

本案已向

國(地區)申請專利

美國 US

申請日期

1999/02/23 09/256,432

案號

主張優先權

有

有關微生物已寄存於

寄存日期

寄存號碼

無



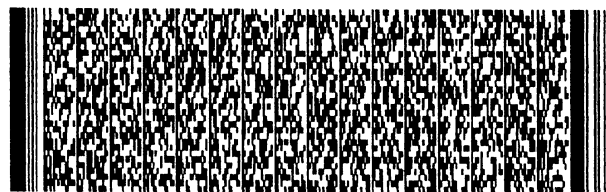
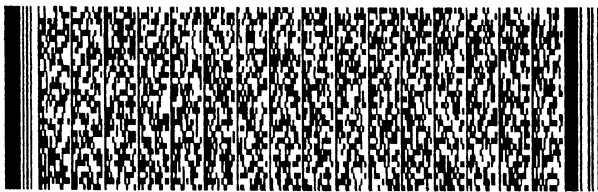
五、發明說明 (1)

發明領域

本發明與電腦檔案及/或電腦程式從一計算裝置編密的傳輸和編密的儲存到另一計算裝置的期間，一種自動地啟動一作業系統的功能之方法和系統有關。

發明背景

電腦檔案經由通訊裝置的保密傳輸，隨著電子流通和電子商務的網際網路之激增，而在重要性方面有所增加。從電腦檔案及/或電腦程式的實際遞送到以數位為基礎的電子傳輸之重要轉變，隨著網際網路成為一無所不在的低成本網路而開始。如在先前的科技進步中，例如從報紙到無線電和然後到電視的變遷中，現今的媒體公司被迫對這些新媒體的出現做出反應。然而，不像先前的科技變遷，作為一支援傳統的列印、無線電和電視工業的所有功能之媒體，網際網路同時也支援電子的商務。現在，許多行業利用網際網路，經由網際網路來販賣或贈送他們的電腦檔案及/或電腦程式，且在大部份的情形下，那些電腦檔案未編加密碼來防止侵害著作權或違法使用。此外，與電腦檔案的保密傳輸和儲存有關的目前方法，無法達成一計算裝置的作業系統之編密功能。目前的方式要求一計算裝置充當一伺服器("伺服裝置")，以與充當一用戶("用戶裝置")的另一計算裝置溝通，來傳遞在用戶裝置的應用程式層次(例如，但不限於，Win32應用程式)編密的檔案。用戶裝置利用在編密的應用程式層次執行之一電腦程式，其被指派一獨特的解密"鍵"。在傳輸程序期間，伺服裝置使用用

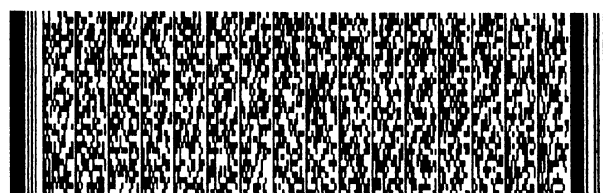
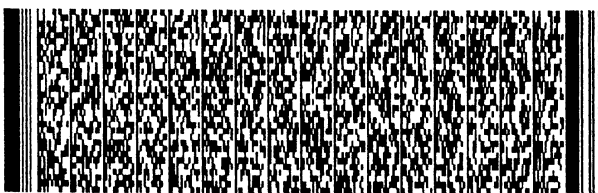


五、發明說明 (2)

戶裝置的解密"鍵"將電腦檔案編加密碼以供儲存。編密的電腦檔案然後經由網際網路傳輸，並儲存到用戶裝置當中、或與其連接的儲存裝置之內。在電腦檔案的解密之後，解密電腦程式傳送一解密的訊號到作業系統，以顯示或，在一聲音檔案的情況，透過語音卡播放。當從解密應用程式傳輸到作業系統時，解密的訊號可能受到破壞，而且此訊號可能被攔截，而很可能造成電腦檔案的非法複製。

微軟公司在1998年出版，一份標題為"微軟公司視窗NT 5.0版，公用鍵基礎"的白皮書，闡述了電腦檔案和電腦程式編密的某些態樣，合併在此處以供參考，(以下稱"視窗2000 PKI白皮書")，細述在作業系統的視窗2000系列產品中(之前稱為視窗NT 5.0)普遍的公用鍵基礎(PKI)的編密功能。視窗2000 PKI白皮書於其封面上陳述，"微軟公司視窗NT 5.0版"引進對視窗平台的一個普遍的公用鍵基礎(PKI)。這利用並擴充在過去幾年所引進的以視窗為基礎的公用鍵(PK)加密服務，提供服務和管理工具的整合集合，以建立、部署、和管理以PK為基礎的應用程式。這允許應用程式開發者在適當時，利用共享的秘密保全機制、或視窗NT中以PK為基礎的保全機制。同時，企業得到能夠根據一致的工具和政策機制，來管理環境和應用程式之優點。

而且，特別強調作業系統的視窗2000系列產品之公用鍵基礎的編密功能，視窗PKI白皮書陳述了，"網路已快速地變成建立、和部署以全球為基礎的資訊有效交換之解決方



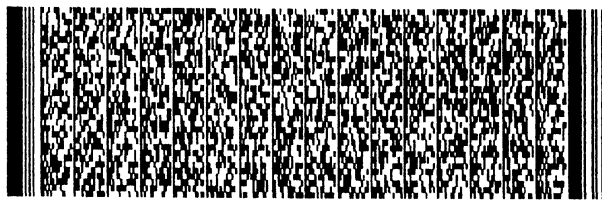
五、發明說明 (3)

法的一個主要元件"。特別是，其中商業目的之使用已戲劇性的成長。對許多使用而言，安全是一主要考量。特別是：伺服器認證-以使用戶能夠確認它們正與其溝通的伺服器。用戶認證-以允許伺服器確認用戶的身分，並以此作為存取控制判斷的基礎。保密性-在用戶和伺服器之間資料的編密，以避免其在公共網際網路聯結上的暴露。

保密插槽層(SSL)和逐漸確立的IETF標準之傳輸層保密(TLS)協定，在處理這些需求方面扮演一重要角色。SSL和TLS是可重疊在其他傳輸協定之上的彈性保密協定。他們仰賴以PK為基礎的認證技術，並使用以PK為基礎的鍵協議來產生每一用戶及/或伺服器會談的一個獨特編密鍵。它們最常與以網路為基礎的應用程式和HTTP協定(稱為HTTPS)有關。

SSL和TLS在視窗平台上由保密通道(schannel)SSPI供給者支援。微軟公司網際網路探險家和網際網路資訊服務兩者，對此功能都使用schannel。因為schannel與微軟公司的SSPI架構整合，它可與多重協定一起使用，以支援認證的及/或編密的通訊。

要取得SSL和TLS協定的完整好處，需要用戶和伺服器者都具有由共同信賴的CA所發行之身分識別，允許各方彼此認證。在這個模式中，識別與證明對應私人鍵的所有權之資料一起交換。然後每一方能使識別有效，並使用識別的公用鍵來驗證私人鍵的所有權。然後包含在識別中的證明資訊可用來補充存取控制判斷。舉例來說，用戶可決定伺



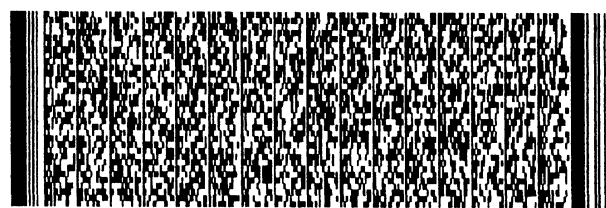
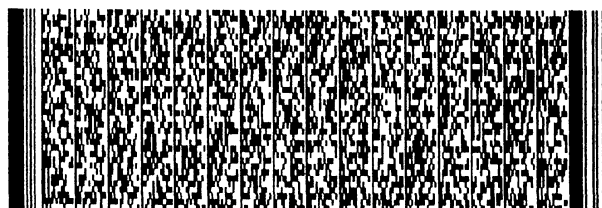
五、發明說明 (4)

伺服器是否為它想要與其進行交易的一個，而伺服器可決定將允許用戶存取什麼資料。

視窗NT 5.0 PKI整合對稍後判斷的支援，當成視窗NT伺服器的一個標準特徵。使用者識別可對作用的目錄中之保密原則(使用者物件)以一對一或多對一的基礎作對應。Schannel能利用這個資訊自動地為用戶合成一個保密符，以便視窗NT ACL機制用來實施對資源的存取控制。這對服務來說是有利的，於其中它們可利用與所使用之用戶認證機制(PK或Kerberos)獨立的同一存取控制機制。

一旦用戶和伺服器經過彼此認證，它們可進行協商一會談鍵並開始保密地溝通。SSL和TLS也時常用在不需要用戶認證的模式中。在企業環境中建議使用相互認證，究竟它允許你利用以視窗為基礎的存取控制機制。而且，PKI大大地簡化識別登錄和管理，減少用戶的負擔。

合併在此處以供參考，微軟公司1998年九月所出版標題為"視窗NT工作站5.0主要利益和能力白皮書"的另一份白皮書中，("視窗2000工作站白皮書")微軟公司提供作業系統的視窗2000系列產品之編密功能的額外細節。視窗2000工作站白皮書於其第30頁陳述，"視窗NT工作站5.0提供對公用鍵保密性的支援，一種在公開的網路例如網際網路上使用的工業標準認證協定。公用鍵最重要的用途是數位簽章，其保證元件的確實性，包括：來自寄件人的電子郵件；不能由其他使用者觀看或編輯的電子郵件；來自己知來源的應用程式和驅動程式；軟體在安裝之後防止變更；確



五、發明說明 (5)

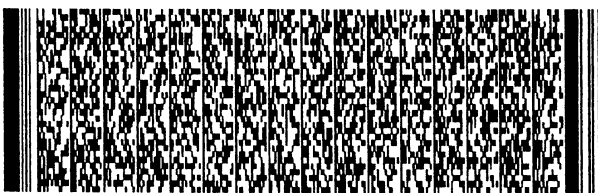
保遠端電腦的身分；允許保密的網際網路通訊；允許強固的編密，例如保密交易所需要的。

而其他的平台，如是正執行網際網路探險家4.0的任何視窗平台，支援公用鍵的使用，視窗NT工作站5.0藉由提供建立識別的更強固之基礎，進一步與其他系統"信任"，並保全識別的儲存。

視窗2000工作站白皮書在其第31頁上陳述擴充保密虛擬私人網路服務，"除今日最普遍的方法PPTP之外，視窗NT工作站5.0支援建立虛擬私人網路的數種新的、更保密的方法，包括：L2TP(第2層通道協定)，PPTP的更保密版本，供通道、位址指派、和認證；IPSEC(IP保密協定)，一種提供最高層次的VPN保密之標準的協定。藉由IPSEC，幾乎在網路層上的所有事物都可編密。這提供在公開網路上由一端到另一端的隱私性、完整性、和確實性。IPSEC方法對應用程式和協定是簡易的。微軟公司正與銷售商緊密地工作，以透過NDIS介面來支援IPSEC的硬體加速。

視窗NT工作站5.0也提供一增強的網路連接對話，讓使用者更易於建立VPN(見"簡易"段落)。

此外，微軟公司在視窗2000 PKI白皮書中討論，作業系統的視窗2000系列產品當中儲存編密功能，描述了一種編密檔案系統(EFS)，其位在視窗2000核心中。微軟公司在視窗2000 PKI白皮書中第21和22頁上陳述，"視窗NT 5.0編密檔案系統(EFS)支援儲存在視窗NT檔案系統(NTFS)中一磁碟上的檔案之簡明編密和解密。使用者可指定個別檔



五、發明說明 (6)

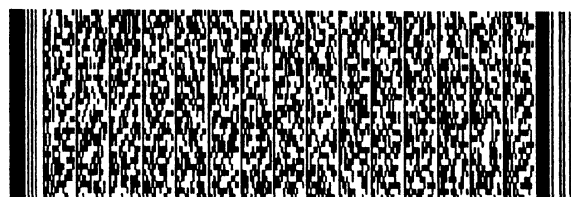
案編密，或其內容要以編密形式保存的檔案夾。應用程式能夠以如未編密檔案相同的方式，存取使用者編密的檔案。然而，他們將不能解密任何其他使用者的編密檔案。

EFS大規模使用以PK為基礎的技術，以提供編密檔案給多重使用者、以及支援檔案復原的機制。為了要這樣做，它利用PK的能力來支援大量的編密而不用先前分享的秘密。在運作中，每個EFS使用者產生一公用鍵對，並取得一EFS識別。此識別將由一企業CA發行在視窗NT 5.0網域中，雖然EFS將產生一自行簽發的識別，給資料分享不是問題的單機運作。除此之外，視窗NT5.0支援一種EFS復原政策，其中可指定信賴的復原代理。這些代理產生一EFS復原公用鍵對，且將由企業CA發行一份EFS復原識別。EFS復原代理的識別以群組政策物件對網域用戶出版。

在運作中，EFS對要編密的每個檔案產生用來編密檔案的隨機鍵。然後使用者的EFS公用鍵用來編密此秘密鍵並將它與檔案相關聯。此外，與每一復原代理的EFS公用鍵一起編密之秘密鍵的一份副本，與此檔案相關聯。秘密鍵沒有普通本文副本儲存在系統中。

當取回此檔案時，EFS簡易地使用使用者的私人鍵打開以使用者的公用鍵編密的秘密鍵之副本。然後這個秘密鍵的副本用來在檔案的讀取和寫入運作期間即時解密檔案。同樣地，復原代理可透過使用存取秘密鍵的私人鍵解密檔案。

視窗2000工作站白皮書於其第28頁上陳述，在微軟公司



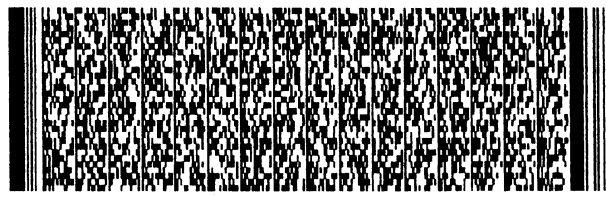
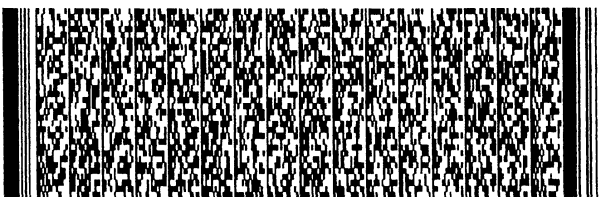
五、發明說明 (7)

的編密檔案系統之保密層次上提供額外的細節，"一種編密的檔案系統(EFS)將檔案編密在一硬式磁碟上。每一檔案使用一隨機地產生的鍵編密，此鍵與使用者的公用及/或私人鍵對獨立。EFS駐在視窗NT核心中，並使用不分頁的暫時儲存庫來儲存檔案編密鍵，確保它們永遠不會與分頁檔案接觸。EFS以一個檔案或目錄的基準支援。編密和解密對使用者是簡易的"。

計算功能的不穩定(例如，但不限於，造成計算系統瓦解的功能)通常在應用程式層次比在作業系統層次更為相關。計算功能越接近作業系統的核心，通常它們越穩定。如果一應用程式層次的解密程式成為損壞或錯誤的，且需要重新安裝另一解密程式，會產生一新的"解密鍵"，而早先對舊的"解密鍵"編密之編密的電腦檔案，不能由最新安裝的解密程式解密。避免在應用程式層次之程式中原有的編密及/或解密弱點，微軟公司已在視窗2000 PKI中採取一些步驟來保護最後的"編密及/或解密鍵"。微軟公司在視窗2000 PKI白皮書第14頁上陳述，"公用鍵對和識別傾向於有高數值。如果它們由於系統失敗而遺失，它們的更換可能耗費時間並造成金錢的損失。為解決這些問題，視窗NT 5.0 PKI支援透過識別-管理的管理工具，備份和回存識別和相關的鍵對兩者之能力"。

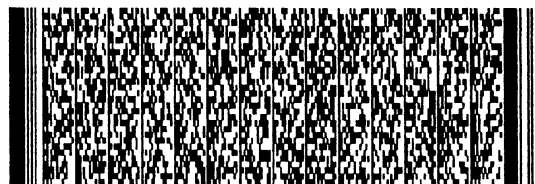
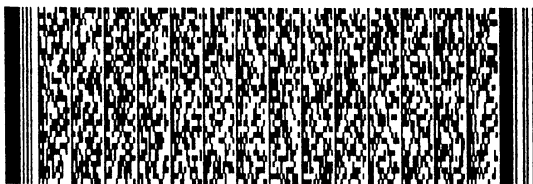
發明概要

本發明提供一種新的和改良的方法與系統，以自動地啟動作業系統的公用鍵基礎和編密檔案系統之一些功能，以



五、發明說明 (8)

