

三、發明人：(共 6 人)

姓 名：(中文/英文)

1. 吉登 艾拉薩
ELAZAR, GIDON
2. 丹 哈卡比
HARKABI, DAN
3. 奈禾米亞 維格頓
WEINGARTEN, NEHEMIAH
4. 艾弗拉罕 哈拉希米
HALACHMI, AVRAHAM
5. 諾雅 卡邁爾
CAMIEL, NOAM
6. 艾倫 富奇斯
FUCHS, ERAN

國 籍：(中文/英文)

- 1.-6.均以以色列 ISRAEL

四、聲明事項：

☐ 主張專利法第二十二條第二項 ☐ 第一款或 ☐ 第二款規定之事實，其事實發生日期為： 年 月 日。

☒ 申請前已向下列國家（地區）申請專利：

【格式請依：受理國家（地區）、申請日、申請案號 順序註記】

☒ 有主張專利法第二十七條第一項國際優先權：

1. 美國；2004年02月03日；60/541,279

2.

☐ 無主張專利法第二十七條第一項國際優先權：

1.

2.

☐ 主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號 順序註記】

☐ 主張專利法第三十條生物材料：

☐ 須寄存生物材料者：

國內生物材料 【格式請依：寄存機構、日期、號碼 順序註記】

國外生物材料 【格式請依：寄存國家、機構、日期、號碼 順序註記】

☐ 不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。

九、發明說明：

【發明所屬之技術領域】

本發明大抵有關數位權利管理。更明確而言，本發明有關遠端實施數位內容策略之方法。

【先前技術】

網際網路全球網路、以及其他資料通訊網路允許許多數位設備互接與交換資訊。數位設備包括個人電腦、膝上型電腦、平板電腦、PDAs、行動電話、MP3播放器、DVD播放器、遊戲機、例如數位照相機的數位記錄裝置等。網際網路與例如電纜與衛星的其他網路或公司或組織網路的特殊使用是要流通數位檔案，明確而言是數位內容檔案。

一數位內容檔案是具有能夠由末端使用者觀看、聆聽、閱讀、播放、執行或其它使用最終用途的資料，且在最終用途的某些點之前是以數字形式儲存及/或呈現。一數位內容檔案可為一音頻檔案、一視訊檔案、一軟體檔案、電子書、一文件、一電腦遊戲或其他類型的內容。

一版權數位內容檔案是在至少一最終用途上具有法律限制的數位內容檔案。例如，使用者在沒有接受來自版權擁有者的許可，對於版權數位內容檔案的其他最終用途，是不能夠建立複本、流通、修改、銷售、及/或執行。版權數位內容檔案的範例是商業電影、商業音樂、電子書、軟體、電腦遊戲等。

例如音頻與視訊的高品質多媒體檔案的原始數位呈現是使用高的資料取樣率將類比資訊轉變成數位資料。此呈現

會消耗大量儲存空間。例如，表示典型3分鐘長度音頻片段(clip)的一WAV格式檔案在大小上容易大於30百萬位元。當未壓縮時，一典型60秒視頻片段會佔用1.5 GB。在例如網際網路之類的網路上的轉移資料具有以金錢條件及以轉移資訊所需時間量來加以量化的成本。轉移愈大的檔案，需要更多的時間來轉移資料，且對於根據連接時間付費的連接而言，需要更多的成本。

為了要減少在網路上儲存及轉移數位多媒體檔案的時間與成本，本領域的專家設計複雜的演算法以將數位內容檔案壓縮成較小的檔案。雖然壓縮技術通常是減損(當解壓縮時，資料不能被正確復原)，但是音頻與視訊的標準壓縮與解壓技術會產生通常對人耳及/或眼睛而言差異可忽視的結果。好的壓縮技術可將一音頻檔案減少到最初大小的百分之十，且一視訊檔案可壓縮更多。舉前述30 MB的WAV編碼3分鐘歌曲為範例，一壓縮版本只佔用3 MB記憶體。

壓縮技術的最出名族系是整個稱為動畫專業組(MPEG)(參考 www.mpeg.org)。MPEG音頻壓縮技術的其中一支家族稱為MP3，簡稱動畫專業組音頻層3。

為了要在一電腦或MP3播放器上播放一MP3音頻檔案，可利用將檔案解壓縮及將一位元流傳送給驅動喇叭的音頻設備的軟體及/或硬體應用。此軟體的一範例是Nullsoft提供的Winamp(<http://www.winamp.com/>)。其存在提供例如微軟公司媒體播放器的音頻與視頻的應用

(<http://www.microsoft.com/>)。

在1990年代末期的網際網路與MP3壓縮的來臨造成音樂通路全球革命。建立對等系統，其中一人可將音樂從一CD複印到電腦，將他壓縮成MP3格式，然後透過在網際網路上傳送檔案而能與數十、數百與甚至數千人分享。提供數位音樂檔案分享應用基礎構造的一最著名軟體系統範例是Napster，且其與一家公司的名稱相同。因為系統多半用於分享版權音樂檔案，而不必將補償提供給藝術家與產生這些工作的記錄的公司，所以Napster被美國法院下令停工。雖然Napster的最初形式不再存在，但是許多類似服務至今大量存在，其中來自全球的使用者可分享包括音樂、電影、軟體應用、遊戲、與其他檔案的任何種類的數位內容。

自它開始以後，由於數位內容"海盜行為"而明顯銳減他們的收入，所以內容擁有者嘗試對抗此現象。到目前為止，例如記錄公司與電影攝影棚的內容擁有者已面對非常有限成功嘗試使用科技解決來解決這些問題。

雖然免費內容下載應用大量存在，但是例如音樂的數位內容付費服務最近亦出現例如 RealNetworks (<http://www.listen.com/>)、Apple(<http://www.apple.com/itunes/>)、與歐洲微軟公司MSN音樂俱樂部的廠商。使用者支付每首歌曲費用，然後下載到他們電腦，他們然後播放或複製到CDs或其他裝置。或者，使用者可簽署於特定時間無限制存取歌曲。這

