應用於數位家庭架構之數位版權管理系統

吳宗杉[1] 陳益森[1*] 李明倫[1] 游子德[2]

[1]國立台灣海洋大學資訊工程學系
[2]佛光大學資訊學系

摘 要

數位版權管理是利用建置於軟硬體的保護技術及適切之管理機制，使數位內容提供者能保護所擁有的數位內容。目前的數位版權管理系統著重於智慧財產權保護，對於使用者如何合理使用數位內容，則較少加以研究。由於家電數位化及網路化的結果，逐漸形成數位家庭的應用概念。本文針對數位家庭內數位內容的版權加以管理，提出兩段式的管控機制，利用憑證授權使用時段的方式，以達到數位內容可以在任何時間、任何地點及任何設備之合理使用的目的。

關鍵詞：數位版權管理，數位家庭，合理使用，數位內容

Digital Rights Management System for Digital Home Applications

Tzong-Sun Wu[1], Yih-Sen Chen[1*], Ming-Lun Lee[1], and Tzu-Te Yu[2]

[1] Department of Computer Science and Engineering, National Taiwan Ocean University
[2] Department of Informaticsy, Fo Guang University

Abstract

Digital rights management (DRM) utilizes the protection techniques of hardware and software, and appropriate management mechanism to equip the digital content providers for protecting their digital contents. Most DRM systems focus on the intellectual property rights protection, but it is less studied for how to fair use the digital contents. Owing to the digitizing and networking of electronic products, the applications of digital home have been gradually conceptualized. The digitized electronic products must meet the family members' requirements such as amusements, safety, communications and learning, etc. That is, each family member in digital home can have access to digital contents with his equipment in any where and any time. Digital home technology can be used to improve the living quality and safety as well as entertainments. In this paper, we concentrate on DRM systems of digital home to propose a two-phase control mechanism realizing the fair use of digital contents at any time, any place and any equipment. Authorized licenses are used to prevent digital contents from unreasonably simultaneous access. The media server grants the access right to each media player for some digital contents with some period of time. Further, the off-line playback of digital contents is also supported.

Key words: digital rights management (DRM), digital home, fair use, digital contents

文稿收件日期 100.12.1; 文稿修正後接受日期 101.10.5;*通訊作者
Manuscript received December 1, 2011; revised October 5, 2012; *Corresponding author

一、前　言

在著作財產權受到法令保障之後，部份業者針對數位內容提出數位版權管理系統，結合硬體與軟體的存取機制，將數位內容設定存取權限，使得數位內容在其生命週期內，從出版到廢止都受到版權的保護，並可持續追蹤與管理數位內容的使用情況 [1]。陸陸續續提出的數位內容版權管理系統有：Microsoft Windows Media DRM [2]、IBM EMMS [3]、Apple iTunes [4]、InterTrust [5] 及 Adobe [6] 等系統，在各自發展下，多數的系統將數位內容授權於單一設備上或其所發展之數位內容具特殊檔案格式，必須在專屬的硬軟體上才能播放使用，造成系統間的不相容，對使用者的諸多限制，造成使用上的不便，降低使用者購買數位內容之合理使用權及使用數位版權管理系統的意願。

隨著數位內容在網際網路應用越來越普遍，個人電腦及行動設備的數位版權管理技術也被廣泛討論[7, 8, 9]，在資訊家電的發展，數位家庭的概念也漸漸地在數位家庭聯盟 ECHONET [10]、OSGI [11]、UPnP™ Forum [12]、DLNA [13]、CELF [14]、UOPF [15] 等組織的推廣下，逐漸在家庭中實現，而數位版權管理技術也在數位家庭中逐漸被探討著 [16, 17, 18]。數位版權管理系統是用來管理使用者使用受保護的數位內容，而不是執行智慧財產權法的機制，所以必須創造一個對使用者更彈性且合理的使用環境 [19, 20]，方能滿足使用者的使用意願及需求。故必須滿足讓使用者可以在任何時間、任何地點及任何設備，其數位家庭內的設備可依授權憑證所分配的時間，合理使用其數位內容 [21]。本文所提之數位版權管理系統，結合密碼學、身分認證、版權描述語言及數位浮水印…等技術，以確保數位內容的安全性。

二、文獻探討

當網路頻寬大幅提升，有線頻寬從現行 ADSL 技術提升到 FTTx 技術，無線傳輸也進入 3.5G 及 WiMAX 高傳輸世代，聲音、影像的即時傳輸不再受到頻寬的限制。家電數位化、網路化已成為趨勢，使得資訊家電的出現與應用已成為未來科技發展的新方向，數位家庭的概念也因此誕生。所謂的數位家庭，即透過數位化及網路技術的整合，家中成員無論在何時何地，都可利用各項家電及個人電子設備，及時操作及存取控制，使得生活更形便利與安全，以及有更好的娛樂享受。其應用包含娛樂、保全、通訊、學習、控制、遠距醫療、居家照護…等。

2001 年，歐洲數位視訊廣播技術發展組織 (Digital Video Broadcasting project, DVB) [22] 提出“授權領域” (authorized domains) 概念，將一個家庭所擁有的電子設備透過網路連結形成一個“授權領域”，合法取得的數位內容就可在授權領域裡的設備之間傳送。2006 年，Lee 等人 [23] 提出數位版權管理系統和數位指紋系統的整合方法。由數位版權管理系統負責數位內容的安全傳播，數位指紋系統負責跟蹤非法的傳播者。當使用者播放數位內容時，數位指紋系統將被啟動，把數位指紋識別碼通過數位版權管理系統直接嵌入解密的數位內容裡。當網路蜘蛛在網際網路上搜尋取得非法傳播的數位內容時，將透過數位指紋伺服器取出非法傳播之數位內容的數位指紋識別碼，以確認非法傳播的使用者身分。

2.1 系統架構介紹

數位版權管理系統其基本架構如圖 1 所示，在數位版權管理系統有四個主要的角色，各自擔任著不同的工作，以建立完整的數位版權管理系統流程，說明如下：

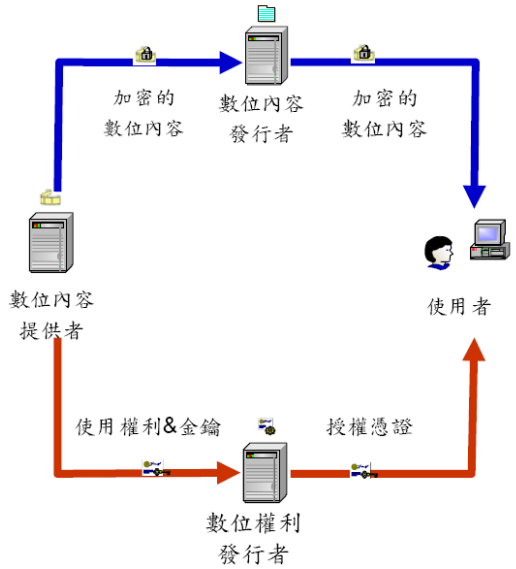

圖 1. 數位版權管理系統示意圖

(1) 數位內容提供者 (content provider)：
為數位內容的版權擁有者，透過密碼學技術保護其擁有數位內容的權利。首先，利用加密金鑰進行加密及封裝其數位內容，以限制數位內容的流通，再將封裝後的數位內容傳送給數位內容發行者。接著訂定數位內容的使用權利，限制數位內容的使用權利，再將使用權利及加密金鑰透過安全的管道傳送給數位權利發行者。

