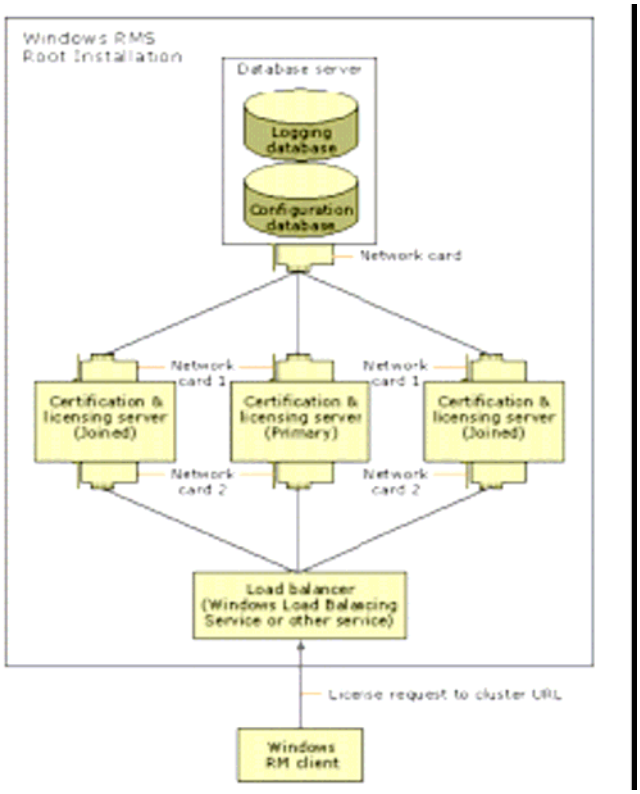

圖 2 Rights Management Services，RMS)架構[3]
(資料來源：Microsoft: http://www.microsoft.com/)

2.1.3.2. InterTrust Rights|System

InterTrust [4] 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版權管理技術，其開發的 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版權管理技術解決方案。

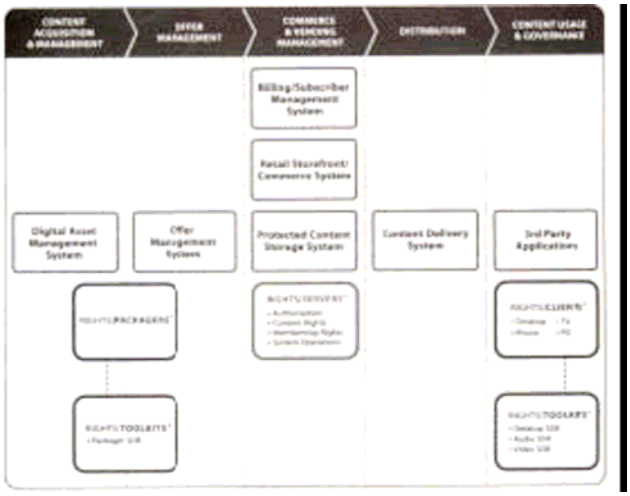

圖 3 (資料來源：InterTrust: http://www.intertrust.com/)

2.2 數位版權管理技術組成元件

一般而言，一個完整的數位版權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[5](如圖 4)。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。

圖 4 數位版權技術概圖
(資料來源: Communication and Multimedia Lab, CSIE, National Taiwan University)

2.2.1 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。依照浮水印的可見度，主要分為兩種：

(1) 隱性浮水印：所嵌入之資料或資訊在視覺上是無法察覺的。
(2) 顯性浮水印：嵌入的資料是可察覺的。

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。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[6]：

(1) Copyright Protection：版權保護是最常見的數位浮水印應用類型。為了辨別所有權，影像在散佈前會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驗證數位資料真確性及竄改偵測。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)[7]。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會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，以查覺是否數位資料已遭到第三者的竄改。
(3) Tracking / Traitor Tracing：賣方在釋出數位內容之前可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，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，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。萬一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。

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[8]，從以展頻通訊觀念來嵌入浮水印(Spread Spectrum Watermark)[9][10]，到利用向量投影概念的 Quantization Watermarking[11][12]，從抽取浮水印需要原始數位內容資訊到 Blind Detection[13]。