些服務確實指定使用者檔案下載後的處理，但是他們可能做與檔案，但是不能成功實施指定的使用策略。

為了要去取未授權對象的版權數位內容的下載與分享，並根據執照屬行數位內容的使用，各種不同保護方法已被內容擁有者使用。通路控制與數位內容使用的集體項是數位權利管理(以下稱為DRM)。DRM系統典型包括永以在一內容儲存伺服器與一數位設備之間內容安全通路的加密方法。此方法典型需要設備包括加密演算法的實施及保持密鑰，為了要得到內容的存取。

在許多情況，用來提供數位內容的軟體應用可實施DRM的一些形式，當使用者嘗試存取數位內容時，DRM形式便能使用，例如用來檢視視訊檔案與聆聽音頻檔案的的微軟公司MediaPlayer已在DRM功能中建立。透過此應用執行的其中一操作是透過使用加密方法與密鑰的內容檔案解碼處理。為了要執行此操作，應用必須存取加密方法與密鑰；因此，加密方法與密鑰必須在應用所及範圍內存在。典型上，加密方法、密鑰、或兩者是存在應用、數位內容檔案本身、或在數位設備儲存中的某處。

例如電腦或PDA的數位設備典型是一開放平台，以允許電腦程式師發展程式。在某些情況，軟體程式的發展是為了設法處理及找出密鑰與一DRM系統的演算法，為了要設法規避DRM及獲得對內容的存取。此處理通常稱為一"攻擊"且如果成功，普遍稱為DRM系統的一"屏蔽"或"解開"密碼保護。執行此功能的電腦程式以下稱為一屏蔽或解開

密碼保護。

成功攻擊的範例在技術是已知的。在2001年，微軟公司媒體播放器是透過使用匿名 "Beale Screamer" (<http://news.com.com/2100-1023-274721.html?legacy=cnet>) 而被程式師解開密碼保護。

攻擊的其他形式包括使用程式工具。例如，在提供應用程式解碼後，軟體除錯器可追蹤及設陷數位內容資訊，以取回"受保護"的資訊。此資訊包括數位內容檔案與描述如何提供的元數據。解開應用程式密碼保護與釋放來自DRM系統的的攻擊程式允許最初數位內容檔案的未授權副本的建構。

同對策一樣，DRM系統使用更複雜的加密方法與編碼不易明瞭技術編。其他方法包括增加防竄改硬體以儲存密鑰。此方法的範例是由Rainbow Technologies Inc. 公司提供的例如 iToken 的加密符號。
(<http://www.rainbow.com/ikey/index.html>)或一智慧卡儲存密鑰與選擇性加密演算法。此解決在將資訊解密的處理中會洩漏密鑰；或者，內部執行加密功能，但是會以能夠被存取的原始形式洩漏最終的結果。

從前述內容保護方法發生的副作用是提供數位內容的軟體應用程式能透過實施前述加密方法與編碼不易明瞭而在保護處理中採用主動部分。既然內容保護實施必須保持秘密，所以只由發展軟體應用程式的組織知道。此外，內容本身必須使用密鑰與只由特殊實施知道的資料予以修正，

使特殊軟體應用程式只是可解密與提供內容的軟件。透過鍵入由特殊軟體應用程式所使用的內容，可利用來使用內容的數位設備類型與多樣性會侷限於發展應用程式組織決定支援的消費者電子設備類型與多樣性。

前述方法證明可減緩，但是不能停止敵手。藉由足夠時間與努力，可撰寫能夠解開一DRM系統保護的電腦程式。熟諳此技者瞭解到此成功的攻擊容易在允許程式師發展程式的一開放式環境執行的軟體應用程式上實施。同樣地，在解密後，加密協同處理器會置於內容容易受損壞。

在沒有控制而可局部有效避免數位內容檔案被複製與散播的另一方法是例如使用者的音頻與視訊的數位內容檔案流。在此情況，檔案未被下載儲存在一數位設備上，但是最好是非常類似一收音機節目的”廣播”。此可確保只有一小區塊的同意在每一特定時刻出現在數位設備上。此的底面是使用者在音樂節目或電影的整個持續時間必須連接到流來源或線上。對照於在數位設備儲存上儲存的檔案，流的另一問題是，已對內容流付費的使用者始終不能夠存取內容。內容流的另一缺點是現階段程式存在是用以記錄流內容及重建最初數位內容的數位副本，而不會對人眼或耳朵建立顯著的不同。

若要概述版權數位內容的流通與控制的既有解決問題，既有的技術可在易受解開密碼保護的開放式計算系統中儲存版權數位內容與提供軟體應用程式。透過將數位內容鍵入特殊格式與一特殊提供的軟體應用程式，用於數位內容

最終用途的不同類型數位設備數量是受限制。此外，內容流解決對於使用者是不方便，且容易設法規避。

清楚地，允許使用者持有與使用版權數位內容之系統、裝置、及方法是一未滿足的需求，但是在版權擁有者所指定的限制內。

【發明內容】

前述缺點與問題將透過本發明描述，並可透過閱讀下面說明而瞭解。

本發明的一目的是要提供一DRM裝置。

本發明的另一目的是要提供用以準備與一DRM裝置使用的版權數位內容之方法。

在仍然本發明的另一目的中，透過使用一DRM裝置提供用以流通及提供版權數位內容之方法與系統。

在一些具體實施例中，下列步驟會發生。在流通前，最初的版權數位內容會被處理，以產生兩個或多個部分(此後稱為檔案)，使得每一分開不能充份用於版權數位內容的最終用途。將版權數位內容處理成兩個檔案將在下面詳細描述。兩個結果處理檔案可被組合成壓縮與加密的一致性檔案，為了要在網路上流通。在一些具體實施例中，一致性檔案包含額外的資料。一致性檔案能以連接的一DRM裝置而在網路上流通到一數位設備。接收的一致性檔案是儲存在DRM裝置。DRM裝置將一致性檔案分成兩個檔案。在適當時間，一檔案、或一檔案的區段能被傳送數位設備供處理，且第二檔案、或第二檔案的區段是在DRM裝

置內部處理。在適當時序上，此處理的結果會被組合在 DRM 裝置、或在數位設備中，以產生末端使用者可使用的資料與內容。在此處理期間既沒有在數位設備上可用的最初內容完整組、亦沒有用來產生在數位設備上可用內容的處理演算法完整組；因此，開啟解開密碼保護的可能性。

