



(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 I404385B1

(45)公告日：中華民國 102 (2013) 年 08 月 01 日

(21)申請案號：098121442

(22)申請日：中華民國 98 (2009) 年 06 月 25 日

(51)Int. Cl. : **H04L29/06 (2006.01)**

(30)優先權：2008/07/01 美國 12/166,039

(71)申請人：斯靈媒體公司 (美國) SLING MEDIA, INC. (US)
美國

(72)發明人：雷歐 帕曼納伯哈 R RAO, PADMANABHA R. (US)

(74)代理人：陳長文

(56)參考文獻：

US 2002/0196939A1

WO 2007/141555A2

審查人員：柯建羽

申請專利範圍項數：38 項 圖式數：4 共 0 頁

(54)名稱

安全位移媒體內容之系統及方法

SYSTEMS AND METHODS FOR SECURELY PLACE SHIFTING MEDIA CONTENT

(57)摘要

本發明提供經由一通信網路將一位移媒體流從一位移裝置安全提供至一遠端播放器之系統及方法。經由該通信網路於該位移裝置處從該遠端播放器接收針對一連接之一請求。回應於針對該連接之該請求，經由該通信網路從一中央伺服器請求一授權憑證。另外，回應於從該中央伺服器接收之該授權憑證，可透過該通信網路在該位移裝置與該遠端播放器間建立該位移媒體流。可基於該授權憑證加密該位移媒體流之至少一部分。

Systems and methods are provided for securely providing a place-shifted media stream from a place shifting device to a remote player via a communications network. A request for a connection is received from the remote player at the place shifting device via the communications network. In response to the request for the connection, an authorization credential is requested from a central server via the communications network. Further, in response to the authorization credential received from the central server, the place-shifted media stream between the place shifting device and the remote player can be established over the communications network. At least a portion of the place-shifted media stream may be encrypted based upon the authorization credential.

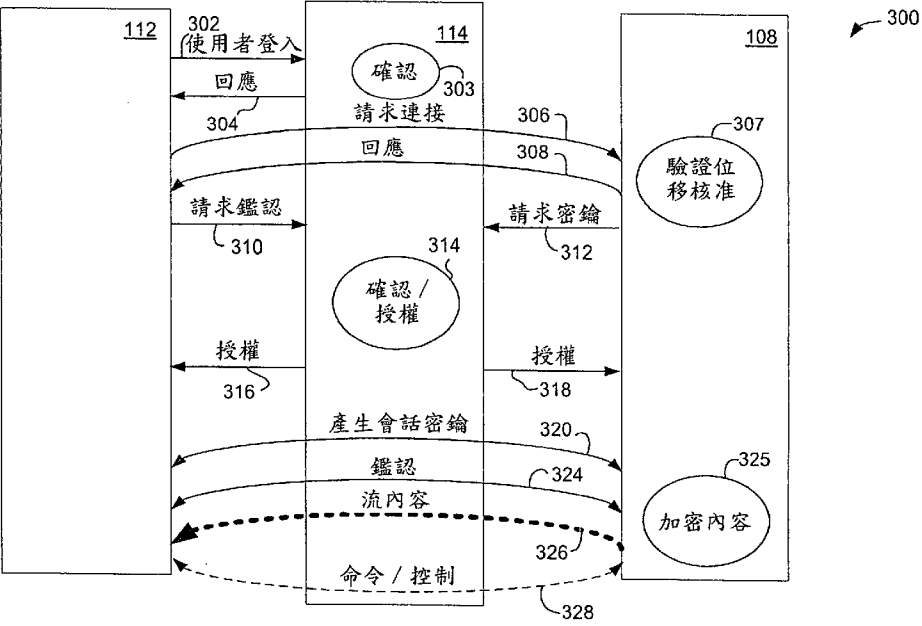


圖 3

108 . . . 位移裝置/
位移器裝置/混合裝置/
組件裝置/裝置
112 . . . 遠端裝置/
遠端檢視器/行動裝置
114 . . . 中央伺服
器/後端伺服器

發明專利說明書

公告本

(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：98/1442

※申請日：98.6.25

※IPC 分類：

一、發明名稱：(中文/英文)

H04L 29/06 (2006.01)

安全位移媒體內容之系統及方法

SYSTEMS AND METHODS FOR SECURELY PLACE SHIFTING MEDIA
CONTENT

二、中文發明摘要：

本發明提供經由一通信網路將一位移媒體流從一位移裝置安全提供至一遠端播放器之系統及方法。經由該通信網路於該位移裝置處從該遠端播放器接收針對一連接之一請求。回應於針對該連接之該請求，經由該通信網路從一中央伺服器請求一授權憑證。另外，回應於從該中央伺服器接收之該授權憑證，可透過該通信網路在該位移裝置與該遠端播放器間建立該位移媒體流。可基於該授權憑證加密該位移媒體流之至少一部分。

三、英文發明摘要：

Systems and methods are provided for securely providing a place-shifted media stream from a place shifting device to a remote player via a communications network. A request for a connection is received from the remote player at the place shifting device via the communications network. In response to the request for the connection, an authorization credential is requested from a central server via the communications network. Further, in response to the authorization credential received from the central server, the place-shifted media stream between the place shifting device and the remote player can be established over the communications network. At least a portion of the place-shifted media stream may be encrypted based upon the authorization credential.

四、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：

108	位移裝置/位移器裝置/混合裝置/組 件裝置/裝置
112	遠端裝置/遠端檢視器/行動裝置
114	中央伺服器/後端伺服器

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】

本發明一般係關於媒體內容之位移，且更特定言之係關於用於改良媒體位移之安全性的系統及方法。

【先前技術】

大多數電視檢視者現在透過內容整合者(例如有線或衛星電視提供者)接收其電視信號。對於直接廣播衛星(DBS)服務的訂戶端，例如，經由廣播接收電視節目，廣播係經由衛星傳送至天線，天線一般位於家或其他結構之外部上。其他客戶透過電纜、無線或其他媒體接收電視節目。節目通常係在接收器處接收，例如「視訊轉換器」(STB)，其解調變接收到的信號並且將解調變之內容轉換成可在電視或其他顯示器上呈現至檢視者的格式。

最近，消費者已對允許在除其主要電視機以外的位置檢視電視或其他媒體內容之「位移」裝置表達明顯興趣。位移裝置通常封包化可透過區域或廣域網路發送至可攜式電腦、行動電話、個人數位助理或能夠為檢視者播放封包化媒體流之其他遠端裝置的媒體內容。因此位移允許消費者從諸如酒店房間、辦公室的遠端位置或可攜式媒體播放器裝置可存取無線或其他通信網路的任何其他位置檢視其媒體內容。

雖然位移確實顯著改良給予檢視者之便利性，許多通信網路(例如網際網路)之固有不安全性質繼續造成挑戰。即，雖然仍需要允許消費者位移其媒體播放體驗，亦需要

確保僅允許授權使用者及播放器存取寶貴媒體內容。

因此需要建立將媒體內容從位移裝置安全位移至遠端媒體播放器的系統及方法。結合附圖及此先前技術段落，從其後詳細說明及隨附申請專利範圍將會明白該等及其他期望特徵及特性。

【發明內容】

提供經由通信網路將位移媒體流從位移裝置安全提供至遠端播放器之各種系統及方法。經由通信網路於位移裝置處從遠端播放器接收用於連接之請求。回應於用於連接之請求，經由通信網路從中央伺服器請求授權憑證。另外，回應於從中央伺服器接收之授權憑證，可透過通信網路在位移裝置與遠端播放器間建立位移媒體流。基於授權憑證加密位移媒體流之至少一部分。

其他具體實施例提供經由通信網路將位移媒體流安全提供至遠端播放器之系統。該系統包含對通信網路之網路介面以及對與通信網路分離之媒體的接收器介面。接收器經組態用以從接收器介面接收媒體內容，且轉碼器經組態用以封包化接收到的媒體內容以便透過通信網路傳輸。至少與網路介面及轉碼器通信的控制電路經組態用以經由網路介面從遠端播放器接收用於連接之請求，回應於用於連接之請求以經由網路介面從中央伺服器請求授權憑證，以及回應於經由網路介面從中央伺服器接收授權憑證以經由網路介面對遠端播放器建立位移媒體流。在各種具體實施例中，可基於授權憑證加密位移媒體流之至少一部分。

