



(19)中華民國智慧財產局

(12)發明說明書公告本 (11)證書號數：TW I388213B1

(45)公告日：中華民國 102 (2013) 年 03 月 01 日

(21)申請案號：098114277

(22)申請日：中華民國 98 (2009) 年 04 月 29 日

(51)Int. Cl. : **H04N7/16 (2011.01)**

(30)優先權：2008/05/16 法國 0802639

(71)申請人：維薩斯股份有限公司 (法國) VIACCESS SA (FR)
法國

(72)發明人：都柏歐柯 基連 DUBROEUCQ, GILLES (FR)

(74)代理人：許世正

(56)參考文獻：

EP	1111924A1	EP	1883239A1
EP	1968316A1	US	2006/0294547A1
US	2007/0294773A1	WO	2007/148512A1

審查人員：徐瑞甫

申請專利範圍項數：15 項 圖式數：10 共 0 頁

(54)名稱

多媒體內容接收與傳送方法，傳送裝置接收裝置，記錄載體與安全處理器

METHODS FOR RECEIVING AND SENDING A MULTIMEDIA CONTENT, RECEIVER, SENDER AND RECORDING CARRIER AND SECURITY PROCESSOR FOR THIS METHOD

(57)摘要

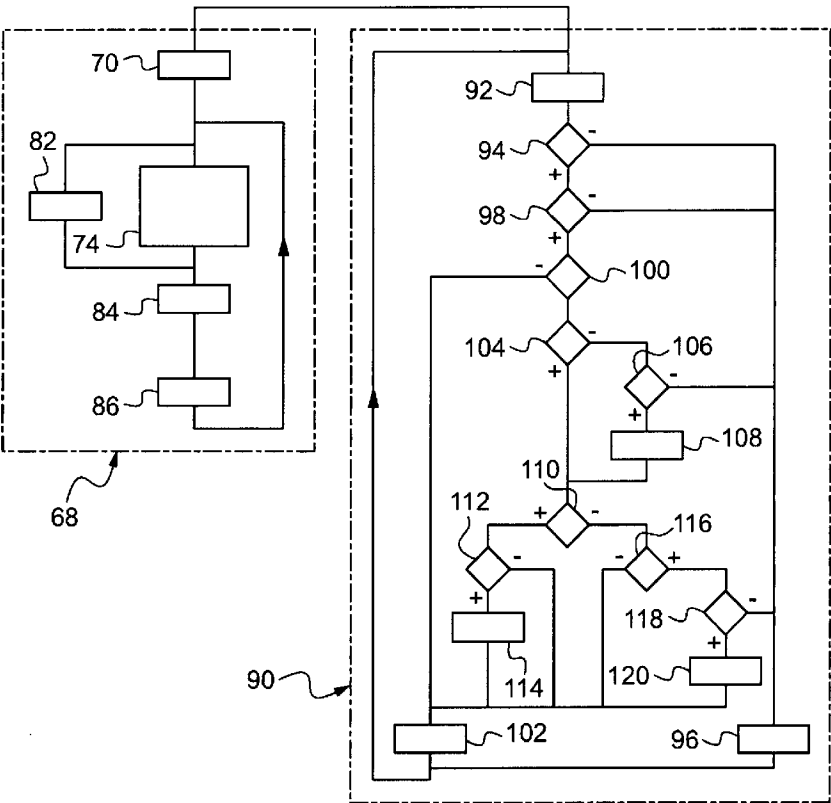
一種多媒體內容之接收與傳送方法，本方法包含：只要第二多媒體內容透過電子接收裝置被觀看，則依照與第二多媒體內容關聯之前進指令函數修正計數器之數值(114)；儲存計數器之數值(114)，第二多媒體內容之非連續觀看之間係由不會修正計數器之數值之另一多媒體內容之觀看打斷；令第一多媒體內容之觀看取決於計數器之預定數值(118)。

This method comprises:

- the modification (114), whenever a second multimedia content is viewed by means of an electronic receiver, of the value of the counter as a function of the instructions on progression associated with this second multimedia content,

- the storage (114) of the value of this counter between non-consecutive viewings of second multimedia contents interspersed with the viewing of another multimedia content that does not modify the value of the counter,

- the making of the viewing of the first multimedia content conditional on a predetermined value of the counter.



第4圖

發明專利說明書

(本說明書格式、順序，請勿任意更動，※記號部分請勿填寫)

※ 申請案號： 98114277

※ 申請日： 98.4.29

※IPC 分類：

H04N 7/16 (2001.01)

一、發明名稱：(中文/英文)

多媒體內容接收與傳送方法，傳送裝置接收裝置，記錄載體與安全處理器

二、中文發明摘要：

一種多媒體內容之接收與傳送方法，本方法包含：只要第二多媒體內容透過電子接收裝置被觀看，則依照與第二多媒體內容關聯之前進指令函數修正計數器之數值(114)；儲存計數器之數值(114)，第二多媒體內容之非連續觀看之間係由不會修正計數器之數值之另一多媒體內容之觀看打斷；令第一多媒體內容之觀看取決於計數器之預定數值(118)。

三、英文發明摘要：

This method comprises:

- the modification (114), whenever a second multimedia content is viewed by means of an electronic receiver, of the value of the counter as a function of the instructions on progression associated with this second multimedia content,
- the storage (114) of the value of this counter between non-consecutive viewings of second multimedia contents interspersed with the viewing of another multimedia content that does not modify the value of the counter,
- the making of the viewing of the first multimedia content conditional on a predetermined value of the counter.

四、指定代表圖：

(一)本案指定代表圖為：第 4 圖。

(二)本代表圖之元件符號簡單說明：

無

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

無

六、發明說明：

【發明所屬之技術領域】

本發明係關於一種第一多媒體內容之接收方法與傳送方法，其中第一多媒體內容之顯示係取決於第二多媒體內容之先前顯示。本發明還關於實施上述方法之接收裝置、傳送裝置、資訊記錄載體與安全處理器。

【先前技術】

多媒體內容係為包含音頻與／或視訊之內容。例如，此多媒體內容可被設計為在電視機上播放。例如，多媒體內容係為電影、視聽節目或音樂片段等。

從微軟公司所申請的美國專利 2007 294 773 中已知這種接收方法。更特別地是，微軟公司之應用描述了第一多媒體內容，即隨選視訊（Video On Demand；簡稱為 VOD）之接收方法，並且隨選視訊之解密（de-scrambling）係取決於第二多媒體內容之初步顯示，在此實例中第二多媒體內容即為廣告材料。

在微軟公司的方法中，接收裝置傳送授權（license），首先只有已經觀看全部廣告時，隨選視訊才可藉由授權被解密。因此，隨選視訊之觀看係取決於廣告之先前觀看。此外，此接收裝置採用各種手段以避免使用者縮短或切斷廣告。例如，接收裝置係採用一些手段以取消快進（fast forward）操作。

因此，這種習知技術之方法強迫電視觀眾觀看緊鄰隨選視訊之前的全部廣告。

然而，這種習知方法之應用領域被限制於隨選視訊。的確，如果這種方法被換位至廣播電視，那麼如果某觀眾偶然無意地錯過於他希望觀看的節目之前開始的廣告，則他將被剝奪觀看此節目的可能性。這樣的操作，對於廣播電視系統來說是無法接受的。

這裡所說之術語“廣播電視”係指相同多媒體內容至多個接收裝置的同步廣播。與隨選視訊不同，廣播電視的使用者無法決定多媒體內容之廣播將要開始的時間。

【發明內容】

因此，本發明的目的在於提供一種第一多媒體內容之接收方法，其中第一多媒體內容之觀看係取決於第二多媒體內容之先前觀看，此接收方法係用於廣播電視領域。

本發明所提供之一種第一多媒體內容之接收方法，其中第二多媒體內容係為與相同計數器之數值之前進指令（instructions on progression）相關聯之唯一內容，當第一與第二多媒體內容之電子接收裝置執行此前進指令時，這些前進指令係依照相同含義修正此相同計數器之全部數值。此方法尤其包含以下步驟：