(2) 數位內容發行者 (content issuer)：
提供數位內容傳播的管道 (如網站、CD...等等)，負責販售或傳播由數位內容提供者合法封裝的數位內容。

(3) 數位權利發行者 (rights issuer)：
由數位內容提供者所訂定的使用權利及加密金鑰，依使用者購買數位內容的需求，產生與數位內容相對應的授權憑證。

(4) 使用者：
經由數位內容發行者或其它管道取得或下載數位內容，在使用數位內容時，數位版權管理系統會連線到數位權利發行者，在身分驗證合法後，使用者取得數位內容相對應的授權憑證，利用授權憑證的使用權利和解密金鑰播放或使用數位內容。

數位版權管理系統在使用者的使用數位內容時，必須先達到數位內容的版權保護，以避免數位內容提供者的權益遭到侵害，所以數位版權管理系統保護的數位內容必須滿足以下要求：

(1) 數位內容可以用密碼學技術，來防止被未授權的使用者存取。
(2) 受保護的數位內容，支援超傳播(super-distribution) [24] 模式。即受保護的數位內容可於使用者之間自由傳播使用，以不同的傳播方式（例如：mail、ftp server、P2P…等）傳送給其它使用者。如果沒有授權憑證的使用者要存取使用數位內容時，使用者必須依照使用權利之要求，向數位權利發行者取得數位內容的授權憑證。
(3) 授權憑證的完整性和真實性，必須被保證並且驗證。
(4) 每個合法使用者的識別碼是唯一。

2.2 Microsoft-Windows Media DRM [2]

Windows Media DRM 是一個具有彈性的數位版權管理平台，讓數位內容提供者和網際網路內容提供者能夠安全地傳播數位內容，而使用者也能輕鬆的使用數位內容，並可提供可攜式裝置和網路裝置強大的功能來取得和存取數位內容。WM DRM 解決方案包含伺服器和用戶端軟體開發套件 (SDK)，伺服器 SDK 是在 Windows Media Rights Manager SDK 下授權，而用戶端 SDK 則會授權為 Windows Media Format SDK 的元件。使用多種加密和防止盜版的技術來保護數位內容與其完整性，可讓應用程式進行保護和播放數位內容。系統架構圖如圖 2。

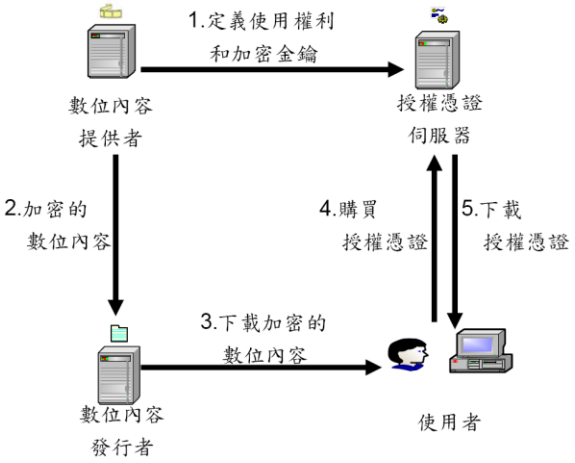

圖 2. Windows Media DRM 系統架構圖

2.3 Open Mobile Alliance-OMA DRM [25]

OMA (Open Mobile Alliance) 由行動通訊服務提供商、設備供應商…等業者所組成，共同開發行動通訊服務並制定公開的標準；協助建立跨國家、使用者和行動端的相容性與互

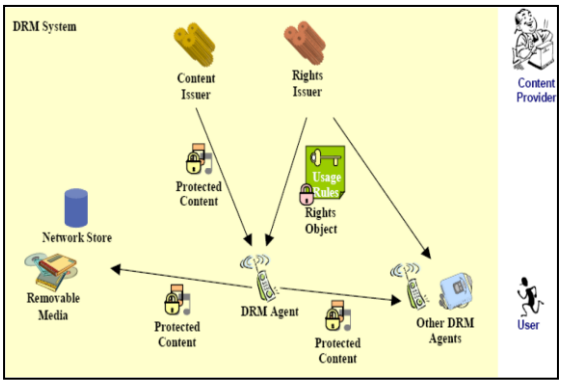

圖 3. OMA DRM 系統架構圖

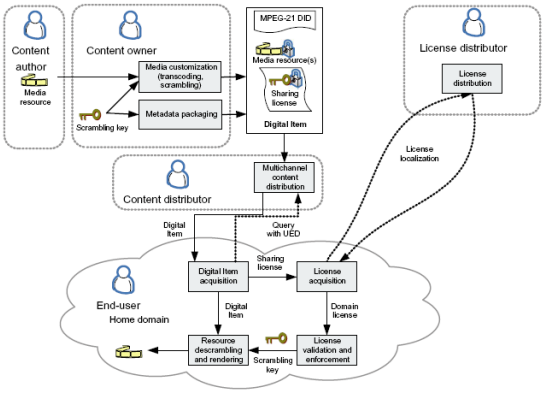

圖 4. TIRAMISU 架構圖

動服務，使行動通訊可以得到快速和廣泛的發展及使用。OMA DRM 為 OMA 所定義的數位版權管理標準，其主要目的為確保數位內容可以在行動設備上能遵循授權憑證的使用規範，藉以保護數位內容提供者的智慧財產權不被非法使用者所侵害，系統架構如圖 3 所示。

2.4 TIRAMISU 系統介紹[26]

2005 年，Marusic 等人 [26] 提出一個基於新興的 MPEG-21 為多媒體內容的標準建構數位版權管理系統-TIRAMISU，達到數位內容標準化，並提出新的金鑰管理系統搭配智慧卡技術，完成數位內容在數位家庭裡設備皆可使用的目標，以解決以往數位版權管理系統推廣所遇到之問題，架構圖如圖 4。授權的數位內容可以在數位家庭的各種設備之間傳播，使用者可能在數位家庭中註冊數張智慧卡，用來驗證播放的設備是數位家庭的合法成員。並可支援數位內容超傳播分配，利用 P2P 分配方式，將數位內容在數位家庭與數位家庭之間傳播。

三、數位家庭之數位版權管理系統

數位版權管理系統是新興的資訊技術應用，目前系統著重於智慧財產權的保護，對於使用者如何合理使用數位內容，則較少加以研究。因此，本文提出兩段式數位版權管理之機制，滿足數位內容可以任何時間、任何地點、在任何設備上皆可合理地使用。為防止數位內容在數位家庭的不同設備卻同時使用的不合理現象，我們採用時段授權的方式，由數位家庭的媒體伺服器，依使用時段需求授予媒體播放器使用其數位內容，不同的媒體播放器可取得不同的使用時段的使用權限。

3.1 系統架構

本文建構一個應用於數位家庭的數位版權管理系統，系統架構如圖 5 所示，其基本角色包含數位內容提供者、數位內容發行者、授權憑證伺服器、購買者，並配合設計需要，新增使用者、數位家庭設備（媒體伺服器及媒體播放器）、設備製造商、網路蜘蛛及數位指紋伺服器…等角色，其各角色與擔任工作分述如下：