其他具體實施例提供將位移媒體流呈現至遠端裝置之使用者的方法，其中透過通信網路將位移媒體流從位移裝置提供至遠端裝置。經由通信網路對中央伺服器鑑認使用者。在中央伺服器之成功鑑認後，請求對位移裝置之連接。在從位移裝置接收回應後，請求授權以經由通信網路從中央伺服器連接至位移裝置。經由通信網路從中央伺服器接收包含授權憑證之授權回應，且建立位移媒體流。在各種具體實施例中，可基於授權憑證加密位移媒體流之至少一部分。

其他具體實施例提供允許將位移媒體流提供至遠端裝置之使用者的方法，其中透過通信網路將位移媒體流從位移裝置提供至遠端裝置。經由通信網路從遠端裝置接收第一請求，其中第一請求包含與使用者相關聯之使用者憑證。驗證使用者憑證以及，回應於成功驗證，將第一回應發送至識別位移裝置之遠端裝置。接著回應於來自遠端裝置之第二請求以將鑑認憑證發送至遠端裝置且回應於來自位移裝置之密鑰請求以將鑑認憑證發送至位移裝置，以藉此允許遠端裝置及位移裝置至少部分基於鑑認憑證建立位移媒體流。在各種具體實施例中，可基於授權憑證加密位移媒體流之至少一部分。

以下詳細說明各種其他具體實施例、態樣及其他特徵。

【實施方式】

以下本發明之詳細說明實質上僅係示範性，而非限制本發明或本發明之應用及使用。再者，亦不受前述技術領域

或以下實施方式內提出的任何理論之限制。

一般而言，透過各種鑑認及/或加密特徵之使用使得媒體內容之位移更加安全。在各種具體實施例中，位移裝置驗證其具有核准能力以提供位移功能。此驗證可係基於在位移裝置上由人設定或修改之「權利」。或者，位移「權利」可基於經由亦提供節目內容至裝置的衛星、電纜或其他連接接收的資訊加以設定或修改。在其他具體實施例中，可實行即時(或幾乎即時)鑑認以對中央伺服器及/或對位移裝置鑑認使用者，及/或以驗證請求遠端播放器/裝置係可信且經核准以接收位移內容。可進一步建構憑證共享環境以便發送及接收裝置從安全中央伺服器接收密碼密鑰及/或其他憑證。從中央伺服器提供之鑑認憑證可用於加密位移媒體流之一些或全部。在各種其他具體實施例中，基於諸如視訊流之品質、遠端媒體播放器之處理能力、插入通信鏈路之頻寬的因素及/或其他因素視情況調整加密數量。本文所說明之各種概念可彼此獨立地部署，或者兩個或兩個以上可以任何方式彼此組合以產生更安全的位移環境。

本文所說明之安全機制在與既能接收電視信號(例如從衛星、電纜、無線或其他來源饋送之信號)也能提供位移功能的硬體同用時可找到特定優點。然而本發明並不限於此，相反，本文所說明之安全特徵可結合習知位移系統及裝置使用，包括與諸如電視接收器、可卸除式媒體播放器、數位或個人錄影機及/或節目內容之其他來源的其他

外部裝置互動的位移系統及裝置。

現在轉看圖式並首先參考圖1，範例性位移系統100合適地包括位移裝置108，其封包化媒體內容以便透過通信網路102傳輸至遠端裝置112。在提供增強安全性之具體實施例中，維持資訊資料庫116之中央伺服器114亦能夠經由網路102與位移裝置108及遠端裝置112通信。儘管圖1僅顯示單一位移裝置108、單一遠端裝置112及單一中央伺服器114，在實務中，系統100可包括任何數目之伺服器114，其能夠與數百、數千或更多位移裝置108互動，其每一者能夠將媒體內容串流至任何數目之不同遠端裝置112。

網路102係能夠在傳送器與接收器間發送訊息的任何數位或其他通信網路。在各種具體實施例中，網路102包括任何數目之公共或私有資料連接、鏈路或支援任何數目之通信協定的網路。例如，網路102可包括網際網路或基於TCP/IP或其他習知協定的任何其他網路。在各種具體實施例中，網路102亦併入無線及/或有線電話網路，例如用於與行動電話、個人數位助理及/或類似物通信的蜂巢式通信網路。網路102亦可併入任何種類之無線或有線區域網路，例如一或多個IEEE 802.3及/或IEEE 802.11網路。因此位移裝置108能夠以任何方式與遠端裝置112通信。此類通信透過廣域鏈路發生，例如，其包括網際網路及/或電話網路；在其他具體實施例中，裝置108與112間之通信可透過併入網路102內之有線或無線區域鏈路發生，且至中央伺服器114之訊息透過亦併入網路102內之廣域鏈路發

生。

位移裝置108係能夠透過網路102發送媒體內容之封包化流的任何組件、硬體、軟體邏輯及/或類似物。在各種具體實施例中，位移裝置102併入適當轉碼器邏輯以將音訊/視訊或其他媒體資料轉換成可透過網路102發送的封包化格式。媒體資料可係任何格式，且可從任何來源接收，例如廣播、電纜或衛星電視節目來源、「隨選視訊」或類似來源、數位視訊光碟(DVD)或其他可卸除式媒體、攝錄影機及/或類似物。在各種具體實施例中，位移器裝置108係可從加州 Foster City 市 Sling Media 公司獲得的各種 SLINGBOX 產品之任何者，其一般能夠從外部數位錄影機(DVR)、視訊轉換器(STB)、有線或衛星節目來源、DVD 播放器及/或類似物接收媒體內容。

在其他具體實施例中，位移器裝置108亦可包括內容接收能力。即，裝置108可係亦提供轉碼及位移特徵的混合 STB 或其他接收器，如以下所更完整地說明。此一裝置可從天線104、數據機、伺服器及/或其他來源接收編碼電視節目105之衛星、電纜、廣播及/或其他信號。接收器可進一步解調變或以其他方式解碼接收到的信號105以擷取節目，其可視情況在本地檢視及/或位移至遠端檢視器112。此類裝置108亦可包括內容資料庫110，其係儲存於硬碟驅動器、記憶體或其他儲存媒體上以視情況支援個人或數位錄影機(DVR)特徵。

在圖1中所解說之範例性具體實施例中，位移裝置係混

合接收器/轉碼器，其在天線104處從衛星106接收數位廣播衛星(DBS)信號105。但等效具體實施例可從電纜連接、廣播來源、可卸除式媒體、可經由網路102存取之服務提供者、任何外部裝置及/或類似物接收節目105。在包括DVR功能性之具體實施例中，可視需要(例如，回應於使用者/檢視者節目指令)將節目儲存於資料庫110內以便其後在相對緊密靠近地定位的電視或其他顯示器上檢視；但不需要在所有實例或具體實施例中儲存節目，且或者可即時提供節目。如上所述，可在實體上連接至裝置108之電視或其他顯示器上呈現內容，或者可透過網路102從裝置108位移至遠端裝置112。

遠端裝置112係能夠從位移裝置108接收媒體流之任何裝置、組件、模組、硬體、軟體及/或類似物。在各種具體實施例中，遠端裝置112係個人電腦(例如「膝上型電腦」或類似的可攜式電腦，儘管亦可使用桌上型電腦)、行動電話、個人數位助理、個人媒體播放器(例如可從法國Igny市Archos公司獲得的ARCHOS產品)或類似物。在許多具體實施例中，遠端裝置112係通用計算裝置，其包括能夠如以下所更完整地說明安全連接至位移裝置108以及能夠視情況接收及對裝置之使用者呈現媒體內容的軟體或韌體內之媒體播放器應用程式。