無論是否透過電子接收裝置觀看第二多媒體內容，均依照與此第二多媒體內容相關聯之前進指令函數，修正計數器之數值；

儲存此計數器之數值，其中第二多媒體內容之非連續觀看之間係由不會修正計數器之數值之另一多媒體內容之觀看打斷；以及

令第一多媒體內容之全部觀看取決於計數器之預定數值。

此處，假設上述方法實施於廣播電視領域，其中電視節目嘗試被製做為取決於先前觀看的廣告。還假設當接收裝置執行前進指令時，前進指令增加計數器之數值。在本文中，即使使用者錯過緊鄰這個電視節目之前開始的廣告，他仍然可被允許觀看這個電視節目。的確，在上述方法中，無論使用者何時觀看廣告，計數器的數值均被增加。因為計數器的數值被記憶，不需要即時地於電視節目之前觀看廣告。例如，使用者可觀看廣告的第一序列，然後改變頻道以觀看電影。觀看此電影將不會修正計數器的數值。然後，一段時間以後，使用者可以查看另一序列的廣告，其中另一序列的廣告繼續增加計數器的數值。因此，即使觀看廣告被觀看其他多媒體內容打斷，計數器無須重置仍可增加。這表示他開始觀看期望之電視節目之前緊鄰的廣告序列時，計數器的數值已經達到足以授權觀看此電視節目之數值。因此，即使他錯過電視節目之前緊鄰的廣告序列，但是他仍然可被授權觀看電視節目。

在以上方法中，第二多媒體內容無須緊鄰第一多媒體內容之前。這使得可在廣播電視領域使用此方法。

此接收方法之實施例包含一或多個下述特性：

在觀看每一第二多媒體內容之前，此方法包含：解多工接收的與前進指令多工之多工資料流，以及依照與第二多媒體內容多工之前進指令函數修正計數器的數值；

此方法包含選擇計數器，計數器之數值必須從若干可能的計

數器中依照與前進指令關聯之此計數器之識別碼被修正；

此方法包含：

接收一組一或多個金鑰效期之第二多媒體內容以及與此組關聯之前進指令，第二多媒體內容之每一金鑰效期分別透過控制字被加密；以及

無論此組之全部金鑰效期何時透過電子接收裝置被解密，均修正計數器之數值；

在第二多媒體內容之金鑰效期之前，此方法包含接收同時廣播至全部接收裝置之一訊息，其中此接收裝置能夠接收第一與第二多媒體內容，此訊息包含解密此金鑰效期所需之控制字之密碼電文 CW*以及與此金鑰效期所屬之組相關聯之前進指令；

無論何時授權藉由電子接收裝置觀看第一多媒體內容，此方法包含依照與前進指令相反之方法修正計數器之數值，從而使得觀看隨後之多媒體內容取決於先前觀看的其他第二補充多媒體內容；

此方法包含：

接收一組第一多媒體內容之一或多個金鑰效期以及與此組關聯之計數器之數值之迴歸指令，每一金鑰效期用各自的控制字被加密；

無論此組之全部金鑰效期何時被解密，根據與前進指令相反之含義，依照與此組關聯之迴歸指令修正計數器之數值；以及

只要計數器之數值達到預定閾值，則禁止解密第一多媒體內

容之下組金鑰效期。

此方法包含：

接收第一加密多媒體內容以及此第一多媒體內容之存取條件，

如果電子接收裝置中沒有記錄與存取條件對應之存取權，則禁止解密第一多媒體內容，並且相反地

如果電子接收裝置中記錄與第一多媒體內容之存取條件對應之存取權，則授權解密第一多媒體內容，以及

只要待越過之計數器之數值已經超過預定閾值，與存取條件對應之存取被寫入接收裝置；

此方法包含限制計數器之數值至預定閾值；

此方法包含自動建立計數器，以回應計數器數值之前進指令之接收。

以上接收方法之實施例更包含以下優點：

多工第二多媒體內容與前進指令，從而可能簡單地將這些前進指令與第二多媒體內容關聯，

使用計數器識別碼，從而能夠同時使用與每一多媒體內容關聯之若干計數器，因此，例如第三多媒體內容之觀看取決於先前觀看的第四多媒體內容，第三與第四內容相異，並且不依賴第一與第二多媒體內容，

修正計數器之數值係取決於解密一或多個金鑰效期，進而可增加系統之安全，

依照前進指令之相反方式，在第一多媒體內容之每一觀看期間，再次修正計數器之數值，使得下一第一多媒體內容之觀看取決於先前觀看之第二附加多媒體內容，

依照迴歸指令修正計數器之數值，當觀看第一多媒體內容時，授權第一多媒體內容之觀看週期取決於已經觀看之第二多媒體之數量，

當計數器之數值達到預定閥值時，存取權用於授權第一多媒體內容之充分觀看，此存取權之記錄授權在預定週期觀看第一多媒體內容，

在計數器之數值上施加最大限制，在第二多媒體內容與第一多媒體內容之間實現輪流觀看；

當接收裝置開始作業或者指定指令透過傳送裝置被傳送時，則自動產生計數器以回應計數器之前進指令之接收，從而避免需要初始化計數器。

本發明之目的還在於提供一種資訊記錄載體，此資訊記錄載體包含指令，當電子計算機執行這些指令時則執行以上方法。

本發明之目的還在於提供一種第一多媒體內容之傳送方法，第一多媒體內容之觀看取決於先前觀看的第二多媒體內容，其中此方法包含：

傳送與傳送的每一第二多媒體內容關聯之計數器數值之前進指令，

在兩個第二多媒體內容之間，傳送與用於修正計數器數值之

指令沒有關聯之其他多媒體內容，以及

傳送與傳送之第一多媒體內容關聯之存取條件，這些存取條件使得第一多媒體內容之全部觀看取決於足夠的計數器數值。

本發明之傳送方法之實施例包含以下特徵：

此方法包含與傳送之第一多媒體內容關聯之計數器數值之迴歸指令之傳送，當被授權觀看第一多媒體內容時，依照與前進指令相反之含義，這些迴歸指令修正計數器之數值。

● 本發明之目的還在於提供一種第一多媒體內容之接收裝置，第一多媒體內容之觀看取決於先前觀看的第二多媒體內容，其中接收裝置包含：

記憶體，係能夠儲存計數器之數值，其中在第二多媒體內容之非連續觀看之間可用另一多媒體內容之觀看打斷，而觀看另一多媒體內容不會修正計數器之數值；以及

電子計算機，能夠：

● 無論何時藉由接收裝置觀看第二多媒體內容，均依照接收的第二多媒體內容關聯之前進指令修正計數器之數值，以及

使全部觀看第一多媒體內容取決於足夠的計數器數值。

本發明之目的還在於一種安全處理器，係能夠被實施於以上接收裝置中。

最後，本發明之目的還在於提供一種第一多媒體內容之傳送裝置，第一多媒體內容之觀看取決於第二多媒體內容之先前觀看，此傳送裝置能夠：

傳送與傳送之每一第二多媒體內容關聯之計數器數值之前進指令，

在兩個第二多媒體內容之間，傳送與計數器數值之前進指令沒有關聯之多媒體內容，以及

傳送與傳送之第一多媒體內容關聯之存取條件，這些存取條件令第一多媒體內容之全部觀看取決於足夠的計數器數值。

【實施方式】

在這些圖式中，相同的參考標號用於代表相同部件。

以下描述中，不再詳細描述本領域眾所周知的特徵和功能。此外，使用的術語係為多媒體內容之存取條件系統之術語。為了理解此術語之更多資訊，讀者可參考以下文檔：

1995 年 12 月 21 日，在布魯塞爾由歐洲廣播聯盟出版之“條件存取系統之功能模型”（“Functional Model of Conditional Access System” EBU Review - Technical European Broadcasting Union, Brussels, BE, No. 266, 21 December 1995）。

「第 1 圖」表示用於廣播多媒體內容之付費電視系統 2。例如，系統 2 係為用於廣播若干編密電視頻道之系統。通常，這些電視頻道之每一頻道或電視頻道組之解密係取決於用戶之預約付費。