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得力有未逮[14]，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版權管理等機制，由數位內容製造的起始端開始進行保護，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，除此之外，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。

2.3 重複影像偵測技術 (copy detection or near-duplicate image detection)

在數位影像智財保護，近年來被廣泛的討論，對於海盜行為的複製數位影像，必須有效的偵測與追蹤。目前在保護數位影像智財的主要的技術有浮水印技術及以數位影像內容為基礎的重複影像偵測技術。浮水印技術是指在數位影像散佈之前，對於所有數位影像增加額外的資訊，使日後能有效的擷取出資訊，來證明數位影像所有權。另外以數位影像內容為基礎的重複影像偵測技術，則是不用增加額外的資訊，直接針對影像本身的獨特內容資訊，作為特徵值，來辨識出近似的影像。例如此方法可適用於影像所有人，利用 Spider 等影像搜尋引擎，在網際網路上，週期性的收集影像，針對所搜尋到的每個影像利用演算法取出的特徵值，並在資料庫紀錄每個影像的特徵值以及所抓取的 URLs，再與原始影像的特徵值，以幾何距離或統計等方式做判斷近似程度，假如近似的話，以 URLs 列出懷疑名單，而影像所有人可再依照名單或浮水印等其他認證技術，來判斷此影像是否合法。

不過不論是浮水印技術或是以數位影像內容為基礎的重複影像偵測技術，當在第三方對於原始影像做修改，例如對原影像檔案格式的轉換、或是做影像幾何的改變、如鏡射、裁減、調整大小、旋轉等其他修改，都會造成上述重複影像偵測的技術，受到影響，造成辨識率下降，而難以辨識出為相似重複的影像。所以目前的研究，就是針對這些影像的改變，做出應對的方法加以克服。其中在以數位影像內容為基礎的重複影像偵測技術中，擷取出特徵值的方法有下列幾種：[15]

2.3.1 以顏色為特徵

在影像處理上，每個像素顏色常以 RGB 模式或 YCbCr 模式表示各種顏色。而將顏色以 RGB 模式或 YCbCr 模式量化後，就可依量化值做為影像比對的方法。常見的有 Color histogram、Color layout by Euclidean metric or statistical analysis。不過此方法，並沒有記錄顏色的位置，或是在強烈顏色變換表現不好，而且當顏色相近但非重複的影像中，可能會判別一樣。所以此方法在重複影像偵測上表現不是很好。

2.3.2 以形狀為特徵

表示形狀方式為藉由影像處理方式來粹取其特徵點。特徵點不僅能夠描繪形狀整體形式，就像面積、外形、主要軸線定位等，而且也能表示形狀邊界區域元素，像形狀尖角、邊的獨特點等，因此，在這種方法上是考慮找出形狀特徵空間上有效點。進而找出兩形狀間相似程度，可以經由數學距離公式計算出形狀上兩點間差距或是以機率統計方式算出近似程度[16]。在此方法，當影像作旋轉，鏡射時能有效偵測，不過在當物體有類似形狀，可能會造成判別成一樣。且在計算的時間上通常會較長。

2.3.3 以內容為特徵

以影像內容，綜合顏色與形狀相對位置，為組成元素做為搜尋特徵資料庫，是以影像中各式組成物比例來判定影像相似度，若有兩張影像具有相似比例組成，意味著這兩張影像相似。其中擷取特徵值的方式又可分為以 Wavelets 計算，例如以 DWT[17]、DCT[18]，來計算出特徵值。不過使用此 Wavelets 的演算法方面，是針對每個影像計算，是存放整體影像的統計資料，在單純對影像調整大小、改變色系或是改變格式下有很好的效果，不過在當影像被裁減、或除了小幅旋轉時，常會被視為不相符。所以除了以 Wavelets 外，還會加強使用 Local descriptor 演算法，例如 Harris detector[19]、Lowe's Difference of Gaussian (DoG) detector[20]等，來粹取 interest point，來加強辨識影像中物件，而此方法辨識效果良好，不過對於時間上的運算也較為長。

