申請日期： 94.10.18	IPC分類 H04N 7/16 (2006.01)
申請案號： 94136416	

(以上各欄由本局填註)

發明專利說明書

一、發明名稱	中 文	數位廣播之權利管理系統及方法
	英 文	
二、發明人（共3人）	姓 名（中文）	1. 梁家愷 2. 劉佳衢 3. 陳宏銘
	姓 名（英文）	1. 2. 3.
	國 籍（中英文）	1. 中華民國 TW 2. 中華民國 TW 3. 中華民國 TW
三、申請人（共1人）	名稱或姓 名（中文）	1. 國立台灣大學
	名稱或姓 名（英文）	1.
	國 籍（中英文）	1. 中華民國 TW
	住居所（營業所）（中 文）	1. 台北市羅斯福路四段一號 （本地址與前向貴局申請者不同）
	住居所（營業所）（英 文）	1.
	代表人（中文）	1. 李嗣涔
	代表人（英文）	1.

一、本案已向

國家(地區)申請專利	申請日期	案號	主張專利法第二十七條第一項國際優先權

無

二、□主張專利法第二十九條第一項國內優先權:

申請案號:

無

日期:

三、主張本案係符合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:

四、□有關生物材料已寄存於國外:

寄存國家:

寄存機構: 無

寄存日期:

寄存號碼:

□有關生物材料已寄存於國內(本局所指定之寄存機構):

寄存機構:

寄存日期: 無

寄存號碼:

□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。

五、發明說明 (1)

【發明所屬之技術領域】

本發明係有關一種數位權利管理系統，應用於數位電視廣播系統，特別是指一種數位廣播之權利管理系統及方法。

【先前技術】

所謂的數位權利管理(Digital Rights Management, DRM，以下僅以縮寫表示)系統，是利用各種資料保護(Cryptology、Conditional Access)、追蹤(Digital Watermarking)、身分認證(Biometric Identification)等等種種的技術，讓數位資料在傳輸與散佈的過程中，不備任意的引用、散佈的機制。透過DRM系統，使用者、創作者與服務提供者的權利都可以經由明確的規範而保護。

電視是一個家庭中多媒體影音資料的主要來源。然而，在數位電視廣播系統(Digital Video Broadcasting System, DVB，以下僅以縮寫表示)中並沒有針對DRM系統作出定義，而僅是延續傳統衛星電視中的有條件存取(Conditional Access, CA，以下僅以縮寫表示)技術。可是當多媒體影音資料通過了CA之後，便完全不再有保護，用戶可以任意的錄影跟散佈。由於數位電視的高品質影音資料是數位傳送，透過數位錄影技術，用戶可以複製出完全相同之多媒體檔案。

目前世界各研究單位與政府機關也意識到這個問題，例如，歐洲正發展中的歐盟第六期研究架構計畫(the

五、發明說明 (2)

Innovative Rights and Access Management Inter-platform Solution, 簡稱TIRAMISU技術），便是針對DVB系統作加強，希望加入DRM之功能。另外，由IBM提出的xCP家庭網路，以及美商湯姆遜公司（Thomson Inc.）提出的Smartright系統係利用智慧卡，此一高安全性的儲存與執行裝置，來監控數位家庭之多媒體散佈與使用的情形。而日本政府也對其國內業界命令期生產之錄影設備，必須符合保護作者、廣播公司與使用者之權利。

由上述得知，尋求一完善且具有擴展性之數位權利管理系統實在具有其急迫性與必要性。

【發明內容】

鑒於以上的問題，本發明的主要目的在於提供一種數位廣播之權利管理系統及方法，應用於數位電視廣播系統，可在不增加額外的硬體設備下，使得多媒體資料可以得到更多的保護，而不被任意轉錄或濫用。

本發明的另一目的在於提供一種數位廣播之權利管理系統及方法，係透過多媒體家庭平台（Multimedia Home Platform, MHP）的功能，使DVB系統之數位視訊接收單元作為可執行程式的平台，監控多媒體資料之錄影與重播，整個監控過程除了驗證使用者權利與多媒體資料本身之外，更可配合加密與數位浮水印的機制，讓整個系統更安全。

因此，為達上述目的，本發明所揭露之數位廣播之權利管理系統，是由數位視訊接收單元、使用者認證單元、

五、發明說明 (3)