3.1.1 數位內容提供者 CP (content provider)：

負責定義數位內容使用權利，進行數位內容的加密及封裝及限制數位內容的流通和使用，並將封裝的內容和使用權利，分別安全地傳送給數位內容發行者及授權憑證伺服器。

3.1.2 數位內容發行者 CI (content issuer)：

負責建立數位內容的傳播管道（例如：網站、音樂光碟…等），傳播由數位內容提供者合法封裝的數位內容給購買者。

3.1.3 授權憑證伺服器 LS (license server)：

負責販售數位內容的授權憑證給購買者，並追蹤、識別在網際網路上非法傳播數位內容的購買者身分。

3.1.4 使用者 U (user)：

向數位家庭完成註冊的合法使用者，可依

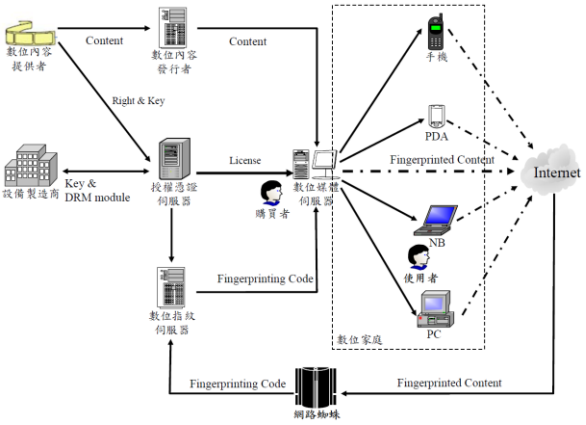

圖 5. 系統架構圖

媒體伺服器之授權，在媒體播放器使用數位內容。

3.1.5 購買者 B (buyer)：

定義為合法購買數位內容的使用者，當購買者取得封裝的數位內容及授權憑證後，可在它擁有的數位家庭範圍內，依授權憑證權限提供使用者在媒體播放器使用數位內容。

3.1.6 數位家庭設備：

可區分為媒體伺服器和媒體播放器兩類，必須能以硬體或軟體方式執行數位版權管理系統，防止惡意的使用者竄改數位版權執行硬體或軟體，並由數位家庭設備形成一個授權的家庭領域，功能說明如下：

(1) 媒體伺服器 S (digital media server)：
媒體伺服器為數位內容發行者所信任之硬體或軟體所組成，例如：數位機上盒、iTunes…等設備，可安裝於數位家庭中，記錄數位家庭領域的所有設備，負責執行媒體播放器的註冊及移除等功能，一個數位家庭領域裡只需一個媒體伺服器，但可有多個媒體播放器。擁有唯一的金鑰對，私鑰存儲於防止竄改的記憶體，公鑰則可透過設備製造商驗證；並對合法註冊的媒體播放器產生共享金鑰，儲存於防止竄改的記憶體中，使用於授權媒體播放器的數位內容加密之用。使用者將取得封裝的數位內容及授權憑證儲存於媒體伺服器，並將封裝的數位內容解密以浮水印技術加入數位指紋識別碼。當使用者提出數位內容的使用需求時，將解密的數位內容以時段分割方式，將媒體伺服器與媒體播放器的共享金鑰加密授權給媒體播放器使用。

(2) 媒體播放器 Px (digital media player)：
媒體播放器為數位內容發行者所信任之硬體或軟體所組成，例如 iPod、MediaPlay…等設備，必須能執行數位版權管理系統的播放設備，向媒體伺服器註冊後，即可取得數位內容進行使用。每個媒體播放器都有唯一的序號，由製造商編號及設備生產序號所組成。向媒體伺服器註冊後，會取得媒體伺服器產生的共享金鑰，儲存於防止竄改的記憶體中，作為數位內容的解密之用。為防止使用者惡意修改媒體播放器之時間，非法使用數位內容，當媒體播放器之時間一經修改，已取得之數位內容授權即失效，需向媒體伺服器重新申請使用時段，方能再使用。

3.1.7 設備製造商 M (manufacturer)：

負責生產和銷售數位家庭設備（媒體伺服器及媒體播放器），並提供所生產的設備金鑰驗證功能，可以讓授權憑證伺服器將購買者註冊的媒體伺服器設備進行驗證。

3.1.8 網路蜘蛛 WS (web spider)：

是一種自動瀏覽網頁的程式，負責在網際網路上搜尋非法傳播的數位內容，利用搜尋引擎來收集網頁內容以及在網頁上讀取網頁上的連結，進而找到新網頁，並將網頁內 HTML 及 Java script 等內容進行過濾，收集及整理有意義的內容。

3.1.9 數位指紋伺服器 FS (fingerprinting server)：

依數位內容版權資訊及購買者資訊製作唯一的數位指紋，負責在媒體伺服器解密的數位內容加入數位指紋，以及從非法傳播數位內容中取出數位指紋識別碼，提供數位指紋之相關資訊給授權憑證伺服器，識別非法傳播者的身分。

3.2 情境說明

數位家庭的功能，即數位家庭內任一種媒體播放器可在任何地方、任何時刻使用數位內容。換句話說，假如每位使用者透過媒體播放器，不管在家、在辦公室或在路上，運用各式通訊技術，連線至數位家庭的媒體伺服器，依授權使用數位內容。情境說明如下：

3.2.1 數位家庭成員註冊：

在數位家庭中的成員及媒體播放器，必須經過數位家庭管理者 (數位家庭成員中共同推選出來的人或是 administrator 授權的人) 在媒體伺服器進行註冊，唯有完成註冊之使用者或媒體播放器，才可依權限使用媒體伺服器

內的數位內容。數位家庭管理者可以控管使用者及媒體播放器之數量及使用權限；使用者之授權可以將購買的數位內容儲存於媒體伺服器；媒體播放器依授權使用數位內容。

3.2.2 購買數位內容：

在數位家庭完成註冊的購買者，透過各種管道取得數位內容，再向授權憑證伺服器購買數位內容之授權憑證，而將數位內容跟授權憑證都儲存於媒體伺服器中。

3.2.3 使用數位內容：

在數位家庭完成註冊的使用者，可向媒體伺服器請求在特定時段、特定已經完成註冊的媒體播放器上使用數位內容。只要該時段尚未被其它使用者請求授權，則該使用者就可取得授權，依其請求之時段使用數位內容，並可支援數位內容預約授權及離線使用的架構。

3.3 系統符號說明與假設

數位版權管理系統，主要負責的功能為數位內容的解密、數位簽章的驗證、金鑰管理、使用權利的解析及數位內容的控管等功能。所使用的符號說明如表 1 所示。而本文主要針對在數位家庭中數位內容之合理使用，故在設計時有兩個假設：

3.3.1 憑證管理中心：

為具公信力的第三者 (trusted third party)，對數位內容提供者、數位內容發行者、授權憑證伺服器、設備製造商、使用者及購買者等角色提供認證及憑證簽發管理等服務，提供具機密性、鑑別性、完整性、不可否認性、接取控制及可用性的資訊通信安全環境與機制。對系統的各成員之身分資訊、金鑰等所作出的一個數位簽章，用來驗證各成員的身分及金鑰的有效性。