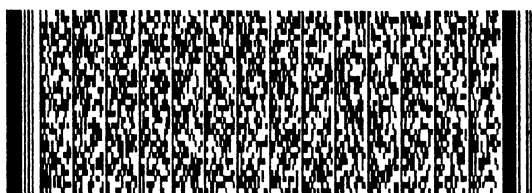
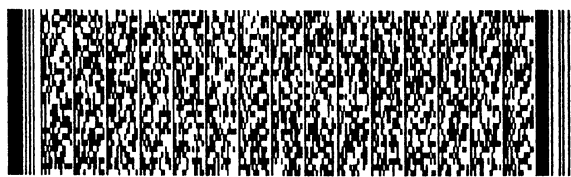
編密電腦檔案或電腦程式供計算裝置之間的電子傳輸，和編密那些電腦檔案或電腦程式供後續的儲存，和限制使用許可及/或權利。本發明指示計算裝置的作業系統，暫時地中止使用者干涉直到編密的傳輸和編密的儲存程序完成，以避免電腦檔案或電腦程式的副本之未經許可的使用。本發明指示伺服器裝置的公用鍵基礎，編密儲存在伺服器裝置當中、或與其連接的電腦檔案或電腦程式(和由伺服器裝置所建立的任何伴隨的許可及/或權利)以供傳輸，然後傳送該電腦檔案或電腦程式到用戶裝置。在用戶裝置收到該電腦檔案或電腦程式(和由伺服器裝置所建立的任何伴隨的許可及/或權利)時，本發明自動地指示用戶裝置的公用鍵基礎，從伺服器裝置所傳輸的該電腦檔案或電腦程式之傳送中(和由伺服器裝置所建立的任何伴隨的許可及/或權利)解密。然後本發明指示用戶裝置的編密檔案系統，根據如伺服器裝置所建立並伴隨著電腦檔案或電腦程式之任何許可及/或權利編密以供儲存，並儲存電腦檔案或電腦程式。本發明將儲存編密程序從傳輸編密程序分離，以用工業標準通訊協定使執行不同作業系統的計算裝置之間能夠編密傳輸，然後有讓不同的作業系統執行它們獨特的或專有的儲存編密程序。此外，最廣泛使用的作業系統支援網際網路的編密傳輸標準，然而，對作業系統不存在以編密儲存為基礎之標準。本發明的一個獨特的好處是它利用多重編密及/或解密程序，在執行不同作業系統的電腦之間，提供編密傳遞和儲存電腦檔案及/或程式一種從一端到另端的解



五、發明說明 (9)

決辦法。取代永久地編密一個電腦檔案及/或程式以使用在一特定解密裝置或電腦之上，本發明指派許可及/或權利給電腦檔案及/或程式，然後分派作業系統的編密功能使電腦檔案及/或程式施行許可及/或權利。以這種方式，可指派有彈性的許可及/或權利給電腦檔案及/或程式，從電腦到電腦之間、從作業系統到作業系統之間，在編密和解密時如果需要都遵循此許可及/或權利。

本發明也提供一種新的和改良的方法及系統，以啟動用戶裝置的公用鍵基礎和編密檔案系統的某些功能，來執行伴隨一特定電腦檔案或電腦程式的任何許可及/或權利。然後那些許可及/或權利(例如但不限於，播放、列印、觀看、使用、複製、移動、再配置的數目，使用的時間期間，使用者的數目等)將由編密檔案系統連同本發明一起施行。作為範例，一用戶裝置所收到的電腦檔案或電腦程式，可能伴隨著如同服裝置所建立的許可或權利，允許用戶裝置的使用者移動該電腦檔案或電腦程式到另一計算裝置("下一用戶裝置")。在這個範例中，本發明將指示用戶裝置和下一用戶裝置的作業系統，阻止使用者干涉直到移動完成。本發明指示用戶裝置的編密檔案系統，解密該電腦檔案或電腦程式。然後本發明指示用戶裝置的公用鍵基礎，編密該電腦檔案或電腦程式(和同服裝置所建立的許可及/或權利)以供傳輸，然後經由通訊裝置傳送電腦檔案或電腦程式到下一用戶裝置。在下一用戶裝置收到該電腦檔案或電腦程式(和同服裝置所建立的許可及/或權利)時，

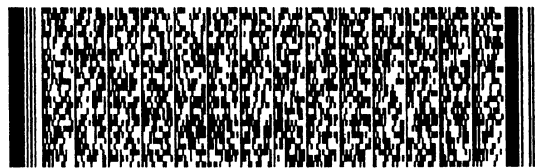


五、發明說明 (10)

本發明自動地指示下一用戶裝置的公用鍵基礎，從用戶裝置所傳輸的該電腦檔案或電腦程式(和伺服裝置所建立的許可及/或權利)之傳送中解密。然後本發明指示下一用戶裝置的編密檔案系統，根據從用戶裝置的傳輸期間伴隨該電腦檔案或、由伺服裝置所建立的許可及/或權利編密以供儲存，和儲存該電腦檔案或電腦程式。

本發明與用來操縱一電腦檔案及/或程式的一種系統有關。此系統包含一伺服裝置，能夠存取一未編密的電腦檔案及/或程式，且其可將未編密的電腦檔案及/或程式編密成一編密的電腦檔案及/或程式並傳送。此系統包含一連接到伺服裝置的連接器，編密的電腦檔案及/或程式於其上傳播，且伺服裝置對其傳遞編密的電腦檔案及/或程式。此系統包含一用戶裝置，其接收編密的電腦檔案及/或程式，並解密編密的電腦檔案及/或程式回到未編密的電腦檔案及/或程式。用戶裝置在接收編密的電腦及/或檔案程式時，不允許對編密的電腦檔案及/或程式的干涉。伺服裝置與用戶裝置是獨立、分離、和不同的。

本發明與用來操縱一電腦檔案及/或程式的一種方法有關。此方法包含中止在用戶裝置的一個使用者對用戶裝置的干涉之步驟。然後有在伺服器裝置編密一未編密的電腦檔案及/或程式的步驟，以形成一編密的電腦檔案及/或程式。接著有沿著連接到用戶裝置和伺服器裝置的連接器，傳遞編密的電腦檔案及/或程式到用戶裝置的步驟。然後有重建使用者對用戶裝置的干涉之步驟。



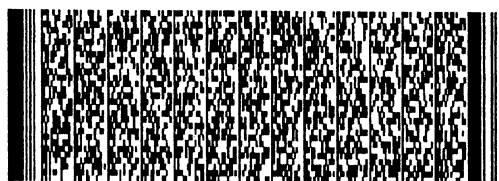
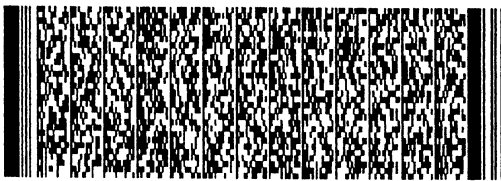
五、發明說明 (11)

圖式概述

在伴隨的圖式中，舉例說明本發明的較佳具體實施例和本發明的較佳實施方法，其中：

圖1是一個可用在進行本發明的教導，以自動地啟動伺服器裝置10的作業系統60之功能的概要圖，以：透過連接到通訊裝置120的收發器70之使用，編密和傳送一電腦檔案及/或程式110、與其相關的許可及/或權利，到一用戶裝置11。圖1是一概要圖，其也可用在進行本發明的教導上，以自動地啟動用戶裝置11的作業系統61之功能，來：透過連接到通訊裝置120的收發器71之使用，從來自伺服器裝置10的傳輸，接收和解密一電腦檔案及/或程式110及其相關的許可及/或權利，並儲存其一份電子副本在隨機存取記憶體81中；使用該相關的許可及/或權利從隨機存取記憶體81將該電腦檔案及/或程式110編密並存檔到儲存體101，然後從隨機存取記憶體81抹除該電腦檔案及/或程式110的任何電子副本；和

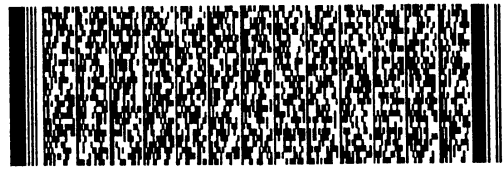
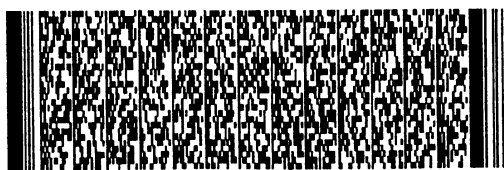
圖2是一個可用在進行本發明的教導，以自動地啟動用戶裝置11的作業系統61之功能的概要圖，以：從儲存體101解密一電腦檔案及/或程式110，並儲存其一份電子副本，和儲存相關的許可及/或權利，在隨機存取記憶體81中；和透過連接到一通訊裝置120的收發器71之使用，編密和傳送一電腦檔案及/或程式110與其相關的許可及/或權利，到一用戶裝置12；然後從隨機存取記憶體81抹除該電腦檔案及/或程式110的任何電子副本；和，然後在



五、發明說明 (12)

該電腦檔案及/或程式110從儲存體101移動到儲存體102的情況中，從儲存體101抹去該電腦檔案及/或程式110的任何電子副本。圖2是一個也可用在進行本發明的教導，以自動地啟動用戶裝置12的作業系統62之功能的概要圖，以：透過連接到通訊裝置120的收發器72之使用，從來自用戶裝置11的傳輸，接收和解密一電腦檔案及/或程式110及其相關的許可及/或權利，並儲存其一份電子副本在隨機存取記憶體82中；使用該相關的許可及/或權利從隨機存取記憶體82將該電腦檔案及/或程式110編密並存檔到儲存體102，然後從隨機存取記憶體82抹除該電腦檔案及/或程式110的任何電子副本；和

圖3是一電腦程式流程圖，其可用在進行本發明的指導，以自動地啟動伺服裝置10的作業系統60之功能，來：透過連接到一通訊裝置120的收發器70之使用，編密和傳送一電腦檔案及/或程式110及與其相關的許可及/或權利，到一用戶裝置11。圖3是一電腦程式流程圖，其也可用在進行本發明的指導，以自動地啟動用戶裝置11的作業系統61之功能，來：透過連接到通訊裝置120的收發器71之使用，從來自伺服裝置10的傳輸，接收和解密一電腦檔案及/或程式110及其相關的許可及/或權利，並儲存其一份電子副本在隨機存取記憶體81中；使用該相關的許可及/或權利從隨機存取記憶體81將該電腦檔案及/或程式110編密並存檔到儲存體101，然後並從隨機存取記憶體81抹除該電腦檔案及/或程式110的任何電子副本；和

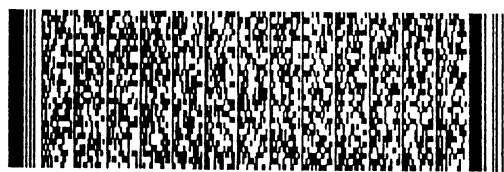
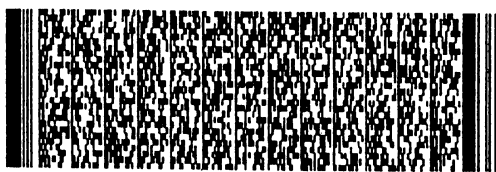


五、發明說明 (14)

可編密此未編密的電腦檔案及/或程式成為一編密的電腦檔案及/或程式並傳遞它。此系統包含一連接到伺服裝置10的連接器，於其上編密的電腦檔案及/或程式傳播，且伺服裝置10對其傳遞編密的電腦檔案及/或程式。此連接器可能是通訊裝置120。此系統包含一用戶裝置11，其接收編密的電腦檔案及/或程式，並將編密的電腦檔案及/或程式解密回未編密的電腦檔案及/或程式。此用戶裝置11在接收編密的電腦及/或檔案程式期間，不允許對編密的電腦檔案及/或程式的干涉。伺服裝置10是與用戶裝置11獨立的、分開的、且不同的。

最好，伺服器裝置指派許可及/或權利給未編密的電腦檔案及/或程式，其識別-在用戶裝置11收到編密的電腦檔案及/或程式之後、或在用戶裝置11將編密的電腦檔案及/或程式解密回未編密的電腦檔案及/或程式之後-用戶裝置11可如何處置未編密的或編密的電腦檔案及/或程式。伺服器裝置最好編密許可及/或權利，並將它們經由連接器傳遞到用戶裝置11。用戶裝置11解密未編密的許可及/或權利。

最好，伺服裝置10包括控制伺服器軟體及/或韌體30，其引起未編密的電腦檔案及/或程式和許可及/或權利的編密，並指示用戶裝置11-在用戶裝置11接收編密的電腦檔案及/或程式和編密的許可及/或權利時-暫時中止使用者干涉。用戶裝置11最好包括控制用戶軟體及/或韌體31，其引起編密的電腦檔案及/或程式的解密。最好，用戶裝



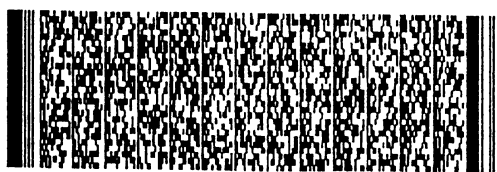
五、發明說明 (16)

到通訊鏈結的發射器，用來傳遞編密的電腦檔案及/或程式和未編密的許可及/或權利到通訊鏈結，且用戶裝置11包括一連接到通訊鏈結的接收器，其從通訊鏈結接收編密的電腦檔案及/或程式和編密的許可及/或權利。連接器最好是網際網路或其他通訊網路的一部份。

本發明與一種用來操縱一電腦檔案及/或程式的方法有關。此方法包含在用戶裝置11中止用戶裝置11的使用者的干涉之步驟。然後有在伺服器裝置編密一未編密的電腦檔案及/或程式，以形成一編密的電腦檔案及/或程式的步驟。接著有沿著一連接到用戶裝置11和伺服器裝置的連接器，傳遞編密的電腦檔案及/或程式到用戶裝置11的步驟。然後有重建用戶裝置11使用者的干涉之步驟。

在傳遞步驟之前，最好有編密未編密的電腦檔案及/或程式的許可及/或權利、並沿著連接器從伺服器裝置傳遞編密的許可及/或權利到用戶裝置11的步驟。最好，在編密未編密的電腦檔案及/或程式步驟之前，有用戶裝置11要求伺服器裝置的未編密的電腦檔案及/或程式的步驟。在要求步驟之後，最好有複製一主要的未編密之電腦檔案及/或程式，以形成未編密的電腦檔案及/或程式的步驟。

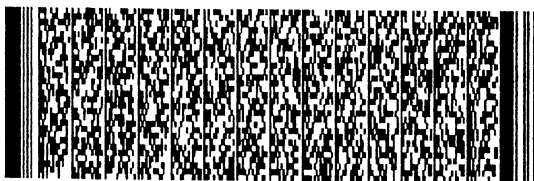
最好，在重建步驟之前，有在用戶裝置11解密編密的電腦檔案及/或程式回到未編密的電腦檔案及/或程式的步驟。在解密步驟之後，最好有在用戶裝置11編密未編密的電腦檔案及/或程式和許可及/或權利、並儲存編密的電腦程式及/或檔案和編密的許可及/或權利在用戶裝置11中的步



五、發明說明 (17)

驟。最好，在儲存步驟之後，有傳遞編密的電腦檔案及/或程式到由連接器連接到用戶裝置11的一下一用戶裝置20的步驟。

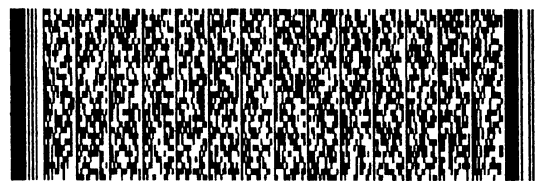
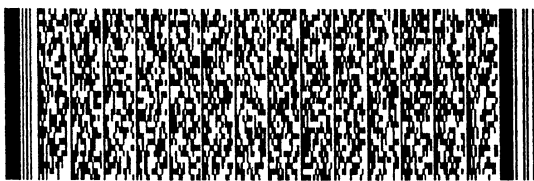
現在參考那些圖式，其中相同的參考號碼指相似的或完全相同的零件之幾個視面，而特別是對圖1和圖3，分別顯示用以啟動計算裝置伺服裝置10和用戶裝置11的作業系統60和61之功能的裝置30和31。裝置30和31分別連接到計算裝置伺服裝置10和用戶裝置11的作業系統60和61。此裝置30包含一種方法或機制，用來啟動一伺服裝置10的作業系統60之功能以：指示裝置31，以指示作業系統61在裝置30和31的功能之執行期間，暫時地中止用戶裝置11的使用者干涉；透過連接到通訊裝置120的一收發器70的使用，進行編密的通訊；透過連接到通訊裝置120的一收發器70的使用，編密和傳送一電腦檔案及/或程式110、及其相關的許可及/或權利，到一用戶裝置11。此裝置31包含一種方法或機制，用來啟動用戶裝置11的作業系統61之功能以：指示作業系統61在裝置30和31的功能之執行期間，暫時地中止用戶裝置11的使用者干涉；透過連接到通訊裝置120的一收發器70的使用，進行編密的通訊；透過連接到通訊裝置120的一收發器71的使用，從來自伺服裝置10的傳輸，接收和解密一電腦檔案及/或程式110、及其相關的許可及/或權利，並儲存其一份電子副本在隨機存取記憶體81中；使用該相關的許可及/或權利，從隨機存取記憶體81編密和存檔該電腦檔案及/或程式110到儲存體101，然後