數位監控單元與儲存單元所構成。數位視訊接收單元是用以接收一個以上的多媒體資料，每個多媒體資料包含一權利表示資料；使用者認證單元是用以儲存使用者認證資料；數位監控單元是用以分析使用者認證單元之使用者認證資料是否符合多媒體資料之權利表示資料，如果條件符合，則對多媒體資料進行加密，並對應產生此多媒體資料之加密鑰匙，然後將加密鑰匙與權利表示資料存入使用者認證單元；而儲存單元是用以儲存加密後之多媒體資料。

其中，儲存單元所儲存之加密後之多媒體資料，是藉由數位監控單元讀取使用者認證單元之使用者認證資料以及多媒體資料的權利表示資料與加密鑰匙，來判斷是否可以播放此多媒體資料，若確定可以播放此多媒體資料，則利用加密鑰匙解密前述加密後的多媒體資料，而得以播放。

此外，本發明所揭露之數位廣播之權利管理之方法，包含下列步驟：首先，接收一個以上之多媒體資料，每個多媒體資料包含一權利表示資料，並從使用者認證單元讀取使用者認證資料，然後，分析使用者認證單元之使用者認證資料是否符合多媒體資料之權利表示資料，如果一切條件符合，則開始對多媒體資料進行加密，並對應產生此多媒體資料之加密鑰匙，接著，將加密鑰匙與權利表示資料存入使用者認證單元，而加密後之多媒體資料則存入儲存單元。

如果要播放儲存單元所儲存之多媒體資料，則可藉由

五、發明說明（4）

從使用者認證單元讀取使用者認證資料以及多媒體資料的權利表示資料與加密鑰匙，來判斷是否可以播放此多媒體資料，若確定可以播放此多媒體資料，則利用加密鑰匙解密前述加密後的多媒體資料，並開始播放。

為使對本發明的目的、構造特徵及其功能有進一步的了解，茲配合圖式詳細說明如下：

【實施方式】

如第1圖所示，為本發明所提供之數位廣播之權利管理系統之示意圖。數位廣播之權利管理系統是由數位視訊收單元10、使用者認證單元20、數位監控單元30與儲存單元40所構成。數位視訊接收單元10可為數位電視機上盒（STB），可透過網路接收多媒體資料50，使用者認證單元20可為智慧卡（Smart card），用以儲存使用者認證資料等驗證與識別資訊。而儲存單元40可為硬碟或數位影音光碟（DVD）等儲存媒體，用以儲存加密後之多媒體資料50。數位監控單元30可以在數位視訊接收單元10來執行。

請參照第2圖所示，為本發明之實施例之數位廣播之權利管理系統之示意圖。本發明之實施例所提供之數位監控單元81可透過錄影監控程式（Record Manager）73與重播監控程式（Display Manager）74來執行。

本實施例之數位廣播之權利管理系統，係建立在DVB系統上，且不論傳輸方式是利用地面廣播或者衛星，此系統皆可適用。根據DVB系統的定義，除了原本之聲音、影像和基本資料之多媒體資料71之外，本實施例在原本之傳

五、發明說明 (5)

輸串流（Transport stream）70中新增了權利表示資料（Rights Expression Data, RED）72，以及錄影監控程式73與重播監控程式74，錄影監控程式73與重播監控程式74是根據DVB-MHP中的定義來執行，權利表示資料72則用來對應於多媒體資料71的權利資料。詳細說明如下：

為了替創作者或廣播服務提供者保護多媒體資料71，在廣播的同時，一個權利表示資料（Rights Expression Data, RED）72會隨著多媒體資料71同時被廣播至每個使用者。在權利表示資料72中，定義了所有關於此多媒體資料71的種種權利，可以包含的有可錄影之使用者之條件，可錄影、散佈之條件，可重複播放之時間、次數限制，發行者的資料，保護的機制等等。多媒體資料71的格式則可以為創作者或廣播服務提供者自行定義，或者遵循國際標準，以提高系統的相容性。而將來統一的國際標準有可能是MPEG-21 part-5: Rights Expression Language（REL, 權利表示語言），這個標準是利用XML格式來定義多媒體資料的權利，並且可以和MPEG-21其他部分相容。

錄影監控程式73也隨著多媒體資料71一同廣播，但與權利表示資料72不同的是，錄影監控程式73不是專屬於某特定的多媒體資料71，廣播服務者可以用同一個錄影監控程式73來保護所有的多媒體資料71。錄影監控程式73是根據DVD-MHP的定義而設計的一個程式，可以在有MHP的數位電視機上盒80來執行。錄影監控程式73利用MHP定義的介面來控制數位電視機上盒80的動作，包含錄製廣播的多