DRM 裝置可處理例如屆滿、有限使用數、複製策略、與用以在數位設備上提供檔案內容的其他使用策略。如果不允許使用者使用某版權數位檔案內容，那麼提供處理不會發生。

【實施方式】

在下面本發明具體實施例的詳細描述中，將參考描述實施本發明特殊具體實施的附圖。熟諳此技者將瞭解到其他具體實施例可實施，而不脫離本發明的精神；因此，未侷制於下列本發明的詳細描述。

圖 1 是 DRM 裝置硬體 110 的一具體實施例圖，其包括一中央處理單元 (CPU) 112、一選擇性系統記憶體 113、一選擇性協同處理器晶片 119、一選擇性非揮發性儲存 114、與將裝置 110 連接到一數位設備 120 的一介面 115。當有選擇性只有一或複數個系統記憶體 113 或非揮發性儲存 114 時，只有一或複數個中央處理單元 112。只有一或複數個介面 115；本發明並不限於此。非揮發性儲存 114 包括在中央處理單元 112，或從中央處理單元 112 分開；通常，DRM 裝置硬體 110 的一些元件或子元件能與 DRM 裝置的其他元件或子元件組合，以供較高的整合及可能降低成本。

中央處理單元112可為具專屬功能的一般用途中央處理單元或一中央處理單元。此外，中央處理單元112包括內部記憶體、與內部非揮發性儲存，且其在本發明的描述中，可分別用於系統記憶體113、及/或非揮發性儲存114的類似目的。中央處理單元112、非揮發性儲存114、及其他元件能夠以一防止竄改的硬體予以實施；或者，中央處理單元112、非揮發性儲存114、及其他元件的一些部份可為防止竄改；本發明並不限於此。

非揮發性儲存114可為數種類型儲存之任一者，包括以半導體為主之媒體，例如唯讀記憶體(ROM)、電可抹除程式規劃唯讀記憶體(EEPROM)、快閃記憶體或電池備援隨機存取記憶體(RAM)；或磁媒體儲存，例如硬碟或軟碟等；或者，其他類型非揮發性儲存，但是本發明並不限於此。

在實際溝通觀點中，介面115可連接DRM裝置110與一數位設備120。實際的觀點可為例如直接經由一條或多條電纜、及/或無線。介面115的溝通觀點允許資料在DRM裝置與數位設備之間交換。介面115可為數種類型介面的任一者，例如PCI、ISA、萬用串列匯流排(USB)、FireWire、IDE、SCSI、RS-232、或其他串列介面、並列介面、快閃記憶(CF)介面、Sony記憶棒介面、多媒體卡(MMC)、安全數碼(SD)、迷你安全數碼、尖端映像記憶技術(xD)、藍芽、InfiniBand、行動電話介面、PDA介面、及/或可用來連接一DRM裝置與一數位設備的任何其他類型介面。

數位設備120可由一或多個數位內容檔案的一些最終用途的末端使用者使用。數位設備120可為數種類型裝置之任一者，例如一個人電腦、膝上型電腦、平板電腦、PDA、行動電話、mp3播放器、DVD播放器、個人視訊播放器、可程式規劃消費者電子、或能與數位內容使用的任何其他裝置。

非揮發性儲存114包含能由中央處理單元112執行的一些指令。非揮發性儲存114尚包含：一選擇唯一裝置序號，例如唯一對公眾與私人密鑰與一簽署確實證明之認證方法。在非揮發性儲存114中儲存的指令允許數位設備120經由介面115存取一部分的非揮發性儲存114，但是要避免存取非揮發性儲存114的另一部分，包括儲存私人密鑰的部份、與儲存在不允許使用者存取的一封閉環境中執行指令的部份。非揮發性儲存亦儲存供認證的複數個方法；本發明並不限於此。

選擇性協同處理器晶片119可連同中央處理單元112處理與格式化最終用途的內容，例如音頻、視訊、遊戲等內容，如此可達成較高的計算能力。協同處理器晶片119可不處理、處理一些、一部份、或全部的數位內容，本發明並不限於此。

用來解碼視訊的協同處理器晶片的範例是用於Sigma Designs公司的機上盒設備與媒體閘道器之EM8485 MPEG-4解碼器(<http://www.sigmadesigns.com/products/em8485.htm>)。

圖2是系統的具體實施例圖，該系統包具一介面215的

DRM裝置210；具一介面221的數位設備220，且該介面221能符合DRM裝置210介面215；一使用者介面222，該使用者介面222可提供給使用者的處理數位內容(例如一視訊、視覺影像、合成音頻、合成視訊遊戲或其他形式)；一網路230；一內容伺服器240，其可為能在網路上傳送數位內容的一電腦；與一授權伺服器250，其可為在網路上傳送認證及/或解密及/或策略及/或格式化資訊的一電腦。根據一具體實施例，此資訊是被嵌入在一或多個檔案。根據一些具體實施例，沒有、一些或全部的數位內容可能有版權，本發明並不限於此。系統包括複數個DRM裝置210、數位設備220、內容伺服器240與授權伺服器250，本發明並不限於此。

介面221可連接數位設備220與DRM裝置210。介面221可為用來連接一裝置與一數位設備的數種類型之任一者。數位設備220的介面221能符合DRM裝置的介面215類型，且是允許資訊在DRM裝置210與數位設備220之間傳遞的一形式。

內容伺服器240是能經由網路230，例如網際網路，以存取的一電腦。內容伺服器240能回應請求以下載版權數位內容例如視訊、音頻、電子書、軟體、遊戲等。

授權伺服器250是能經由網路230，例如網際網路，以存取的一電腦。一授權伺服器250能回應請求以下載資訊，例如認證及/或解密及/或策略及/或格式化資訊。此資料包括：DRM裝置策略使用的策略定義、DRM裝置格式化器

使用的格式化定義、DRM裝置解密器使用的解密定義、DRM裝置驗證設備使用的認證定義、數位內容檔案、數位內容檔案部分、有關使用者的資訊、有關數位內容檔案或數位內容檔案部分的一或多個最終用途權利的資訊(使用者可存取所有可能的最終用途、或少於所有可能的最終用途)、有關係統的廠商/擁有者/操作員的資訊、有關特殊DRM裝置210的資訊、及其他資訊。資訊可由DRM裝置210及/或數位設備220使用。當使用者進行數位內容的最終用途或準備允許使用者進行數位內容的最終用途時，資訊便可使用。