3.3.2 媒體伺服器：

在數位家庭中與各種消費性電子產品(如個人電腦、PDA、手機、電視、數位相機、音響和隨身聽等設備)形成一個數位家庭網路，並由媒體伺服器提供媒體播放器註冊或移除

表 1. 符號說明

符號	說明
E[Data]	用公鑰系統對資料 (Data) 加密
E(Data)	用私鑰系統對資料 (Data) 解密
H(Data)	對資料 (Data) 進行雜湊函數運算
C	數位內容
R	數位內容的使用權利
L	授權憑證，包含使用權利 R 和加密金鑰 K_C
ID_C	數位內容的識別碼
ID_U	使用者的識別碼
ID_B	購買者的匿名識別碼 $ID_B = H(ID_U\|\|s)$
P_B	購買者的付款資訊
ID_S	媒體伺服器的識別碼
ID_{P_x}	媒體播放器 x 的識別碼
ID_{Fp}	數位內容的數位指紋識別碼
ID_L	數位內容的授權憑證識別碼
KS	數位內容的加密金鑰種子 $KS = H(SK_{CP})$
K_C	數位內容加密金鑰 $K_C = H(KS\|\|H(C))$
PK_{CP}, K_{CP}	數位內容提供者的公鑰及私鑰
PK_{LS},SK_{LS}	授權憑證伺服器的公鑰及私鑰
PK_M, SK_M	設備製造商的公鑰及私鑰
PK_U, SK_U	使用者的公鑰及私鑰
PK_B, SK_B	購買者的公鑰及私鑰
PK_S, SK_S	媒體伺服器的公鑰及私鑰
K_{P_x}	媒體播放器 x 的金鑰
$K_{S\_P_x}$	媒體伺服器與媒體播放器 x 的共享金鑰
TR_x	媒體播放器 x 要求數位內容的授權使用時間
TS_x	媒體播放器 x 的電子時戳
s	隨機產生的亂數
||	連結符號

的功能，成為一個動態的群組，稱為“數位家庭領域”。媒體伺服器與多個媒體播放器串連在一個數位家庭網路下，並能互相分享及交換

資料，將數位家庭內所有的數位內容統一透過單一的媒體伺服器來控管。

3.4 系統流程

本文以數位內容的授權憑證取得與保護為議題，將數位家庭中的數位版權管理系統流程分為數位內容封裝階段、數位家庭註冊階段、購買者註冊階段、數位內容購買階段、數位內容使用階段及數位內容追蹤階段等六個階段。分別敘述如下：

3.4.1 數位內容封裝階段

數位內容提供者必須對其擁有的數位內容制訂使用權利，利用數位內容加密金鑰對數位內容進行加密及封裝，將封裝後的數位內容傳送給數位內容發行者；把數位內容識別碼、加密金鑰及使用權利傳送給授權憑證伺服器，以製作成授權憑證，如圖 6 所示。步驟如下：

步驟一、數位內容提供者產生數位內容加密金鑰

數位內容提供者依數位內容的使用權限，定義其數位內容的使用權利；利用數位內容提供者之私鑰進行雜湊運算，產生數位內容之加密金鑰種子 $KS = H(SK_{CP})$；再以加密金鑰種子 KS 與數位內容之雜湊值 H(C)，再進行一次雜湊運算，產生數位內容加密金鑰 $K_C = H(KS||H(C))$。

步驟二、數位內容提供者傳送使用權利及加密金鑰給授權憑證伺服器

數位內容提供者完成定義數位內容的使用權利後，以授權憑證伺服器之公鑰對數位內容的識別碼 ID_C、加密金鑰 K_C 及使用權利 R 進行加密 $E_{PK_{LS}}[ID_C, K_C, R]$ 並傳送給授權憑證伺服器；授權憑證伺服器將數位內容的識別碼、加密金鑰及使用權利儲存於資料庫中，等待購買者購買數位內容的授權憑證。

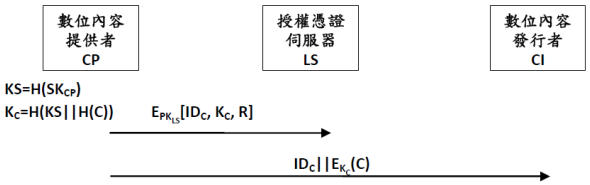

圖 6. 數位內容封裝階段

步驟三、數位內容提供者將加密的數位內容傳給數位內容發行者

數位內容提供者利用數位內容雜湊值與數位內容加密金鑰結合雜湊函數運算產生的數位內容加密金鑰，以數位內容加密金鑰對數位內容進行加密 $E_{K_C}(C)$，再對加密的數位內容進行封裝，並把數位內容識別碼 ID_C 放於封裝的數位內容檔頭之中，將封裝後的數位內容傳送給數位內容發行者進行建立傳送管道。

3.4.2 數位家庭註冊階段

將使用者及媒體播放器登錄於媒體伺服器，形成一個信任的數位家庭領域，讓“授權領域”的使用者及媒體播放器可以合理使用媒體伺服器擁有的數位內容，如圖 7 所示。

步驟一、使用者向媒體伺服器註冊

使用者必須先向媒體伺服器註冊，在媒體伺服器登錄使用者識別碼 ID_U，並設定使用者之使用權限，成為數位家庭中的合法授權使用者。

步驟二、媒體伺服器傳送匿名識別碼給使用者

當媒體伺服器收到使用者識別碼後，隨機產生一組亂數，並將使用者識別碼與亂數進行雜湊運算，再將雜湊值 $H(ID_U||s)$ 傳送給使用者。當使用者向授權憑證伺服器註冊時，作為使用者的匿名識別碼。

步驟三、媒體播放器向媒體伺服器註冊

媒體播放器必須向媒體伺服器進行註冊，登錄其媒體播放器識別碼 ID_{P_x}，設定媒體播放器的使用權限，作為數位家庭中合法授權的媒體播放器。

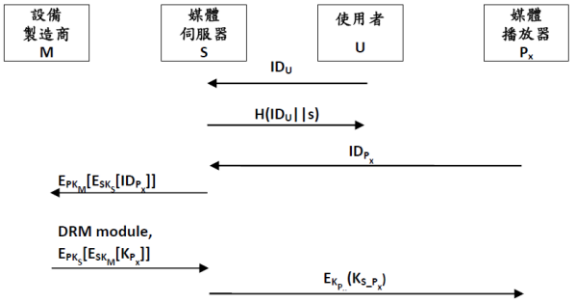

圖 7. 數位家庭註冊階段

步驟四、媒體伺服器向設備製造商驗證媒體播放器

媒體伺服器收到媒體播放器識別碼之後，從識別碼中得知媒體播放器的設備製造商資訊，將媒體播放器識別碼向設備製造商進行設備識別，以取得媒體播放器的硬體資訊及設備金鑰。

步驟五、設備製造商傳送媒體播放器的相關資訊給媒體播放器

設備製造商收到媒體伺服器傳送的媒體播放器識別碼 ID_{P_x}，即提供媒體播放器的硬體及 DRM 模組資訊，以確認媒體伺服器提供的數位內容可於媒體播放器使用；並將媒體播放器內建的設備金鑰 $E_{PK_M}[E_{SK_S}[ID_{P_x}]]$，傳送給媒體伺服器，作為媒體伺服器與媒體播放器間傳送共享金鑰加密 $E_{PK_S}[E_{SK_M}[K_{P_x}]]$ 之用。