系統 2 包含編密多媒體內容之至少一個傳送裝置 4 以及能夠解密傳送裝置 4 所廣播的多媒體內容之多個接收裝置。為了簡化「第 1 圖」，圖中僅僅表示接收裝置 6。例如，其他接收裝置與接

收裝置 6 相同。

接收裝置 4 包含擾碼器 10，藉由控制字 CW，當接收到多媒體內容時，擾碼器 10 能夠擾亂透過埠 12 接收的明文多媒體內容。為此，擾碼器 10 使用記憶體 14 中包含的控制字。編密多媒體內容被發送至多工器 16 之輸入。

多媒體內容之擾碼係為加密操作，控制字係為用於擾亂多媒體內容之加密金鑰。

傳送裝置 4 還包含控制字之產生器 18。產生器 18 規律地修正記憶體 14 中包含的控制字。用於擾亂多媒體內容之控制字之兩次修正之間的時間間隔被稱為金鑰週期。

只要產生器 18 產生新的控制字，產生器 20 則產生新的授權控制訊息 ECM (entitlement control message; ECM) 訊息。每一授權控制訊息更包含：

控制字之密碼電文 CW*，以及

編碼多媒體內容之存取條件。

密碼電文 CW*係為一段資訊，此資訊本身係為擾亂多媒體內容所必須的，但是卻不足以擾頻多媒體內容。例如，使用接收裝置已知的服務金鑰或者控制字之參考或者接收裝置中包含的控制字之密碼電文加密控制字，從而得到密碼電文 CW*。

存取條件被設計為與接收裝置中預先記錄的存取權比較。僅僅當關聯多媒體內容之存取條件與預先記錄的存取權對應時，多媒體內容之解碼才被授權。例如，存取條件可以為與多媒體內容

關聯之位準 (moral level)。

產生器 20 所產生的授權控制訊息被傳送至多工器 16 之輸入。

這裡，產生器 20 連接包含節目之網格 24 之記憶體 22。

多工器 16 用於多工編密多媒體內容與包含 CW*密碼電文之授權控制訊息，此密碼電文係為解擾此多媒體內容所需要的。因此，多工器 16 建立多工資料流，且透過資訊傳輸網路 30 被廣播至全部接收裝置。當編密多媒體內容被傳送時，此多工過程能夠實現授權控制訊息之傳送之暫時同步。

例如，網路係為封包交換網路，例如網際網路或衛星電視廣播網路。

接收裝置 6 包含解擾器 40，解擾器 40 被提供天線 42 以接收傳送裝置 4 所廣播的多媒體內容。解擾器 40 還包含解多工器 44，解多工器 44 解多工接收的多工資料流，從而傳送編密多媒體內容至解擾器 40 並且傳送授權控制訊息類型之訊息至安全處理器 48。

處理器 48 可拆卸地連接解擾器 40。例如，處理器 48 係為一晶片卡。

處理器 48 包含電子計算機 50 並且獲得控制字 CW，其中電子計算機 50 能夠處理每一授權控制訊息以解密密碼電文 CW*，控制字 CW 能夠使得多媒體內容被解擾。處理器 48 能夠傳送此控制字 CW 至解擾器 40。

電子計算機 50 連接包含指令之記憶體 52，當電子計算機 50 執行指令時，指令用於執行「第 4 圖」之方法。另外，此記憶體

52 包含預先記錄的存取權 54 以及若干計數器 56。在「第 1 圖」中，圖中僅僅表示一個計數器 56。其他計數器之結構和使用由適合計數器 56 之特別實例之以下描述而得出。

接收裝置 6 連接電視機 60，電視機 60 能夠顯示解擾器 40 所解擾之多媒體內容。

「第 2 圖」表示網格 24 之結構之例子。本文中網格係為包含以下行之表格：

- CM-ID 行，被設計以包含多媒體之識別碼，
- W-ID 行，被設計以包含接收裝置 6 之計數器之識別碼，
- Nb-TK 行，被設計以包含用於增加計數器之數值之步驟號碼，
- TK-C 行，被設計以包含用於縮減計數器之當前數值之步驟號碼，

- I-TK-A 行，被設計以包含待產生之計數器之識別碼，以及
- A-Max 行，被設計以包含計數器之數值之最大閾值。

- 增加或縮減步驟也可被稱為"點 (points)"或"訊標 (tokens)"。

因此，透過接收裝置中待增加、縮減或建立之計數器之有關資訊元素之 CM-ID 行之識別碼，網格 24 能夠實現多媒體內容之關聯。

「第 3 圖」表示計數器 56 之結構之例子。本文中計數器 56 包含：

- W-ID 欄位，被設計以包含計數器 56 之識別碼，

- TK-A 欄位，被設計以儲存計數器 56 之當前數值，

A-Max 欄位，被設計以包含計數器 56 之數值之最大閾值，以及

LUD 欄位，被設計以包含計數器 56 之數值之最新更新之日期。

例如，日期用日、時、分與秒的形式表示。

現在將結合「第 4 圖」之方法描述特定實例中系統 2 之運作，尋求令非推廣內容之觀看取決於先前觀看之推廣內容。例如：

非推廣內容係為電影或電視節目，以及

推廣內容係為廣告序列。

系統 2 開始用於傳送編碼多媒體內容之步驟 68。

首先，在廣播多媒體內容之前，在步驟 70 期間，對於待廣播的每一推廣或非推廣多媒體內容來說，網格 24 係被操作者用提供的資訊填充。更特別地，對於每一推廣內容來說，CM-ID、W-ID、Nb-TK、I-TK-A 與 A-Max 行用資訊填充，而 TK-C 行為空。例如本文中，對於每一推廣內容來說，CM-ID、W-ID、Nb-TK、I-TK-A 與 A-Max 行分別包含以下數值：CP1、C1、"10"、"10"與"30"。識別碼 CP1 係為與每一推廣內容關聯之數值，識別碼 C1 係為計數器 56 之數值。

對於每一非推廣內容來說，CM-ID、W-ID 與 TK-C 行被填充，而 Nb-TK、I-TK-A 與 A-Max 行未被填充。本文中，這組 Nb-TK、I-TK-A 與 A-Max 分別包含以下數值：CNP1、C1 與"1"。識別碼 CP1 係為與每一非推廣內容關聯之數值。

然後，在廣播多媒體內容之每一金鑰效期期間，在步驟 74 處，產生器 20 產生授權控制訊息。授權控制訊息包含：

控制字 CW 之密碼電文 CW*，在下一金鑰效期期間，擾碼器 10 用以擾亂多媒體內容，

視具體情況，授權多媒體內容之解擾所需要的一或多個存取條件，以及

視具體情況，計數器 56 之前進或迴歸（regression）指令。

本文中，包含前進指令之授權控制訊息被表示為 ECMCP。包含迴歸指令之授權控制訊息被表示為 ECMCNP。既不包含計數器 56 之迴歸指令也不包含計數器 56 之前進指令之授權控制訊息被表示為 ECMN。

更特別地，當正在廣播的多媒體內容為推廣多媒體內容時，產生器 20 產生 ECMCP 訊息。

「第 5 圖」所示係為此 ECMCP 訊息之可能結構之一個例子。

ECMCP 訊息包含以下欄位：

HD 欄位，係為 ECMCP 訊息之標頭欄位，包含能夠使用此訊息之全部資料，例如用於解密密碼電文 CW* 之服務金鑰之索引與／或安全處理器中有關服務區域之識別碼，

CW* 欄位，包含用於擾亂推廣內容之控制字 CW 之密碼電文 CW*，

D 欄位，包含當前日期，

AC 區域，視具體情況，包含推廣內容之一或多個存取條件，

CU 區域，包含前進指令，

WCR 區域，包含計數器之產生指令，以及

S 欄位，包含此 ECMCP 訊息之簽名。

通常，在 ECMCP 訊息中，沒有關於計數器 56 之數值之存取條件。

CU 區域包含：

W-ID 欄位，打算用於包含待增加之計數器之識別碼，以及

Nb-TK 欄位，包含計數器之數值必須被增加之步驟數。

例如，遞增步長等於“1”。

WCR 區域包含：

I-TK-A 欄位，包含待產生之計數器之初值，以及

A-Max 欄位，包含待產生之計數器之最大閥值。

在接收期間，S 欄位中包含的簽名用於驗證 ECMCP 訊息之完整性。例如，此簽名係透過應用至之 ECMCP 訊息之內容之散列（hash）或訊息鑑別碼（Message Authentication Code；MAC）而得到。