五、發明說明（6）

媒體資料，讀取廣播的權利表示資料71，讀取、寫入智慧卡83，保護、加密錄製的多媒體資料71。

重播監控程式84也隨著多媒體資料71一同廣播，但與權利表示資料72不同的是，重播監控程式74不是專屬於某個特定的多媒體資料71，廣播服務者可以用同一個錄影監控程式74來保護所有的多媒體資料71。錄影監控程式74是根據DVD-MHP的定義而設計的一個程式，可以在有MHP的數位電視機上盒80來執行。重播監控程式74利用MHP定義的介面來控制數位電視機上盒80的動作，包含播放先前錄製多媒體資料71，讀取先前儲存的權利表示資料72，讀取、寫入智慧卡83，解密錄製的多媒體資料71，並且播放錄製的多媒體資料71。

整個系統利用上面所定義的三項資料和程式來運作。當使用者錄影的時候，系統會藉由錄影監控程式83來保護廣播的多媒體資料71；當使用者想要播放先前錄影的多媒體資料71時，系統會藉由重播監控程式84來保護廣播的多媒體資料71。

請一併參照第2圖與第3圖所示，第3圖為本實施例之監控錄影流程之動作，其流程包括下列步驟：

當受到本系統保護之多媒體資料被播放時，錄影監控程式也開始運作。

如步驟S100，若使用者利用遠端控制器（Remote controller）90對數位電視機上盒80下達錄影的指令，錄影監控程式73偵測到此一命令，會開始檢驗智慧卡83中的

五、發明說明 (7)

使用者認證資料是否符合多媒體檔案71之權利表示資料72。

然後，如步驟S110，如果錄影監控程式73確認一切條件符合，則如步驟S120。錄影監控程式73開始擷取廣播中的多媒體資料71，對其進行加密之封裝過程。在此，如步驟S130，錄影監控程式同時把加密鑰匙、權利表示資料存入智慧卡83，以作為存取多媒體資料71之憑證。

最後，錄影監控程式73把加密後的多媒體資料71存入儲存媒體82內。

接著，請參照第4圖所示，為本實施例之監控播放流程之動作，其流程包括下列步驟：

如步驟200，當使用者利用遠端控制器90對數位電視機上盒80下達要播放先前錄製的多媒體檔案71的命令時，重播監控程式74偵測到此一命令，會開始讀取智慧卡83中的使用者認證資料、多媒體資料71之權利表示資料72與加密鑰匙，根據使用者認證資料是否符合權利表示資料72，去判斷是否可以播放此多媒體檔案71。

如步驟S210，如果重播監控程式74確認可以播放此多媒體資料71，則開始讀取存在儲存媒體82中的加密後的多媒體資料71，重播監控程式74再利用智慧卡83中的加密鑰匙對此加密後的多媒體資料71解密，並且開始播放。

其中，錄影時亦可利用對多媒體資料添加數位浮水印的方式，可以在多媒體資料被任意散佈後，創作者或廣播服務提供者可以反向追查散佈者。因此，數位浮水印中必

五、發明說明（8）

須包含使用者的資料，任何此類的演算法都可以在此利用。

如果重播監控程式否定其播放要求，則重播監控程式會同時嘗試解讀數位浮水印中的內容。並且，如果此多媒體資料有任何的播放次數限制，則更新相關紀錄至智慧卡之中。

本實施例所提供之數位廣播之權利管理系統及方法，可以運用任何一個加密演算法來保護多媒體資料；有些演算法運算量太大，可能需要額外的硬體輔助，因此不適合在本實施例之系統中，而任何快速的加密演算法，或者有效率的針對多媒體資料的加密演算法，都可以使用在本實施例之系統中。

再者，如果儲存媒體可轉移至其他硬體，如個人電腦或手機系統，則該硬體也必須要有讀取使用者認證單元之功能，與可在此平台執行之重播監控程式。在其他平台之重播監控程式不需要再符合MHP之規定。

此外，原本的數位廣播系統中的有條件讀取（Conditional Access）系統，和本系統並不衝突，此系統對於廣播的多媒體資料可提供更多的保護。

綜合上述，本發明所提供之數位廣播之權利管理系統，乃藉由MHP的功能，使DVB系統的數位視訊接收單元成為可執行程式的平台，利用DVB的廣播系統，DRM的執行程式和權利定義可以經由廣播頻道下載，而MHP-STB提供的安全機制也可以確保程式的安全性和可靠性。其次，當多媒