五、發明說明 (18)

並從隨機存取記憶體81抹去該電腦檔案及/或程式110的任何電子副本；指示作業系統61，在裝置30和31的功能之執行完成時，回復用戶裝置11的使用者干涉。

現在參考那些圖式，其中相同的參考號碼指出相似的或完全相同的零件之幾個視面，而特別是對圖2和圖4，分別顯示用以啟動計算裝置用戶裝置11和下一用戶裝置12的作業系統61和62之功能的裝置31和32。裝置31和32分別連接到計算裝置用戶裝置11和下一用戶裝置12的作業系統61和62。此裝置31包含一種方法或機制，用來啟動一用戶裝置11的作業系統61之功能以：指示作業系統61在裝置31和32的功能之執行期間，暫時地中止用戶裝置11的使用者干涉；指示裝置32，以指示作業系統62在裝置31和32的功能之執行期間，暫時地中止下一用戶裝置12的使用者干涉；透過連接到通訊裝置120的一收發器71的使用，進行編密的通訊；從儲存體101解密一電腦檔案及/或程式110，並儲存其一份電子副本、和儲存相關的許可及/或權利在隨機存取記憶體81中；透過連接到通訊裝置120的一收發器71的使用，編密和傳送一電腦檔案及/或程式110、及其相關的許可及/或權利，到一下一用戶裝置12；然後並從隨機存取記憶體81抹去該電腦檔案及/或程式110的任何電子副本；和，在從儲存體101移動該電腦檔案及/或程式110到儲存體102的情況中，接著從儲存體101抹除該電腦檔案及/或程式110的任何電子副本；指示作業系統61，在裝置31的功能之執行完成時，回復用戶裝置11的使用者干涉。



五、發明說明 (19)

此裝置32包含一種方法或機制，用來啟動下一用戶裝置12的作業系統62之功能來：指示作業系統62在裝置31和32的功能之執行期間，暫時地中止下一用戶裝置12的使用者干涉；透過連接到通訊裝置120的一收發器71的使用，進行編密的通訊；透過連接到通訊裝置120的一收發器72的使用，從來自用戶裝置11的傳輸接收和解密一電腦檔案及/或程式110、及其相關的許可及/或權利，並儲存其一份電子副本在隨機存取記憶體82中；使用該相關的許可及/或權利，從隨機存取記憶體82編密和存檔該電腦檔案及/或程式110到儲存體102，然後並從隨機存取記憶體82抹去該電腦檔案及/或程式110的任何電子副本；指示作業系統62，在裝置32的功能之執行完成時，回復下一用戶裝置12的使用者干涉。

現在參考圖1和圖3，本發明的一個較佳具體實施例包含下列各項：

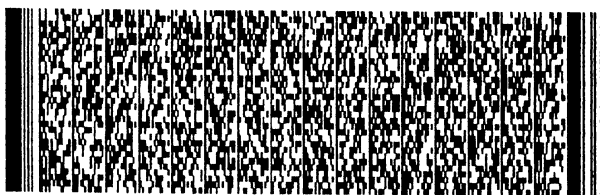
- 10 伺服裝置
- 11 用戶裝置
- 20 伺服介面
- 21 用戶介面
- 30 控制伺服軟體及/或韌體(也稱為"伺服CSS及/或F")
- 31 控制用戶軟體及/或韌體(也稱為"用戶CCS及/或F")
- 40 公用鍵基礎



五、發明說明 (20)

- 41 公用鍵基礎
- 50 編密檔案系統
- 51 編密檔案系統
- 60 作業系統
- 61 作業系統
- 70 收發器
- 71 收發器
- 80 隨機存取記憶體(也稱為"RAM")
- 81 隨機存取記憶體(也稱為"RAM")
- 90 處理器
- 91 處理器
- 100 儲存體
- 101 儲存體
- 110 電腦檔案及/或程式(也稱為"檔案及/或程式")
- 120 通訊裝置

在圖1和圖3中，下列元件已經可在商業上買到：伺服裝置10，用戶裝置11，伺服介面20，用戶介面21，公用鍵基礎40，公用鍵基礎41，編密檔案系統50，編密檔案系統51，作業系統60，作業系統61，收發器70，收發器71，隨機存取記憶體80(也稱為"RAM 80")，隨機存取記憶體81(也稱為"RAM 81")，處理器90，處理器91，儲存體100，儲存體101，電腦檔案及/或程式110(也稱為"檔案及/或程式110")，和通訊裝置120。控制伺服軟體及/或韌體30(也稱為"伺服CSS及/或F 30")，和控制用戶軟體及/或韌體31

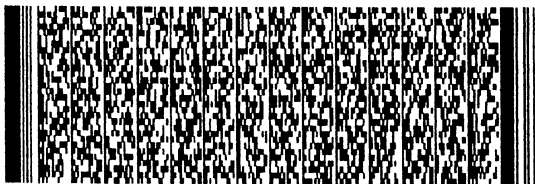


五、發明說明 (21)

(也稱為"用戶CCS及/或F 31")是本發明的新指導。

現在參考圖2和圖4，本發明的一個較佳具體實施例包含下列各項：

- 11 用戶裝置
- 12 下一用戶裝置
- 21 用戶介面
- 22 下一用戶介面
- 31 控制用戶軟體及/或韌體(也稱為"用戶CCS及/或F")
- 32 控制用戶軟體及/或韌體(也稱為"下一用戶CCS及/或F")
- 41 公用鍵基礎
- 42 公用鍵基礎
- 51 編密檔案系統
- 52 編密檔案系統
- 61 作業系統
- 62 作業系統
- 71 收發器
- 72 收發器
- 81 隨機存取記憶體(也稱為"RAM")
- 82 隨機存取記憶體(也稱為"RAM")
- 91 處理器
- 92 處理器
- 101 儲存體



五、發明說明 (22)

102 儲存體

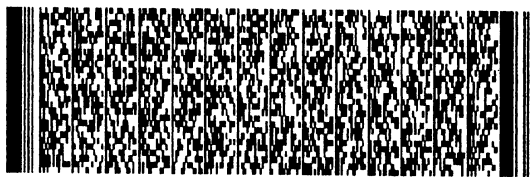
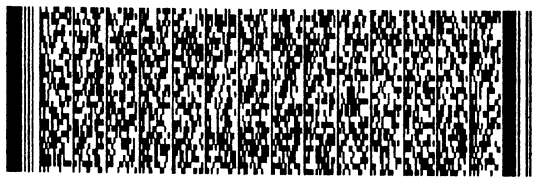
110 電腦檔案及/或程式(也稱為"檔案及/或程式")

120 通訊裝置

在圖2和圖4中，下列元件已經可在商業上買到：用戶裝置11，下一用戶裝置12，用戶介面21，下一用戶介面22，公用鍵基礎41，公用鍵基礎42，編密檔案系統51，編密檔案系統52，作業系統61，作業系統62，收發器71，收發器72，隨機存取記憶體81(也稱為"RAM 81")，隨機存取記憶體82(也稱為"RAM 82")，處理器91，處理器92，儲存體101，儲存體102，電腦檔案及/或程式110(也稱為"檔案及/或程式110")，和通訊裝置120。控制用戶軟體及/或韌體31(也稱為"用戶CCS及/或F 31")，和控制用戶軟體及/或韌體32(也稱為"下一用戶CCS及/或F 32")是本發明的新指導。

伺服裝置10(例如，但不限於，網路伺服器，個人電腦，Mac，PalmPC，膝上型電腦等)是一種方法或機制，其能電子地與其他計算裝置溝通。伺服裝置10也是一種方法或機制，電腦檔案可由其傳送到其他計算裝置。伺服裝置10可能包含一影像顯示器，音頻喇叭，和其他計算週邊。

用戶裝置11(例如，但不限於，網路伺服器，個人電腦，Mac，PalmPC，膝上型電腦等)是一種方法或機制，電腦檔案可藉其往來傳送到其他計算裝置。用戶裝置11也是一種方法或機制，電腦檔案可藉其從其他計算裝置接收。用戶裝置11可能包含一影像顯示器，音頻喇叭，和其他計算



五、發明說明 (23)

週邊。

下一用戶裝置12(例如,但不限於,網路伺服器,個人電腦,Mac, PalmPC,膝上型電腦等)是一種方法或機制,電腦檔案可藉其往來傳送到其他計算裝置。下一用戶裝置12也是一種方法或機制,電腦檔案可藉其從其他計算裝置接收。下一用戶裝置12可能包含一影像顯示器,音頻喇叭,和其他計算週邊。

伺服介面20(例如,但不限於,網路伺服器商業軟體,如微軟公司的商業伺服器)是一種方法或機制,其可接收和執行從另一計算裝置所傳輸的請求。

用戶介面21(例如,但不限於,網路瀏覽器軟體,如微軟公司的網際網路探險家)是一種方法或機制,其可傳送請求到另一計算裝置,且可顯示伺服介面20和下一用戶介面22的內容。

下一用戶介面22(例如,但不限於,網路瀏覽器軟體,如微軟公司的網際網路探險家)是一種方法或機制,其可傳送請求到另一計算裝置,且可顯示用戶介面21的內容。

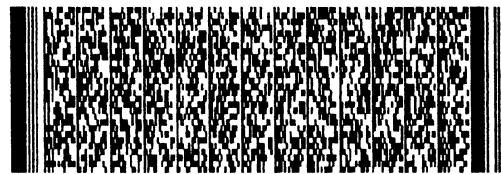
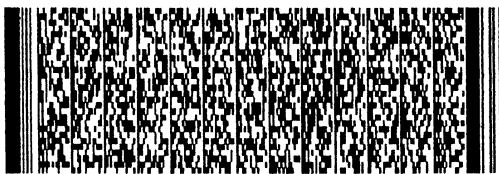
控制伺服軟體及/或韌體30是一種方法或機制,以指示作業系統60、或其通訊程式,經由通訊裝置120與一用戶裝置11溝通。控制伺服軟體及/或韌體30也是一種方法或機制,以指示控制用戶軟體及/或韌體31,指示作業系統61在控制伺服軟體及/或韌體30、和控制用戶軟體及/或韌體31的功能之執行期間,暫時地中止用戶裝置11的使用者干涉。控制伺服軟體及/或韌體30也是一種方法或機制,



五、發明說明 (24)

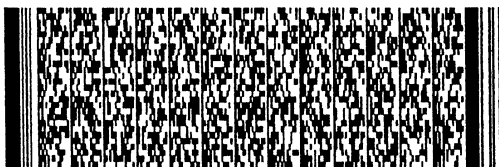
以經由通訊裝置120接收來自控制用戶軟體及/或韌體31的指令。控制伺服軟體及/或韌體30也是一種方法或機制，以讓伺服裝置10的使用者能夠建立與一電腦檔案及/或程式110有關的第三者使用許可及/或權利，藉此限制用戶裝置11或下一用戶裝置12對此電腦檔案及/或程式110的使用。控制伺服軟體及/或韌體30也是一種方法或機制，以自動地指示伺服裝置10的公用鍵基礎40，編密並傳送與一電腦檔案及/或程式110有關的使用許可及/或權利，和經由通訊裝置120編密並傳送一電腦檔案及/或程式110到一用戶裝置11。控制伺服軟體及/或韌體30可能具體實施在電腦編碼軟體(例如，但不限於，以電腦語言c++寫的程式)，以執行所描述的功能。

控制用戶軟體及/或韌體31是一種方法或機制，以自動地指示作業系統61、或其通訊程式，經由通訊裝置120與伺服裝置10或下一用戶裝置12溝通。控制用戶軟體及/或韌體31也是一種方法或機制，以經由通訊裝置120從一控制伺服軟體及/或韌體30接收指令。控制用戶軟體及/或韌體31也是一種方法或機制，以指示作業系統61在控制伺服軟體及/或韌體30、和控制用戶軟體及/或韌體31的功能之執行期間，暫時地中止用戶裝置11的使用者干涉。控制伺服軟體及/或韌體31也是一種方法或機制，以自動地指示用戶裝置11的公用鍵基礎41，從與一電腦檔案及/或程式110有關的使用許可及/或權利之傳送中接收並解密，和經由通訊裝置120從伺服裝置10所傳輸的電腦檔案及/或程式



五、發明說明 (25)

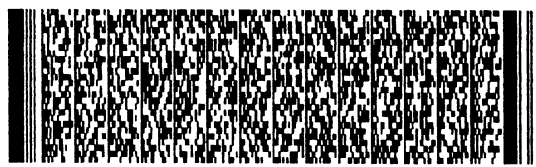
110 的傳送中接收並解密，並放置其一份電子副本在隨機存取記憶體81中。控制用戶軟體及/或韌體31也是一種方法或機制，以自動地指示用戶裝置11的編密檔案系統51，使用與該電腦檔案及/或程式110有關、且由伺服裝置10所傳輸的該許可及/或權利，從隨機存取記憶體81再叫出一電腦檔案及/或程式110，並編密與存檔其一份電子副本到儲存體101。控制用戶軟體及/或韌體31是一種方法或機制，以指示作業系統61在控制伺服軟體及/或韌體30、和控制用戶軟體及/或韌體31的功能之執行完成時，回復用戶裝置11的使用者干涉。控制用戶軟體及/或韌體31是一種方法或機制，以指示作業系統61在控制用戶軟體及/或韌體31、和控制用戶軟體及/或韌體32的功能之執行期間，暫時地中止用戶裝置11的使用者干涉。控制用戶軟體及/或韌體31是一種方法或機制，以指示控制用戶軟體及/或韌體32，指示作業系統62在控制用戶軟體及/或韌體31、和控制用戶軟體及/或韌體32的功能之執行期間，暫時地中止下一用戶裝置12的使用者干涉。控制用戶軟體及/或韌體31也是一種方法或機制，以經由通訊裝置120從一下一用戶裝置12的控制用戶軟體及/或韌體32接收指令。控制用戶軟體及/或韌體31也是一種方法或機制，以自動地指示一用戶裝置11的編密檔案系統51，從儲存體101解密一電腦檔案及/或程式110，並將其一份電子副本放置在隨機存取記憶體81中。控制用戶軟體及/或韌體31也是一種方法或機制，以自動地指示用戶裝置11的公用鍵基礎41，



五、發明說明 (26)

編密並經由通訊裝置120傳送一電腦檔案及/或程式110到下一用戶裝置12。控制用戶軟體及/或韌體31也是一種方法或機制，以指示作業系統61在控制用戶軟體及/或韌體31的功能執行完成時，回復用戶裝置11的使用者干涉。控制用戶軟體及/或韌體31可具體實施在電腦編碼軟體(例如，但不限於，以電腦語言c++寫的程式)中，以執行以上所描述的功能。控制用戶軟體及/或韌體31有許多具體實施例類似於那些控制用戶軟體及/或韌體32。

控制用戶軟體及/或韌體32是一種方法或機制，以自動地指示作業系統62、或其通訊程式，經由通訊裝置120與用戶裝置12或電子地溝通。控制用戶軟體及/或韌體32也是一種方法或機制，以經由通訊裝置120從用戶裝置11的控制用戶軟體及/或韌體31接收指令。控制用戶軟體及/或韌體32也是一種方法或機制，以指示作業系統62在控制用戶軟體及/或韌體31、和控制用戶軟體及/或韌體32的功能之執行期間，暫時地中止下一用戶裝置12的使用者干涉。控制用戶軟體及/或韌體32也是一種方法或機制，以自動地指示下一用戶裝置12的公用鍵基礎42，從與一電腦檔案及/或程式110有關的使用許可及/或權利之傳送中接收並解密，和經由通訊裝置120從用戶裝置11所傳輸的電腦檔案及/或程式110的傳送中接收並解密，並放置其一份電子副本在隨機存取記憶體82中。控制用戶軟體及/或韌體32也是一種方法或機制，以自動地指示下一用戶裝置12的編密檔案系統52，使用與該電腦檔案及/或程式110有關、且