為了補全 CU 與 WCR 區域之數值，產生器 20 使用廣播多媒體內容之識別碼與網格 24 之內容。例如，W-ID、Nb-TK、I-TK-A 與 A-Max 欄位分別為以下數值：C1、“10”、“10”與“30”。

「第 6 圖」表示與每一廣播非推廣內容關聯之 ECMCNP 訊息之結構之例子。ECMCNP 之結構等於 ECMCP 訊息之結構，除了以下之外：

它不包含 CU 與 WCR 區域，以及

AC 區域包含取決於計數器 56 之數值之存取條件。

本文中，此存取條件透過以下欄位被編碼：

A-CND1 欄位，用於包含存取條件之識別碼，

W-ID 欄位，用於包含其數值必須被驗證之計數器之識別碼，
以及

TK-C 欄位，用於包含計數器之數值之迴歸指令。

本文中，迴歸指令對應一系列遞減步驟，必須縮減計數器之當前數值。遞減步長（step）被選擇為等於“1”。

正如在 ECMCNP 之實例中，W-ID 與 TK-C 欄位的數值透過非推廣內容之識別碼與網格 24 之內容而得到。這裡，W-ID 與 TK-C 欄位分別包含數值 C1 與“1”。

AC 區域可以包含其他存取條件。例如，在「第 6 圖」中，圖中表示第二存取條件之第一 A-CND2 欄位。

ECMN 訊息之結構或者缺乏包含計數器之數值之前進指令或者迴歸指令之欄位，或者包含與計數器 56 不同之計數器之數值之前進或迴歸指令。因此，訊息之結構係從上述授權控制訊息之結構而推理得出。

與步驟 74 並行，在步驟 82 期間，廣播之多媒體資料內容之每一金鑰效期透過當前控制字 CW 被擾亂。

然後，在步驟 84 中，編密多媒體內容及其關聯的授權控制訊息被多工以產生多工資料流。

在步驟 86 中，此多工資料流藉由傳送裝置 4 透過網路 30 被廣播至接收裝置。

對於每一金鑰效期，循環重複步驟 74、82、84 與 86，從而廣播多媒體內容之連續金鑰效期。

同時，每一接收裝置完成步驟 90，以接收這些編密多媒體內容。

起初，在步驟 92 中，解擾器 40 接收並解多工此接收的多工資料流。然後，編密多媒體內容被傳送至解擾器 46，而授權控制訊息被傳送至處理器 48。

在步驟 94 中，電子計算機 50 驗證接收的授權控制訊息之簽名 S。如果授權控制訊息受到破壞，電子計算機 50 繼續步驟 96 以禁止解擾多媒體內容。例如，在步驟 96 期間，處理器 48 禁止密碼電文 CW*之解密，這樣可能解擾多媒體內容。在步驟 96 處，因此不會授權觀看明文形式的多媒體內容。

若非如此，在步驟 98 處，電子計算機 50 比較接收之授權控制訊息中包含的存取條件與存取權 54。在步驟 98 中，TK-C 欄位定義的存取條件未被確定。如果記憶體 52 未包含存取條件之對應的存取權，然後電子計算機 50 繼續步驟 96。

若非如此，繼續步驟 100 以驗證接收的授權控制訊息中計數器識別碼之存在。在 CU 區域之 W-ID 欄位或者 AC 區域之 W-ID 欄位中尋找此識別碼。

如果授權控制訊息中不包含計數器識別碼，然後此多媒體內

容之觀看取決於推廣內容之先前觀看。例如，可以為不包含任何 CU 區域之 ECMN 訊息以及令計數器之數值產生影響之存取條件。在這種條件下，操作直接地先於步驟 102，其中電子計算機 50 解密密碼電文 CW* 以獲得控制字 CW，並且將其傳送至解擾器 46。然後，解擾器 46 透過此控制字解擾接收的多媒體內容之以下金鑰效期，並且傳送解擾之多媒體內容至電視機 60，電視機 60 則以明文形式顯示。因為多媒體內容以使用者可直接觀看與理解的方式被顯示，所以授權觀看此多媒體內容。

若非如此，在步驟 104 期間，電子計算機 50 檢查以查看步驟 100 中發現的計數器識別碼對應記憶體 52 中已經存在的計數器。如果答案為否，然後在步驟 106 中，電腦檢查以查看 WCR 區域是否存在於接收的授權控制訊息中。如果答案為否，然後處理器 48 直接地前往步驟 96。如果答案為肯定，然後在步驟 108 處，電子計算機 50 用「第 3 圖」描述之結構在記憶體 52 中建立計數器。建立的計數器之 W-ID、TK-A、A-Max 與 LUD 欄位之數值分別從接收的授權控制訊息之 W-ID、I-TK-A、A-Max 與 D 欄位之數值開始。因此，如果在第一次接收非推廣內容時尚未存在計數器 56，在步驟 108 處自動地建立此計數器。

如果 W-ID 欄位中包含的識別碼對應之計數器已經存在於記憶體 52 中或者在步驟 108 之結束處，電子計算機 50 繼續步驟 110 以檢查接收的授權控制訊息中 Nb-TK 欄位之存在。

如果答案為是，接收的授權控制訊息係為 ECMCP 訊息。然

後，在步驟 112 處，電子計算機 50 檢查以查看此計數器之 LUD 欄位中包含的日期是否先於接收的權利訊息之 D 欄位中包含的日期。

如果答案為是，然後在步驟 114 處，藉由接收的授權控制訊息之 Nb_TK 欄位中指示的步驟號，電腦 50 增加此計數器 56 之 TK-A 欄位中包含的數值。在步驟 114 處，如果需要，電腦則限制電腦值數值之增加，從而不會超出 A-Max 欄位中指示的閾值。然後，計數器之新數值被儲存，直到下一次重複步驟 114 為止。

在步驟 114 處，在接收的授權控制訊息之 D 欄位中包含的日期的基礎上，計數器 56 之 LUD 欄位也被更新。

在步驟 114 之結束處或者如果用於更新計數器 56 之最後日期在接收的授權控制訊息中包含的日期之後，處理器直接地前往步驟 102。

如果接收的權利訊息中不存在 Nb-TK 欄位，這表示此訊息係為 ECMCNP 訊息。然後，電子計算機 50 前往步驟 116，以檢查接收的授權控制訊息之 AC 區域中 TK-C 欄位之存在。如果有效接收的授權控制訊息包含此欄位，那麼這表示當前廣播的多媒體內容係為其觀看取決於其他多媒體內容之先前觀看之多媒體內容。

在這種情況下，在步驟 118 處，電子計算機 50 檢查以查看步驟 100 處識別的計數器之當前數值比 TK-C 欄位中包含的數值高。如果答案為否，操作係直接地執行步驟 96，因此禁止觀看此多媒體內容。

若非如此，在步驟 120 處，依照接收之授權控制訊息之 TK-C 欄位中包含的數值所定義的步驟數，電子計算機 50 縮減識別計數器之當前數值。在步驟 120 處，計數器之 LUD 欄位中包含的日期也被接收的授權控制訊息中包含的日期所替代。

在步驟 120 之結束處，或者如果在步驟 116 處授權控制訊息不包含 TK-C 欄位，操作直接地執行步驟 102。

「第 7 圖」給出計數器 56 之數值之進展之例子。

在「第 7 圖」中，最上條表示時間上連續的非推廣內容 130、推廣內容 131 與非推廣內容 132。

資料條 134 表示八個連續的金鑰效期 CP1 至 CP8，覆蓋接收內容 130 至 132 期間之時間間隔。

資料條 136 表示授權控制訊息之傳送瞬時。本文中，在其關聯之多媒體內容之金鑰效期先前的金鑰效期期間，每一授權控制訊息被傳送至接收裝置。因此，訊息 ECM2 至 ECM9 分別關聯金鑰效期 CP2 至 CP9。當此欄位為負時，方括號之間的數值表示授權控制訊息之 TK-C 欄位中包含的數值，或者當此欄位為正時，方括號之間的數值表示 Nb-TK 欄位中包含的數值。因此，可注意到 ECM5 與 ECM6 訊息係為與內容 131 關聯之 ECMCP 訊息。表示的其他訊息係為 ECMCNP 訊息。