根據一些具體實施例，內容伺服器240與授權伺服器250能夠以經由網路互接及不直接互接的分開實體加以實施。根據其他具體實施例，內容伺服器240與授權伺服器250是直接互接。根據其他具體實施例，內容伺服器240與授權伺服器250是以單一的實體實施，本發明並不限於此。

在一DRM裝置210中實施的驗證設備是在網路上加入一遠端伺服器的DRM裝置驗證處理。驗證設備可實施數個驗證方法之一，包括將裝置ID編號傳送給遠端伺服器。另一驗證設備使用只由DRM裝置210與伺服器知道的一密鑰，並根據挑戰DRM裝置210的驗證，為了要確認它是否佔有密鑰。在此一驗證處理的一些具體實施例中，伺服器可將一加密訊息傳送給DRM裝置210，且驗證設備至少解碼訊息，並將它傳回伺服器。在一些具體實施例中，相同的密鑰能夠以多種方法用來驗證，例如，透簽署一純文字訊息

及/或解碼一加密的訊息。在一些具體實施例中，驗證設備可透過執行一連串操作而回應挑戰，例如訊息解密、結果處理、結果加密、及將它傳回伺服器供驗證。對於發生的驗證處理而言，密鑰能在驗證處理前儲存在DRM裝置210。儲存的密鑰可在所有DRM裝置上同樣儲存的單一密鑰，或每一DRM裝置210之唯一的專屬密鑰。在後者情況，伺服器應該預先知道那一密鑰是儲存在DRM裝置。

驗證的另一方法是使用一公用與私人密鑰與一數位簽章。在此一具體實施例中，驗證設備具存取在DRM裝置210中儲存的一私人密鑰與一符合的公用密鑰。私人密鑰必須保持秘密，但是公用密鑰便要公開。伺服器然後使用以DRM裝置210公用密鑰予以加密的一訊息來挑戰驗證設備，以確保它能存取符合的私人密鑰。在一些具體實施例中，驗證設備簽署一份訊息，但是不必然要將訊息加密。或者，伺服器可從DRM裝置210接收一數位簽章，此數位簽章包含裝置識別資訊，例如裝置序號或裝置及/或裝置的公用密鑰、及/或有關裝置、伺服器、的額外資訊、操作系統或任何其他資訊的組織。DRM裝置210識別資訊是透過信賴的權威者進行數位簽章，例如裝置的廠商、伺服器的擁有者、操作系統的組織、及/或形成裝置數位簽章的另一信賴權威。驗證設備的一些具體實施例可驗證DRM裝置210及/或DRM裝置210的使用者。

DRM裝置210中的解密器是加入將加密的數位內容或一部份的數位內容轉換成一解密形式的處理。一解密器可實

施一或多個數種方法：例如 DES、3DES、AES、與 IDEA；及/或非對稱演算法，例如 RSA、Diffie-Hellman、橢圓曲線、及/或其他。一解密器可實施一或複數個解密方法。一解密器包括混雜演算法，例如 DSA、MD2、MD4、MD5、HMAC及/或 SHA1、及/或其他，以取回一簽署，並檢查接收資料的起源與完整性。用於此操作的解密密鑰或複數個解密密鑰可在一或複數個來源中開始。例如，例如經由數位設備 220 而從數位設備 220 接收、及/或從一網路伺服器接收的解密密鑰資料是儲存在 DRM 裝置 210 的非揮發性儲存中。在一些具體實施例中，DRM 裝置 210 可接收至少部分解密的數位內容。在此具體實施例中，顯然地，解密器可以或不能處理已解密的部分。解密器可至少部分解密，例如，完全解密一部分的數位內容檔案、及/或執行一或多個解密步驟；對於整個或部分數位內容而言，其可為完全的解密處理或者一部分的完全解密處理。在一些具體實施例中，數位內容可至少部分未加密接收。

在 DRM 裝置 210 中的策略是加入確認數位內容或部分數位內容最終用途的適任處理，以允許或不允許一些操作，例如到解密、格式化、搜尋、及/或將輸出傳送數位設備。確認可檢查一或數個適任選項，包括使用數位內容之權利、使用多達某日的數位內容之權利、使用在某日期間的數位內容之權利、使用在某日期後的數位內容之權利、使用某累積使用時間的數位內容之權利、使用某次數的數

位內容之權利、傳送數位內容之權利、修改數位內容之權利、將重疊資訊加入數位內容之權利、將數位內容儲存在DRM裝置210及/或另一位置之權利、將重疊資訊儲存在裝置及/或另一位置之權利、複製數位內容之權利、複製一些部分數位內容之權利、複製特殊部分數位內容之權利、與有關數位內容的最終使用或流通的末端使用者之其他權利。這些能透過產生可能是一或多個可能動作結果的策略而被檢查，其中這些可能動作可為例如允許輸出傳送數位設備220、不允許輸出傳送給數位設備220、抹除數位內容檔案或部分的數位內容檔案、及/或允許或不允許一些操作，例如當在數位內容最終使用時使用者可執行的搜尋、編輯、儲存、及其他操作。

在DRM裝置210中的格式化器是加入提供使用者最終用途的數位內容使用者使用。在一些具體實施例中，在選擇性協同處理器晶片119可用的場合，格式化器可將協同處理器晶片當作它一部分格式化操作使用；本發明並不限於此。

在一些具體實施例中，數位內容是至少一編碼數位音頻檔案，例如MP3、MP3-pro、Ogg-vorbis、AAC、DTS、Dolby、ADPCM、WMA等(有關數位音頻格式的取樣清單，請參考<http://sox.sourceforge.net/AudioFormats.html>)。格式化器可如同部分的提供處理而將數位內容解碼，例如將一編碼的MP3檔案轉換成稍後提供給能呈現給使用者最終用途的音頻信號之一解碼的原始WAV檔案。在其他具體實

施例中，在數位內容是至少一編碼的數位音頻檔案的場合，格式化器只能部分解碼檔案。在一些具體實施例中，在數位內容是至少一編碼的數位音頻檔案的場合，格式化器可處理一或多個檔案以產生用於提供音頻的一輸出，例如，檔案可包含描述在目標音頻中某些頻率或振幅的資料。