五、發明說明 (9)

體資料通道DRM系統而進入儲存裝置時，可利用下載的程式對這些多媒體資料機加密或增加數位浮水印。使用者和多媒體資料的認證資料等重要資料，可利用智慧卡來存取，讓使用者可以方便攜帶和使用。此外，由於本實施例利用軟體來實現數位權利管理的機制，因此，當系統某部分功能遭到破壞之後，可以輕易更改局部的程式，並藉由廣播系統更新，而不需要更改硬體。

雖然本發明以前述之實施例揭露如上，然其並非用以限定本發明。在不脫離本發明之精神和範圍內，所為之更與潤飾，均屬本發明之專利保護範圍。關於本發明所界定之保護範圍請參考所附之申請專利範圍。

圖式簡單說明

【圖式簡單說明】

第1圖係本發明所提供之數位廣播之權利管理系統之示意圖；

第2圖係本發明之實施例所提供之數位廣播之權利管理系統之示意圖；

第3圖係本發明之實施例所提供之數位廣播之權利管理系統之監控錄影流程之動作示意圖；及

第4圖係本發明之實施例所提供之數位廣播之權利管理系統之監控播放流程之動作示意圖。

【主要元件符號說明】

10　數位視訊接收單元

20　使用者認證單元

30　數位監控單元

40　儲存單元

50　多媒體資料

60　使用者

70　傳輸串流

71　多媒體資料

72　權利表示資料

73　錄影監控程式

74　重播監控程式

80　數位電視機上盒

81　數位監控單元

82　儲存媒體

圖式簡單說明

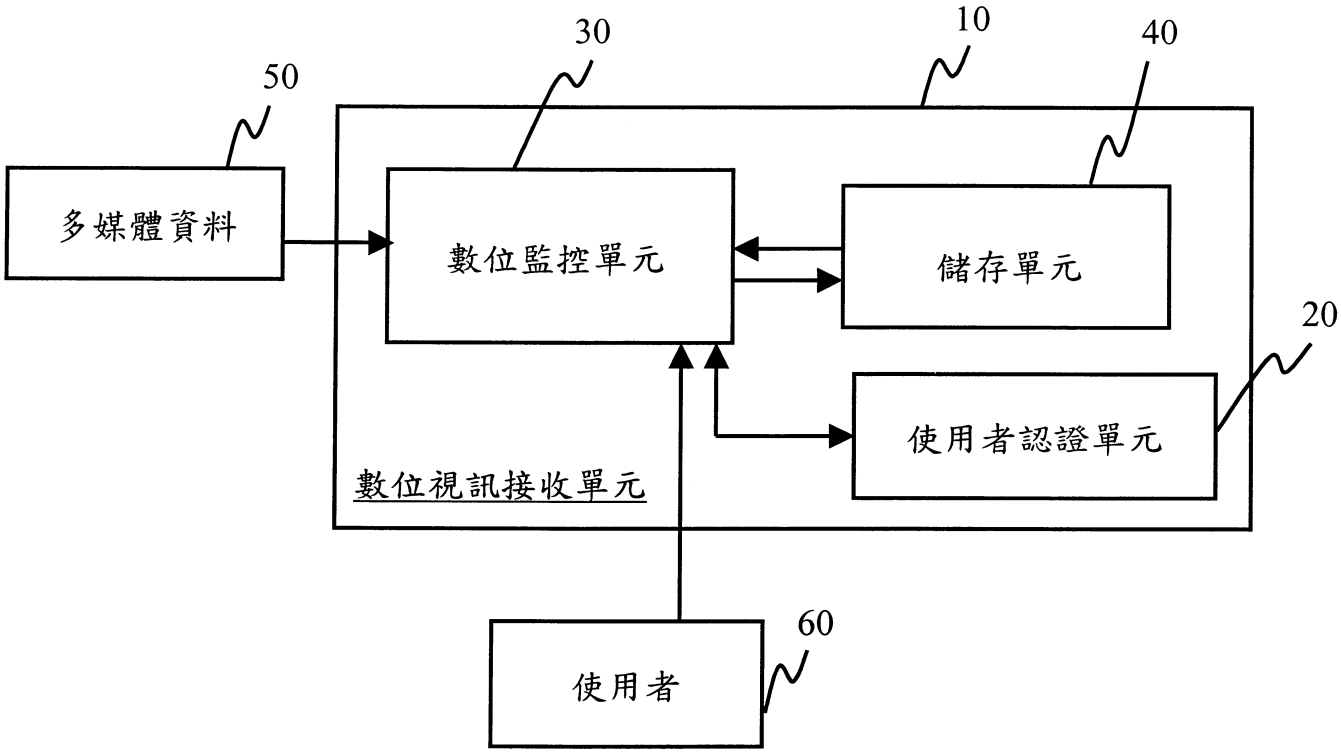
83　智慧卡

90　遠端控制器

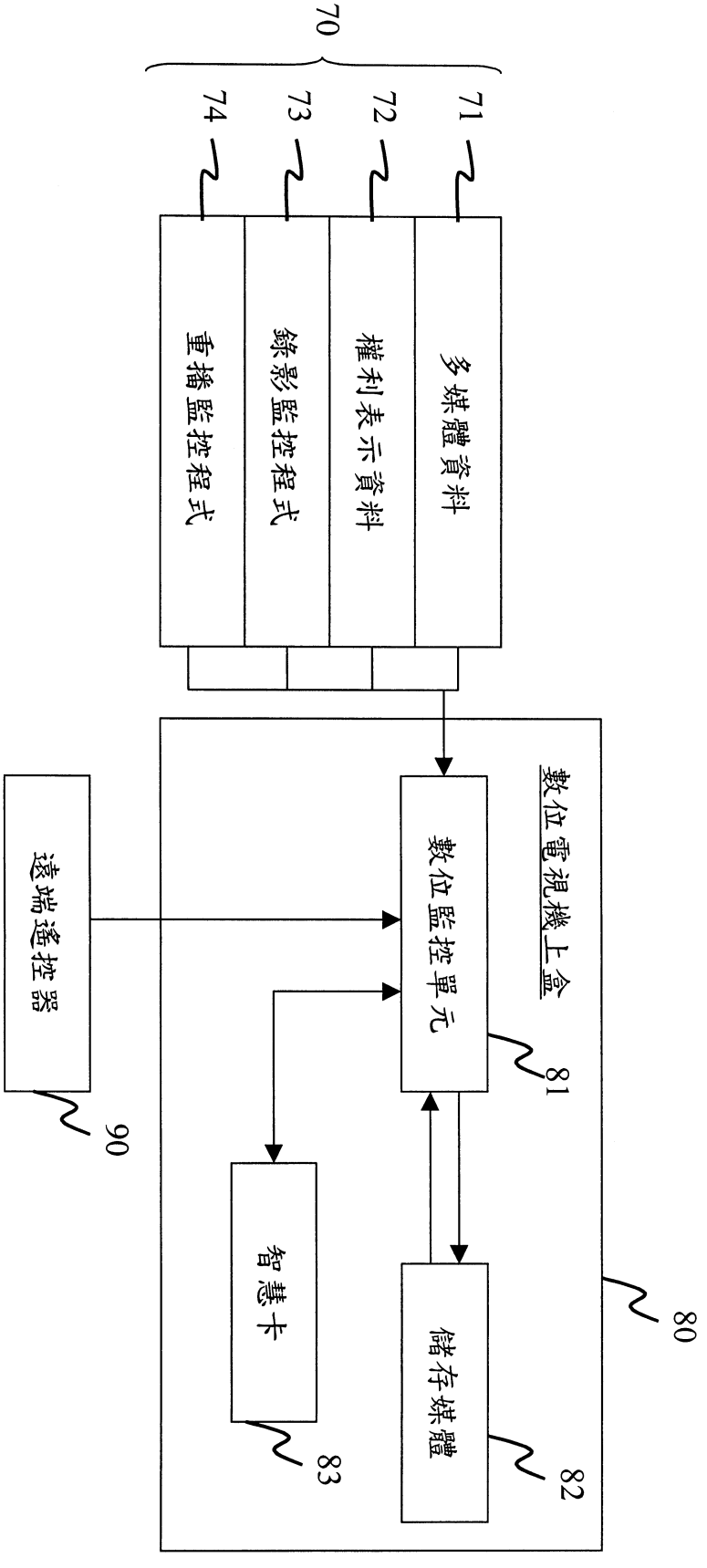
四、中文發明摘要　（發明名稱：數位廣播之權利管理系統及方法）

本發明係揭露一種數位廣播之權利管理系統及方法，應用於數位電視廣播系統，其利用多媒體家庭平台的功能，可在多媒體資料被錄製或重播時，分析使用者資料是否符合多媒體資料的使用權利，再配合加密或解密的過程，來監控多媒體資料之錄製與重播，藉以避免多媒體資料被轉錄或濫用。