步驟六、媒體伺服器為媒體播放器產生共享金鑰

媒體伺服器收到設備製造商傳送的硬體及 DRM 模組資訊，確認媒體伺服器提供的數位內容可於媒體播放器後，產生媒體伺服器與媒體播放器共享的數位內容加密金鑰 $E_{K_{P_x}}$ $(K_{S\_P_x})$，其中 $K_{S\_P_x}=H(SK_S||K_{P_x}||S)$，傳送給媒體播放器，儲存於媒體播放器的防竄改記憶體中，作為媒體伺服器將數位內容授權給媒體播放器加解密之用。

3.4.3 購買者註冊階段

購買者向授權憑證伺服器註冊，以利購買者購買數位內容的授權憑證，並將合法取得的數位內容儲存於媒體伺服器中，以提供數位內容給數位家庭中的媒體播放器使用，如圖 8 所示。

步驟一、購買者向授權憑證伺服器註冊

購買者先向授權憑證伺服器註冊，除了提供購買者的匿名識別碼及付款資訊以外，還要提供購買者儲存數位內容及授權憑證的媒體伺服器識別碼等 $E_{PK_{LS}}[E_{SK_B}[ID_B, P_B, ID_S]]$ 資訊，註冊成為可以在授權憑證伺服器購買數位內容的購買者。

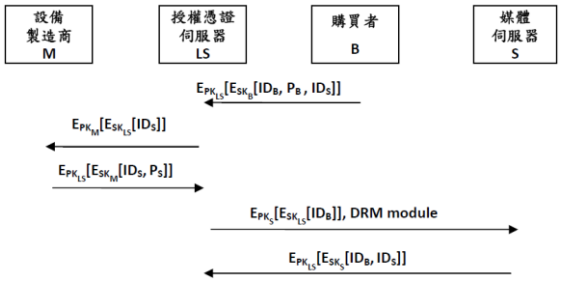

圖 8. 購買者註冊階段

步驟二、授權憑證伺服器向設備製造商驗證媒體伺服器

授權憑證伺服器收到購買者的註冊資訊，對購買者的匿名識別碼及付款資訊進行驗證，在確認無誤後，將使用者儲存數位內容及授權憑證的媒體伺服器識別碼 $E_{PK_M}[E_{SK_{LS}}[ID_S]]$ 傳送給設備製造商進行設備識別，以確保購買者提供的媒體伺服器是合法的。

步驟三、設備製造商傳送媒體伺服器的相關資訊給授權憑證伺服器

設備製造商收到授權憑證伺服器傳送的媒體伺服器識別碼後，即提供媒體伺服器的硬體及 DRM 模組資訊，以確認授權憑證伺服器提供的數位內容可於媒體伺服器使用；並將媒體伺服器的公鑰 $E_{PK_{LS}}[E_{SK_M}[ID_S, P_S]]$ 傳送給授權憑證伺服器，作為授權憑證伺服器與媒體伺服器間傳送資訊加解密之用。

步驟四、授權憑證伺服器向媒體伺服器驗證購買者的匿名識別碼

授權憑證伺服器收到設備製造商傳送媒體伺服器的公鑰 $E_{PK_S}[E_{SK_{LS}}[ID_B]]$ 後，以購買者註冊的匿名識別碼對媒體伺服器進行驗證，以確認使用者已向媒體伺服器註冊是合法的購買者，並將授權憑證伺服器相關的 DRM 模組資訊提供給媒體伺服器使用。

步驟五、媒體伺服器回覆授權憑證伺服器驗證結果

媒體伺服器收到授權憑證伺服器傳送到驗證資訊 $E_{PK_{LS}}[E_{SK_S}[ID_B, ID_S]]$ 後，從資料庫中比對購買者的匿名識別碼，以識別購買者的身分，確認購買者已向媒體伺服器進行註冊。驗證後，再將註冊資訊

(ID_B, ID_S) 回傳給授權憑證伺服器，以確認媒體伺服器的身分。經過授權憑證伺服器確認使用者的匿名識別碼及媒體伺服器的資訊無誤後，購買者即註冊成功，可以合法購買數位內容。

3.4.4 數位內容購買階段

數位內容購買階段如圖 9 所示，已經向授權憑證伺服器註冊的購買者，在取得封裝的數位內容後，如果尚未取得數位內容的授權憑證就無法使用數位內容，必須先向授權憑證伺服器購買取得授權憑證後，儲存於購買者的媒體伺服器，以供數位家庭裡的媒體播放器使用。在此階段中，購買者購買喜愛之數位內容，取得封裝的數位內容並儲存於數位媒體伺服器內。至於如何進行數位付款交易，有興趣的讀者可參考行動付款研究文獻 [27, 28, 29, 30] 以取得更多相關技術。

步驟一、數位內容發行者傳送數位內容給媒體伺服器

購買者選擇喜愛之數位內容 C，從數位內容發行者建置的網站下載或利用其它管道取得封裝的數位內容並儲存媒體伺服器 $ID_C||E_{K_C}(C)$。如果媒體伺服器尚未取得授權憑證，就無法使用封裝的數位內容，必須向授權憑證伺服器購買，並取得數位內容的授權憑證後，才可在數位家庭內合法使用數位內容。

步驟二、購買者向授權憑證伺服器購買數位內容授權憑證

當媒體伺服器未取得授權憑證，無法使用封裝的數位內容時，購買者從封裝的數位內容取得數位內容識別碼及授權憑證伺服器的資訊後，向授權憑證伺服器購買數位內容的授權憑證，傳送購買者的匿名識別碼及數位內容識別碼給授權憑證伺服器 $E_{PK_{LS}}[E_{SK_B}[ID_C, ID_B]]$，做為購買者購買數位內容的識別資料。

步驟三、授權憑證伺服器傳送授權憑證給媒體伺服器

授權憑證伺服器收到購買者購買數位內容的資訊，由授權憑證伺服器產生購買者購買的授權憑證 $L=\{ID_L, ID_S, ID_C, E_{PK_S}[K_C], R]$，作為購買者的數位家庭使用數位內容的依據。

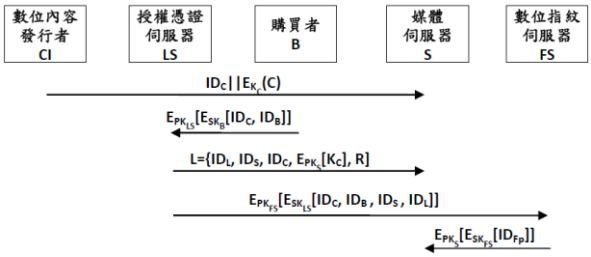

圖 9. 數位內容購買階段

步驟四、授權憑證伺服器傳送授權憑證資訊給數位指紋伺服器

授權憑證伺服器將購買者購買數位內容的授權憑證資訊 (ID_C, ID_B, ID_S, ID_L) 傳送給數位指紋伺服器 $E_{PK_{FS}}[E_{SK_{LS}}[ID_C, ID_B, ID_S, ID_L]]$，由數位指紋伺服器產生購買者購買數位內容授權憑證的唯一識別資料 ID_{FP}，作為追蹤數位內容的擁有者身分之用。