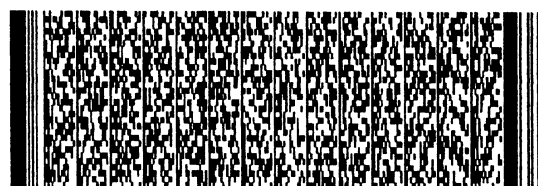
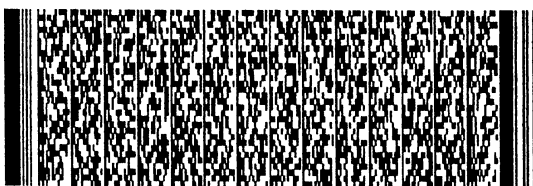


五、發明說明 (27)

由用戶裝置11所傳輸的該許可及/或權利，從隨機存取記憶體82再叫出一電腦檔案及/或程式110，並編密與存檔其一份電子副本到儲存體102。控制用戶軟體及/或韌體32是一種方法或機制，以指示作業系統62在控制用戶軟體及/或韌體31、和控制用戶軟體及/或韌體32的功能之執行完成時，回復下一用戶裝置12的使用者干涉。控制用戶軟體及/或韌體32可具體實施在電腦編碼軟體(例如，但不限於，以電腦語言c++寫的程式)中，以執行以上所描述的功能。控制用戶軟體及/或韌體32有許多具體實施例類似於那些控制用戶軟體及/或韌體31。

伺服裝置10的公用鍵基礎40(例如，但不限於，微軟公司視窗2000伺服器系列產品的公用鍵基礎，之前以微軟公司視窗NT伺服器5.0版聞名)是一種密碼學方法或機制，其提供公用編密和私人解密鍵，使伺服裝置10能夠使用編密的通訊協定(例如，但不限於，保密插槽層(SSL)，傳輸層保密(TLS)，虛擬私人網路(VPN)等)經由通訊裝置120來進行編密的通訊。伺服裝置10的公用鍵基礎40也是一種密碼學方法或機制，其提供公用編密和私人解密鍵給作業系統60的其他元件、或在作業系統60上執行的應用程式。

用戶裝置11的公用鍵基礎41(例如，但不限於，微軟公司視窗2000專業版的公用鍵基礎，之前稱為微軟公司視窗NT工作站5.0版)是一種密碼學方法或機制，其提供公用編密和私人解密鍵，使用戶裝置11能夠使用編密的通訊協定(例如，但不限於，保密插槽層(SSL)，傳輸層保密(TLS))

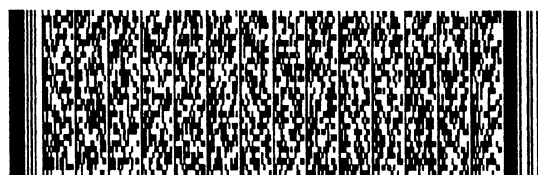


五、發明說明 (28)

， 虛 擬 私 人 網 路 (VPN) 等) 經 由 通 訊 裝 置 120 進 行 編 密 的 通 訊 。 用 戶 裝 置 11 的 公 用 鍵 基 礎 41 也 是 一 種 密 碼 學 方 法 或 機 制 ， 其 提 供 公 用 編 密 和 私 人 解 密 鍵 給 作 業 系 統 61 的 其 他 元 件 、 或 在 作 業 系 統 61 上 執 行 的 應 用 程 式 。

下 一 用 戶 裝 置 12 的 公 用 鍵 基 礎 42 (例 如 ， 但 不 限 於 ， 微 軟 公 司 視 窗 2000 專 業 版 的 公 用 鍵 基 礎 ， 之 前 稱 為 微 軟 公 司 視 窗 NT 工 作 站 5.0 版) 是 一 種 密 碼 學 方 法 或 機 制 ， 其 提 供 公 用 編 密 和 私 人 解 密 鍵 ， 使 該 下 一 用 戶 裝 置 12 能 夠 使 用 編 密 的 通 訊 協 定 (例 如 ， 但 不 限 於 ， 保 密 插 槽 層 (SSL) ， 傳 輸 層 保 密 (TLS) ， 虛 擬 私 人 網 路 (VPN) 等) 經 由 通 訊 裝 置 120 進 行 編 密 的 通 訊 。 下 一 用 戶 裝 置 12 的 公 用 鍵 基 礎 42 也 是 一 種 密 碼 學 方 法 或 機 制 ， 其 提 供 公 用 編 密 和 私 人 解 密 鍵 給 作 業 系 統 62 的 其 他 元 件 、 或 在 作 業 系 統 62 上 執 行 的 應 用 程 式 。

編 密 檔 案 系 統 50 (例 如 ， 但 不 限 於 ， 微 軟 公 司 視 窗 2000 伺 服 器 的 編 密 檔 案 系 統 ， 之 前 以 微 軟 公 司 視 窗 NT 伺 服 器 5.0 版 聞 名) 是 方 法 或 機 制 ， 以 允 許 伺 服 裝 置 的 使 用 者 手 動 地 挑 選 電 腦 檔 案 或 檔 案 夾 來 編 密 或 解 密 。 編 密 檔 案 系 統 50 也 是 一 種 方 法 或 機 制 ， 以 使 用 一 隨 機 地 產 生 且 秘 密 的 編 密 及 / 或 解 密 鍵 ， 編 密 一 電 腦 檔 案 及 / 或 程 式 110 。 編 密 檔 案 系 統 50 也 是 一 種 方 法 或 機 制 ， 以 使 用 公 用 鍵 基 礎 40 的 公 用 編 密 鍵 ， 編 密 該 隨 機 地 產 生 的 秘 密 編 密 及 / 或 解 密 鍵 ， 並 把 它 存 檔 到 儲 存 體 100 和 使 該 隨 機 地 產 生 的 秘 密 編 密 及 / 或 解 密 鍵 與 該 電 腦 檔 案 及 / 或 程 式 110 相 關 聯 。 編 密 檔 案 系 統 50 也 是 一 種 方 法 或 機 制 ， 以 使 用 公 用 鍵 基 礎 40 的 私 人 解 密

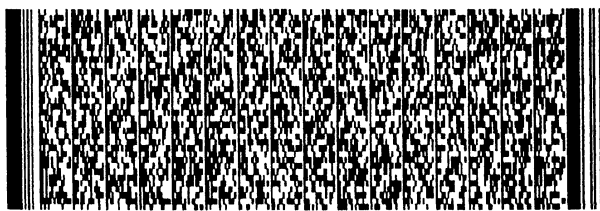


五、發明說明 (29)

鍵，來解密與該電腦檔案及/或程式110有關的該隨機地產生的秘密編密及/或解密鍵的副本，然後在伺服器裝置10的讀取和寫入運作期間，即時使用該隨機地產生的秘密編密及/或解密鍵，解密該電腦檔案及/或程式110。

編密檔案系統51(例如，但不限於，微軟公司視窗2000專業版的編密檔案系統，之前以微軟公司視窗NT工作站5.0版聞名)是一種方法或機制，以允許用戶裝置的使用者手動地挑選電腦檔案或檔案夾來編密或解密。編密檔案系統51也是一種方法或機制，以使用一隨機地產生且秘密的編密及/或解密鍵，編密一電腦檔案及/或程式110。編密檔案系統51也是一種方法或機制，以使用公用鍵基礎41的公用編密鍵，編密該隨機地產生的秘密編密及/或解密鍵，並把它存檔到儲存體101和使該隨機地產生的秘密編密及/或解密鍵與該電腦檔案及/或程式110相關聯。編密檔案系統51也是一種方法或機制，以使用公用鍵基礎41的私人解密鍵，來解密與該電腦檔案及/或程式110有關的該隨機地產生的秘密編密及/或解密鍵的副本，然後在用戶裝置11的讀取和寫入運作期間，即時使用該隨機地產生的秘密編密及/或解密鍵，解密該電腦檔案及/或程式110。

編密檔案系統52(例如，但不限於，微軟公司視窗2000專業版的編密檔案系統，之前以微軟公司視窗NT工作站5.0版聞名)是一種方法或機制，以允許下一用戶裝置12的使用者手動地挑選電腦檔案或檔案夾來編密或解密。編密檔案系統52也是一種方法或機制，以使用一隨機地產生且



五、發明說明 (30)

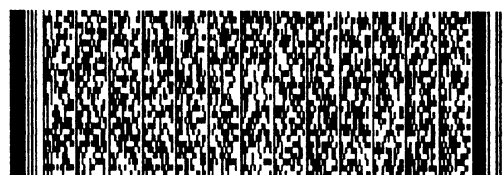
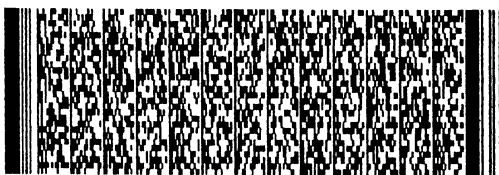
秘密的編密及/或解密鍵，編密一電腦檔案及/或程式110。編密檔案系統52也是一種方法或機制，以使用公用鍵基礎42的公用編密鍵，編密該隨機地產生的秘密編密及/或解密鍵，並把它存檔到儲存體102和使該隨機地產生的秘密編密及/或解密鍵與該電腦檔案及/或程式110相關聯。編密檔案系統52也是一種方法或機制，以使用公用鍵基礎42的私人解密鍵，來解密與該電腦檔案及/或程式110有關的該隨機地產生的秘密編密及/或解密鍵的副本，然後在下一用戶裝置12的讀取和寫入運作期間，即時使用該隨機地產生的秘密編密及/或解密鍵，解密該電腦檔案及/或程式110。

作業系統60(例如，但不限於，微軟公司視窗2000伺服器，之前以微軟公司視窗NT伺服器5.0版聞名)是一種方法或機制，以允許伺服裝置10的計算功能。

作業系統61(例如，但不限於，微軟公司視窗2000專業版，之前以微軟公司視窗NT工作站5.0版聞名)是一種方法或機制，以允許用戶裝置11的計算功能。

作業系統62(例如，但不限於，微軟公司視窗2000專業版，之前以微軟公司視窗NT工作站5.0版聞名)是一種方法或機制，以允許下一用戶裝置12的計算功能。

收發器70(例如，但不限於，數據機，纜線數據機，網路介面卡等)是一種方法或機制，以經由通訊裝置120電子地送出和接收通訊訊號。收發器70是一種方法或機制，連接到伺服裝置10及/或作業系統60，或由其軟體及/或韌體



五、發明說明 (31)

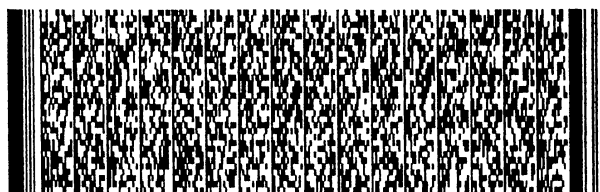
使用，以經由通訊裝置120電子地溝通。收發器70連接到伺服裝置10，且連接到通訊裝置120。

收發器71(例如，但不限於，數據機，纜線數據機，網路介面卡等)是一種方法或機制，以經由通訊裝置120電子地送出和接收通訊訊號。收發器71是一種方法或機制，連接到用戶裝置11及/或作業系統61，或由其軟體及/或韌體使用，以經由通訊裝置120電子地溝通。收發器71連接到用戶裝置11，且連接到通訊裝置120。

收發器72(例如，但不限於，數據機，纜線數據機，網路介面卡等)是一種方法或機制，以經由通訊裝置120電子地送出和接收通訊訊號。收發器72是一種方法或機制，連接到下一用戶裝置12及/或作業系統62，或由其軟體及/或韌體使用，以經由通訊裝置120電子地溝通。收發器72連接到下一用戶裝置12，且連接到通訊裝置120。

隨機存取記憶體80(也稱為"RAM 80")是一種方法或機制，由伺服裝置10的作業系統60用來暫時地儲存電腦檔案、作業系統60使用的電腦程式或其他電腦資訊、在作業系統60上或該伺服裝置10的其他電腦週邊裝置上執行的電腦程式。

隨機存取記憶體81(也稱為"RAM 81")是一種方法或機制，由用戶裝置11的作業系統61用來暫時地儲存電腦檔案、作業系統61使用的電腦程式或其他電腦資訊、在作業系統61上或該用戶裝置11的其他電腦週邊裝置上執行的電腦程式。



五、發明說明 (32)

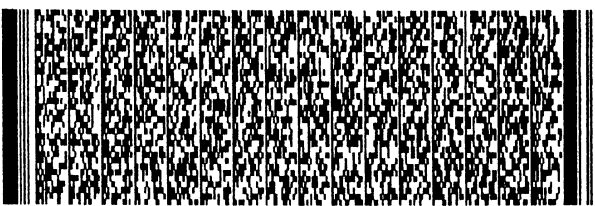
隨機存取記憶體82(也稱為"RAM 82")是一種方法或機制，由下一用戶裝置12的作業系統62用來暫時地儲存電腦檔案、作業系統62使用的電腦程式或其他電腦資訊、在作業系統62上或該下一用戶裝置12的其他電腦週邊裝置上執行的電腦程式。

處理器90是伺服裝置10的一種方法或機制，以電子地處理作業系統60的、在該作業系統60上或該伺服裝置10的其他電腦週邊裝置上執行的其他電腦程式之指令。處理器90也是伺服裝置10的一種方法或機制，以電子地處理該伺服裝置10的其他週邊軟體及/或韌體裝置之指令。

處理器91是用戶裝置11的一種方法或機制，以電子地處理作業系統61的、在該作業系統61上或該用戶裝置11的其他電腦週邊裝置上執行的其他電腦程式之指令。處理器91也是用戶裝置11的一種方法或機制，以電子地處理該用戶裝置11的其他週邊軟體及/或韌體裝置之指令。

處理器92是下一用戶裝置12的一種方法或機制，以電子地處理作業系統62的、在該作業系統62上或該下一用戶裝置12的其他電腦週邊裝置上執行的其他電腦程式之指令。處理器92也是下一用戶裝置12的一種方法或機制，以電子地處理該下一用戶裝置12的其他週邊軟體及/或韌體裝置之指令。

儲存體100是在伺服裝置10中、或與其連接的一種方法或機制，其可用來從該伺服裝置10的隨機存取記憶體80，電子地存檔電腦程式或電腦檔案的數位碼之一份電子副本



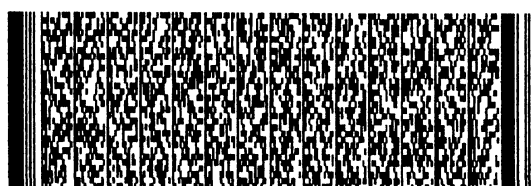
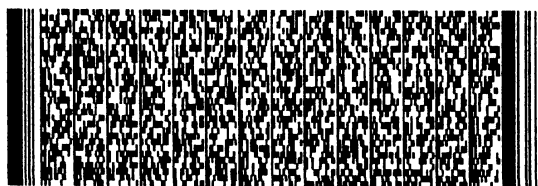
五、發明說明 (33)

。 儲存體101是在用戶裝置11中、或與其連接的一種方法或機制，其可用來從該用戶裝置11的隨機存取記憶體81，電子地存檔電腦程式或電腦檔案的數位碼之一份電子副本。

儲存體102是在下一用戶裝置12中、或與其連接的一種方法或機制，其可用來從該下一用戶裝置12的隨機存取記憶體82，電子地存檔電腦程式或電腦檔案的數位碼之一份電子副本。

電腦檔案及/或程式110是一種電腦檔案或一種電腦程式[例如，但不限於，一文書處理文件(也就是MS Word，Lotus WordPro)、試算表檔案(例如，但不限於，Lotus 1-2-3、MS Excel)、一聲音檔案(例如，但不限於，MP3、WAV、AUI)、一影像檔案(例如，但不限於，AVI、MPEG)、一可執行程式(例如，但不限於，EXE)等]。

通訊裝置120(例如，但不限於，電話線路、纜線電視線、同軸纜線、光纖、無線電、蜂巢式、衛星、序列纜線、平行纜線、紅外線的通訊、通用序列匯流排[USB]纜線、網際網路、區域網路、乙太網路、一般網路等)是一種方法或機制，與其連接的計算裝置可藉其電子地溝通。通訊裝置120也是一種方法或機制，與其連接之計算裝置可藉其啟動編密通訊協定(例如，但不限於，保密插槽層(SSL)、傳輸層保密(TLS)、虛擬私人網路(VPN)等)來傳送和接收編密的訊號。通訊裝置120分別連接到伺服裝置10、用

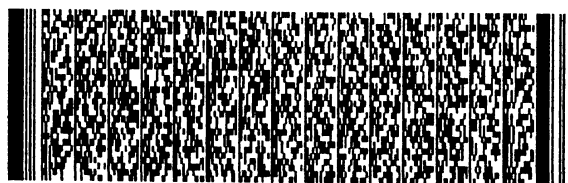


五、發明說明 (34)