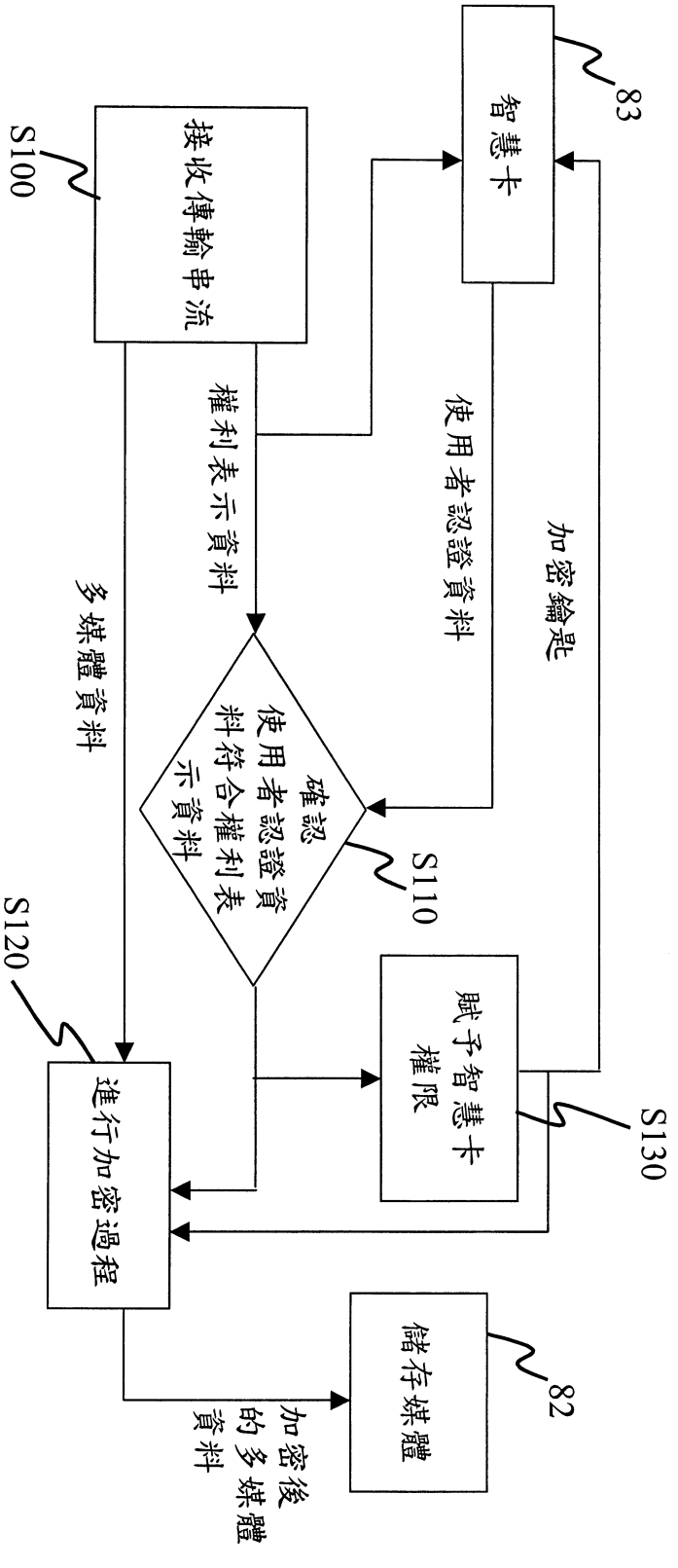
五、英文發明摘要　（發明名稱：）



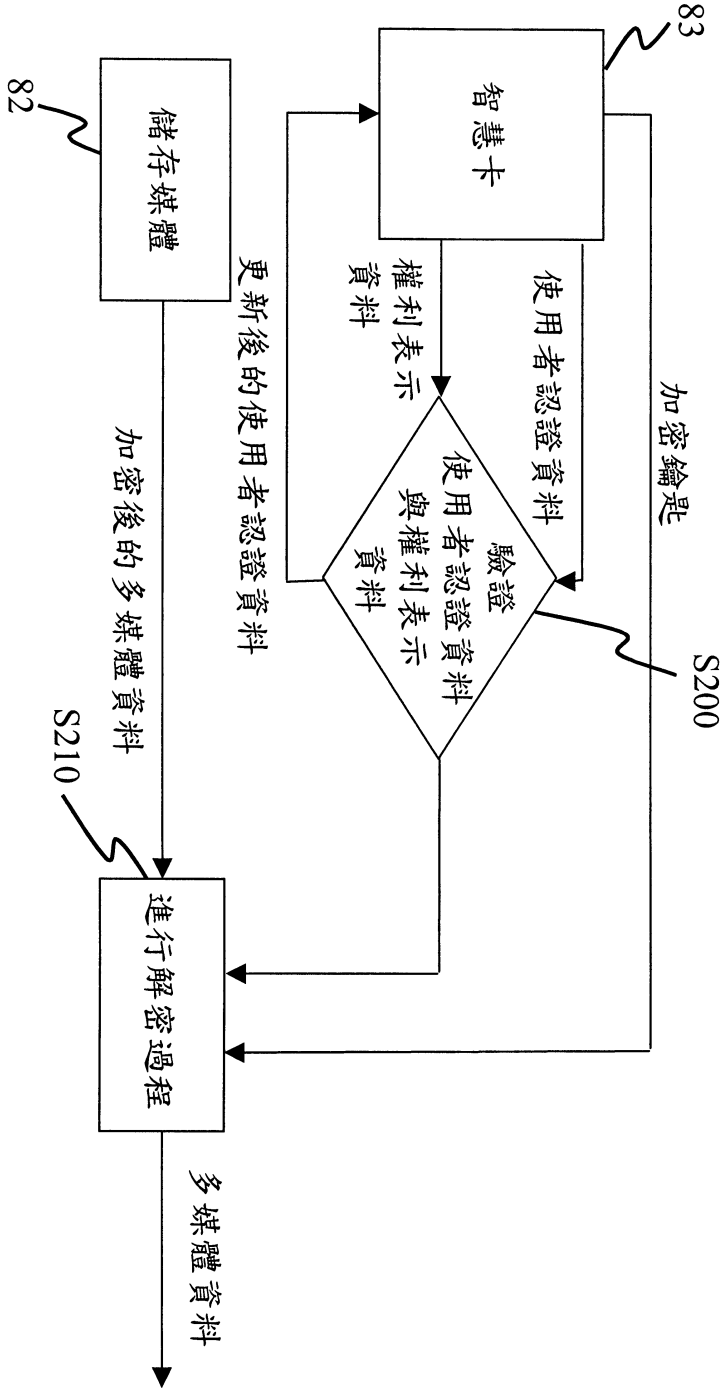
第1圖


70
71
72
73
74
多媒體資料
權利表示資料
錄影監控程式
重播監控程式
數位電視機上盒
80
數位監控單元
81
儲存媒體
82
智慧卡
83
遠端遙控器
90

第2圖


83
智慧卡
加密鑰匙
使用者認證資料
接收傳輸串流
S100
權利表示資料
多媒體資料
確認使用者認證資料符合權利表示資料
S110
賦予智慧卡權限
S130
S120
進行加密過程
儲存媒體
82
加密後的多媒體資料

第3圖


83
智慧卡
使用者認證資料
加密鑰匙
S200
驗證使用者認證資料與權利表示資料
權利表示資料
更新後的使用者認證資料
儲存媒體
82
加密後的多媒體資料
S210
進行解密過程
多媒體資料

第4圖

六、指定代表圖

(一)、本案代表圖為：第 1 圖

(二)、本案代表圖之元件符號簡單說明：

10 數位視訊接收單元

20 使用者認證單元

30 數位監控單元

40 儲存單元

50 多媒體資料

60 使用者

六、申請專利範圍

1．一種數位廣播之權利管理系統，包含有：

一數位視訊接收單元，用以接收一個以上之多媒體資料，且該多媒體資料包含一權利表示資料；

一使用者認證單元，用以儲存一使用者認證資料；

一數位監控單元，用以確認該使用者認證單元之該使用者認證資料符合該多媒體資料之該權利表示資料，對該多媒體資料加密，並對應產生一該多媒體資料之加密鑰匙，將該加密鑰匙與該權利表示資料賦予該使用者認證單元；及