步驟五、數位指紋伺服器傳送數位指紋給媒體伺服器

數位指紋伺服器利用授權憑證資訊 (ID_C, ID_B, ID_S, ID_L) 進行雜湊函數運算，產生購買者的數位指紋，傳送 $E_{PK_S}[E_{SK_{FS}}[ID_{FP}]]$ 給媒體伺服器。當媒體伺服器從數位內容授權憑證取出數位內容解密金鑰，以數位內容解密金鑰對封裝的數位內容進行解密時，媒體伺服器的 DRM 模組會以浮水印技術將數位指紋加入解密的數位內容，然後由媒體伺服器依數位內容在數位家庭的使用權利對解密的數位內容進行加密，以授權數位內容在數位家庭領域使用。所以限制數位內容僅能在數位家庭的設備使用，此時的數位內容已失去超傳播功能，不可再傳播給其它使用者或設備。

3.4.5 數位內容使用階段

數位內容使用階段如圖 10 所示，假設在數位家庭領域中有三個媒體播放器 (P_A, P_B, P_C)，分別依使用者的數位內容使用需求，向媒體伺服器請求使用數位內容的授權，媒體伺服器參照數位家庭中所擁有之數位內容使用授權，依各媒體播放器請求的使用時段，搭配數位浮水印技術，用媒體伺服器與媒體播放器

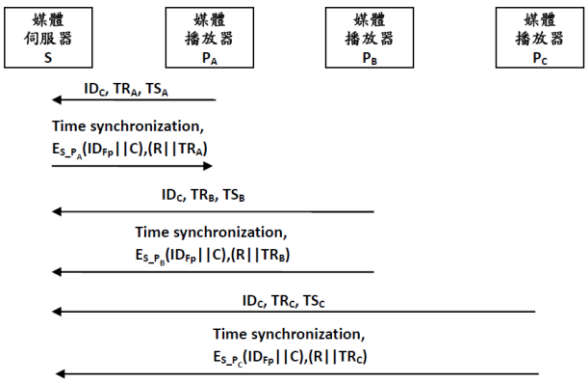

圖 10. 數位內容使用階段

的共享金鑰 $K_{S\_P_X}$ 將加入數位指紋的數位內容及授權憑證進行加密，再傳送給媒體播放器，當媒體播放器收到加密的數位內容之後，不管在連線或離線環境，均可在授權時段內使用數位內容，以達到數位內容合理使用的目標。

步驟一、媒體播放器向媒體伺服器請求數位內容使用授權

不同的使用者可於數位家庭內不同的媒體播放器 (P_A, P_B, P_C) 用數位內容，所以媒體播放器依使用者的使用需求向媒體伺服器請求數位內容的使用時段授權 ID_C, TR_A, TS_A，將數位內容在不同時段提供給不同的媒體播放器使用，以確保數位內容提供者及購買者的權益不會損害。

步驟二、媒體伺服器授權數位內容使用時段給媒體播放器

當媒體伺服器收到數位家庭內的媒體播放器的使用數位內容請求時，媒體伺服器利用 NTP (network time protocol) 或 SNTP (simple network time protocol) 等技術與媒體播放器進行時間同步。再依其請求的數位內容的使用時段檢查是否已提供授權，如請求使用時段尚未授權給其它媒體播放器，則依其請求時段提供授權使用數位內容。如請求使用時段已授權其它媒體播放器使用，則無法依其請求時段提供授權使用數位內容。當媒體伺服器完成授權確認後，將取得的數位內容使用權利加註授予媒體播放器的使用時段，再與解密的數位內容用媒體伺服器與媒體播放器的共享金鑰進行加密，再傳送給授權的媒體播放器 $E_{S\_P_A}(ID_{Fp}||C),(R||TR_A)$。授權的媒體播放器取得授權的數位內容後，依媒體伺服器的授權利用共享金鑰進行解密使用數位內容。

步驟三、媒體播放器播放數位內容

在數位家庭中，媒體伺服器以時間方式管理數位內容的授權，以控管數位內容在一個時間點只授權一個媒體播放器使用。媒體播放器向媒體伺服器請求使用數位內容時，媒體伺服器與媒體播放器先進行時間同步 (Time Synchronization)。之後媒體播放器取得授權的數位內容後 $E_{S\_P_X}(ID_{Fp}||C)$, $(R||TR_X)$，依授權的時段使用數位內容，並記錄每次使用時間，如有發現使用時間與次數發生異常時，即註銷數位內容之使用權限，以避免媒體播放器之時間被人為調整，惡意破壞數位內容使用限制。

3.4.6 數位內容追蹤階段

數位內容追蹤階段如圖 11 所示，在浩瀚的網際網路世界中，包含著成千上萬的非法網頁，提供非法的多媒體檔案下載，利用網路蜘蛛在網際網路上搜尋非法傳播的數位內容，協助數位內容提供者尋找非法使用者，從非法傳播的數位內容中取出數位指紋識別碼，由數位指紋伺服器識別指紋識別碼資訊，以利授權憑證伺服器檢舉購買者的非法行為。

步驟一、網路蜘蛛在網際網路上搜尋非法傳播之數位內容

為防止購買者非法散佈授權的數位內容，數位內容發行者在網際網路上設置功能強大的搜尋軟體--網路蜘蛛，在網際網路上搜尋非法散佈的數位內容 $ID_{Fp}||C$。一旦發現非法傳播的數位內容時，立即下載取得非法傳播的數位內容，作為檢舉購買者非法行為之依據。

步驟二、網路蜘蛛將搜尋到之非法數位內容傳送給數位指紋伺服器

當網路蜘蛛從網際網路搜尋到非法傳播

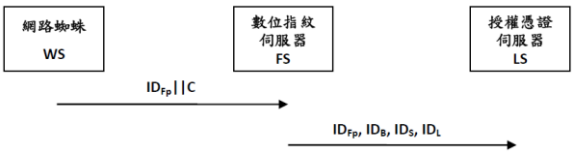

圖 11. 數位內容追蹤階段

的數位內容後，將非法傳播的數位內容 $ID_{Fp}||C$ 傳送給數位指紋伺服器，取出數位指紋識別碼，進而找出非法傳播數位內容之購買者身分。

步驟三、數位指紋伺服器取出數位指紋識別碼傳送給授權憑證伺服器

當數位指紋伺服器由非法傳播的數位內容取出的數位指紋識別碼，識別驗證購買者的身分後，將此份資料 ID_{Fp}, ID_B, ID_S, ID_L 傳送給授權憑證伺服器，由授權憑證伺服器對非法的購買者進行停權等相關程序，以減少數位內容提供者所擁有的數位內容之版權損失。

四、討論與分析

本章節將進一步探討數位版權管理系統之安全性及功能分析。如第二章所述，數位版權管理系統保護的數位內容必須滿足使用者的使用數位內容時，必須先達到數位內容的版權保護，以避免數位內容提供者的權益遭到侵害；彙整數位版權管理之相關文獻 [2, 25, 26] 內容，健全的數位版權管理系統必須滿足以下要求：超傳播、授權憑證、安全機制、使用隱私、使用識別、數位家庭架構、合理使用。就系統功能分別敘述如下並進行相關文獻等所提之系統架構進行比較(如表 2):