戶裝置11、和下一用戶裝置12的收發器70、71、和72。

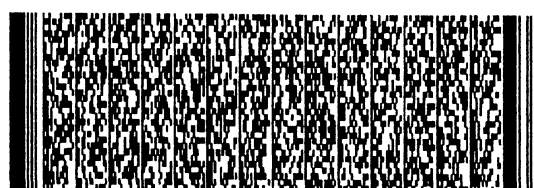
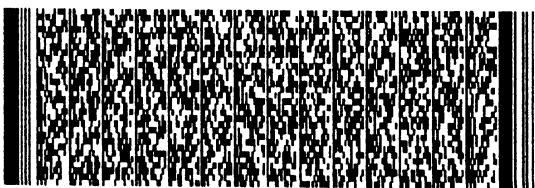
伺服裝置10的使用者把一個電腦檔案存檔及/或程式110存檔到與伺服裝置10連接、或在其內部的儲存體100。伺服裝置10的使用者在伺服介面20和儲存體100中該電腦檔案及/或程式110的位置之間，建立一聯結、關係或其他形式的電子關聯(集體稱為"超連結")。伺服裝置10的收發器70連接到一通訊裝置120。伺服裝置10的使用者透過控制伺服軟體及/或韌體30，輸入(例如，但不限於，經由鍵盤，滑鼠等輸入)要與電腦檔案及/或程式110相關聯的許可及/或權利。該許可包括，但不限於，移動或複製等，而該權利包括，但不限於，使用的次數、使用的截止日期、對第三者的許可及/或權利的指派等。

用戶裝置11的使用者經由通訊裝置120與伺服裝置10溝通。用戶裝置11的收發器71連接到一通訊裝置120。用戶裝置11的使用者在用戶裝置11的影像顯示器上觀看伺服介面20，並識別與想要的電腦檔案及/或程式110有關的超連結。用戶裝置11的使用者使用用戶介面21經由通訊裝置120來開始一超連結傳輸請求(例如，但不限於，滑鼠雙點一與該電腦檔案及/或程式110有關的超連結)，以從伺服裝置10取得該電腦檔案及/或程式110。這個請求開始一系列控制伺服軟體及/或韌體30、然後是控制用戶軟體及/或韌體31自動化的動作。首先，控制伺服軟體及/或韌體30指示控制用戶軟體及/或韌體31，以指示用戶裝置11的作業系統61，暫時地中止使用者干涉，以避免任何形式的未



五、發明說明 (35)

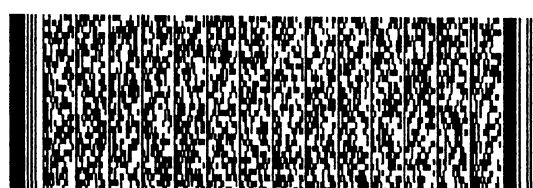
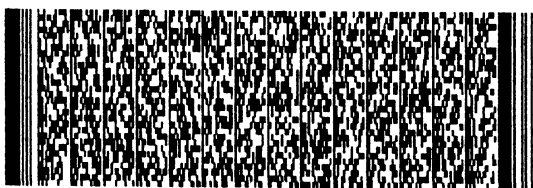
經認可之資料或指令，透過在伺服器裝置10抑或用戶裝置11之內部或外部的的方法或機制，輸入到、或遍佈伺服器裝置10或用戶裝置11，例如，但不限於，透過鍵盤、滑鼠、或其他實際方法或機制的使用之使用者輸入或控制；電腦程式；巨集；或能夠以任何方式影響本發明的軟體及/或韌體之功能、能夠以任何方式影響本發明所利用的任何軟體及/或韌體之功能的任何其他方法或機制，並在傳輸請求的執行期間避免對電腦檔案及/或程式110任何形式未經認可的存取、使用、控制。然後控制用戶軟體及/或韌體31指示用戶裝置11的作業系統61暫時中止使用者干涉。然後控制用戶軟體及/或韌體31指示控制伺服器軟體及/或韌體30，傳送電腦檔案及/或程式110到用戶裝置11。然後控制伺服器軟體及/或韌體30指示伺服器裝置10的作業系統60之公用鍵基礎40，使用編密的通訊協定(例如，但不限於，保密插槽層(SSL)、傳輸層保密(TLS)、虛擬私人網路(VPN)等)編密和傳送電腦檔案及/或程式110及其相關的許可及/或權利到用戶裝置11。然後伺服器裝置10的作業系統60從儲存體100再取出電腦檔案及/或程式110；放置電腦檔案及/或程式110的一份電子副本在隨機存取記憶體80之內；並經由通訊裝置120編密和傳送電腦檔案及/或程式110到用戶裝置11。然後用戶裝置11的作業系統61之公用鍵基礎41，使用編密的通訊協定(例如，但不限於，保密插槽層(SSL)、傳輸層保密(TLS)、虛擬私人網路(VPN)等)從傳送當中，接收和解密該電腦檔案及/或程式110，並放置該電腦檔案



五、發明說明 (36)

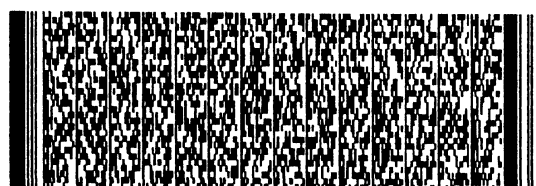
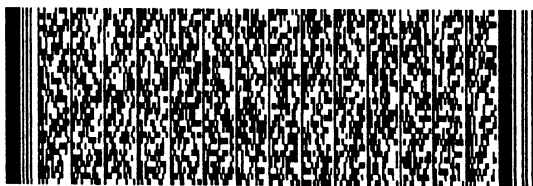
及/或程式110的一份電子副本到隨機存取記憶體81之內。然後控制用戶軟體及/或韌體31自動地指示用戶裝置11的編密檔案系統51，使用伺服裝置10所傳輸的相關許可及/或權利從隨機存取記憶體81編密和存檔電腦檔案及/或程式110的該電子副本到儲存體101，和然後從隨機存取記憶體81抹去電腦檔案及/或程式110的任何電子副本。然後用戶裝置11的作業系統61之控制用戶軟體及/或韌體31指示用戶裝置11的作業系統61重建使用者干涉。

用戶裝置11的使用者可遵照與其相關的許可及/或權利，使用存檔在儲存體101中的電腦檔案及/或程式110，就像該電腦檔案及/或程式110未編密一樣。不是由編密檔案系統51所執行之電腦檔案及/或程式110的複製或移動，將不會適當地編密供用戶裝置11之外的計算裝置上使用。依照該許可及/或權利，用戶裝置11的使用者可利用控制用戶軟體及/或韌體31啟動編密檔案系統51的功能，以執行從儲存體101移動或複製電腦檔案及/或程式110到下一用戶裝置12的儲存體102。用戶裝置12的收發器72連接到通訊裝置120。用戶裝置11的使用者觀看用戶介面21和下一用戶介面22的一個(例如，但不限於，如視窗2000作業系統所使用的)視窗，其在用戶裝置11的影像顯示器上分別顯示儲存體101對儲存體102的有關內容。使用者識別與要從儲存體101移動到儲存體102之電腦檔案及/或程式110相關的物件(例如，但不限於，圖像)(以下稱"圖像")。用戶裝置11的使用者使用他們的電腦滑鼠從用戶介面21視窗



五、發明說明 (37)

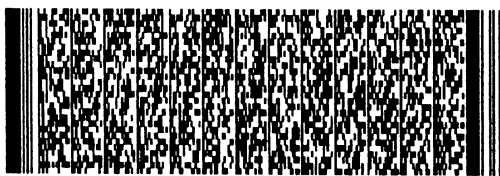
移動與電腦檔案及/或程式110有關的圖像(例如,但不限於,一圖形使用者介面拖放動作)到下一用戶介面22視窗。與該電腦檔案及/或程式110有關之該圖像的拖放,會啟動控制伺服軟體及/或韌體30、然後是控制用戶軟體及/或韌體31自動化的一系列動作。首先,控制用戶軟體及/或韌體31指示用戶裝置11的作業系統61,暫時地中止使用者干涉,以避免透過用戶裝置11抑或下一用戶裝置12內部或外部的的方法或機制,任何形式未經認可的資料或指令輸入到或遍佈用戶裝置11或下一用戶裝置12,例如,但不限於,藉由鍵盤、滑鼠、或其他實際方法或機制的使用之使用者輸入或控制;電腦程式;巨集;或任何能夠以任何方式影響本發明的軟體及/或韌體的功能、能夠以任何方式影響本發明所利用的任何軟體及/或韌體的其他方法或機制,並避免在傳輸請求的執行期間任何形式對電腦檔案及/或程式未經認可的存取、使用、控制。然後控制用戶軟體及/或韌體31指示控制用戶軟體及/或韌體32,指示下一用戶裝置12的作業系統62,在傳輸請求執行期間暫時地中止使用者干涉(例如,但不限於,鍵盤或滑鼠干涉、程式或巨集指令等)。然後控制用戶軟體及/或韌體32指示下一用戶裝置12的作業系統62,暫時地中止使用者干涉。然後控制用戶軟體及/或韌體32指示控制用戶軟體及/或韌體31,傳送該電腦檔案及/或程式110到下一用戶裝置12。然後控制用戶軟體及/或韌體31指示編密檔案系統51,從儲存體101再取出和解密該電腦檔案及/或程式110及其相關的許



五、發明說明 (38)

可及/或權利，並存檔其一份電子副本在隨機存取記憶體81中。然後控制用戶軟體及/或韌體31指示用戶裝置11的作業系統61之公用鍵基礎41，經由通訊裝置120，從隨機存取記憶體81編密並傳送該電腦檔案及/或程式110的電子副本及其相關的許可及/或權利，到下一用戶裝置12。然後控制用戶軟體及/或韌體32指示下一用戶裝置12的公用鍵基礎42，從該電腦檔案及/或程式110及其相關的許可及/或權利的傳送中接收和解密，並放置其一份電子副本在隨機存取記憶體82中。在從儲存體101移動該電腦檔案及/或程式110到儲存體102的情況中，在下一用戶裝置12接收電腦檔案及/或程式110到隨機存取記憶體82內時，下一用戶裝置12的控制用戶軟體及/或韌體32自動地指示用戶裝置11的控制用戶軟體及/或韌體31，指示用戶裝置11的作業系統61刪除在儲存體101或隨機存取記憶體81中電腦檔案及/或程式110的所有副本。然後控制用戶軟體及/或韌體31指示作業系統61，重建用戶裝置11的使用者干涉。然後控制用戶軟體及/或韌體32自動地指示下一用戶裝置12的作業系統62之編密檔案系統52，使用從用戶裝置11傳輸來的相關許可及/或權利，從隨機存取記憶體82編密和存檔電腦檔案及/或程式110的該電子副本到儲存體102，然後並從隨機存取記憶體82抹去電腦檔案及/或程式110的所有電子副本。然後控制用戶軟體及/或韌體32指示作業系統62，重建下一用戶裝置12的使用者干涉。

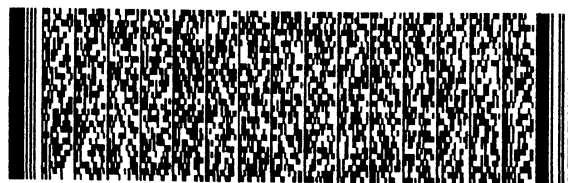
當電腦檔案及/或程式110未編密時，下一用戶裝置12的



五、發明說明 (39)

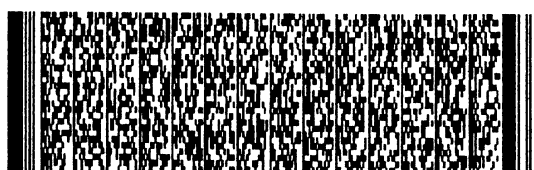
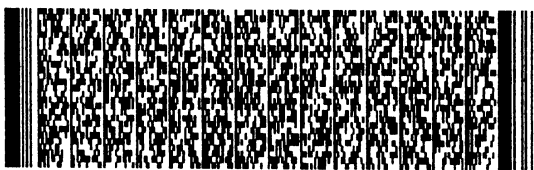
使用者可遵照原本由伺服裝置10建立並傳輸到用戶裝置11然後到下一用戶裝置12的許可及/或權利，使用電腦檔案及/或程式110。不是由下一用戶裝置12的編密檔案系統52結合下一用戶裝置12的控制用戶軟體及/或韌體32執行的電腦檔案及/或程式110之複製或移動，將不會適當地編密供下一用戶裝置12以外的計算裝置上的使用。

作為範例，伺服裝置10的使用者將伺服裝置10的收發器70連接到帶有後續通訊連接到網際網路的通訊裝置120。伺服裝置10的使用者存檔一聲音檔案(例如，但不限於，以MP3格式)，為一電腦程式及/或檔案110在儲存體100中，並指派它一個聯結(例如，但不限於，TCP及/或IP超連結)到一伺服介面20(例如，但不限於，一網頁)。用戶裝置11的使用者將用戶裝置11的收發器71連接到帶有後續通訊連接到網際網路的通訊裝置120。用戶裝置11的使用者能夠在用戶裝置11的影像顯示器上用戶介面21當中，觀看伺服介面20的一個副本。用戶裝置11的使用者藉由使用用戶裝置11的電腦滑鼠在與MP3聲音檔案有關的超連結上雙點，選取MP3聲音檔案以下載到用戶裝置11，其顯示在用戶裝置11的影像顯示器上的用戶介面21上。雙點動作指示用戶介面21，經由通訊裝置120傳送一電子請求，從伺服裝置10下載MP3聲音檔案到用戶裝置11。在收到傳輸請求時，伺服介面發訊給控制伺服軟體及/或韌體30，以開始各種自動功能。控制伺服軟體及/或韌體30首先指示(經由通訊裝置120)控制用戶軟體及/或韌體31，以指示用戶裝



五、發明說明 (40)

置11的作業系統61暫時中止使用者干涉。控制用戶軟體及/或韌體31然後指示(經由通訊裝置120)控制伺服軟體及/或韌體30,以傳送MP3聲音檔案。控制伺服軟體及/或韌體30指示作業系統60從儲存體100再取出MP3聲音檔案、和其相關的許可及/或權利,並將其一份電子副本放置在隨機存取記憶體80中。然後控制伺服軟體及/或韌體30指示公用鍵基礎40經由通訊裝置120,編密和傳送MP3聲音檔案的一份電子副本、及其相關的許可及/或權利到用戶裝置11。此時,控制伺服軟體及/或韌體30已經結束它傳輸程序的部分,而與控制伺服軟體及/或韌體30有關的程式結束。在用戶裝置11收到MP3聲音檔案、和其相關的許可及/或權利時,公用鍵基礎41從傳送中解密MP3聲音檔案和其相關的許可及/或權利,並儲存其一份電子副本在隨機存取記憶體81中。然後控制用戶軟體及/或韌體31指示用戶裝置11的編密檔案系統51,使用伺服裝置10所傳送相關的許可及/或權利,從隨機存取記憶體81編密和存檔MP3聲音檔案的該電子副本到儲存體101。然後控制用戶軟體及/或韌體31指示編密檔案系統51或作業系統61,從隨機存取記憶體81抹去MP3聲音檔案的任何電子副本。然後用戶裝置11的作業系統61之控制用戶軟體及/或韌體31,指示用戶裝置11的作業系統61重建使用者干涉。此時,控制用戶軟體及/或韌體31已經結束它儲存程序的傳輸和編密部分,而與控制用戶軟體及/或韌體31有關的程式結束。現在用戶裝置11的使用者能夠播放MP3聲音檔案,而編密檔案系統



五、發明說明 (41)

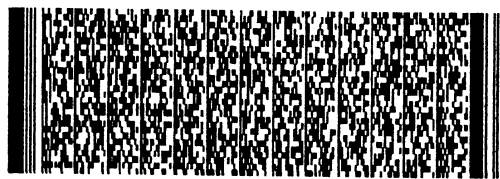
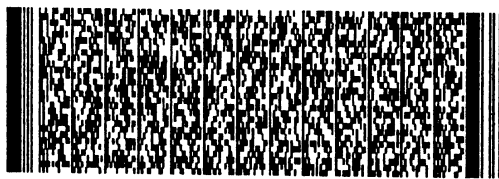
51 遵照編密檔案系統51所使用的許可及/或權利來編密MP3聲音檔案。