可基於可用計算及通信資源以及消費者需求調配許多不同位移情況。在各種具體實施例中，消費者可能希望在家、辦公室或其他結構中位移內容，例如從位移裝置108

至位於另一房間內之桌上型或可攜式電腦。在此類具體實施例中，通常將透過在結構內操作之有線或無線區域網路提供內容流。在其他具體實施例中，消費者可能希望透過寬頻或類似網路連接將內容從主要位置位移至位於第二家、辦公室、酒店或其他遠端位置內的電腦或其他遠端裝置112。在其他具體實施例中，消費者可能希望經由行動鏈路(例如 GSM/EDGE 或 CDMA/EVDO 連接、IEEE 802.11「Wi-fi」鏈路及/或類似物)將內容位移至行動電話、個人數位助理、媒體播放器、視訊遊戲機、汽車或其他車輛媒體播放器及/或其他裝置。可用於各種平臺的位移應用程式之數個範例係由加州 Foster City 市 Sling Media 公司提供，但是本文所說明之概念也可結合可從任何來源獲得的產品及服務使用。

如開始處所述，一般需要維持位移程序之安全性以確保未授權使用者及未授權播放器無法存取節目內容。由於在裝置內可用的寶貴內容之數量可非常大，當位移裝置108係整合接收器/DVR/位移器時尤其如此。為了維持連接之安全性，則各種具體實施例在信任域或授權區120(其可包括位移器裝置108本身)以及藉由服務提供者或其他信任實體維持之任何後端伺服器114、118周圍建立邏輯阻障。藉由需要使用者在安全基礎架構100內互動，可實施適當鑑認或其他安全性機制以防止對包含於信任域120內之資源的未授權存取。

為此目的，服務提供者可提供中央伺服器114，其透過

網路102與位移裝置108及/或行動裝置112互動。伺服器114係能夠回應用於經由網路102接收的資訊之程序請求的任何電腦系統或其他計算資源。例如，伺服器114可維持資料庫116，其視情況包括使用者帳戶資訊以及密碼密鑰或與各種位移裝置108相關聯的其他鑑認憑證。

中央伺服器114以任何方式促進遠端裝置112與位移裝置108間的安全交易。在各種具體實施例中，遠端裝置102之使用者能夠藉由接觸中央伺服器114在網路102上定位位移裝置108，採用userid/密碼對或其他憑證對伺服器114鑑認，且接著接收允許對與資料庫116內之使用者相關聯的一或多個位移裝置108之後續連接請求的資訊。遠端裝置112則能夠經由網路102直接接觸位移裝置108以請求連接。在從位移裝置108及遠端裝置112兩者接收連接請求後，中央伺服器114合適地提供密碼密鑰或其他憑證，其可用於在裝置108與112間視情況且如以下所更完整地說明建立安全媒體流。因此即使不需要以邏輯或實體方式將伺服器114插入通信裝置108與112間，中央伺服器114能夠顯著協助維持位移媒體流之安全性。

在其他具體實施例中，涉及使用者鑑認及/或密鑰管理之伺服器114可與用於額外安全性之一或多個後端伺服器118通信。後端伺服器118可存取記帳資訊，例如，其可針對在伺服器114處接收之資訊交互檢查，以確保請求服務之使用者已正確地為此類服務付費，已維持帳戶聲譽良好，及/或類似情況。對後端伺服器118之查詢可透過除開

網路102之安全鏈路即時(或幾乎即時)處理。在各種具體實施例中，例如，後端伺服器118可加入於至裝置108的衛星或有線電視信號之提供商。在此類具體實施例中，伺服器118可用於確保記帳適應性，但可以任何方式額外地(或替代地)致能對使用者之其他服務。例如，採用伺服器114鑑認之使用者可訂購服務(例如位移特徵之致能)，發出指令以購買付費選看節目或在與裝置108相關聯之DVR上記錄節目，支付帳單，及/或透過網路102之便利性採用後端伺服器118相對於使用者之帳戶採取某一其他動作。在其中使用者已訂購額外服務或內容之具體實施例中，伺服器118可協調經由衛星116(或等效的電纜連接或類似物)發送之訊息以視情況更新裝置108上之設定。由於信任域120內之安全連接係從伺服器114至位移裝置108存在，可致能新服務及特徵而無需橫跨相對不安全網路102之資料傳輸。

圖2提供關於範例性位移裝置108之額外細節，其視情況包括接收器208、解碼器214及位移轉碼器204。儘管圖2說明除位移外能夠接收及解碼內容之混合裝置108，本文提出之概念可等效地應用於僅提供在外部接收器、DVR、媒體播放器、伺服器及/或類似物處接收及/或解碼的媒體內容之位移的裝置108。其他具體實施例可從圖2中所示者併入額外或替代處理模組，可省略圖2中所示之一或多個模組，及/或可以不同於圖2中所示之範例性配置的任何其他方式不同地組織各種模組。

可以任何方式在邏輯上及實體上實施裝置108。圖2顯示

可呈現在範例性裝置108內之各種邏輯及功能特徵；圖式中所示的每一模組可採用任何種類之硬體、軟體、韌體及/或類似物實施。各種模組之任何者可採用任何種類之通用或專用積體電路實施，例如任何種類之微處理器、微控制器、數位信號處理器、程式化陣列及/或類似物。例如，任何數目的圖2中所示之模組可係實施為「晶片上系統」(SoC)，其在任何適當控制邏輯205之控制下使用任何合適的處理電路。在各種具體實施例中，控制邏輯205視情況在整合式SoC或實施接收器208、傳輸選擇器212、解碼器214、顯示處理器218及/或磁碟控制器206的其他處理器內執行。在此類具體實施例中，整合式SoC處理器可與採用分離處理器實施之轉碼器模組204以及任何其他輸入或輸出裝置互動以基於從本地或遠端使用者接收之輸入產生所需輸出。在其他具體實施例中，亦可將轉碼器204併入至SoC設計內。例如，加州Irvine市的Broadcom Corporation公司生產數種處理器模組(例如，型號BCM 7400處理器系列)，其能夠支援衛星及/或電纜接收器系統之SoC實施方案，但是也可等效地使用來自任何數目之其他供應商的產品。在其他具體實施例中，各種不同晶片、電路或組件可係互連且彼此相互關連以實施圖2中所表示之接收及解碼功能。

裝置108之各種具體實施例因此包括任何數目之適當模組，其用於獲得及處理特定具體實施例所需的媒體內容。該等模組之每一者可係使用在任何數目之半導體晶片內執

行的邏輯或其他處理邏輯實施於硬體及/或軟體之任何組合內。

控制邏輯205之各種具體實施例可包括能夠控制各種組件裝置108之任何電路、組件、硬體、軟體及/或韌體邏輯。在裝置108內執行之各種常式、方法及程序通常係在控制邏輯205之控制下執行，如以下所更完整地說明。在許多具體實施例中，相對於圖3說明的各種安全性及鑑認特徵主要係在控制邏輯205內執行，該控制邏輯可在裝置108內之任何處理器上執行。

如上所述，裝置108之許多具體實施例包括接收器208，其係能夠經由一或多個內容來源105接收媒體內容的任何硬體、軟體、韌體及/或其他邏輯。在各種具體實施例中，內容來源105可視情況包括有線電視、DBS、廣播及/或其他節目來源。接收器208適當地選擇所需輸入來源且將接收到的內容提供至適當目的地以供進一步處理。在各種具體實施例中，可將接收到的節目即時(或幾乎即時)提供至傳輸流選擇模組212或用於直接解碼及呈現至使用者之其他組件。或者，在提供DVR功能性之具體實施例中，接收器208可將從任何來源接收之內容提供至磁碟或其他儲存媒體。在此類具體實施例中，裝置108亦可包括磁碟控制器模組206，其與內部或外部磁碟、記憶體及/或在資料庫110內儲存內容的其他裝置互動，如上所說明。

在圖2中所示之具體實施例中，裝置108亦包括適當網路介面210，其使用協定之任何實施方案或其他特徵操作以

藉由在網路102上之裝置108支援通信。在各種具體實施例中，網路介面210支援習知LAN、WAN或其他協定(例如廣泛用於網際網路上之TCP/IP或UDP/IP協定套件)以允許裝置108視需要在網路102上通信。網路介面210通常使用任何種類之LAN轉接器硬體介接網路102，例如提供於裝置108內的習知網路介面卡(NIC)或類似物。