3. 數位版權管理架構

為了保護數位智慧財產並避免數位盜版，一個有效預防未授權存取的機制是必要的。因此，DRM 的機制就是用來保護這類高價值的數位資產，並監控其分散使用與管理，其 DRM 的核心概念就是在有數位許可的權利下使用數位物件，此一許可為一數位資料，其資料內容包括使用數位內容的某些特定使用規則。這些特定的使用規則可以包括一些標準的範圍，例如可讀取次數、瀏覽權利、列印權利、儲存權利…等。透過數位許可，在使用者使用數位內容的同時，內容提供者可以掌握更多的控制權。

不同的商業模式在 DRM 的執行方式上是不同的，其所制定使用內容的規則也是不同的，但是基本的 DRM 流程卻是相同的，根據典型的 DRM 模型，一般來說該架構包括下列四個實體：內容提供者(Content

Provider)、內容傳播者(Distributor)、權限控管中心(Clearinghouse)與消費者(Consumer/User)。

其中內容提供者會將權限控管中心所提供之控管格式，編入數位內容內，不同的商業模式下，所提供的控管格式亦不相同，而這些數位內容將被加密或包裝，目前多數影像相關之數位內容提供者，大多採用浮水印技術來對內容編碼，以做為辨識該內容之使用權。接下來，這些受到保護的數位內容，便可傳送到內容傳播者所提供之環境進行傳播，例如：網頁伺服器或串流伺服器，而擁有權限之消費者便可透過權限控管中心，取得數位內容的許可，進而對數位內容進行權限內的合法使用。此外，在商業角度來運作，消費者必需在電子商務的交易平台下進行付款機制後，使用權限的認證才會傳遞至消費者。

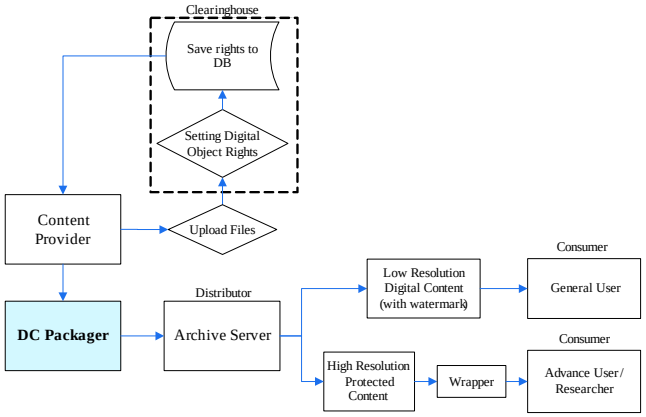

圖 5 數位版權技術架構圖

在本文中也是以典型的數位版權管理架構為基礎，實作數位版權管理系統，圖為本文所建立之數位版權系統架構，也是一個基礎架構，在這個架構之下提供一套結合數位物件保護技術與數位版權管理，並達到對數位內容保護的解決方案。

表 1 使用者與群組設定內容表

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)

在系統設計上，本文將針對不同的實體進行分析，並描述在此一架構上不同實體的操作流程與環境。對於內容提供者而言，需要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，例如：可以清楚掌控所有數位內容、支援數位內容權限設定…等，另外，此一工具也必需能夠有效的保護他們釋出的數位內容。因此圖內的內容提供者，可以透過多媒體中心提供的視覺化操作環境，並透過 web FTP 上傳數位內容，並針對不同的使用者與群組設定數位內容權限，其權限如表 1 所示。

對於系統傳播者而言，如何在不改變原有之系統架構下，導入數位版權管理機制是極具挑戰性的工作。在本文之數位版權管理架構下的典藏系統，僅需增加一個 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，因此可以讓系統傳播者的負荷減至最低。

在此一架構下為因應不同需求之消費者的使用，本文針對數位內容品質的需求度較低，通常能滿足在 500*500 pixels 以下之數位影像瀏覽需求者，定義為一般使用者，一般使用者可以透過具簡易操作介面之多媒體中心，通過基本認證（帳號、密碼）後，便可以透過線上觀賞數位內容（具浮水印保護）。另一類對數位內容的品質有較高的需求，本架構中定義為進階使用者/研究者，其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 等相關軟體，便可透過多媒體中心線上存取數位內容，以進行研究。