在一些具體實施例中，數位內容是至少一編碼的數位視訊檔案，例如 MPEG1、MPEG2、MPEG4、WMV、DIVX、XVID、3IVX、H.263、H.264、Quick time 6、Real、視窗媒體等（有關數位視訊格式的取樣清單，請參考 http://www.webopedia.com/Multimedia/Video/Video_Formats/）。

格式化器可如同一部分提供處理而解碼數位內容，例如將編碼的 MPEG2 檔案轉換成一解碼的 YUV 檔案。在其他具體實施例中，在數位內容是至少一編碼的數位視頻檔案的場合，格式化器只能部分解碼檔案。在一些具體實施例中，在內容是至少一編碼的數位視頻檔案的場合，格式化器可處理一個或多個檔案，以產生用於提供視頻的一輸出，例如，檔案可包含描述影響目標視訊呈現的某些訊框或在訊框中色彩的資料。

在一些具體實施例中，在內容是至少一軟體應用程式或一遊戲的場合，格式化器可產生一些屬性，例如影像、執行時間碼或用來建立或想像一軟體情節或遊戲場景的演算法輸出。

在一些具體實施例中，內容是至少一數位書、或一部分

的數位書，且格式化器可至少從供它呈現內容的產生一配置圖。在格式化器的其他具體實施例中，數位內容是至少一數位書、或一部分的數位書，且格式化器是至少從內容產生一影像。

數位設備 220 可經由介面 221 而從 DRM 裝置 210 接收資料，並將資料傳送給他。數位設備 220 可處理資料。數位設備 220 可準備供提供的數位內容檔案。數位設備 220 可例如透過在一電腦螢幕上顯示電子書的一頁、或將音頻信號傳送給音頻處理電子與最後是喇叭，而實質提供數位內容。

圖 3 是準備與一 DRM 裝置 110 使用的一原始數位音頻或視訊內容檔案 C 的一方法流程圖。原始數位內容檔案準備的實施包括壓縮數位內容的步驟，為了使數位內容檔案佔用較少的儲存空間，並在傳送時，消耗較少的網路資源。

在準備與一 DRM 裝置使用的數位內容檔案中，會有數個假設。首先，如果整個數位內容檔案 C 隨時在一數位設備上完全出現，它將會是有間隙；因此，在至少部分的數位內容檔案必須始終儲存在別處，明確而言是在 DRM 裝置。其次，對於成本減少目的而言，DRM 裝置可能具有比主機數位設備較弱的計算能力。此表示 DRM 裝置不能夠執行需要的所有計算以準備檔案 C 呈現。因此，當準備供呈現的內容檔案 C 時，部分的資料處理必須在主機數位設備上執行。

在步驟 301 中，內容 C 是以原始數位形式當作檔案 C 存在

以預備提供。在一些具體實施例中，內容C是一文件、影像、音頻檔案、視訊檔案、軟體、遊戲、前述的部份或組合、或任何其他類型數位內容，本發明並未受此限制。

在步驟302中，檔案C可被處理以產生檔案A與B，使得存在轉換 $f()$ 、 $g()$ 、 $h()$ ：

$$C \approx F = f(g(A), h(B))$$

其中在檔案 $g(A)$ 與 $h(B)$ 上的執行的復合演算法 f 將會產生 F ，且 F 是原始檔案 C 的一相同副本或一幾乎相同檔案(人的視覺、聲音及其他知覺)。相較於由末端使用者所使用的最初內容檔案 C ，一幾乎相同副本檔案 F 是可提供具最小品質降低或沒有品質降低的一檔案。檔案A與B是取自最初檔案 C 的數位內容檔案，但是在它自己上的每一者沒有當作一適度可提供數位內容檔案使用處理所需的決定性資料。透過使用轉換 $f()$ 、 $g()$ 與 $h()$ ，檔案A與B可在檔案 F 中重建。

在一些具體實施例中，檔案A是用於在數位設備上的處理，且檔案B是用於在DRM裝置中的處理。在此情況，數位設備沒有可用的檔案B。

根據一些具體實施例，轉換 $f()$ 可重製最初檔案 C 的正確副本，使得：

$$C = F = f(g(A), h(B))。$$

檔案A與B與轉換 $f()$ 、 $g()$ 、 $h()$ 可被調整成不同類型的內容調整，本發明並未受此限制。

一最初視訊檔案 C 的範例是以未壓縮視訊格式等的YUV

家族格式化的一檔案。

在一些具體實施例中，對於包含一版權電影的數位內容檔案C而言，劃分檔案C的範例可為包含視訊資訊的至少一處理形式之檔案A、與包含音頻資訊的至少一處理MPEG形式之檔案B，其中檔案A是不包含任何音頻的至少一壓縮MPEG形式，且檔案B是至少符合壓縮的音頻。

在視訊檔案C是以未壓縮視訊格式的YUV家族格式化的一些具體實施例中，檔案A包含至少Y與U通道，且檔案B至少包含V通道。

在檔案C是一視訊檔案的一些具體實施例中，檔案B包含檔案C的一編碼形式的至少一些密鑰訊框，且檔案A包含至少訊框間，且訊框間包括產生檔案F所需的其餘資訊。

在一些具體實施例，有關音頻檔案C與視訊檔案C的音頻部分是檔案A，其包含能使用在F再生的至少某音頻範圍；與檔案B，其包含其餘的頻率範圍。

在一些具體實施例，有關音頻檔案C與視訊檔案C的音頻部分是檔案A，其是與虛擬資料一起填入，且檔案B可保持移除虛擬資料所需的所有資訊。

在數位內容檔案C是時間導向的一些具體實施例中，檔案A可為檔案C的一時間混合版本，其中每一混合片段是數秒中長。在此情況，檔案B包含未混合檔案A的所需的資訊。每一混合片段的長度可小於、等於、或大於數秒鐘，本發明並未受此限制。每一混合片段的長度可不同，

本發明並不限於此。

在數位內容檔案是時間導向的一些具體實施例中，除了具有遺失的片段之外，檔案A是類似檔案C。遺失的片段可構成檔案B。可瞭解到，愈多的檔案A遺失片段，便有較低的可用檔案A。