此外，用戶裝置11的使用者然後決定傳遞MP3聲音檔案到下一用戶裝置12，而在這個範例中，使用者可根據與MP3聲音檔案有關的許可及/或權利這樣做。用戶裝置11的使用者連接用戶裝置11的收發器71到一帶有後續通訊連接到網際網路的通訊裝置120。下一用戶裝置12的使用者連結下一用戶裝置12的收發器72到一帶有後續通訊連接到網際網路的通訊裝置120。用戶裝置11的使用者在用戶裝置11的影像顯示器上觀看用戶介面21和下一用戶介面22的一個副本，其分別顯示儲存體101和儲存體102的有關內容。使用者識別與要從儲存體101移動到儲存體102有關的MP3聲音檔案之物件(例如，但不限於，圖像)(以下稱"圖像")。用戶裝置11的使用者使用其電腦滑鼠從用戶介面21視窗移動與MP3聲音檔案有關的圖像(例如，但不限於，一圖形使用者介面拖放動作)到下一用戶介面22視窗。與MP3聲音檔案有關之該圖像的拖放，會啟動控制用戶軟體及/或韌體31、然後是控制用戶軟體及/或韌體32自動化的一系列動作。首先，控制用戶軟體及/或韌體31指示用戶裝置11的作業系統61，在傳輸請求的執行期間暫時地中止使用者干涉(例如，但不限於，鍵盤或滑鼠干涉、程式或巨集指令等)。然後控制用戶軟體及/或韌體31指示控制用戶軟體及/或韌體32，指示下一用戶裝置12的作業系統62，在傳輸請求的執行期間暫時中止使用者干涉(例如，但不限於



五、發明說明 (42)

，鍵盤或滑鼠干涉、程式或巨集指令等)。然後控制用戶軟體及/或韌體32指示下一用戶裝置12的作業系統62暫時中止使用者干涉。然後控制用戶軟體及/或韌體32指示控制用戶軟體及/或韌體31傳送MP3聲音檔案到下一用戶裝置12。然後控制用戶軟體及/或韌體31再取出與MP3聲音檔案有關、且由編密檔案系統51所使用之許可及/或權利，並指示編密檔案系統51從儲存體101再取出和解密MP3聲音檔案，並存檔其一份電子副本在隨機存取記憶體81中。然後控制用戶軟體及/或韌體31指示用戶裝置11的作業系統61之公用鍵基礎41，從隨機存取記憶體81編密並傳送MP3聲音檔案的電子副本及其相關的許可及/或權利，經由通訊裝置120到下一用戶裝置12。然後控制用戶軟體及/或韌體32指示下一用戶裝置12的公用鍵基礎42，從MP3聲音檔案及其許可及/或權利的傳輸接收和解密，並放置其一份電子副本在隨機存取記憶體82中。在從儲存體101移動MP3聲音檔案到儲存體102的情況，在由下一用戶裝置12接收MP3聲音檔案到隨機存取記憶體82中時，下一用戶裝置12的控制用戶軟體及/或韌體32自動地指示用戶裝置11的控制用戶軟體及/或韌體31，指示用戶裝置11的作業系統61及/或編密檔案系統51，刪除儲存體101或隨機存取記憶體81中的MP3聲音檔案之所有副本。然後控制用戶軟體及/或韌體31指示作業系統61重建用戶裝置11的使用者干涉。然後控制用戶軟體及/或韌體32自動地指示下一用戶裝置12的作業系統62之編密檔案系統52，使用從用戶裝置11所傳輸的

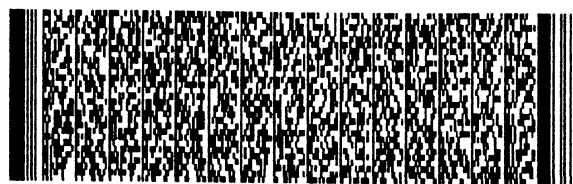
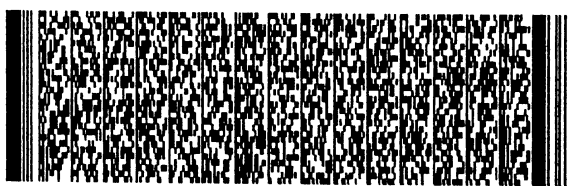


五、發明說明 (43)

相關許可及/或權利，從隨機存取記憶體82編密和存檔MP3聲音檔案的該電子副本到儲存體102，然後並從隨機存取記憶體82抹去MP3聲音檔案的所有電子副本。然後控制用戶軟體及/或韌體32指示作業系統62，重建下一用戶裝置12的使用者干涉。此時，控制用戶軟體及/或韌體32已經結束其儲存程序的傳輸和編密部分，而與控制用戶軟體及/或韌體32有關的程式結束。現在下一用戶裝置12的使用者能夠播放MP3聲音的檔案，然而，在這個範例中用戶裝置11的使用者不能夠播放MP3聲音檔案，因為檔案已經"移動"，且在"移動"程序期間，MP3聲音檔案的所有副本在"移動"程序結束時從用戶裝置11抹去。此外，由於MP3聲音檔案已經由編密檔案系統51編密以在下一用戶裝置12上使用，MP3聲音檔案的傳統移動或複製將不被編密檔案系統51許可，而只有利用控制用戶軟體及/或韌體32之MP3聲音檔案的移動或複製會被編密檔案系統51許可。

在此處所稱的"方法或機制"指35 U.S.C. 第112節，第6段。"方法或機制"的"方法"一詞遵從35 U.S.C. 第112節，第6段，而"方法或機制"的"機制"一詞未遵從35 U.S.C. 第112節，第6段。

雖然本發明已經在前面具體實施例中詳細描述作為例證，但應了解此細節僅是為了說明之目的，而熟知該項技藝人士可在其中進行變更而不離開本發明的精神和範疇，除非它在下列申請專利範圍所描述之外。

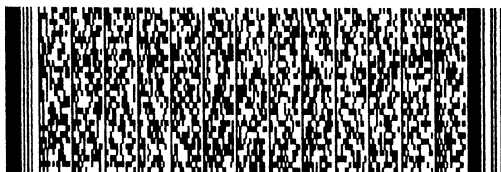


四、中文發明摘要 (發明之名稱：用以操縱電腦檔案及/或程式之系統及方法)

一種用來操縱一電腦檔案及/或程式的系統。此系統包括一伺服器裝置，能夠存取一未編密的電腦檔案及/或程式，且其可將未編密的電腦檔案及/或程式編加密碼成一編密的電腦檔案及/或程式並傳遞。此系統包括一連接到伺服器裝置的一連接器，於其上編密的電腦檔案及/或程式傳播，且伺服器裝置對其傳遞編密的電腦檔案及/或程式。此系統包括一用戶裝置，其接收編密的電腦檔案及/或程式，並將編密的電腦檔案及/或程式解密回未編密的電腦檔案及/或程式。當在收到編密的電腦及/或檔案程式的時間當中，用戶裝置不允許對編密的電腦檔案及/或程式的干涉。伺服器裝置與用戶裝置獨立、分開和不同。一種用以操縱一電腦檔案及/或程式的方法。此方法包括中止用戶裝

英文發明摘要 (發明之名稱：A SYSTEM AND METHOD FOR MANIPULATING A COMPUTER FILE AND/OR PROGRAM)

A system for manipulating a computer file and/or program. The system includes a serving device having access to a computer file and/or program which is unencrypted and which can encrypt the unencrypted computer file and/or program to become an encrypted computer file and/or program and transfer it. The system includes a connector connected to the serving device on which the encrypted computer file and/or program travels and to which the serving device transfers the



四、中文發明摘要 (發明之名稱：用以操縱電腦檔案及/或程式之系統及方法)

置的一用戶裝置之使用者的干涉之步驟。然後是在伺服器裝置將一未編密的電腦檔案及/或程式編加密碼，以形成一編密的電腦檔案及/或程式的步驟。接著是將編密的電腦檔案及/或程式沿著一連接到用戶裝置和伺服器裝置的連接器，傳遞到用戶裝置的步驟。然後是由使用者重建用戶裝置的干涉之步驟。

英文發明摘要 (發明之名稱：A SYSTEM AND METHOD FOR MANIPULATING A COMPUTER FILE AND/OR PROGRAM)

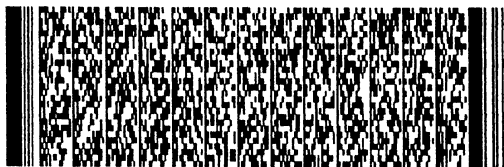
encrypted computer file and/or program. The system includes a client device which receives the encrypted computer file and/or program and decrypts the encrypted computer file and/or program back to the unencrypted computer file and/or program. The client device does not allow intervention to the encrypted computer file and/or program during a time when the encrypted computer and/or file program is received. The serving device is separate, apart and distinct from the



四、中文發明摘要 (發明之名稱：用以操縱電腦檔案及/或程式之系統及方法)

英文發明摘要 (發明之名稱：A SYSTEM AND METHOD FOR MANIPULATING A COMPUTER FILE AND/OR PROGRAM)

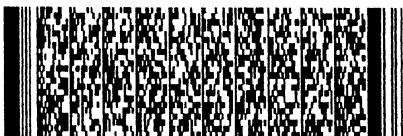
client device. A method for manipulating a computer file and/or program. The method includes the steps of suspending intervention by a user at a client device of the client device. Then there is the step of encrypting an unencrypted computer file and/or program at the server device to form an encrypted computer file and/or program. Next there is the step of transferring the encrypted computer file and/or program to the client device along a connector connected to the client device



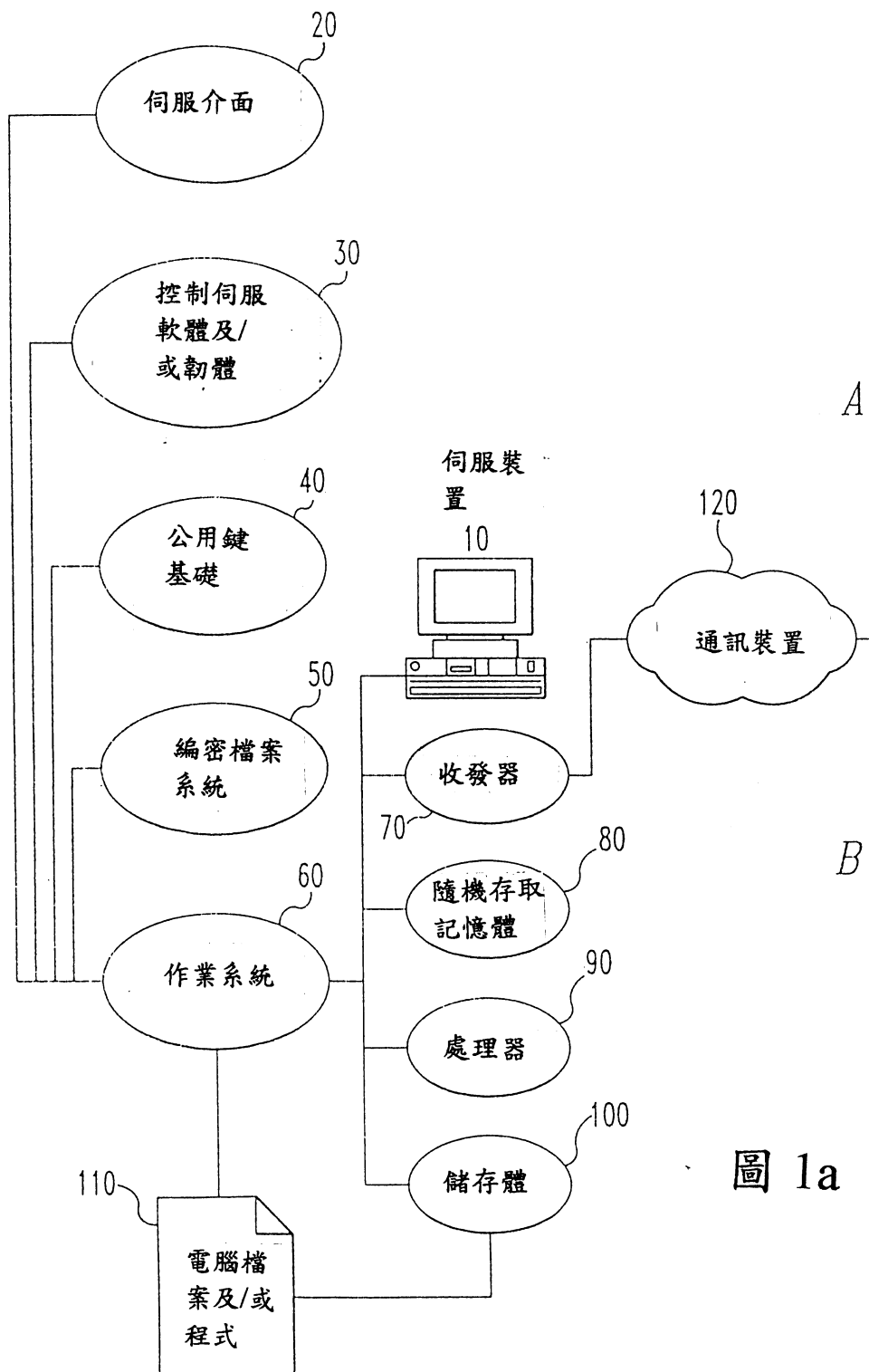
四、中文發明摘要 (發明之名稱：用以操縱電腦檔案及/或程式之系統及方法)

英文發明摘要 (發明之名稱：A SYSTEM AND METHOD FOR MANIPULATING A COMPUTER FILE AND/OR PROGRAM)

and the server device. Then there is the step of reestablishing the intervention of the client device by the user.