資料條 138 表示計數器 56 之 TK-A 欄位之數值。資料條 140 用灰色表示期間可觀看非推廣內容之金鑰效期以及用黑色表示不可觀看非推廣內容之金鑰效期。

更特別地，在金鑰效期 CP1 期間，計數器 56 的數值等於“1”。因此，因為 ECM2 訊息之 TK-C 欄位等於“1”，金鑰效期 CP2 期間多媒體內容之解擾被授權。在金鑰效期 CP1 期間，ECM2 訊息之處理導致計數器 56 之數值遞減“1”，這樣金鑰效期 CP2 期間此數值為“0”。

然後，金鑰效期 CP2 期間，ECM3 訊息之 TK-C 欄位之數值與計數器 56 之當前數值比較。這次，計數器 56 之數值小於 TK-C 欄位之數值。因此，下一金鑰效期 CP3 期間，非推廣多媒體內容之解擾被禁止。此例子中，「第 4 圖」之執行方法還導致在金鑰效期 CP4 期間禁止觀看內容 130。

在金鑰效期 CP4 期間，電子計算機 50 接收訊息 ECM5，其中 MB-TK 欄位之數值等於“10”。因此，在金鑰效期 CP5 期間，計數器 56 之數值被增加 10，並且內容 131 之觀看被授權。

在下一金鑰效期 CP5 期間，另一 ECMCP 訊息被接收，這樣計數器 56 之數值再次被增加“10”。

然後，為了解擾內容 132，僅僅 ECMCNP 訊息被接收。因此，計數器 56 之數值在每一金鑰效期 CP6 與 CP7 之結束處被減縮“1”。然而，因為計數器 56 之數值大於訊息 ECM7 與 ECM8 之 TK-C 欄位中包含的數值，在金鑰效期 CP6 與 CP7 期間內容 132 之觀看被授權。

因此，將要理解的是，「第 7 圖」之方法授權非推廣內容之觀看週期，係為事前觀看的推廣內容之週期之函數。例如，本文中

觀看非推廣內容之授權時間直接地與觀看的推廣內容之時間成比例。因此，此方法鼓勵使用者觀看推廣內容，同時允許使用者更加靈活地在他的計數器中收集與消磨點數。

「第 8 圖」表示 ECMCP 訊息之結構之另一可能實施例。此實施例中，除了不包含任何 WCR 區域之外，ECMCP 訊息與「第 5 圖」描述的訊息相同。因此，此實施例中，例如計數器 56 之計數器必須在記憶體 52 中或者在傳送期間或者在處理器 48 之製造期間或者透過授權管理訊息(Entitlement Management Message；EMM)被初始化。

現在將參考「第 9 圖」與「第 10 圖」描述「第 4 圖」之方法之另一實施例。

「第 9 圖」之方法除了以下步驟之外，係與「第 4 圖」之方法相同：

在步驟 74 處，產生的 ECMCP 訊息之結構如「第 10 圖」所示，

消除步驟 110、116、118 與 120，以及

步驟 114 之後被引入步驟 162 與 164。

除了 WCR 區域被 RI-C 區域替代之外，「第 10 圖」所示之 ECMCP 訊息之結構與「第 5 圖」所示之 ECMCP 訊息結構相同。RI-C 區域包含指令，如果計數器之數值超出預定閾值 S1，此指令將新的存取權寫入記憶體 52。新的存取權對應非推廣內容之存取條件。更特別地，RI-C 區域包含：

TK-S 欄位，用於包含閾值之數值 S1，以及

RI 數值，當得到閾值 S1 時，包含待記錄於記憶體 52 中的存取權。

較佳地而言，在此實施例中，ECMCNP 訊息缺乏迴歸指令。因此，ECMCNP 訊息之結構與習知授權控制訊息之結構絕對沒有區別。

在步驟 114 增加計數器之數值之後，在步驟 162 中電子計算機 50 檢查以查看計數器的新數值是否已經達到 TK-S 欄位中包含的閾值 S1。如果答案為否定，本發明直接地執行步驟 102。如果答案為肯定，在步驟 164 處電子計算機 50 寫入 RI 欄位中包含的存取權至記憶體 52。然後，再次在步驟 164 處，計數器 56 之數值被重新設置。例如，計數器之數值被重新設置為零或者被縮減數值 S。不重新設置計數器之數值，還可能將閾值 S1 之數值增加一判定的步長值。

此實施例中，每一非推廣內容與存取條件 A-CND 關聯。只要記憶體 52 不包含與此存取條件對應之存取權，則禁止觀看此非推廣內容。當計數器之數值達到閾值 S1 時，然後與此條件 A-CND 對應之存取權自動地被記錄至記憶體 52。因此，被授權觀看接收的下一非推廣內容。如同在「第 4 圖」之實施例中，鼓勵觀看者觀看推廣內容。此外，存取權之記錄能夠實現非推廣內容之可視週期之準確設置。例如，記憶體 52 中記錄的新的存取權授權觀看當日之頻道以及僅僅觀看次日之頻道。

還可能存在很多其他實施例。例如，觀看非推廣多媒體內容可以採用擾亂此內容之外的手段被阻止。此實施例中，上述方法可以被應用於第一與第二多媒體內容未被擾亂之情況中。

作為變體，當解擾器透過電纜接收多媒體內容時，天線 42 被網路配解器替換。例如，電纜係為網際網路電纜。

本文中，對於若干不同的非推廣多媒體內容，計數器之識別碼能夠實現「第 4 圖」與「第 9 圖」之方法之使用與實施，從而提交這些非推廣多媒體內容其一之觀看至特定計數器之數值。在一個特定實施例中，計數器識別碼可以為觀看之頻道號之函數。

然而，作為變體，僅僅一個計數器則可用於全部的非推廣內容。這種情況下，可省略計數器之識別碼。

「第 4 圖」與「第 9 圖」之方法可被修正為，僅僅當推廣內容之一組若干連續金鑰週期已經全部被看到時，才授權增加計數器。為此，授權控制訊息包含一組金鑰週期之開始之指示，然後這組金鑰週期之結束處廣播的後續授權控制訊息包含這組金鑰效期之結束之指示。此外，在這組金鑰效期期間，金鑰效期組之識別碼以及這組金鑰效期之連續性之計數器被插入接收的每一授權控制訊息。根據此資訊，電子計算機 50 確定這組金鑰效期已經即時一個挨一個地全部被接收。如果此次檢查的結果為肯定，計數器的數值則增加 Nb-TK 欄位所指示的步驟數。如果答案為否，即如果金鑰效期之一未被解擾，則計數器的數值保持不變。透過及時或暫時地同步這組金鑰效期與推廣內容，可鼓勵使用者無須改

變中間的頻道而觀看整個推廣內容。

推廣內容之整個分段擴展若干金鑰效期，為了控制計數器 56 之遞增以觀看這種推廣內容之另一方法包含報告這組金鑰效期之開始與結束至與此組關聯之每一授權控制訊息，以及增加本地授權管理訊息之簽名之片段，其中此訊息包含日期、計數器之識別碼以及計數器必須增加之 Nb-TK 欄位之數值。在接收裝置本地建立的授權管理訊息中包含的識別碼之對應計數器增加之前，與透過聯繫此組關聯之授權控制訊息中包含的全部簽名片段而獲得的簽名比較，電子計算機 50 檢查此訊息之簽名。如果兩個簽名一致，則授權增加此計數器之數值。若非如此，則被禁止。

在這些授權控制訊息中，如果可自由地存取推廣內容，則可省略 AC 區域。

已經描述特別實例中推廣內容關聯之前進指令，其中這些指令對應一遞增步長，不同金鑰效期此遞增步長恆定。因此，計數器之遞增與觀看的推廣內容之金鑰效期數直接成比例。作為變體，遞增步長並非恆定，並且在推廣內容之兩個金鑰效期之間變化。