傳輸流選擇模組212係能夠從可用來源選擇所需媒體流之任何硬體及/或軟體邏輯。在圖2中所示之具體實施例中，流選擇模組212能夠產生用於呈現於一或多個輸出介面228上的視訊信號。在各種具體實施例中，流選擇模組212亦能夠將經編碼視訊信號236提供至轉碼模組204，但此特徵完全係可選。然而，在此類具體實施例中，轉碼模組204將針對封包化及透過網路102的後續發送而解碼視訊信號236，如其他處所說明。

然而，更通常地說，流選擇模組212回應檢視者輸入(例如，經由控制邏輯205)以簡單地將從實況來源105或從儲存器110接收的經編碼內容切換至一或多個解碼器模組214。裝置108可視需要包括用於解碼、解壓縮及/或以其他方式處理接收到的/儲存的內容之任何數目之解碼器模組214。一般而言，解碼器模組214解壓縮或以其他方式處理來自流選擇模組212之接收到的內容，以擷取在流內編碼之MPEG或其他媒體流。接著可藉由顯示處理器模組218處理經解碼內容以按任何適當格式為檢視者建立顯示。

顯示處理器模組218包括任何適當硬體、軟體及/或其他

邏輯以視需要在介面 242、244、246 處建立所需螢幕顯示。在各種具體實施例中，顯示處理模組 218 亦能夠針對隨具體實施例而變更的電子程式導引、設置及控制、輸入/輸出促進及/或其他特徵產生螢幕上顯示(on screen display；OSD)。此類顯示通常並非包含於接收到的或儲存的廣播流內，但仍對與裝置 108 或類似物互動之使用者有用。接著可以任何所需格式將產生之顯示(包括接收到的/儲存的內容及任何其他顯示)呈現至一或多個輸出介面 228。在各種具體實施例中，顯示處理器 218 產生以任何標準格式(例如用於標準清晰度電視信號之 ITU656 格式或用於高清晰度電視信號之任何格式)編碼之輸出信號，其可在介面 228 處容易地轉換至標準及/或高清晰度電視信號。

在混合接收器/位移器裝置 108 中，亦可提供硬體或軟體切換器 226，其允許將一或多個輸出通道轉移至轉碼模組 204 以便透過網路 102 位移。在此類具體實施例中，切換器 226 視情況合適地將來自輸出通道(例如通道 228)之一的輸出以解碼及解壓縮形式重新引導至轉碼模組 204。例如，可將以 ITU656 格式編碼之輸出信號作為輸入提供至轉碼模組 204 以支援對可在網路 102 上容易地發送之媒體格式的數位至數位轉換。在其他具體實施例中，可以任何格式將數位或類比信號提供至轉碼器 204。

為此目的，轉碼模組 204 係能夠產生媒體流的任何硬體、軟體、韌體及/或其組合，該媒體流能夠在網路 102 上投送至遠端裝置 112。在各種具體實施例中，將轉碼模組

實施於具有數位信號處理能力的半導體晶片內，例如可從德州 Dallas 市 Texas Instruments Corporation 獲得之 DAVINCI 型處理器，但其他具體實施例可使用任何種類之處理器或其他電路(包括用於實施圖 2 中所示之任何其他組件的相同處理器或其他電路)以實施轉碼功能。一般而言，轉碼模組 204 接收藉由解碼器 214 或 216 解碼(且視需要藉由顯示處理器 218 或 220 進一步處理)之經解碼信號 234 或已編碼流 236，實行數位至數位轉換以建立處於所需格式內且具有所需參數之媒體流，以及提供經轉換流以便在網路 102 上傳輸。包括轉碼能力之位移系統的一範例係在美國專利公開案 2006/0095471 中說明，但其他位移及/或轉碼特徵可實施於替代具體實施例之廣泛陣列內。圖 2 顯示轉碼模組 204 之輸出 238，其包括針對使用網路介面 210 之傳輸提供的位移視訊流。在替代具體實施例中，可提供不同網路介面 210，例如駐留於模組 204 本身內之堆疊。在各種具體實施例中，可需要透過任何種類之實體或邏輯安全性技術確保轉碼模組 204 與裝置 108 之其他組件間的任何晶片間通信。可在實體上嵌入至印刷電路板內的信號接針上提供信號 234、236 及/或 238，例如，以使得存取此類信號變得更困難。而且，可以任何方式在模組間加密或編碼信號 234、236 及/或 238，以在實體上攔截此類信號的事件中防止未授權使用。

接著，在操作中，位移裝置 108 從 DBS、電纜或其他來源 105 合適地接收一或多個媒體流，其可係視需要儲存於

DVR 資料庫 110 或類似物內。可以壓縮形式(例如信號 236)及/或解壓縮形式(例如信號 234)將接收到的及/或儲存的內容提供至轉碼模組 204，其適當地將接收到的信號轉換至可透過網路 110 發送至遠端裝置 112 之格式。位移程序之控制，包括關於安全性或鑑認之任何通信，可在執行於裝置 108 內的控制邏輯 205 之方向下發生。

圖 3 顯示在位移裝置 108 與遠端裝置 112 間安全建立位移媒體流之範例性程序 300。圖 3 顯示藉由涉及於安全性程序 300 內之實體 108、112、114 的每一者傳送及接收之訊息，以及可藉由系統 100(圖 1)內的一或多個實體實行之其他動作。在實務中，可採用藉由一或多個實體 108、110、112 執行之各種方法實施總體程序 300，如以下所更完整地說明。一般而言，可將圖 3 中所示之方法步驟的每一者實施於軟體或韌體內，其可係儲存於記憶體、大量儲存器或對執行裝置可用的任何其他儲存媒體內，且其可在與執行裝置相關聯之任何處理器或控制電路上執行。

程序 300 通常始於遠端裝置 112，其採用登入請求接觸中央伺服器(步驟 302)。例如，此可藉由遠端裝置 102 之使用者開啟媒體播放器應用程式或以其他方式起始檢視位移媒體之程序而起始。步驟 302 可包括提供與使用者相關聯之任何種類的識別資訊，例如任何種類之 userid/密碼對。或者，步驟 302 可提供數位簽名、任何其他密碼憑證、生物特徵量測資訊及/或任何其他種類之識別資訊以確保使用者之身分。步驟 302 亦可包括數位簽名、識別項或與媒體

播放器應用程式或裝置112之其他組件相關聯之其他憑證以確保應用程式經授權以參與程序300。中央伺服器114以任何方式(例如，藉由查詢圖1中之資料庫116)合適地確認接收到的資訊(步驟303)。若確認成功，使用者經識別，則可傳送回應訊息(步驟304)。在媒體播放器應用程式過期的事件中，此類資訊可用於提示使用者以獲得更新之軟體或用於任何其他目的。

回應訊息304包括允許遠端裝置建立對所需位移裝置108之連接的任何資訊。在各種具體實施例中，回應304可包括關於與使用者在目錄或其他列表內之帳戶相關聯的一或多個位移裝置108之位址資訊(例如，網際網路協定(IP)位址)。回應304亦可包括針對增加之便利性藉由使用者建立的使用者偏好設定或其他設定。

在中央伺服器114之成功鑑認後，遠端裝置112能夠經由網路102請求對特定位移裝置108之連接(步驟306)。可使用可藉由位移裝置108接收或解譯的任何合適協定或其他格式傳送此請求。在範例性具體實施例中，回應304包括與位移裝置108相關聯之IP位址或其他識別項，其允許遠端裝置112直接經由網路102接觸所需位移裝置108。

位移裝置108能夠以任何方式驗證實行位移之能力(步驟307)。在各種具體實施例中，裝置108經由除網路102外之分離資料連接接收旗標或其他指示，其指示位移「權利」之可用性。例如，在其中裝置108包括接收電纜或衛星信號之能力的具體實施例中，可將位移致能訊息嵌入至分別

經由電纜或衛星連接發送至裝置108的信號105內。在其他具體實施例中，可藉由裝置108警告實體上靠近裝置108之人以授權位移。在任一情形中，裝置108可不接受位移請求直至在裝置上明確地致能位移「權利」。此可藉由在確認使用者對連接之請求前檢查位移經核准(步驟307)，如圖3中所示，或者藉由僅忽略用於位移連接之請求306直至接收用於位移之核准來驗證。