在系統流程上，本文之數位版權管理架構整合 OpenDream，其伺服器端將數位內容封包流程如下：

(1) On-Line ImageTransfer: 當使用者提出數位內容使用需求後，多媒體中心在線上產生一組原始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（授權資訊寫入檔案表頭中，並嵌入浮水印），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 影像透過網路釋出給使用者。

其客戶端將數位內容傳播流程如下：

(1) 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。
(2) 使用者透過瀏覽器送出數位內容使用需求後（此時使用者已經通過帳號/密碼的身份認證），瀏覽器便向封裝器（Wrapper）送出數位內容使用需求。

封裝器將被保護的數位內容解密之後，再根據表頭內的權限設定，讓瀏覽器只能對該解密後的 djvu 影像檔進行權限允許範圍的使用。

4. 數位版權管理技術-以數位典藏系統為例

4.1 應用實例

針對上述對 DRM 的相關架構及保護機制，我們以數位典藏管理系統來呈現 DRM 機制對於圖片上的應用實例。

(1) 圖片存取

在數位典藏管理系統上欲觀看一張圖片時，操作方式通常是點閱圖片，再針對點閱的圖展開出現更大張的圖。圖片的存取保護，若以呈現長寬為 100pixel 的小圖而言，只是一種索引的概念，並不是主要的保護重點，但是若出現的圖是長寬 500pixel 甚至更大，就是圖片 DRM 機制中重要的一環；所以可否執行「點閱觀看」的這個動作，對圖片版權管理來說就是一種牽涉到使用者的身分、存取權限的保護動作。圖片存取限制以(圖 6)為例：

圖 6 圖片存取限制圖

(2) 圖片保護設定

當使用者有權瀏覽圖片時，除了相關 MetaData 的呈現之外，還有告知圖片的使用設定、瀏覽限制、期限及版權宣告單位(圖 7)，可依據設定資料做圖片保護機制。圖片受到保護機制管理後，在使用上會受到保護機制的約束，即使是將檔案下載後也會受限制於管理機制的設定。圖片的權限是根據不同圖片擁有者者自行的設定而不同，並不是每張圖去做限制，如(圖 8)設定方式可知。

(3) 圖片瀏覽

當圖片瀏覽時，有圖片文字附加版權的宣告，但若無文字敘述時，圖片就沒有對任何侵權行為有抵擋的能力，於是我們運用數位典藏系統呈現圖片時，還可讓圖片擁有者選擇是否要在圖片上加上有保護機制的顯性浮水印呈現畫面如圖 9 所示。

圖 7 瀏覽圖及保護設定

圖 8 設定保護項目

圖 9 加上顯性浮水印的圖

(4) 浮水印偵測

圖片的保護不光是被動的抵抗，如：加浮水印，也可主動的出擊，如：浮水印偵測機制。以下就對浮水印偵測機制做說明：

本文研發一種偵測圖片內文字浮水印的機制，可用於判斷文字浮水印的存在與否，也由此可知圖片是否被無授權盜用，我們將懷疑被盜用的圖擷取下來後，使用數位典藏系統上的浮水印偵測，選取方式如(圖10、圖11)。