本文中，已經描述特定實例之計數器，其中當看到推廣內容時計數器的數值被增加，當看到非推廣內容時計數器的數值被縮減。另一實施例中，此計數器之數值之變化之意義相反，即當觀看推廣內容時縮減計數器，當觀看非推廣內容時增加計數器。

超過一預定閾值則授權觀看非推廣內容，此預定閾值之數值

之遞增操作可替代計數器之數值之遞增。

增量步長 (increment step) 或縮量步長 (decrement step) 無須為整數。可以為有理數或實數。

在加密金鑰之管理之特定實例中，使用授權控制訊息或授權管理訊息之描述可被應用至傳送控制字之密碼電文以傳送多媒體內容之金鑰管理之各種方法中。

計數器無須被登記在安全處理器之記憶體中。例如，作為變體，藉由安全處理器中包含的金鑰，計數器的數值以加密形式被記錄在解擾器中。

處理器 48 非可拆卸地被整合於解碼器或者解擾器中。相反，解擾器可拆卸。

本文上述內容還可被應用至令觀看非推廣內容取決於相同推廣內容之先前觀看之一定次數。此實例中，例如計數器的數值依照此特定推廣內容之觀看次數被增加。所述授權控制訊息之結構以及上述方法保持不變。僅僅改變方法之使用。

本文上述內容還可被應用至隨選視訊之情況。例如，上述方法可被實施以令隨選視訊之自由觀看取決於先前觀看之一定時間之推廣內容。此實例中，例如這些推廣內容為恰好在隨選視訊之前播放的內容。

第一和第二多媒體內容可以為與非推廣及推廣內容而各自不同。例如，第二內容可以為電視系列之第一劇集，第一多媒體內容可以為此系列之最後劇集。因此，使用者被吸引以查看包含第

一劇集之全部劇集。通常，上述所看內容並非限制於第一與第二多媒體內容之特定類型。

【圖式簡單說明】

第 1 圖所示係為編密多媒體內容之廣播系統之結構示意圖；

第 2 圖所示係為第 1 圖之系統中使用的程式之網格之示意圖；

第 3 圖所示係為第 1 圖之系統中使用的計數器之結構示意圖；

第 4 圖所示係為第一多媒體內容之傳送與接收之方法流程圖，其中第一多媒體內容之觀看取決於第二多媒體之先前觀看；

第 5 圖所示係為第 1 圖之系統中使用的 ECMCP 訊息之結構示意圖；

第 6 圖所示係為第 1 圖之系統中使用的 ECMCNP 訊息之結構示意圖；

第 7 圖所示係為當應用第 4 圖之方法時用於顯示計數器數值之序列之時序示意圖；

第 8 圖所示係為 ECMCP 訊息之另一實施例之結構示意圖；

第 9 圖所示係為第一多媒體內容之傳送與接收方法之另一實施例之流程圖，其中第一多媒體之觀看取決於先前所看的其他多媒體內容；以及

第 10 圖所示係為第 9 圖之方法中使用的 ECMCNP 訊息之結構示意圖。

【主要元件符號說明】

2	系統
4	傳送裝置
6	接收裝置
10	擾碼器
12	埠
14	記憶體
16	多工器
18	產生器
20	產生器
22	記憶體
24	網格
30	網路
40	解擾器
42	天線
44	解多工器
46	解擾器
48	安全處理器
50	電腦
52	記憶體
54	存取權
56	計數器

60		電視機	
130、131、132		內容	
134、136、138、140			資料條

七、申請專利範圍：

1. 一種第一多媒體內容之接收方法，該第一多媒體內容之觀看取決於編密第二多媒體內容之先前觀看，該第二多媒體內容係為與存取控制訊息相關聯之唯一內容，該存取控制訊息包含用於解擾之一控制字之密碼電文以及一相同計數器之數值之前進指令，當該第一與第二多媒體內容之一電子接收裝置執行該前進指令時，該前進指令係依照相同含義修正該相同計數器之全部數值，其特徵在於，該方法包含：

無論何時透過該電子接收裝置觀看一第二多媒體內容，均依照該第二多媒體內容之相關前進指令之函數，修正該計數器之數值(114)；

儲存該計數器之數值(114)，該第二多媒體內容之非連續觀看之間係由不會修正該計數器之數值之另一多媒體內容之觀看打斷；

令該第一多媒體內容之觀看取決於該計數器之一預定數值(118; 98)；以及

無論何時授權該電子接收裝置觀看該第一多媒體內容，該方法均包含依照與前進指令相反之含義修正該計數器之數值(120; 164)。

2. 如請求項第 1 項所述之第一多媒體內容之接收方法，其中在觀看每一第二多媒體內容之前，該方法包含解多工所接收的一多工資料流(92)，該多工資料流包含與前進指令多工之該第二多

媒體內容，並且其中該計數器之數值之修正係為與該第二多媒體內容多工之前進指令之函數。

3. 如請求項 1 所述之第一多媒體內容之接收方法，其中該方法包含從若干可能的計數器中選擇該計數器(112)，該計數器之數值必須依照與前進指令相關聯之該計數器之一識別碼函數被修正。
4. 如請求項 1 所述之第一多媒體內容之接收方法，其中該方法包含：

接收該第二多媒體內容之一組一或多個金鑰效期以及與該組相關聯之前進指令(92)，該第二多媒體內容之每一金鑰效期係透過各自的控制字被解擾；以及

只要該組之全部金鑰效期透過該電子接收裝置被解擾，則修正該計數器之數值(114)。

5. 如請求項第 4 項所述之第一多媒體內容之接收方法，其中在該第二多媒體內容之一金鑰效期之前，該方法包含接收同時廣播至全部接收裝置之一訊息，該接收裝置能夠接收該第一與第二多媒體內容，該訊息包含解擾該金鑰效期所需之該控制字之密碼電文以及與該金鑰效期所屬的該組相關聯之前進指令。
6. 如請求項 1 所述之第一多媒體內容之接收方法，其中該方法包含：

接收該第一多媒體內容之一組一或多個金鑰效期以及與該組相關聯之該計數器之數值之迴歸指令(92)，每一金鑰效期係透

過各自的控制字被加密；

只要該組之全部金鑰效期被解擾，則依照與該前進指令相反之含義並依照與該組相關聯之該迴歸指令之函數，修正該計數器之數值(120)；以及

只要該計數器之數值達到一預定閾值，則禁止解擾該第一多媒體內容之下一組金鑰效期。

7. 如請求項 1 所述之第一多媒體內容之接收方法，其中該方法包含：

接收該第一編密多媒體內容以及該第一多媒體內容之存取條件；

如果沒有存取權與該電子接收裝置中記錄的該存取條件對應，則禁止解擾該第一多媒體內容，並且相反地；

如果一存取權與該電子接收裝置中記錄的該第一多媒體內容之該存取條件對應，則授權解擾該第一多媒體內容；以及

只要該計數器之數值超出一預定閾值，則將與存取條件對應之一存取權寫入該接收裝置。

8. 如請求項 1 所述之第一多媒體內容之接收方法，其中該方法包含限制該計數器之數值為一預定閾值。

9. 如請求項 1 所述之第一多媒體內容之接收方法，其中該方法包含自動創建該計數器(108)，以回應接收該計數器之數值之前進指令。

10. 一種資訊記錄載體，其特徵在於：該資訊記錄載體包含指令，

當該指令被一電子計算機執行時，該指令係用於執行上述請求項第 1~9 項其一所述之第一多媒體內容之接收方法。

11. 一種第一編密多媒體內容之傳送方法，其中該第一編密多媒體內容之觀看取決於編密第二多媒體內容之先前觀看，該第二多媒體內容係為與存取控制訊息相關聯之唯一內容，該存取控制訊息包含用於解擾之一控制字之一密碼電文以及該第一與第二多媒體內容之一電子接收裝置之一相同計數器之數值之前進指令，當該前進指令被該電子接收裝置執行時，該前進指令係依照相同含義修正該相同計數器之全部數值，其特徵在於，該方法包含：