在數位內容檔案C是時間導向的其他具體實施例(例如MP3格式的一WAV音頻檔案編碼)中，相等持續時間的訊框能被壓縮成MP3格式。在本發明中，WAV格式的檔案C是被分成略長於正常訊框大小的長度。與正常相同大小的訊框部分能被編碼成MP3並儲存在檔案A。其餘部分是以沒有壓縮的WAV格式儲存在檔案B。沒有檔案A或檔案B可被分開使用。嘗試只根據檔案A聆聽歌曲將會在每一訊框的結束上造成略微跳躍。

在檔案C是一軟體應用程式或一遊戲的一些具體實施例，檔案A包含在DRM裝置上執行的碼，而檔案B包含在數位設備上執行的碼。檔案A與檔案B需要同時執行，為了使軟體應用程式或遊戲正常發揮功能。在DRM裝置上執行的檔案A的碼是未決定的。在檔案A中的碼是軟體應用程式的一中央部分，所以它不能夠由在數位設備上執行的檔案A中的其他電腦程式設計者的碼所取代。

熟諳此技者瞭解到有各種不同方法處理將一檔案C處理成檔案A與檔案B，而不致脫離本發明的精神。處理可透過組合一起而可將最初檔案C的相同副本或幾乎相同副本重製的單一或複數個轉換達成；本發明並未受此限制。熟

諸此技者瞭解到檔案C可被分成超過兩個檔案A與B，例如，一連串的檔案 $A_1 \dots A_n$ 、 $B_1 \dots B_m$ 與轉換 $g_1() \dots g_l()$ 與 $h_1() \dots h_k()$ ，而不脫離本發明的精神。

在步驟303中，檔案A與B可使用更多的資訊以選擇性修改及選擇性進一步處理。在一些具體實施例中，一封裝檔案P中的檔案A、B與一些改善是相同的。

在一些具體實施例，額外資訊可為有關數位內容C的詮釋資料，例如標題、建立者、大小、版權通知、與描述數位內容C的任何其他類型資訊。在一些具體實施例中，額外的資訊可為描述最終用途可在內容上實施的內容使用策略。在一些具體實施例中，額外的資訊可為描述最終用途能於使用一指定DRM裝置的內容上實施的內容使用策略。在一些具體實施例中，額外的資訊可為描述最終用途能於連接到一指定數位設備的一指定DRM裝置上實施的內容使用策略。在一些具體實施例中，一浮水印可應用。在一些具體實施例中，檔案P可為例如加密的進一步處理。

圖4是透過使用DRM裝置110而提供一數位內容檔案的範例方法流程圖。

在步驟401中，檔案P是經由一網路而流通到DRM裝置，且該DRM裝置是連接至一主機數位設備。

在步驟402中DRM裝置可從檔案P擷取檔案A與檔案B。此能遵從使用者請求以使用內容；或者，只要接收檔案P便立即執行；或者，由於任何其他觸發事件或在任何時刻執行；本發明並不限於此。

在步驟403中，DRM裝置應用可基於指定的請求而檢查使用策略。在DRM裝置應用中的使用策略可加入確認內容檔案或一部分內容檔案的最終用途的適任處理，以允許或不允許一些操作，例如解密、格式化、及/或將一輸出傳送給數位設備。確認可檢查一個或數個適任選項，包括使用內容檔案之權利、使用多達某日的內容檔案之權利、使用在某日期間的內容檔案之權利、使用在某日期後的內容檔案之權利、使用某累積使用時間的內容檔案之權利、使用某次數的內容檔案之權利、轉移內容檔案之權利、及內容檔案最終用途的末端使用者有關的其他權利。這些可透過策略檢查，以產生可能是一個或多個可能動作的結果，這些可能動作可例如允許輸出傳送到數位設備、不允許輸出傳送到數位設備、抹除內容或部分內容、及/或當在內容檔案最終用途時，使用者可執行的其他操作。如果允許使用者存取內容檔案，步驟404便會開始。如果不允許使用者存取內容檔案，便會通知使用者，且序列會結束。

在步驟404中，DRM裝置將檔案A傳送到主機數位設備供計算 $g(A)$ 。

在步驟405中，DRM裝置處理檔案B以產生 $h(B)$ ，且主機數位設備處理檔案A以產生 $g(A)$ 。

在步驟406中， $g(A)$ 是從主機數位設備傳送到DRM裝置。

在步驟407中，DRM裝置是計算 $F=f(g(A), h(B))$ 。

在一些具體實施例中， $h(B)$ 是從DRM裝置傳送到主機數

位設備供計算 $F=f(g(A), h(B))$ 。

在步驟408中，檔案F是準備用於最終用途。

熟諳此技者了解到在格式化處理期間沒有檔案B是在數位設備220上出現。

熟諳此技者了解到將檔案C劃分成檔案A與B允許DRM裝置210在格式化處理中管理數位設備220的計算功率。此會造成一較低成本的中央處理單元112，而且也許是DRM裝置210的其他元件。

根據一些具體實施例，DRM裝置220的內部處理是將額外資料加入重新組合的版權數位內容檔案F。在一些具體實施例中，一數位浮水印可被加入。在此階段上加入一數位浮水印允許將裝置的唯一識別使用在浮水印，如此稍後允許版權內容流通的裝置識別。

在一些具體實施例中，額外的資料是被加入檔案只為了將它擴大。檔案F的流通將會是更困難或高成本。一範例是將一檔案從500 MB擴大到1000 MB。一500 MB檔案可被燒入CD；然而，擴大的檔案不可能由於限制在大約700 MB的一CD容量。檔案F是透過使用額外的虛擬資料將它填塞而擴大。

在一些具體實施例中，轉換 $f()$ 、 $g()$ 、與 $h()$ 可能會降低至少一部分的數位內容。

在一些具體實施例，在內容是一軟體應用程式或一遊戲的場合，轉換 $h()$ 可取決於來自數位設備的輸入，例如遊戲狀態；與在某時間或事件上來自使用者的輸入。在一些具

體實施例中，轉換 $h()$ 包括一些演算法，以根據前述來自數位設備的輸入而產生能由應用的資料。雖然本發明是參考特殊具體實施例描述，但是不構成限制。各種不同變更與修改可達成具體實施例，而不致脫離從本發明的範圍或精神。