可以任何方式致能或停用位移，及/或可基於遠端裝置112之位置或能力以不同方式應用。例如，位移裝置108可經組態用以辨識服務之數個「層」，以便僅針對區域網路，例如，或者僅針對廣域網路致能位移。此類功能性可藉由(例如)在致能有限位移時將裝置108及112之IP或其他網路位址相比較來實施。可藉由僅更新提供至裝置108的位移「旗標」或其他資料以任何方式且在任何時間基礎上致能、停用或以其他方式調整任何特定裝置108內之位移。

若在裝置108上致能位移，則經由網路102將回應訊息308傳送至遠端裝置112。在各種具體實施例中，裝置112亦將請求312提交至用於授權憑證之中央伺服器114，該授權憑證可用於確保位移媒體流，如以下所說明。在從位移裝置108接收回應308後，遠端裝置112亦將請求310提交至中央伺服器114以獲得授權憑證，其容許與特定位移裝置108之安全通信。在各種具體實施例中，授權憑證係密碼密鑰，例如容許基於共享秘密的後續安全通信之對稱加密

密鑰或類似物。例如，與先進加密標準(AES)或資料加密標準(DES)演算法相關聯的任何長度(例如64或128位元)之習知密鑰可用於各種具體實施例中。在各種具體實施例中，授權憑證與特定位移裝置108相關聯，且可在任何時間基礎上更新。可在週期性或非週期性基礎上更新密鑰，例如，或者可回應於針對增加之安全性的每一請求312以提供唯一密鑰。

在接收請求310及312後，中央伺服器114合適地確認且授權位移會話(步驟314)。步驟314可涉及查詢後端伺服器118，例如，以確保針對特定使用者、遠端裝置112及/或位移裝置108核准位移。或者，可使用資料庫116(圖1)或類似物在中央伺服器處以本地方式解決驗證。若核准交易，則將授權憑證作為訊息316從伺服器114發送至遠端裝置，且作為訊息318發送至位移裝置108。在其中已將憑證儲存於裝置108內的具體實施例中，訊息318可不必包括憑證之另一複本，但可相反地提供採用遠端裝置112之位移經核准的指示。授權憑證通常將使用相對安全連接(例如安全超文字傳輸協定(HTTPS)或類似物)提供以防止任何第三方透過竊聽或類似技術獲得憑證。

當位移裝置108及遠端裝置112兩者已從中央伺服器114接收授權316、318時，則可經由網路102直接在兩個裝置108、112間建立安全連接。例如，可使用習知技術(例如，如AES、DES或其他演算法中所提出)且使用從中央伺服器114提供之參數藉由每一方產生會話密鑰320。此會話

密鑰可係基於接收到的鑑認憑證，例如，以允許確保通信之相互加密/解密。通常基於接收到的憑證且亦基於通信裝置已知的一或多個其他參數協商會話密鑰。可將該等參數嵌入至先前提供之軟體(例如提供至裝置112之媒體播放器應用程式內及/或對裝置108之韌體更新內)內以進一步增強位移安全性。可以任何方式(例如，根據熟知加密協定，例如AES、DES及/或類似物)定義且可在任何時間基礎上更新該等參數。在圖3中所說明之密碼系統變得減弱之事件中，例如，可需要對裝置108之韌體更新及/或對裝置112之播放器更新以在從中央伺服器114接收任何未來核准(例如訊息316、318)前更新各種參數。

在各種具體實施例中遠端裝置112之使用者亦可與位移裝置108分離地鑑認(步驟324)以進一步增強程序300之安全性。此鑑認可涉及將與使用者相關聯之userid/密碼對、數位簽名、生物特徵量測資料及/或任何其他識別資訊提供至位移裝置108。在以任何方式建立位移會話前可藉由使用者組態此類資訊。儘管圖3將鑑認步驟324顯示為發生於會話密鑰之協商後，此類鑑認可發生於程序300中之任何點。例如，鑑認324可在密鑰請求312之置放前發生。其他具體實施例可完全消除步驟324中之額外鑑認，或者使此類鑑認在使用者或任何管理員之判斷下可選。

當鑑認完成且各種加密參數正確就位時，可透過網路102將位移媒體流326提供至遠端裝置102。通常，加密包含於媒體流326內之內容的一些或全部(步驟325)，如下文

所更完整地說明。可在操作期間以任何方式調整媒體流326內之內容的轉碼、加密及傳輸(步驟328)。在各種具體實施例中，與遠端播放器112相關聯之媒體播放器應用程式將命令及控制資訊提供至裝置108，其可用於視需要調整或以其他方式控制轉碼、加密或傳輸。

從裝置108、112及中央伺服器114之變更觀點看，則圖3中說明用於建立安全位移會話之各種方法。相對於位移裝置108，例如，合適地建立安全連接包括從遠端裝置接收用於連接之請求306、驗證位移特徵在裝置307內可用以及接著請求用於來自中央伺服器的會話之核准(步驟312)的廣泛步驟。回應於接收到的核准(步驟318)，其可包括密碼密鑰或其他鑑認憑證，位移裝置108能夠基於接收到的憑證建立安全媒體流326。可藉由與裝置108相關聯的任何處理電路或邏輯執行此方法之各種步驟，包括顯示為在圖2中操作的控制邏輯205。

相對於遠端裝置112，將初始請求置放至中央伺服器114，其採用關於位移裝置108之位址或其他資訊作出回應304。遠端裝置112接著能夠從位移裝置請求連接(步驟306)，以及在從裝置108接收回應308後請求密鑰或其他憑證。接收到的憑證接著可用於協商或以其他方式建立安全媒體流326之參數，且解密作為流之部分傳輸的內容。此方法之各種步驟可在媒體播放器應用程式或在遠端裝置112上執行的其他軟體內執行。

相對於中央伺服器114，從遠端裝置112接收且視情況確

認(步驟303)初始請求302。若請求有效，提供關於位移裝置108之資訊(步驟304)以允許遠端裝置112直接接觸位移裝置108。在從裝置112、108(分別)接收後續請求310、312後，中央伺服器114合適地以任何適當方式確認及授權會話，且以任何方式將密鑰或其他鑑認憑證發送至遠端裝置112及/或位移裝置108。裝置108及112接著能夠基於共享憑證獨立地協商安全媒體流326之參數。此方法之各種功能及其他特徵可視情況在與伺服器114及/或後端伺服器118(圖1)相關聯之一或多個處理器上執行。

圖4顯示關於用於將安全媒體流326從位移裝置108發送至遠端裝置112的範例性技術之額外細節。圖4中所示之各種步驟可在駐留於裝置108內的軟體、韌體及/或硬體邏輯內執行，例如顯示為結合圖2中之各種其他模組(包括轉碼器模組204)操作的控制邏輯205。

如上所述，位移裝置108以任何方式接收鑑認憑證(例如密碼密鑰)(步驟402)。在某些具體實施例中可為每一請求之會話提供唯一憑證，或者可將密鑰/憑證安全儲存於裝置108內以便結合多個位移會話使用。在任一事件中，可使用任何技術，例如習知AES密碼術，基於在兩個裝置間共享之秘密資訊與遠端裝置112協商用於特定位移會話之會話密鑰及/或其他參數(步驟404)。

在某些具體實施例中，資源可用於加密媒體流326之虛擬整體。但在其他具體實施例中(步驟406)，可不必或不需加密整個流。在其中轉碼之媒體流與接收到的信號相比

具有相對低品質(例如，相對低位元解析度)之具體實施例中，例如，可減少或消除密碼術。而且，當遠端裝置具有有限計算資源(例如行動電話或類似物)時，強密碼術之計算需求可減損使用者體驗。同樣，若媒體流326係透過相對低頻寬鏈路(例如，相對慢電話連接)傳輸，藉由密碼術施加之新增延遲不合需要。因此，藉由位移裝置應用之密碼術的層級可基於諸如發送之媒體流的品質、遠端裝置112之處理能力及/或插入通信網路102之頻寬的因素加以選擇(步驟408)。