傳送與傳送之每一第二多媒體內容相關聯之該存取控制訊息(86)；

在兩個第二多媒體內容之間傳送與包含有用於修正計數器數值之指令之存取控制訊息沒有關聯的其它多媒體內容(86)；以及

令該第一多媒體內容之觀看取決於該計數器之一預定數值(118; 98)；以及

傳送與傳送的該第一多媒體內容相關聯之存取條件，該存取條件令該第一多媒體內容之觀看取決於該計數器之一預定數值(86)。

12. 如請求項第 11 項所述之第一編密多媒體內容之傳送方法，其中該方法包含：傳送與傳送的該第一多媒體內容相關聯之該

計數器之數值之迴歸指令(86)，當授權觀看該第一多媒體內容時，該迴歸指令能夠增加該相同計數器之數值與該預定數值之間的差值。

13. 一種第一編密多媒體內容之接收裝置，其中該第一編密多媒體內容之觀看取決於編密第二多媒體內容之先前觀看，該第二多媒體內容係為與存取控制訊息相關聯之唯一內容，該存取控制訊息包含用於解擾之一控制字之一密碼電文以及一相同計數器之數值之前進指令，當該前進指令被第一與第二多媒體內容之該電子接收裝置執行時，該前進指令係依照相同含義修正該相同計數器之全部數值，其特徵在於，該接收裝置包含：

一記憶體，係能夠儲存該計數器之數值，其中該第二多媒體內容之非連續觀看之間係由不會修正該計數器之數值的另一多媒體內容之觀看打斷；以及

一電子計算機(52)，係能夠：

只要一第二多媒體內容透過該接收裝置被觀看，則依照所接收的與該第二多媒體內容相關聯之前進指令之函數，修正該計數器之數值；

令該第一多媒體內容之觀看取決於該計數器之一預定數值；以及

只要授權透過該電子接收裝置觀看該第一多媒體內容，則依照與該前進指令相反之含義修正該計數器之數值。

14. 一種安全處理器，係能夠實施於符合請求項 13 所述之該接收

裝置中，其特徵在於，該安全處理器包含一電子計算機，係能夠：

只要一第二多媒體內容透過該接收裝置被觀看，則依照所接收的與該第二多媒體內容相關聯之前進指令之函數，修正該計數器之數值；

令該第一多媒體內容之觀看取決於該計數器之一預定數值；以及

只要授權透過該電子接收裝置觀看該第一多媒體內容，則依照與該前進指令相反之含義修正該計數器之數值。

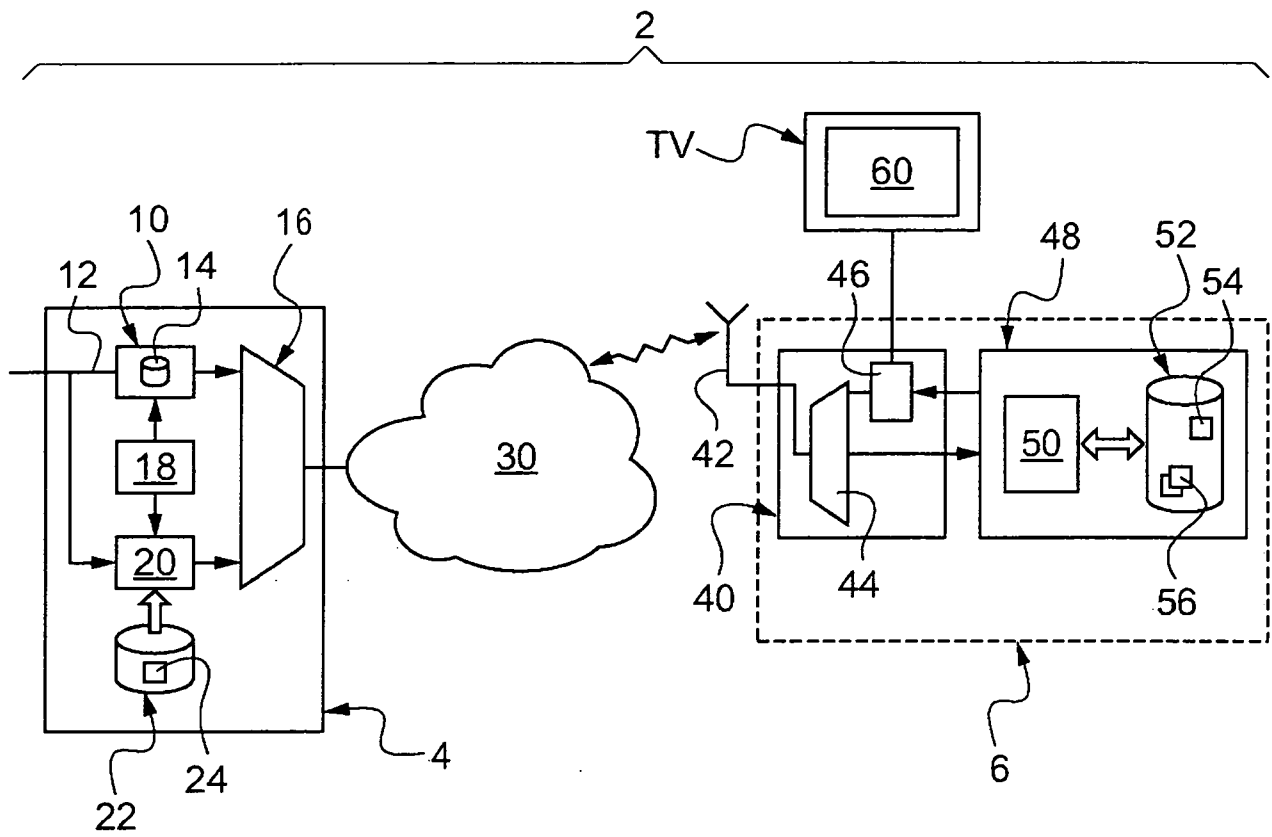
15. 一種第一編密多媒體內容之傳送裝置，其中該第一編密多媒體內容之觀看取決於編密第二多媒體內容之先前觀看，該第二多媒體內容係為與存取控制訊息相關聯之唯一內容，該存取控制訊息包含用於解擾之一控制字之一密碼電文以及該第一與第二多媒體內容之一電子接收裝置之一相同計數器之數值之前進指令，當該前進指令被該第一與第二多媒體內容之該電子接收裝置執行時，該前進指令係依照相同含義修正該相同計數器之全部數值，其特徵在於，該傳送裝置(4)係能夠：