【圖式簡單說明】

前面與其他目的、觀點與優點可從以上本發明具體實施例連同附圖的詳細描述而更加瞭解，其中：

圖1是DRM裝置的一具體實施例方塊圖；

圖2是系統的一具體實施例方塊圖；

圖3是用以準備與DRM裝置使用的一數位內容檔案之方法流程圖；

圖4是透過使用DRM裝置而提供一數位內容檔案的方法流程圖。

【主要元件符號說明】

110, 210	數位權利管理(DRM)裝置硬體
112	中央處理單元
114	非揮發性儲存
113	系統記憶體
119	協同處理器晶片
115, 215, 221	介面
120, 220	數位設備
222	使用者介面
230	網路

240

内容伺服器

250

授權伺服器

五、中文發明摘要：

多種不同具體實施例包括控制版權數位內容的流通與使用之裝置、系統、及方法。

六、英文發明摘要：

十一、圖式：

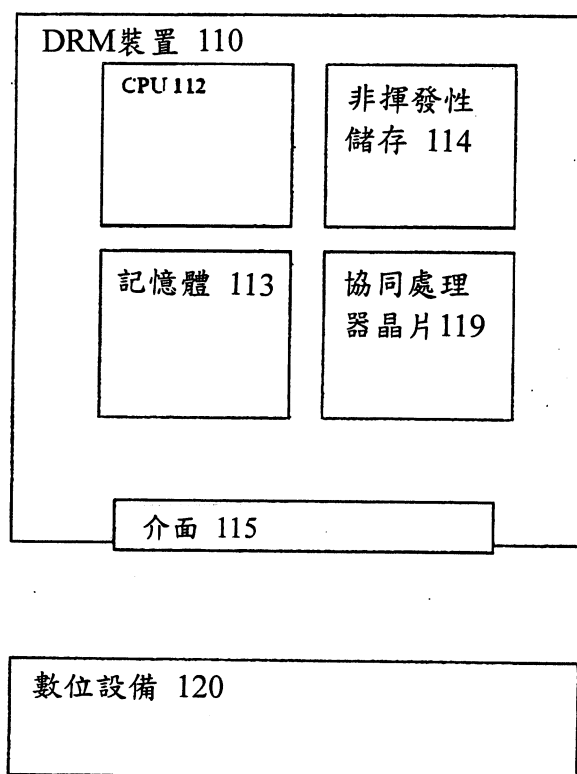


圖 1

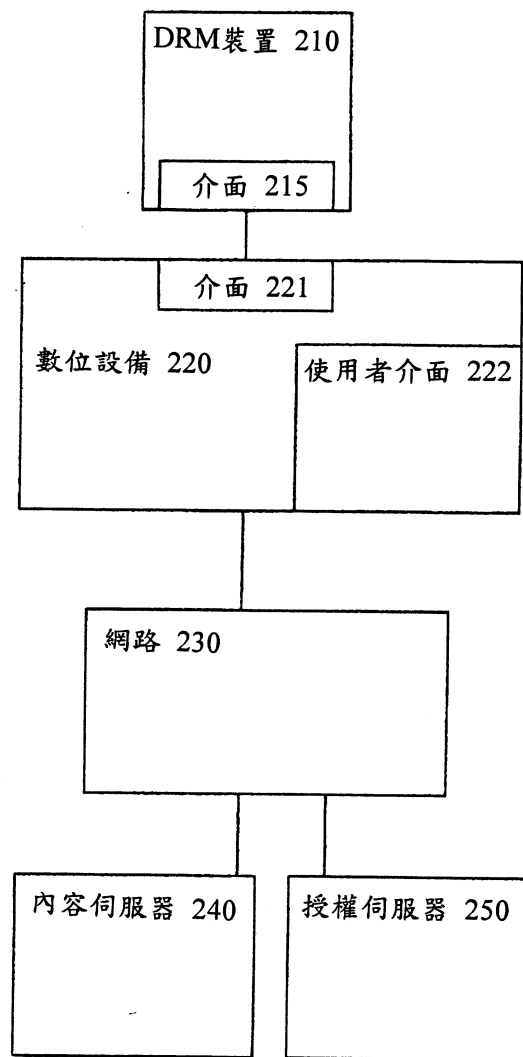


圖2

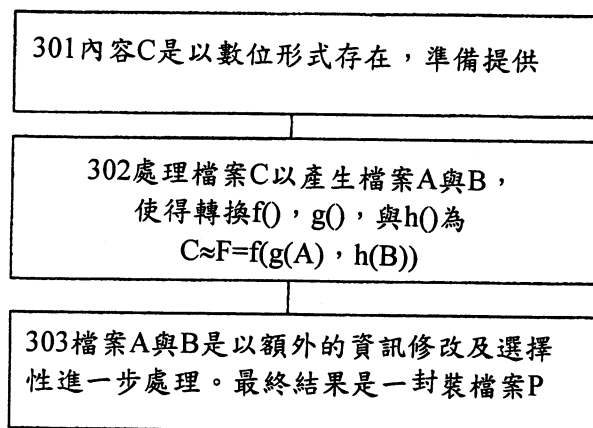


圖3

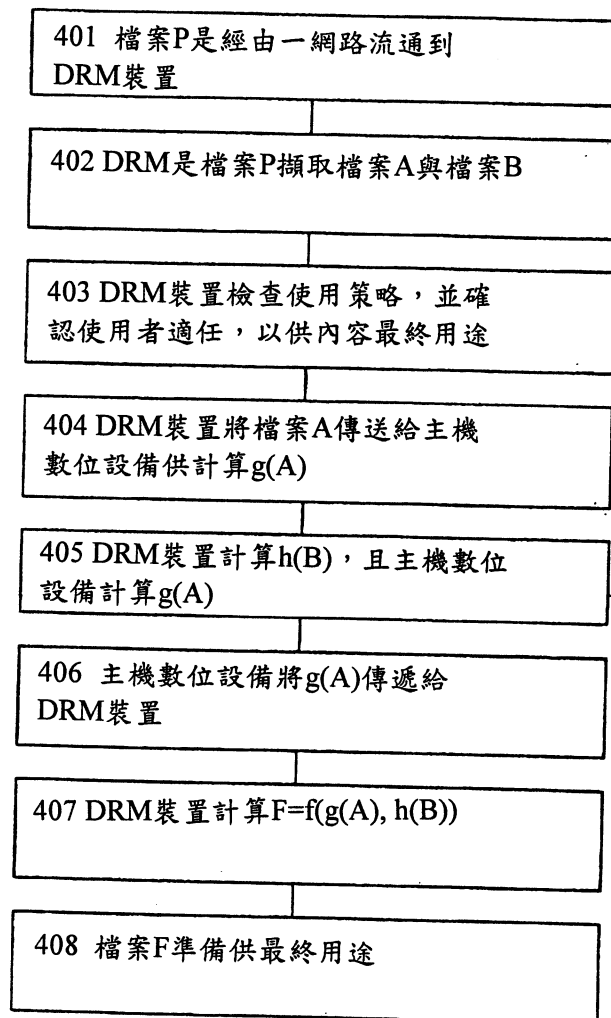


圖 4

七、指定代表圖：

(一)本案指定代表圖為：第 (3) 圖。

(二)本代表圖之元件符號簡單說明：

(無元件符號說明)

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

(無)

發明專利說明書

中文說明書替換頁(96年8月)

(本說明書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫)

※ 申請案號：094103425

※ 申請日期：94.2.3.

※IPC 分類：G06F ^{1/00} (2006.01)

一、發明名稱：(中文/英文)

溝通數位資料之方法，處理資料檔案之方法及數位權利管理模組
METHOD OF COMMUNICATING DIGITAL DATA, METHOD OF
PROCESSING A DATA FILE AND DIGITAL RIGHTS
MANAGEMENT MODULE

二、申請人：(共 1 人)

姓名或名稱：(中文/英文)

美商桑迪士克安全內容方案公司

SANDISK SECURE CONTENT SOLUTIONS, INC.

代表人：(中文/英文)

1. 羅伯特 W 希特

HIRT, ROBERT W.

2. 茱蒂 布朗納

BRUNER, JUDY

住居所或營業所地址：(中文/英文)

美國加州桑尼貝市卡斯本可特140號

140 CASPIAN COURT, SUNNYVALE, CA 94089, U. S. A.

國 籍：(中文/英文)

美國 U.S.A.

十、申請專利範圍：

1. 一種在一通訊網路上溝通數位資料之方法，其包含：
將該數位資料分成至少第一與第二資料單元；
在一通訊網路上傳送該等資料單元；
在至少第一與第二電子系統的不同個別之一個或多於一個中，處理在通訊網路上所接收資料的該等至少第一與第二單元；
將在該第一電子系統中被處理的資料單元予以組合；及使用在該第二電子系統中該等被組合之資料單元。