可以任何方式應用密碼術(步驟410)。在各種具體實施例中，可取決於各種因素以任何數目之「層級」應用密碼術，其範圍從無加密，至部分加密，至整個流之加密。此意義上之「部分加密」可指僅加密媒體流之特定訊框，及/或僅加密一或多個訊框之特定區塊。即，藉由僅加密發送之媒體的一部分，可維持安全性而無需過度增加計算額外負擔。在習知MPEG型視訊流中，例如，可加密更基礎之視訊訊框(例如I訊框)，且減少之加密係應用於更高度壓縮之訊框(例如P訊框及/或B訊框)。僅加密構成各種訊框的巨集塊之一部分可同樣減小計算需求。作為一範例，「高」層級加密可加密媒體流326之每一傳出訊框，而「中」層級可加密較少數量，例如I、P及/或B訊框之一些或全部中在大約百分之25至75間的區塊。可針對任何所需之解析度等級新增額外層級。

在其他具體實施例中，可以任何方式(包括隨機地)指派

加密之特定區塊。即，可隨機地選擇特定區塊以進一步增強系統之安全性。隨機化加密之區塊就擴展處理器負載亦可具有另一優點，藉此在加密期間進一步改良系統性能。可以任何方式將特定隨機選擇之區塊喚出至接收方，例如透過標頭識別、控制訊息及/或類似物以促進媒體流326之有效解密。

因此以任何方式將媒體流326加密及發送至遠端裝置108(步驟412)直至位移會話完成(步驟414)。如上所述，流326之各種轉碼、加密及/或傳輸參數可在操作期間視需要加以調整(步驟416)。若連接102之頻寬應降級，例如，或者遠端裝置112之處理能力變得過載，可能需要降低媒體流之品質及/或減少在步驟410中應用之加密的數量。可視情況向上或向下調整用於轉碼及/或加密媒體流326之各種參數的任何者以補償變化條件(步驟418)。在範例性具體實施例中，可依據視訊位元率及/或視訊解析度設定及/或調整加密層級。例如，可始終在相對高層級下加密高清晰度視訊，而在某些具體實施例中可在較低層級下加密標準清晰度視訊，特別係在視訊位元率相對較低時。可橫跨廣泛範圍之替代具體實施例建立各種加密參數及準則。

使用本文所說明之各種系統、方法及其他概念，可實現若干優點。藉由需要對中央伺服器及/或對位移裝置之鑑認，例如，對位移內容之存取可限於授權使用者。另外，可透過對中央伺服器之鑑認及/或用於產生會話密鑰之系統秘密的使用拒絕未授權媒體播放器應用程式。使用中央

伺服器允許在安全性破壞之事件中方便地升級/更新密鑰或播放器應用程式，藉此顯著增強系統可再新性。另外，串流內容係端對端加密，藉此減少不信任或未核准第三方之存取。可基於視訊品質、環境因素及/或類似物調整應用之加密層級，從而進一步改良系統性能。如開始處所述，可選擇性地應用各種特徵，且不會在所有具體實施例中找到所有特徵。

本文所使用之詞語「範例性」意味著「用作一範例、實例或解說」。本文說明為範例性的任何實施方案不必解釋為較佳具體實施例或優於其他具體實施例。

雖然前述詳細說明將為熟習本技術之人士提供用於實施本發明之各種具體實施例的方便途徑，應明白以上說明之特定具體實施例僅係範例，而非以任何方式限制本發明之範疇、可應用性或組態。相反，可在所說明之元件的功能及配置內作出各種變化，而不致背離本發明之範疇。

【圖式簡單說明】

上文已結合以下圖式說明範例性具體實施例，其中相似數字表示相似元件，以及

圖1係範例性安全位移系統之方塊圖；

圖2係範例性位移裝置之方塊圖；

圖3係顯示用於建立位移裝置與遠端裝置間的安全位移之範例性程序之資料流程圖；以及

圖4係用於將加密媒體流發送至遠端播放器之範例性程序的流程圖。

【主要元件符號說明】

100	位移系統
102	通信網路
104	天線
105	數位廣播衛星信號/內容來源/實況 來源
106	衛星
108	位移裝置/位移器裝置/混合裝置/組 件裝置/裝置
110	內容資料庫/儲存器
112	遠端裝置/遠端檢視器/行動裝置
114	中央伺服器/後端伺服器
116	資料庫
118	後端伺服器
120	授權區
204	位移轉碼器
205	控制邏輯
206	磁碟控制器
208	接收器
210	網路介面
212	傳輸選擇器/流選擇模組/傳輸流選 擇模組
214	解碼器/解碼器模組
218	顯示處理器

226	切 換 器
228	輸 出 介 面 / 通 道
234	經 解 碼 信 號 / 信 號
236	視 訊 信 號 / 已 編 碼 流 / 信 號
238	輸 出 / 信 號
242 、 244 、 246	介 面

七、申請專利範圍：

102年3月8日修正
第1頁(本)

1. 一種可由一位移裝置執行以經由一通信網路將一位移媒體流從該位移裝置安全提供至一遠端播放器之方法，該方法包含：

經由該通信網路於該位移裝置處從該遠端播放器接收針對一連接之一請求；

回應於針對該連接之該請求而經由該通信網路從一遠端位置中央伺服器請求一授權憑證，其中該遠端位置中央伺服器係與該遠端播放器及該位移裝置兩者分離，其中該授權憑證係由該遠端位置中央伺服器產生以授權於該遠端播放器及該位移裝置之間之一位移會話，且其中該授權憑證係從該遠端位置中央伺服器經由該通信網路提供至該遠端播放器及該位移裝置；以及

使用從該遠端位置中央伺服器接收之該授權憑證而透過該通信網路在該位移裝置與該遠端播放器間建立該位移會話，以安全地從該位移裝置提供該位移媒體流至該遠端播放器。

2. 如請求項1之方法，其中基於該授權憑證加密該位移媒體流之至少一部分，該授權憑證係從該遠端位置中央伺服器所接收。
3. 如請求項1之方法，其進一步包含驗證在請求該授權憑證前核准該位移裝置與該遠端播放器間之位移。
4. 如請求項3之方法，其中該驗證至少部分係基於該遠端播放器之一位置。

5. 如請求項3之方法，其中該驗證至少部分係基於經由與該通信網路分離之一媒體接收之一核准。
6. 如請求項1之方法，其進一步包含在建立該位移媒體流前於該位移裝置處鑑認該遠端播放器之一使用者。
7. 如請求項1之方法，其中該授權憑證包含亦從該遠端位置中央伺服器提供至該遠端播放器之一對稱加密密鑰。
8. 如請求項7之方法，其中回應於在該遠端位置中央伺服器處從該遠端播放器接收的一請求而透過該通信網路將該對稱加密密鑰從該遠端位置中央伺服器提供至該遠端播放器。
9. 如請求項8之方法，其中該位移媒體流之該建立包含至少部分基於從該遠端位置中央伺服器接收之該對稱加密密鑰於該遠端播放器及該位移裝置之間，來協商用於該位移媒體流之加密參數。
10. 如請求項1之方法，其進一步包含選擇用於該位移媒體流之複數個可用加密層級之一，且其中基於該授權憑證加密該位移媒體流之至少一部分。
11. 如請求項10之方法，其中至少部分基於該位移媒體流之一品質決定該選定加密層級。
12. 如請求項10之方法，其中至少部分基於該遠端播放器之一處理能力決定該選定加密層級。
13. 如請求項10之方法，其中至少部分基於該通信網路之一頻寬決定該選定加密層級。
14. 如請求項1之方法，其中基於經由與該通信網路分離之

一媒體接收且在該位移裝置處解碼的媒體內容而提供該位移媒體流。

15. 如請求項14之方法，其進一步包含驗證在請求該授權憑證前核准該位移裝置與該遠端播放器間之位移，其中該驗證至少部分係基於經由與該通信網路分離之該媒體接收的一核准。

16. 如請求項14之方法，其中與該通信網路分離之該媒體包含一衛星鏈路。

17. 一種經由一通信網路將一位移媒體流安全提供至一遠端播放器之系統，該系統包含：

對該通信網路之一網路介面；

一接收器，其經組態用以從與該通信網路分離之一媒體接收媒體內容；

一轉碼器，其經組態用以封包化該接收到的媒體內容以便透過該通信網路傳輸；以及

控制電路，其至少與該網路介面及該轉碼器通信，其中該控制電路經組態用以：經由該網路介面從該遠端播放器接收針對一連接之一請求、回應於針對該連接之該請求而經由該網路介面從一遠端位置中央伺服器請求一授權憑證、以及於從該遠端位置中央伺服器接收該授權憑證之後，經由該網路介面與該遠端播放器建立一位移會話，以提供該位移媒體流至該遠端播放器，其中該遠端位置中央伺服器係與該遠端播放器及該系統兩者分離，其中該授權憑證係由該遠端位置中央伺服器產生，