4.1 系統功能分析

4.1.1 超傳播

受保護的數位內容可於使用者之間自由的傳播使用，以不同的傳播方式（例如：mail、ftp server、P2P 等）傳送給其它使用者。

4.1.2 授權憑證

授權憑證是規範著數位內容的授權使用範圍，例如：數位內容的提供者、授權者、使用次數、使用期限、使用權限及授權憑證的移轉限制…等等。

4.1.3 安全機制

在數位版權管理系統中，其安全機制不只具備加解密技術，還要包含身分認證、權利描述語言、數位浮水印等安全技術，才能確保數位內容的安全。

表 2. 功能分析比較表

	WM DRM [2]	OMA DRM [25]	TIRAMISU [26]	本機制
超傳播	○	○	○	○
使用憑證	獨立	皆可	獨立	皆可
安全機制	○	○	○	○
使用隱私	○	－	－	○
使用識別	設備	設備	智慧卡	設備
數位家庭	╳	╳	○	○
合理使用	低	低	中	高
備註：○：表符合；╳：表不符合；－：表未提及				

4.1.4 使用隱私

在驗證使用者發佈授權憑證時，保護使用者的資訊，避免個人資料外洩，所以能保護使用者隱私。

4.1.5 使用識別

不同的系統，使用不同的使用識別機制，即每個註冊的使用者或設備都有不同的認證授權金鑰，所以一個授權憑證也只能授權給一個使用者或設備使用，也就能限定數位內容給單一設備或使用者使用。

4.1.6 數位家庭架構

在數位家庭架構下，數位媒體伺服器與多個數位媒體播放器串連在一個數位家庭網路下，並能互相分享及交換資料，將數位家庭內所有的數位內容統一透過單一的數位媒體伺服器來控管。

4.1.7 合理使用

在不侵害著作財產權的情況下，合理重製、暫時重製及有條件移轉等，是對於使用者的合理使用的保障。

4.2 系統功能比較

4.2.1 超傳播

WM DRM、OMA DRM 及 TIRAMISU 等數位版權管理系統，其數位內容傳播方式均符

合超傳播方式，可避免使用者每購買一個數位內容，系統就必須對數位內容進行封裝作業，可大幅減輕系統的負荷。本文所提之媒體伺服器及媒體播放器，在數位家庭外，媒體伺服器收到封裝的數位內容後，可以再將封裝的數位內容傳送給其它使用者或媒體伺服器，達到數位內容超傳播之功能。但在數位家庭內，媒體伺服器將封裝的數位內容依授權憑證進行解密後，可依媒體播放器使用時段需求，以媒體伺服器與媒體播放器之共享金鑰加密，傳送給媒體播放器使用。故在數位家庭內媒體播放器取得的數位內容是不可提供可其它使用者或媒體播放器使用，也就是不支援數位內容超傳播功能。

4.2.2 授權憑證

在 WM DRM 及 TIRAMISU 等數位版權管理系統架構，因配合數位內容具有超傳播功能，所以授權憑證均採用一個獨立的版權檔案格式，把數位內容和授權憑證分開製作及傳送，以提昇系統之效能。而 OMA DRM 所採用的數位內容傳播方式有三種：限制轉送、結合授權憑證、與授權憑證分開，所以授權憑證可採用獨立的版權檔案格式，也可採用與數位內容合併之格式。本文所提之架構，在數位家庭外，數位內容符合超傳播之功能，所以授權憑證採用與數位內容分開的版權檔案格式。但在數位家庭內，媒體伺服器重新將數位內容、授權憑證及授權時段重新加密傳送給媒體播放器使用，所以授權憑證和數位內容是結合在一起的，以確保數位內容的安全及符合合理使用之目標。

4.2.3 安全機制

在 WM DRM、OMA DRM 及 TIRAMISU 等數位版權管理系統，對數位內容和授權憑證進行加密保護以外，並對使用者或設備進行身分證認，以確保數位內容之安全。本文所提之機制，利用對稱式加密技術對數位內容進行加密和以非對稱式加密技術對授權憑證加密，達到數位內容之安全性。利用公開金鑰基礎建設的架構，在數位家庭註冊階段、數位內容購買階段及數位內容使用階段對使用者、媒體伺服器及媒體播放器進行身分證認及識別，達到交易訊息在傳遞與交換過程中，滿足身分認證、機密性、資料完整性及不可否認性之安全需求。數位家庭使用數位內容時，媒體伺服器對數位內容進行解密時，媒體伺服器的 DRM 模組會將數位指紋伺服器產生的數位指紋以數位浮水印技術嵌入數位內容中，作為數位內容被非法傳播時追蹤非法傳播者之身分。

4.2.4 使用隱私

在 OMA DRM 及 TIRAMISU 系統架構並未提及使用者隱私權保護，而 WM DRM 系統有提供隱私權保護機制，但使用憑證時不需提供個人資訊，避免在授權憑證交易或使用過程中被洩露。而本文所提機制，使用者先以使用者識別碼向媒體伺服器註冊，然後由媒體伺服器以使用者識別碼及隨機產生的亂數計算產生使用者的匿名識別碼，作為使用者向授權憑證伺服器註冊之用。當購買者向授權憑證伺服器購買數位內容授權憑證時，將授權憑證授權給購買者的媒體伺服器，由媒體伺服器提供數位內容給數位家庭的所有使用者的媒體播放器使用，如此可避免因使用者直接使用數位內容而洩露個人資訊。

4.2.5 使用識別

WM DRM 及 OMA DRM 系統採用硬體設備資訊做為授權憑證識別碼，TIRAMISU 所提之數位版權管理系統採用使用者的智慧卡做為授權憑證識別碼。本文所提之機制，以使用者的媒體伺服器硬體資訊作為授權憑證識別碼，當授權憑證伺服器將數位內容授權憑證授權給媒體伺服器，供數位家庭內的使用者在媒體播放器使用數位內容。

4.2.6 數位家庭架構

WM DRM 及 OMA DRM 等數位版權管理系統，將數位內容直接授權給使用者或播放器，並未支援數位家庭架構；TIRAMISU 提出使用智慧卡及新的金鑰管理架構，以達到數位內容可在數位家庭的設備間使用。本文所提機制，由一個媒體伺服器和多個媒體播放器組成數位家庭領域，一個媒體伺服器可接受多個使用者及媒體播放器註冊。完成註冊後，使用者與媒體播放器可依授權使用數位內容，且可加入不同的媒體伺服器。

4.2.7 合理使用

在 WM DRM 及 OMA DRM 等數位版權管理系統，將授權憑證授權給設備，造成數位內容僅能在特定設備使用，無法達到在任何設備都可使用的目標；TIRAMISU 提出使用智慧卡及新的金鑰管理架構，以達到數位內容可在數位家庭的設備間使用，但是同時有多張智慧卡使用一個數位內容之問題。本文所提之機制，係由購買者向授權憑證伺服器購買授權憑證，再將數位內容及授權憑證授權及儲存於媒體伺服器中，當數位家庭註冊的使用者及媒體播放器提出數位內容的使用時段需求時，媒體伺服器將數位內容的使用權依時段授權給不同的媒體播放器，以達到任何時間、任何地點、任何設備皆可使用的合理保障。