圖式



圖式

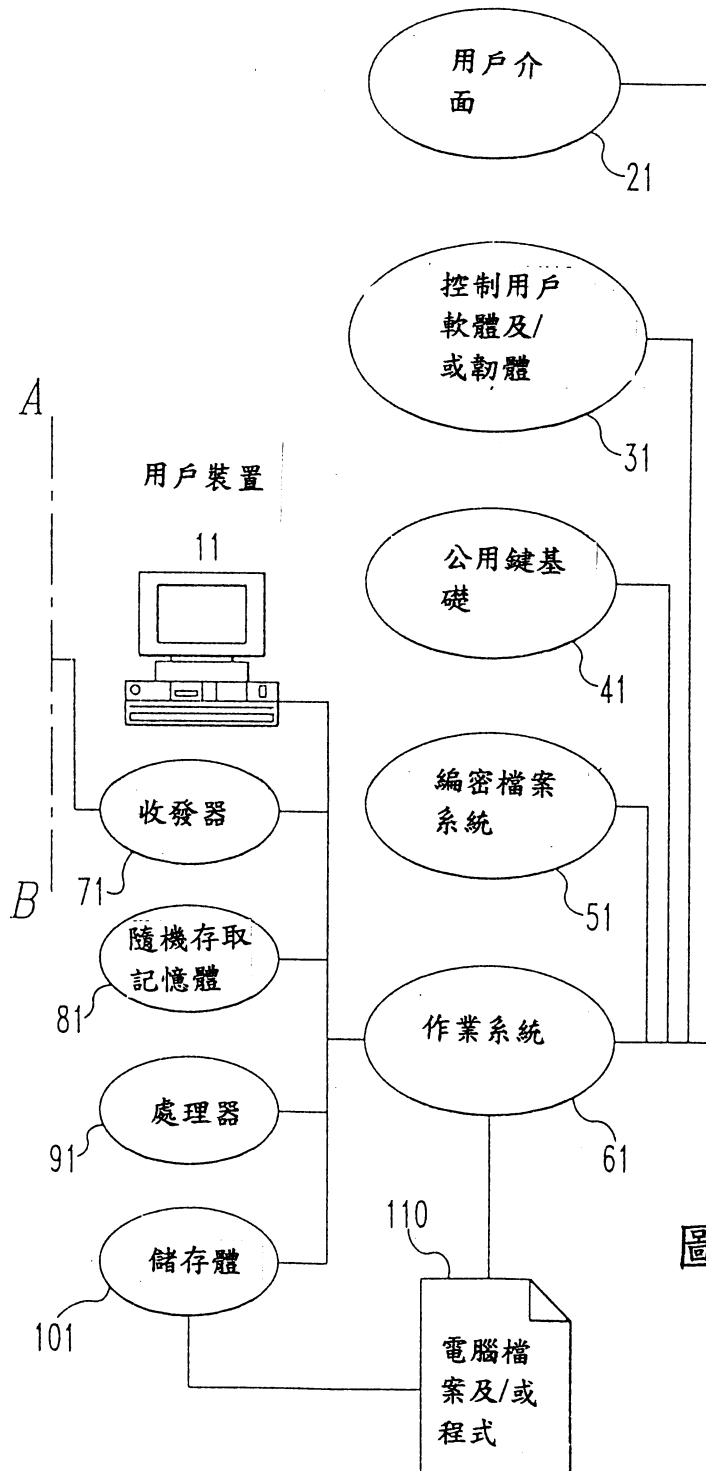
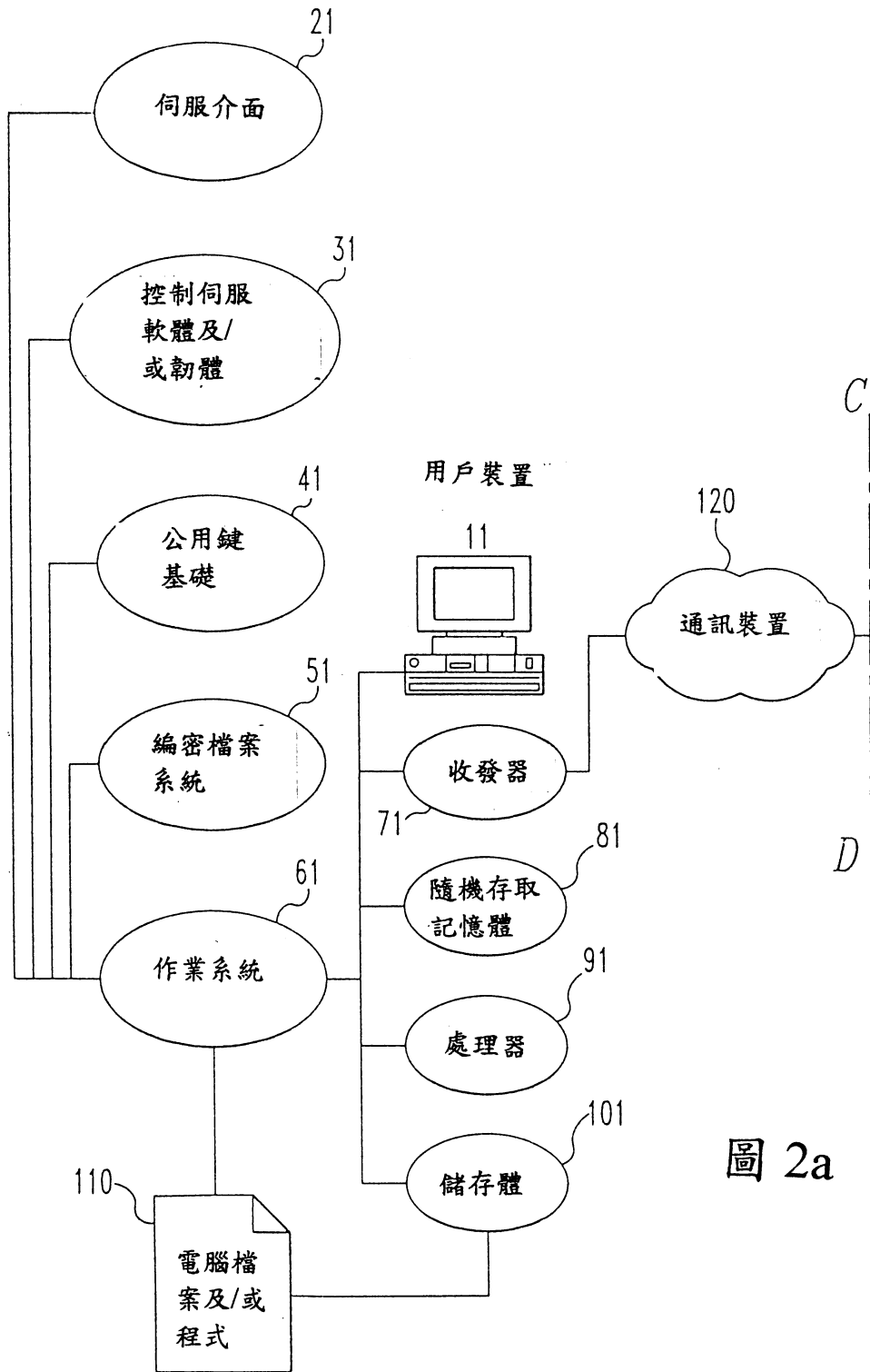
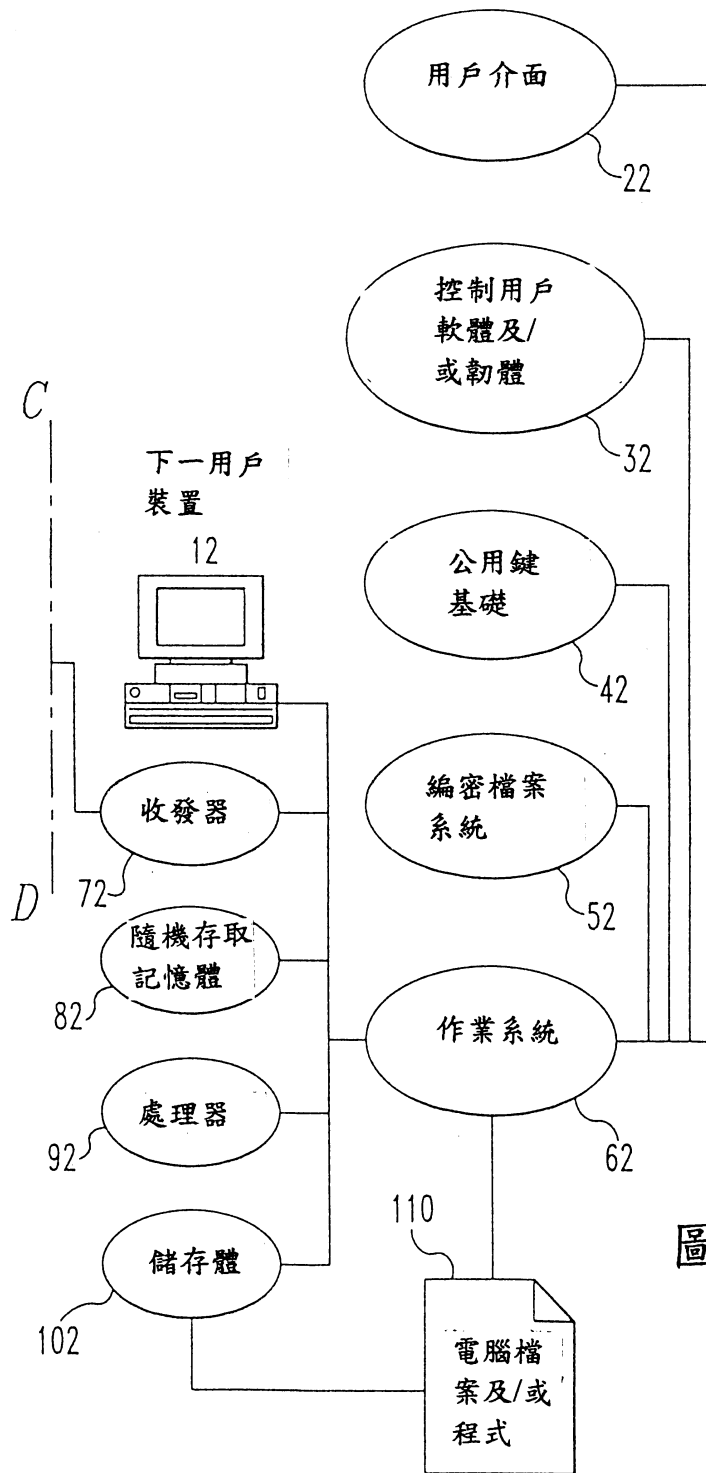


圖 1b

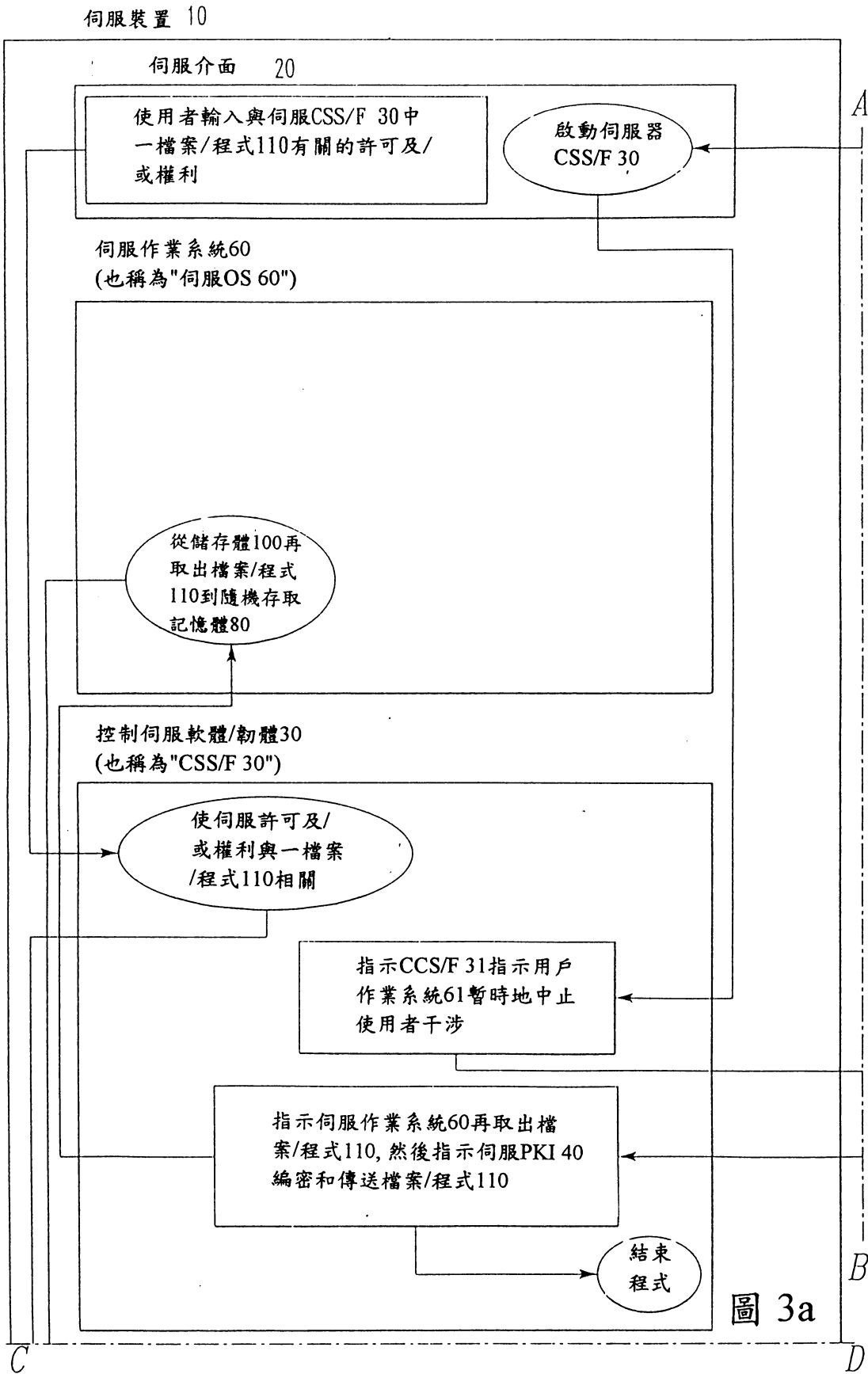
圖式



圖式



圖式



圖式

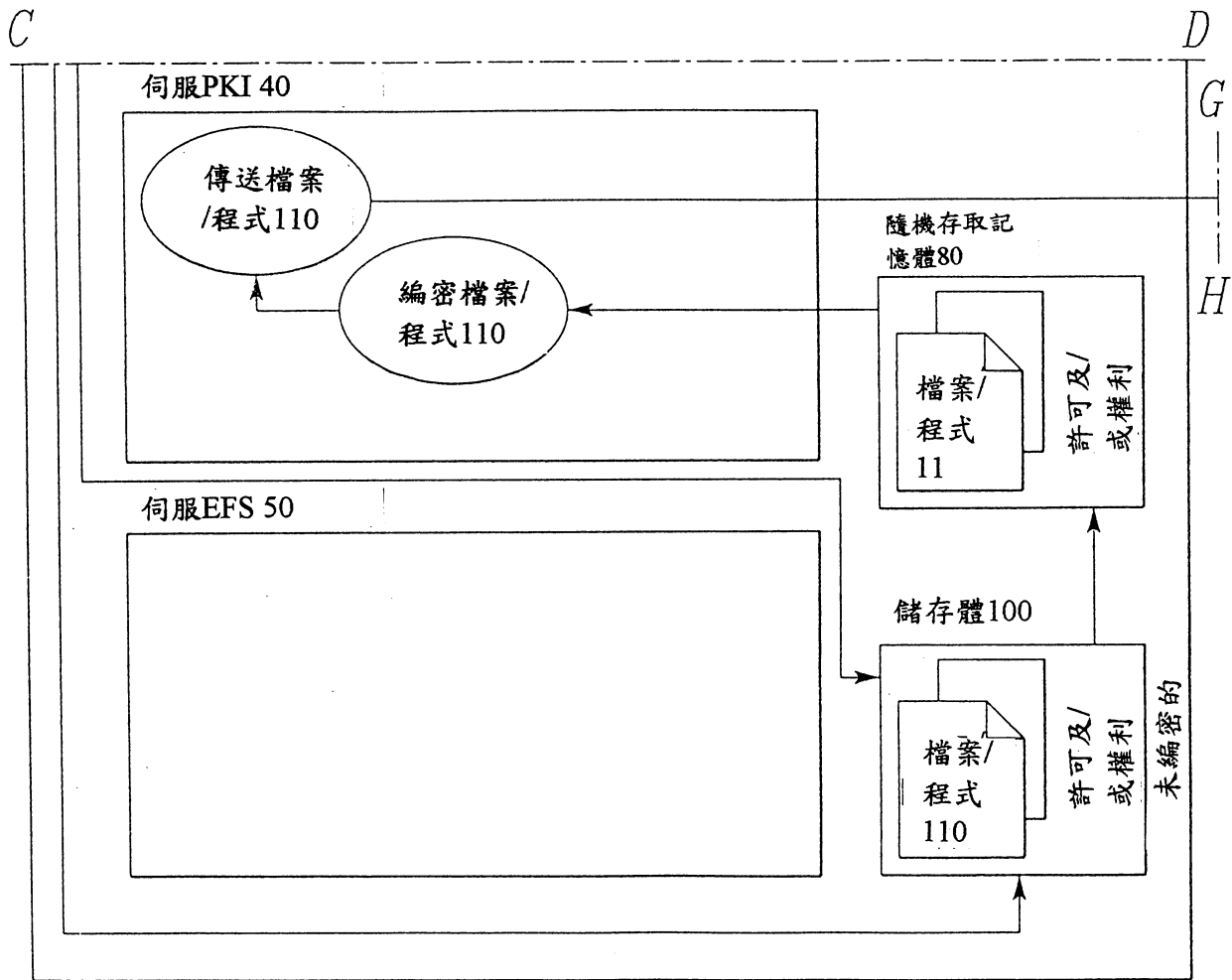
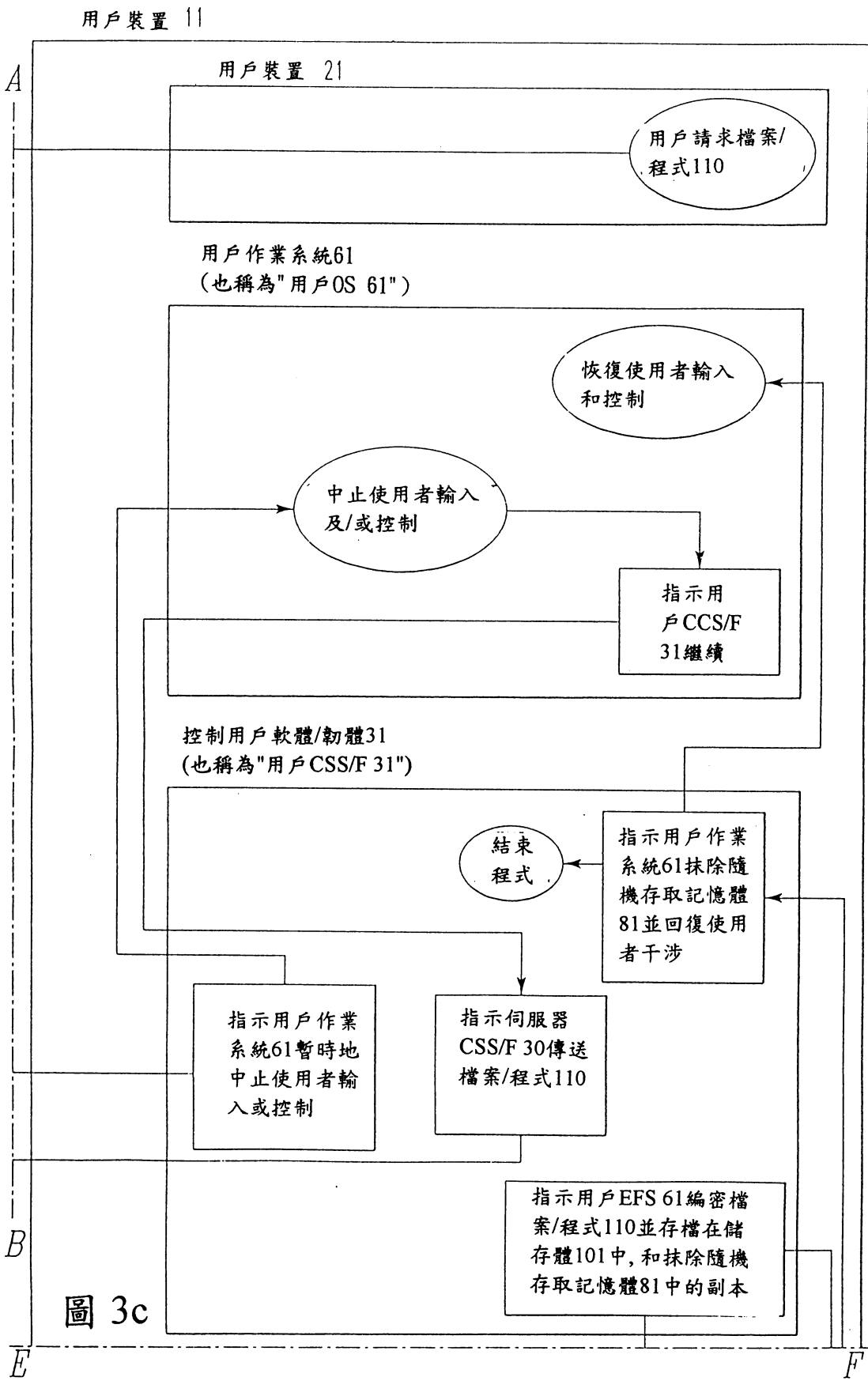