一儲存單元，用以儲存該加密後之多媒體資料。

2．如申請專利範圍第1項所述之數位廣播之權利管理系統，其中該儲存單元係硬碟或數位影音光碟（DVD）。

3．如申請專利範圍第1項所述之數位廣播之權利管理系統，其中該數位監控單元係可對該多媒體資料添加一數位浮水印。

4．如申請專利範圍第1項所述之數位廣播之權利管理系統，其中該使用者認證單元係為一智慧卡。

5．如申請專利範圍第1項所述之數位廣播之權利管理系統，其中該數位視訊接收單元係為一數位電視機上盒（STB）。

6．如申請專利範圍第1項所述之數位廣播之權利管理系統，其中該數位監控單元係包括一錄影監控程式與一重播監控程式。

六、申請專利範圍

7．如申請專利範圍第6項所述之數位廣播之權利管理系統，其中該儲存單元係藉由該錄影監控程式確認該使用者認證單元之該使用者認證資料符合該多媒體資料之該權利表示資料，對該多媒體資料加密後，而得以錄製該加密後之該多媒體資料。

8．如申請專利範圍第6項所述之數位廣播之權利管理系統，其中該儲存單元所儲存之該加密後之多媒體資料，係藉由該重播監控程式讀取該使用者認證單元所具有的該使用者認證資料、該多媒體資料之該權利表示資料與該加密鑰匙，判斷該使用者認證資料符合該多媒體資料，並以該加密鑰匙對該加密後之多媒體資料解密後，而得以播放。

9．如申請專利範圍第6項所述之數位廣播之權利管理系統，其中該錄影監控程式與該重播監控程式係可隨著該多媒體資料一同被該數位視訊接收單元所接收，以控制該多媒體資料之錄製與重播。

10．一種數位廣播之權利管理方法，其步驟包含：

接收一個以上之多媒體資料，且該多媒體資料包含一權利表示資料，並自一使用者認證單元讀取一使用者認證資料；

確認該使用者認證資料符合該多媒體資料之該權利表示資料；

對該多媒體資料加密，並對應產生一該多媒體資料之加密鑰匙，將該加密鑰匙與該權利表示資料賦予該

六、申請專利範圍

使用者認證單元；及

儲存該加密後之多媒體資料。

11．如申請專利範圍第10項所述之數位廣播之權利管理方法，其中該確認該使用者認證資料符合該多媒體資料之該權利表示資料之步驟後，更包括一對於該多媒體資料添加一數位浮水印之步驟。

12．如申請專利範圍第10項所述之數位廣播之權利管理方法，其中該使用者認證單元係為一智慧卡。

13．如申請專利範圍第10項所述之數位廣播之權利管理方法，其中該儲存該加密後之多媒體資料之步驟後，更包括一讀取該使用者認證單元所具有的該使用者認證資料、該多媒體資料之該權利表示資料與該加密鑰匙之步驟。

14．如申請專利範圍第13項所述之數位廣播之權利管理方法，其中該讀取該使用者認證單元所具有的該使用者認證資料、該多媒體資料之該權利表示資料與該加密鑰匙之步驟之後，更包括一判斷該使用者認證資料符合該多媒體資料之步驟。

15．如申請專利範圍第14項所述之數位廣播之權利管理方法，其中該判斷該使用者認證資料符合該多媒體資料之步驟，更包括一以該加密鑰匙對該加密後之多媒體資料解密之步驟。

16．如申請專利範圍第15項所述之數位廣播之權利管理方法，其中該以該加密鑰匙對該加密後之多媒體資料解

六、申請專利範圍

密之步驟，更包括一播放該解密後之多媒體資料之步驟。

17．如申請專利範圍第15項所述之數位廣播之權利管理方法，其中該接收該多媒體資料之步驟，係包括接收一重播監控程式，以控制該被加密後之多媒體資料之重播。

18．如申請專利範圍第17項所述之數位廣播之權利管理方法，其中該儲存該加密後之多媒體資料之步驟，係藉由該重播監控程式讀取該使用者認證單元所具有的該使用者認證資料、該多媒體資料之該權利表示資料與該加密鑰匙，判斷該使用者認證資料符合該多媒體資料，並以該加密鑰匙對該加密後之多媒體資料解密後，而得以播放該多媒體資料。

19．如申請專利範圍第10項所述之數位廣播之權利管理方法，其中該接收該多媒體資料之步驟，係包括接收一重播監控程式，以控制該被加密後之多媒體資料之重播。

20．如申請專利範圍第19項所述之數位廣播之權利管理方法，其中在該接收該多媒體資料之步驟，更包含接收一錄影監控程式，以執行該確認該使用者認證資料符合該多媒體資料之該權利表示資料之步驟、該對該多媒體資料加密之步驟，以及控制該儲存該加密後之多媒體資料之步驟得以進行。