傳送與傳送之每一多媒體內容相關聯之存取控制訊息；

在兩個第二多媒體內容之間傳送與計數器數值之前進指令沒有關聯的其它多媒體內容；以及

傳送與傳送的該第一多媒體內容相關聯之存取條件，該存取條件令該第一多媒體內容之觀看取決於該計數器之一預定

數值。



第1圖

24

CM_ID	W-ID	Nb_TK	TK_C	I_TK_A	A_Max
CP1	C1	10		10	30
CNP1	C1		1		

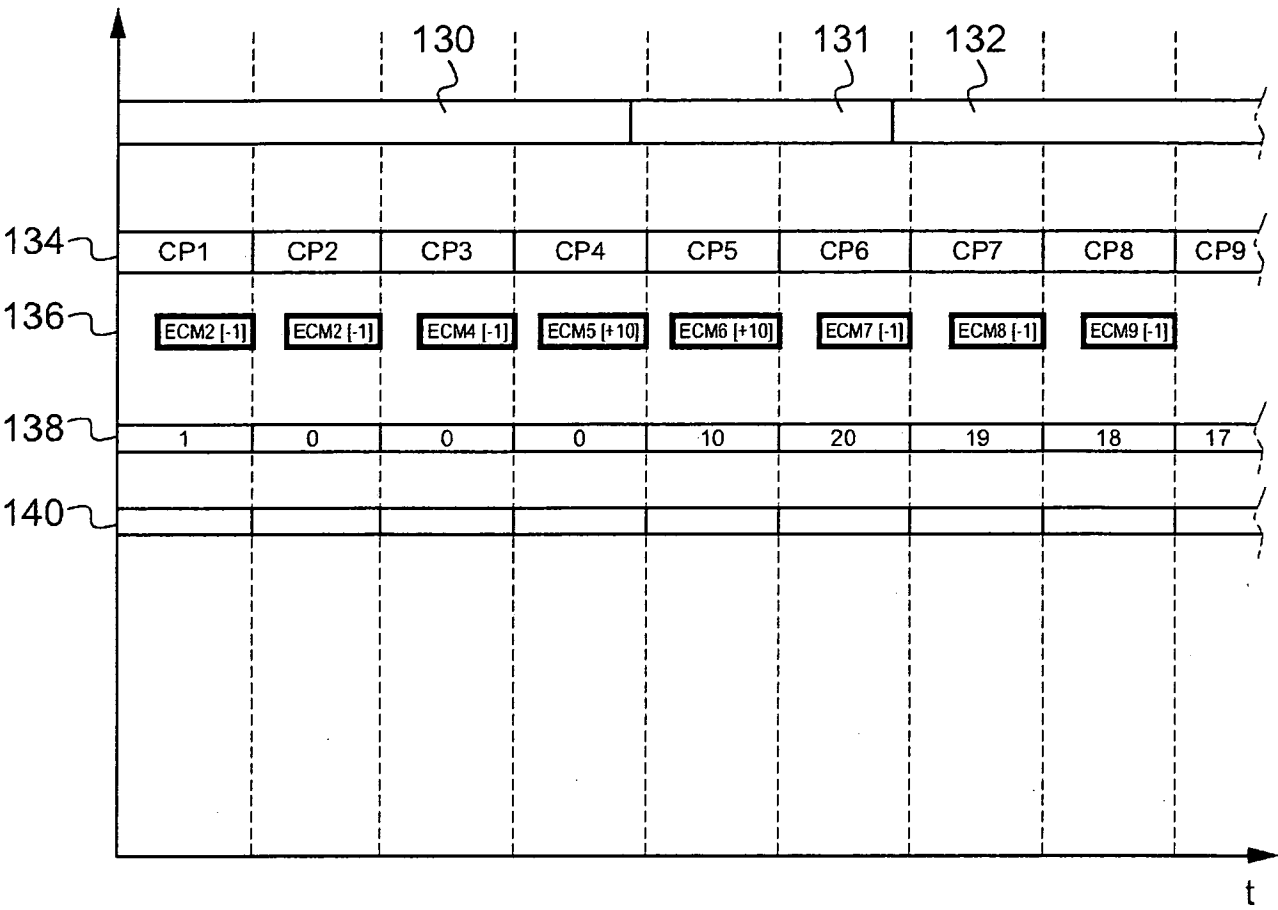
第2圖

56

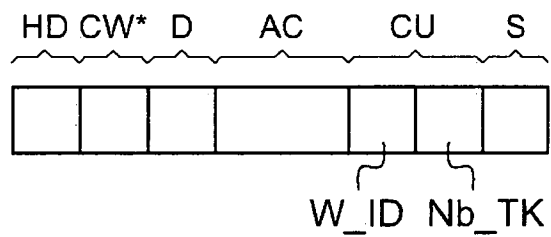
W_ID	TK_A	A_Max	LUD
------	------	-------	-----

第3圖

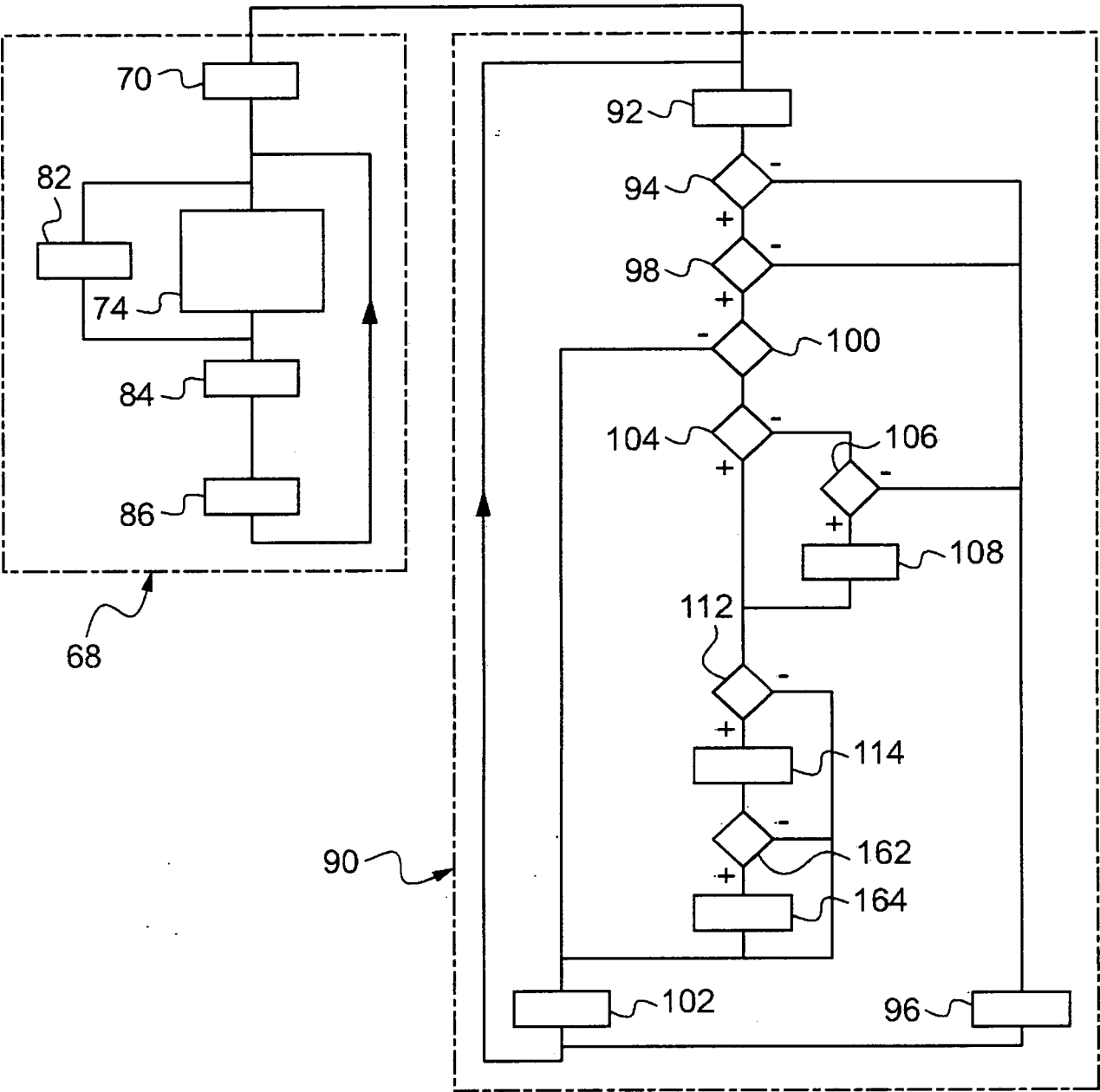
第 2 頁



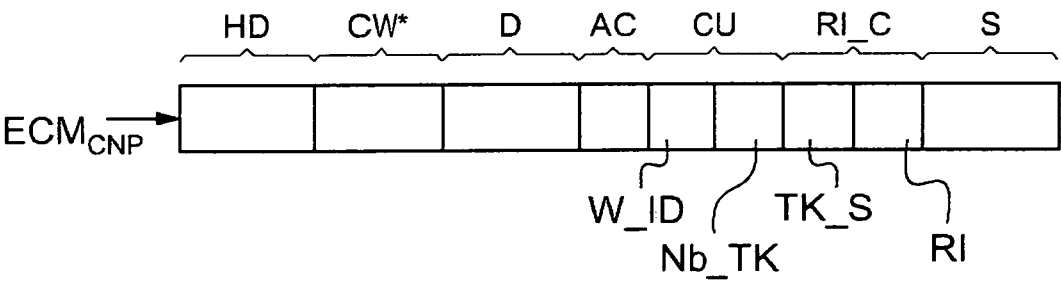
第7圖



第8圖



第9圖



第10圖