且其中該授權憑證係從該遠端位置中央伺服器經由該通信網路提供至該遠端播放器及該系統以授權於該遠端播放器及該系統之間之該位移會話。

18. 如請求項17之系統，其中該控制電路進一步經組態用以至少部分基於從該遠端位置中央伺服器接收之該授權憑證，來與該遠端播放器協商用於該位移媒體流之加密參數。
19. 如請求項17之系統，其中該控制電路進一步經組態用以基於從該遠端位置中央伺服器接收之該授權憑證加密該位移媒體流之至少一部分。
20. 如請求項19之系統，其中該控制電路進一步經組態用以僅加密該位移媒體流之一部分。
21. 如請求項20之系統，其中至少部分基於該位移媒體流之一品質決定該部分之大小。
22. 如請求項20之系統，其中該加密部分對應於包含於該位移媒體流內之視訊訊框的選定區塊。
23. 如請求項22之系統，其中隨機選擇該等區塊。
24. 如請求項17之系統，其中該接收器係一直接廣播衛星接收器，其中與該通信網路分離之該媒體係可由該直接廣播衛星接收器接收之一衛星廣播，且其中該控制電路進一步經組態用以驗證在請求來自該遠端位置中央伺服器之該授權憑證前認可該位移裝置與該遠端播放器間之位移，其中該驗證係執行於該位移裝置且基於在該位移裝置經由可由該直接廣播衛星接收器接收之該衛星廣播接

收的一認可。

25. 如請求項17之系統，其中該接收器經組態用以解碼該媒體內容以及將該解碼媒體內容提供至該轉碼器。

26. 一種將一位移媒體流呈現至一遠端裝置之一使用者的方法，其中透過一通信網路將該位移媒體流從一位移裝置提供至該遠端裝置，該方法包含：

經由該通信網路對一中央伺服器鑑認該使用者；

在該中央伺服器之成功鑑認後，請求對該位移裝置之一連接；

在從該位移裝置接收一回應後，請求授權以經由該通信網路從該中央伺服器連接至該位移裝置，其中該中央伺服器係與該遠端裝置及該位移裝置兩者分離；

經由該通信網路從該中央伺服器接收一授權回應，其中該授權回應包含由該中央伺服器產生以授權於該遠端裝置及該位移裝置之間之一位移會話之一授權憑證，且其中該授權憑證係從該中央伺服器經由該通信網路提供至該遠端裝置及該位移裝置；以及

使用該授權憑證透過該通信網路建立與該位移裝置的該位移會話以安全地於該遠端裝置接收來自該位移裝置之該位移媒體流。

27. 如請求項26之方法，其中至少部分基於該授權憑證加密該位移媒體流之至少一部分。

28. 如請求項26之方法，其進一步包含經由該通信網路對該位移裝置鑑認該使用者。

29. 如請求項26之方法，其中該授權憑證包含亦從該中央伺服器提供至該位移裝置之一對稱加密密鑰。
30. 如請求項29之方法，其進一步包含至少部分基於該接收到的授權憑證協商用於與該位移裝置之該位移媒體流之加密參數。
31. 如請求項27之方法，其進一步包含僅解密該位移媒體流之一部分。
32. 如請求項31之方法，其中至少部分基於該位移媒體流之一品質決定該部分之大小。
33. 一種可由一中央伺服器執行以安全地允許將一位移媒體流提供至一遠端裝置之一使用者的方法，其中透過一通信網路將該位移媒體流從一遠端位置位移裝置提供至該遠端裝置，該方法包含：

於該中央伺服器經由該通信網路從該遠端裝置接收一第一請求，其中該第一請求包含與該使用者相關聯之一使用者憑證，且其中該中央伺服器係與該遠端裝置及該位移裝置兩者分離；

於該中央伺服器驗證該使用者憑證以及，回應於成功驗證，自該中央伺服器將一第一回應發送至識別該遠端位置位移裝置之該遠端裝置；以及

回應於該中央伺服器所接收之來自該遠端裝置之一第二請求，該中央伺服器產生用於授權於該遠端裝置及該遠端位置位移裝置之間之一影像串流會話之一鑑認憑證，且發送該中央伺服器產生之該鑑認憑證至該遠端裝

置及該遠端位置位移裝置兩者並藉此允許該遠端裝置及該遠端位置位移裝置使用該中央伺服器產生之該鑑認憑證建立從該遠端位置位移裝置至該遠端裝置之該位移媒體流。

34. 如請求項33之方法，其中至少部分基於該鑑認憑證加密該位移媒體流。
35. 如請求項33之方法，其中回應於來自該遠端位置位移裝置之一密鑰請求將該鑑認憑證發送至該位移裝置。
36. 如請求項33之方法，其進一步包含確認該使用者經授權以連接至該遠端位置位移裝置。
37. 如請求項36之方法，其中該確認包含查詢具有與該使用者相關聯之一項目的一帳戶伺服器。
38. 如請求項37之方法，其中該帳戶伺服器與一服務提供者相關聯，該服務提供者經由與該通信網路分離之一媒體將媒體內容提供至該遠端位置位移裝置。