圖 10 在典藏系統中如何選取偵測機制

圖 11 浮水印偵測機制

偵測程式啟動後，就如(圖 12)，會先提出個安全諮詢視窗。這是為了要徵求同意可存取使用者端的檔案。所以選擇「是」。

圖 12 啟動偵測程式畫面

按「是」之後，選擇「Open Image」 

開啟圖檔，選取要偵測的圖檔。

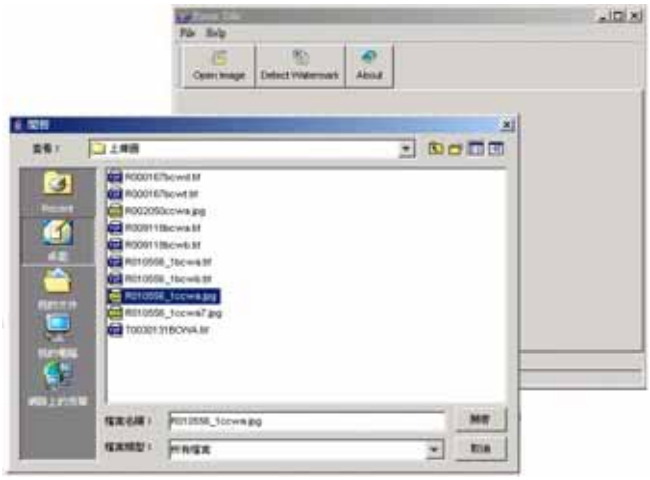

圖 13 選取欲偵測的圖片

載入欲偵測的圖片之後，按下 

「Detect Watermark」開始執行偵測程式，若出現結果如(圖14)，則表示無法從圖片抽出文字浮水印，圖片非有吾人放入之專屬版權宣告，此圖未侵權。

圖 14 無加入文字浮水印圖片的偵測畫面

若出現畫面如(圖 15)，偵測出現「Academia Sinica 2005」字樣，表示此圖有吾人放入之浮水印，可續追查來源找出侵權者，或透過法律途徑追討。

圖 15 有加入文字浮水印圖片的偵測畫面

浮水印偵測是一種可讓使用者對圖片做偵測檢查的工具，這樣的工具若是結合前端的 Image Spy 程式，設定後主動去偵測其他網站圖檔或照片，我們系統尚未將 Image Spy 程式與偵測程式做結合，但預期這樣的機制可以對 DRM 的機制上就多了一層防護，也更加完備。

5. 結論與未來展望

數位典藏的意義不僅只是侷限在狹義的資料的數位化與管理，更進一步有推廣與教育的意義，因此，透過系統化的規劃與管理，以便利與安全的機制來吸引更多的民眾，更有其廣大的意義。然而在數位典藏的傳播上所面臨的安全問題，卻是目前急需解決的，數位內容的傳播與否，與數位內容所受到的保護以及其版權的管理息息相關，一個可信賴的管理平台，將可讓數位內容提供者在釋出數位資產的同時更有保障。

因此，本文提出一個數位版權管理的實行架構，並實作於數位典藏系統上之管理實例，透過此一架構，不僅易於整合至典藏系統，更能有效的保護典藏系統上的數位影像內容，一般使用者亦不需要改變對數位影像內容瀏覽方式的習慣，其可使用之權限，已於系統端給與並套用於瀏覽器上。透過本文所提之數位版權管理系統，將可有效的對數位內容進行保護，進而讓合法使用者安心使用擁有合法版權之數位內容。

6. 參考文獻

[1] 數位典藏型國家科技計劃，http://www.ndap.org.tw/

[2] 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

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

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

[5] 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

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

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

[8] 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

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

[10] 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

[11] 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

[12] 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

[13] 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

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

[15] 田馥銘, "Fractal-based Image Database Retrieval", 國立中山大學資訊工程學系碩士論文,2001

[16] Dong-Qing Zhang, Shih-Fu Chang "Detecting image near-duplicate by stochastic attributed relational graph matching with learning", Proceedings of the 12th annual ACM international conference on Multimedia, 2004

[17] E. Y. Chang, J. Z. Wang. C. Li. and G. Wiederhald. "RIME: A Replicated Imare Detector for the World-Wtde-Web" P m . SPIE: Multimedia Sforogt ad~rckivingS ystems, Vol. 111, 1998.

[18] C. Kim, "Content-based Image Copy Detection" Signul Pmcessing: Image Cornmunicudnn, Vol. 18, pp. 169-184,2003

[19] Chun-Shien Lu, Chao-Yong Hsu, Shih-Wei Sun, Pao-Chi Chang "Robust mesh based hashing for copy detection and tracing of images", IEEE Multimedia and Expo, 2004. ICME '04. 2004 IEEE International Conference on, 2004

[20] Yan Ke, Rahul Sukthankar, Larry Huston "Efficient Near-duplicate Detection and Sub-image Retrieval", Proceedings of the 12th annual ACM international conference on Multimedia, 2004