2. 如請求項1之方法，其中該數位資料包括具有視頻與音頻部份的多媒體資料，而且其中該第一單元包括沒有該音頻部份資料的視頻部份壓縮資料，且該第二單元包括該音頻部份的壓縮資料。
3. 如請求項1之方法，其中該數位資料是具有複數個部份的一視頻信號，而且其中該第一單元包括少於所有部份的資料，且該第二單元包括其他該等部份的資料。
4. 如請求項1之方法，其中該數位資料包括編碼的資料訊框，而且其中該第一單元包括其至少一些密鑰訊框，且該第二單元包括其餘訊框間。
5. 如請求項1之方法，其中該數位資料包括一音頻信號的資料，而且其中該第一單元包括至少某音頻範圍的資料，且該第二單元包括其餘音頻範圍的資料。
6. 如請求項1之方法，其中該數位資料包括一音頻信號的資料，而且其中該第一單元包括音頻資料加上虛擬資

料，且該第二單元包括將該虛擬資料從該第一單元移除所需資訊的資料。

7. 如請求項1之方法，其中該數位資料是一時間導向信號，而且其中該第一單元包括數位資料的一時間混合版本，且該第二單元包括解混合該第一單元之資料所需資訊的資料。
8. 如請求項1之方法，其中該數位資料是一時間導向信號，而且其中該第一單元包括遺失其片段的數位資料，且該第二單元包括該等遺失片段的資料。
9. 如請求項1之方法，其中該數位資料是一編碼的WAV音頻檔案，並分成長於一特定長度的資料訊框，而且其中該第一單元包括該等訊框之特定長度的資料，且該第二單元包括該等訊框的其餘資料。
10. 如請求項1之方法，其中該數位資料是軟體，而且其中該第一單元包括能由該第一電子系統執行的軟體碼，且該第二單元包括能由該第二電子系統執行的軟體碼。
11. 一種處理一資料檔案之方法，該方法在一連接一數位設備與一數位權利管理(DRM)裝置的組合中，用以處理經由該數位設備接收之資料檔案，其包含：

以至少第一與第二分開的資料單元的形式接收該檔案資料；

處理在DRM裝置中資料的該第一資料單元與在該數位設備中資料的該第二資料單元；

在該DRM裝置中將該等被處理之第一與第二資料單元

予以組合；及

使用在該數位設備中的該被組合資料。

12. 如請求項11之方法，其中該處理包括將該等第一與第二資料單元之至少一者予以解碼。

13. 如請求項11之方法，其中該等透過數位設備接收的第一與第二資料單元被加密，而且其中該處理包括將在該DRM裝置中該第一資料單元予以解密，及將在該數位設備中的該第二資料單元予以解密。

14. 如請求項11之方法，其中該DRM裝置是可移去地與該數位設備連接。

15. 一種數位權利管理(DRM)模組，其包含：

一微處理器；

一半導體記憶體；

一介面，用以與該模組進出溝通資料；及

該DRM模組的功能可：

可從經由該介面接收的一資料檔案擷取至少第一與第二部分；

處理該被接收資料檔案的該第一部分以形成一被處理的第一部分；

經由該介面而傳回該被接收資料檔案的該第二部分；

在處理之後，經由該介面而接收資料檔案的該第二部分，當作一被處理的第二部分；

將該資料檔案的該被等處理的第一與第二部分予以組合；及

經由該介面而傳送回該等資料檔案之被組合之被處理部分的至少一表示。

16. 如請求項15之模組，其中該處理該第一部分以形成一被處理的第一部分及該處理該第二部分當作一被處理的第二部分包括將經由該介面電路所接收資料檔案的該等第一與第二部分之解密。