4.3 系統效能分析

本文所提兩段式數位版權管理系統，係一新的架構模組，各階段的加解密及雜湊運算，均可採用現行的安全方法。為方便分析所提架構之計算成本，將各項計算複雜度所使用到的參數定義如下：TA：用公鑰加密系統對資料加密運算所花費的時間。TS：用私鑰加密系統對資料加密運算所花費的時間。TH：計算單向雜湊函數運算所需的時間。n：媒體播放器個數。表 3 為所提架構之計算複雜度。

五、結　論

數位家庭將是數位內容達到合法使用的一個平台，將數位內容提供給數位家庭內的授權設備使用，TIRAMISU 提出之數位家庭的數位版權管理系統，雖然可達到合理使用，卻無法保障數位內容提供者之所有權，發生使用者在同一時段，在不同設備使用同一個數位內容不合理的情形。

本文結合密碼學、身分認證、版權描述語言及數位浮水印…等技術，提出一個應用於數位家庭的數位版權管理機制，以兩段式數位版權管理架構，進行數位內容使用權利的管理。當購買者購買數位內容取得授權憑證後，將數位內容及授權憑證存放於媒體伺服器中，供已授權的媒體播放器使用。媒體伺服器負責數位家庭內的數位版權管理，依購買者所取得的數位內容版權及使用者的數位內容使用需求，將數位內容依使用時段授權給媒體播放器，媒體播放器依授權時段使用數位內容。除了符合數位版權管理系統的安全性及授權憑證可靠性外，更利用在數位家庭裡授權憑證的使用時間控管方式，管制數位內容在同一時間點，只有授權給一個設備使用，改進在數位家庭中無法控管使用數位內容數量的缺點。滿足數位版權管理系統之功能，達到數位內容具超傳播性、授權憑證具獨立性、數位內容具安全性、使用者使用具隱私性、唯一之使用識別及合理使用之需求。透過 MPGE-21 及數位家庭等的架構，有效整合支援數位版權管理架構的硬體及軟體。當共通的平台及軟硬體設備普及後，鼓勵購買者購買合法的數位內容，並賦予合理使用數位內容的權利，以減少盜版的數位內容，保障數位內容創作者的智慧財產權，有利於數位內容產業的發展。

表 3. 各階段之計算複雜度

項目	計算複雜度
數位內容封裝階段	TA + TS + 3TH
數位家庭註冊階段	4TA + TS + TH
購買者註冊階段	10TA
數位內容購買階段	7TA + TS
數位內容使用階段	nTS

參考文獻

[1] Internet Data Center, available at http://www.idc.com/, Jul. 2011.
[2] Windows Media Digital Rights Management, available at http://www.microsoft.com/windows/windowsmedia/tw/drm/, Jul. 2011.
[3] IBM EMMS, available at ftp://service.boulder.ibm.com/software/emms/pdfs/emms_brochure.pdf, Jul. 2011.
[4] Apple iTunes, available at http://www.apple.com/itunes/, Jul. 2011.
[5] InterTrust, available at http://www.intertrust.com/, Jul. 2011.
[6] Adobe, available at http://www.adobe.com/, Jul. 2011.
[7] Trimeche, M. and Chebil, F., "Digital Rights Management for Visual Content in

Mobile Applications," Control, Communications and Signal Processing, pp. 95-98, 2004.

[8] Raivio, Y. and Luukkainen, S., "Digital Rights Management in the Mobile Environment," International Conference on E-business, pp. 18-28, 2006.

[9] Yoon, E. J., Kim, J. S., Cho, B., H ., and Yoo, K. Y., "Efficient OMA DRM v2.0 ROAP for Protecting a Rights Object for a De- vice," Future Generation Communication and Networking Symposia, Vol. 2, pp. 9-13, 2008.

[10] Energy Conservation and Homecare Network, available at http://www.echonet.gr.jp/, Jul. 2011.

[11] Open Service Gateway Initiative, available at http://www.osgi.org, Jul. 2011.

[12] UPnP™ Forum, available at http://www.upnp.org/, Jul. 2011.

[13] Digital Living Network Alliance, available at http://www.dlna.org/home, Jul. 2011.

[14] Consumer Electronics Linux Forum, available at http://celinuxforum.org/, Jul. 2011.

[15] Ubiquitous Open Platform Forum, available at http://www.uopf.org/, Jul. 2010.

[16] Popescu, B. C., Crispo, B., Tanenbaum, A. S., and Kamperman, F. L. A. J., "A DRM Secu- rity Architecture for Home Networks," 4th ACM Workshop on Digital Rights Ma- nagement, pp. 1-10, 2004.

[17] Zhang, Z. Y., Pei, Q. Q., Ma, J. F., and Yang, L., "Security and Trust in Digital Rights Ma- nagement: A Survey," International Journal of Network Security, Vol. 9, No. 3, pp. 247-263, 2009.

[18] Zhang, L. L., Zhang, Z. Y., Niu, D. M., Shen, S., and Ye, C. Q., "A DRM System Based on PKI," 4th Genetic and Evolutionary Com- puting, pp. 522-525, 2010.

[19] Arnab, A. and Hutchison, A., "Fairer Usage Contracts for DRM," 5th ACM Workshop on Digital Rights Management, pp. 1-7, 2005.

[20] Jamkhedkar, P. A. and Heileman, G. L., "Di- gital Rights Management Architectures," Computers & Electrical Engineering Vol. 35, No. 2, pp. 376-394, 2009.

[21] Beekhuyzen, J., Jackson, M., Singh, S., and Waycott, J., "Fair Use and Users' Expe- rience of Sharing Music," 5th ACM Work- shop on Digital Rights Management, pp. 8-16, 2005.

[22] Digital Video Broadcasting Project, available at http://www.dvb.org/, Jul. 2011.

[23] Lee, J. S. and Yoon, K. S., "The System Integration of DRM and Fingerprinting," 8th International Conference on Advanced Communication Technology, Vol. 3, pp. 20-22, 2006.

[24] Mori, R. and Kawahara, M., "Superdistribution: the Concept and the Architecture," Transactions on the Institute of Electronics, Information and Communication Engineers, Vol. E73, No. 7, pp. 1133-1146, 1990.

[25] Open Mobile Alliance, available at http://www.openmobilealliance.org/, Jul. 2011.

[26] Marusic, B., Dobravec, S., Cuetos, P. d., Concolato, C., Piron, L., and Tasic, J.F., "TIRAMISU: A Novel Approach to Content Representation and Key Management for Seamless Superdistribution of Protected Media," Signal Processing: Image Communication, Vol. 20, No. 9-10, pp. 947-971, 2005.

[27] Meng, B. and Xiong, Q. X., "Research on Electronic Payment Model," 8th Computer Supported Cooperative Work in Design Proceedings, Vol. 1, pp. 597- 602, 2004.

[28] Sadeghian, M., Dadjou, S., Meghdadi, M., Safari, L., and Sadeghian, S., "The Design and Construction of an Intelligent Taxi Electronic Payment System," Intelligent Control and Automation, Vol. 2, pp. 413-417, 2011.

[29] Jiang, C. J. and Song, W. G., "An Online Third Party Payment Framework in E-Commerce," 2nd International Conference on Advanced Computer Control, Vol. 5, pp. 242-245, 2010.

[30] Po, C. C., Fong, S., and Lei, P., "On Designing an Efficient and Secure Card-based Payment System Based on ANSI X9.59-2006," IEEE International Workshop on Anti-counterfeiting Security Identification, pp. 427-430, 2007.