八、圖式：

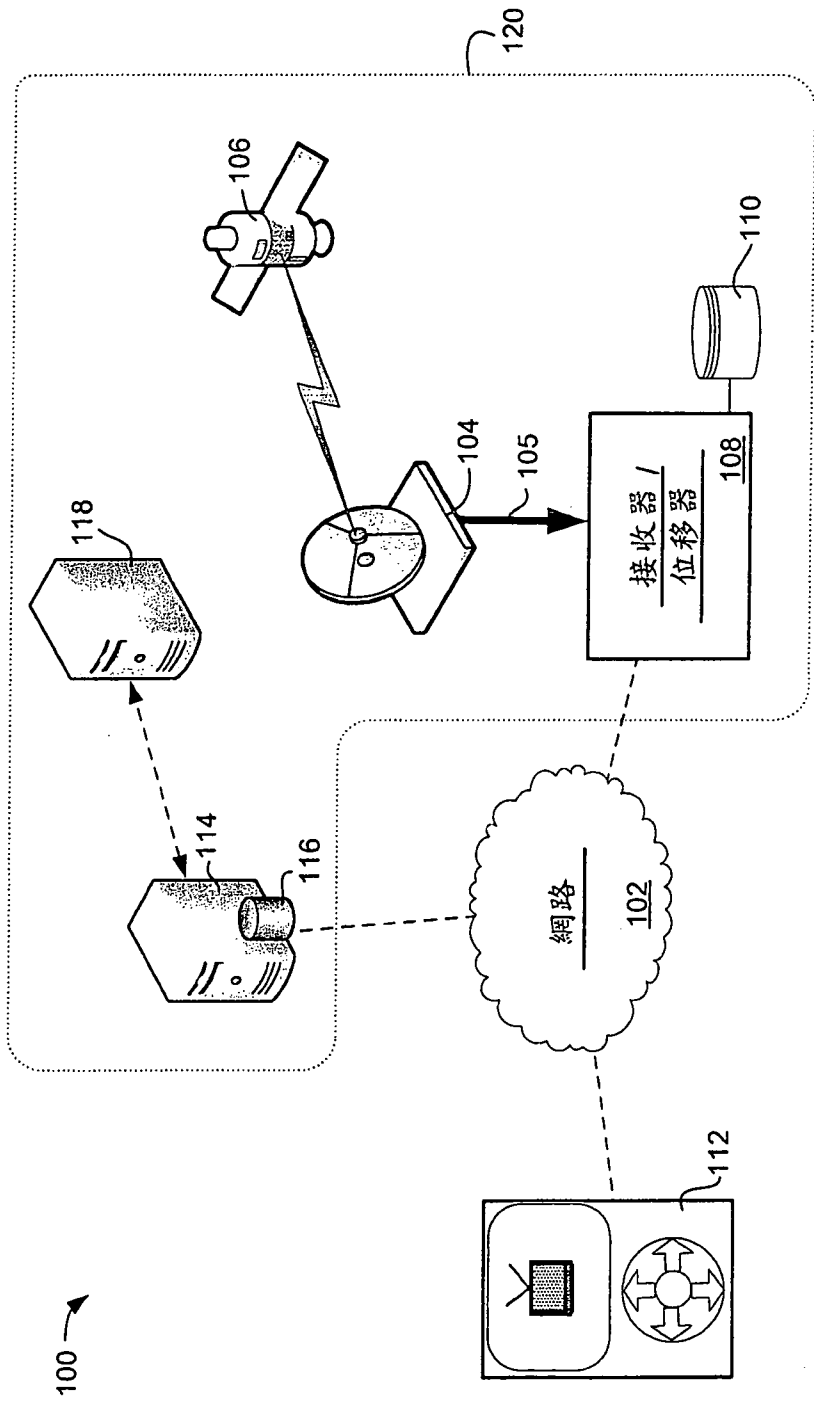


圖 1



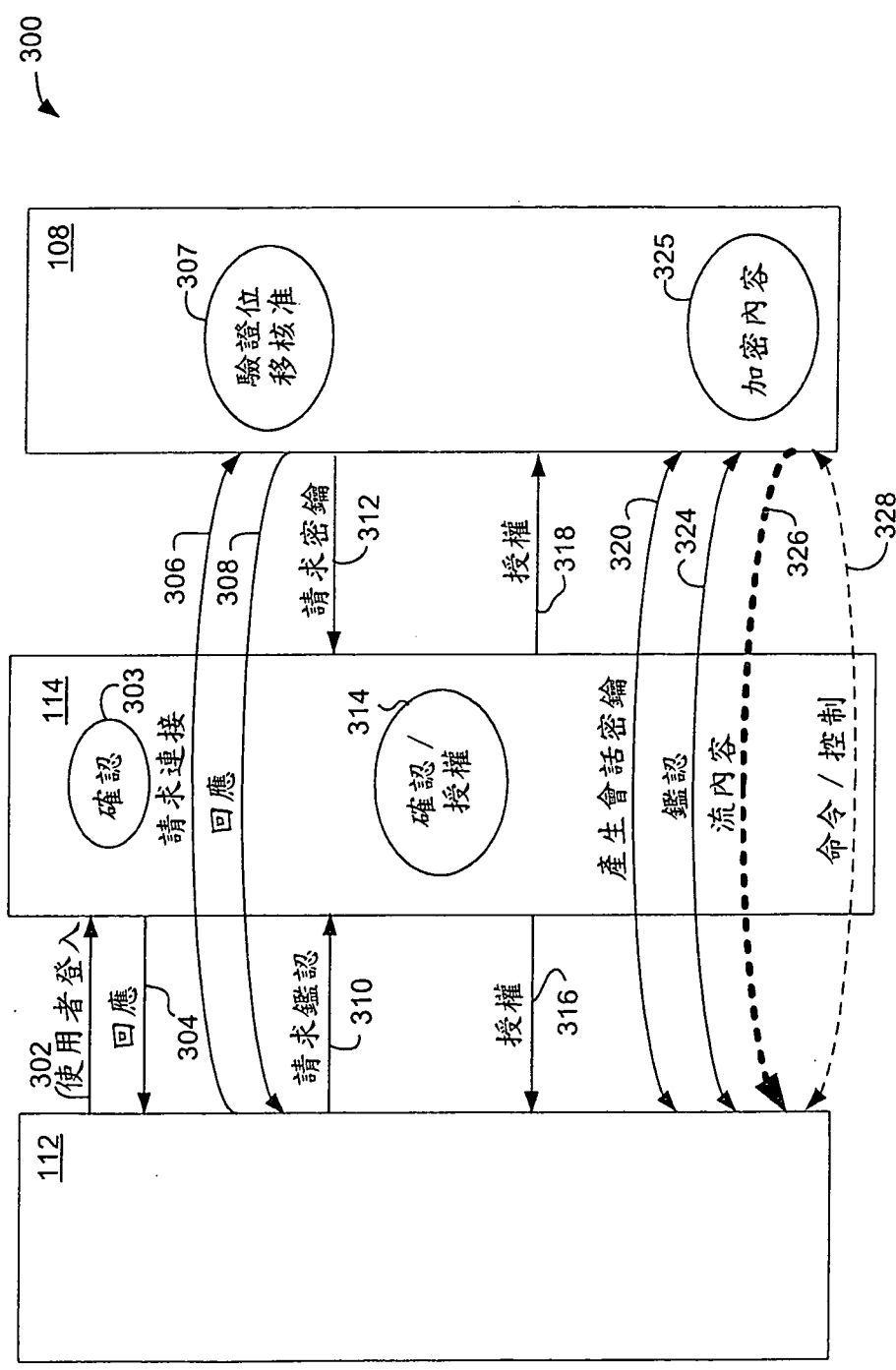


圖 3

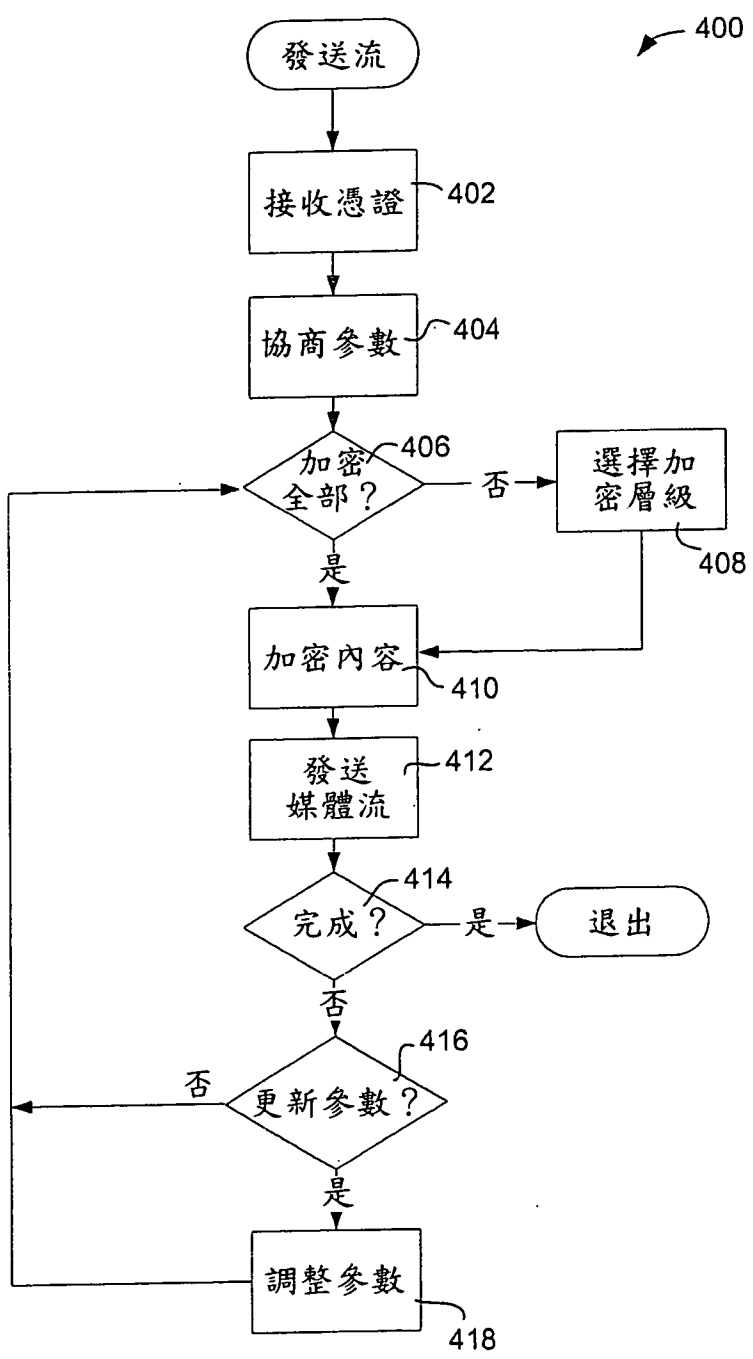


圖 4