圖 3b

圖式



圖式

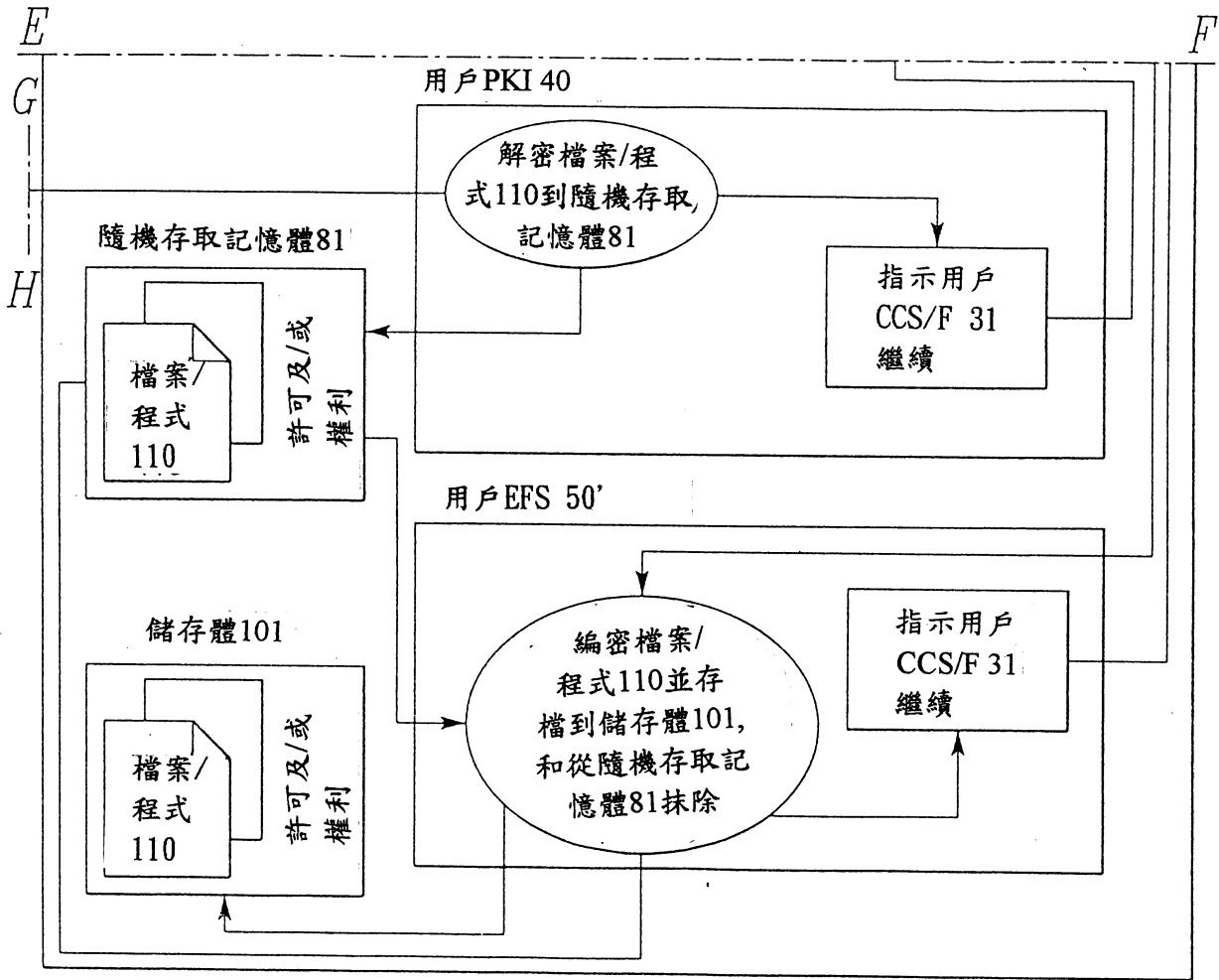
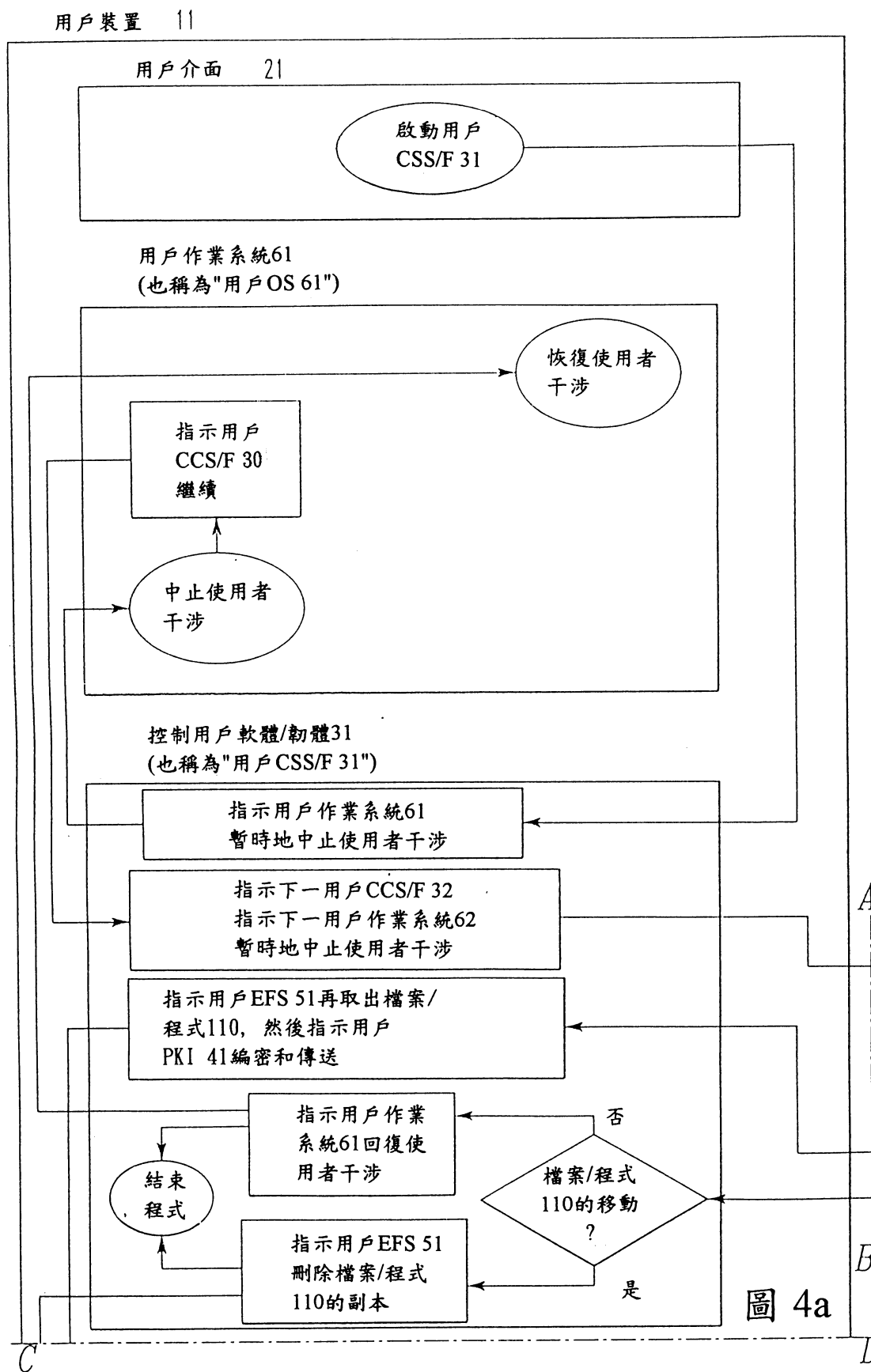


圖 3d

圖式



圖式

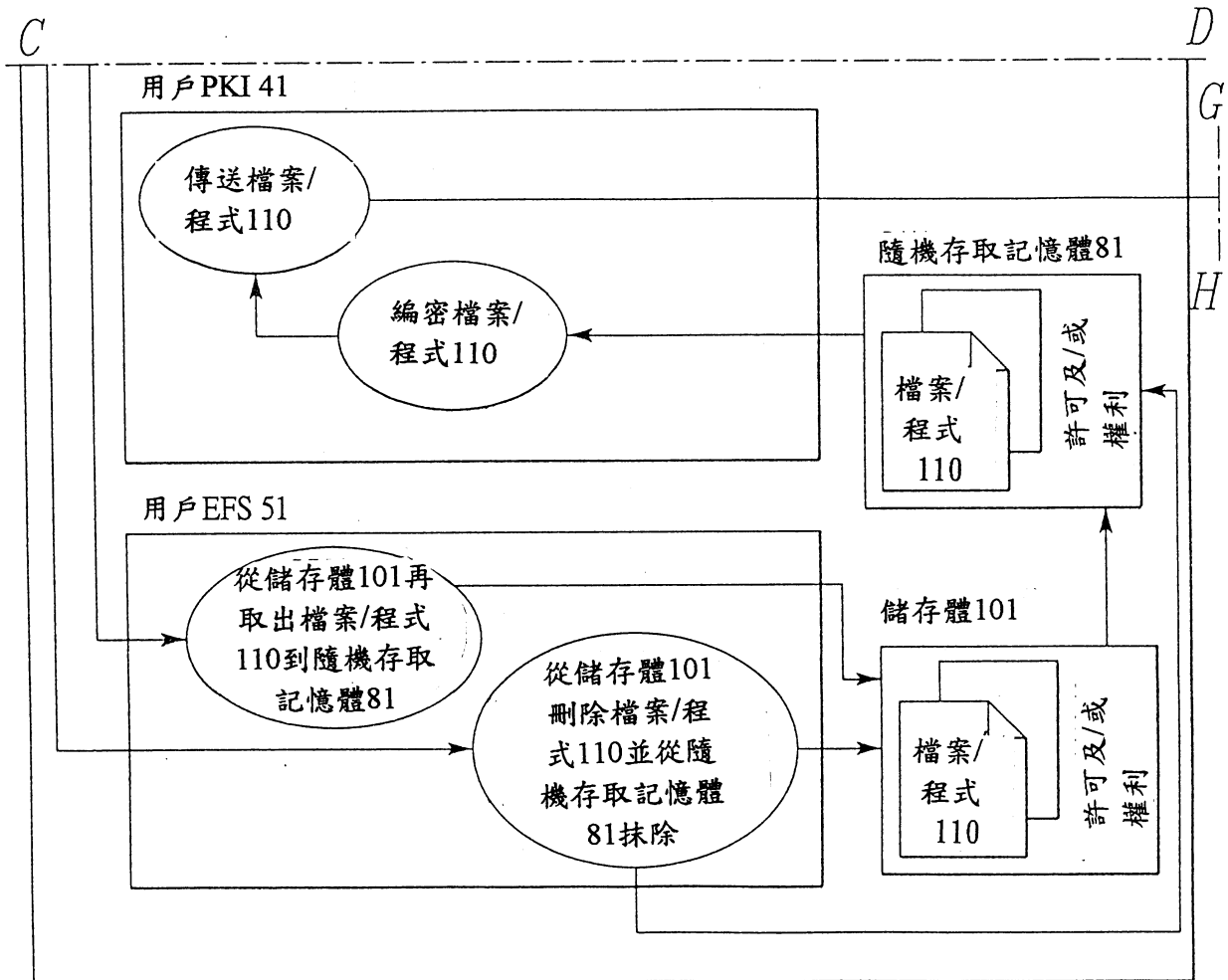
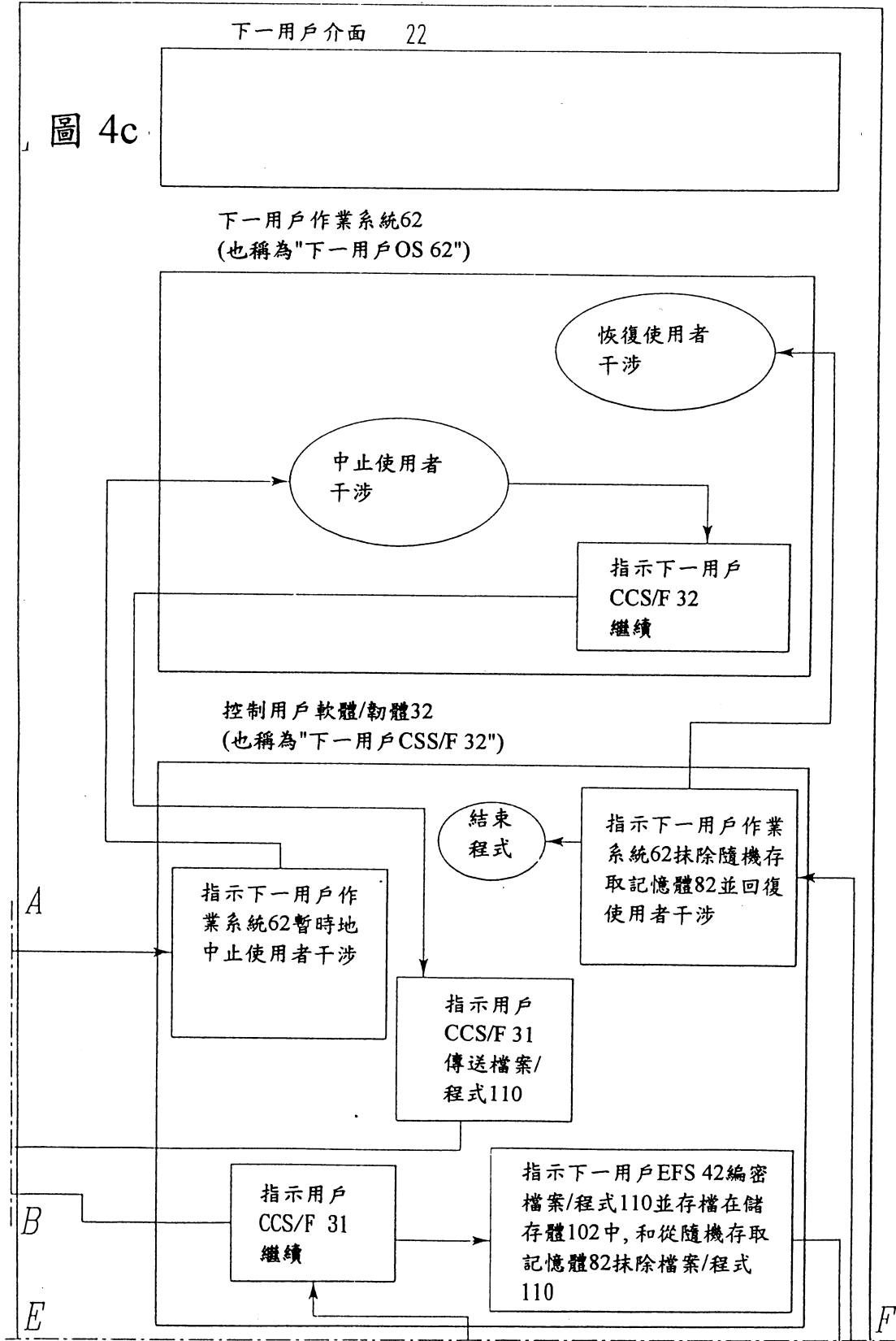


圖 4b

圖式

下一用戶裝置 12

圖 4c



圖式

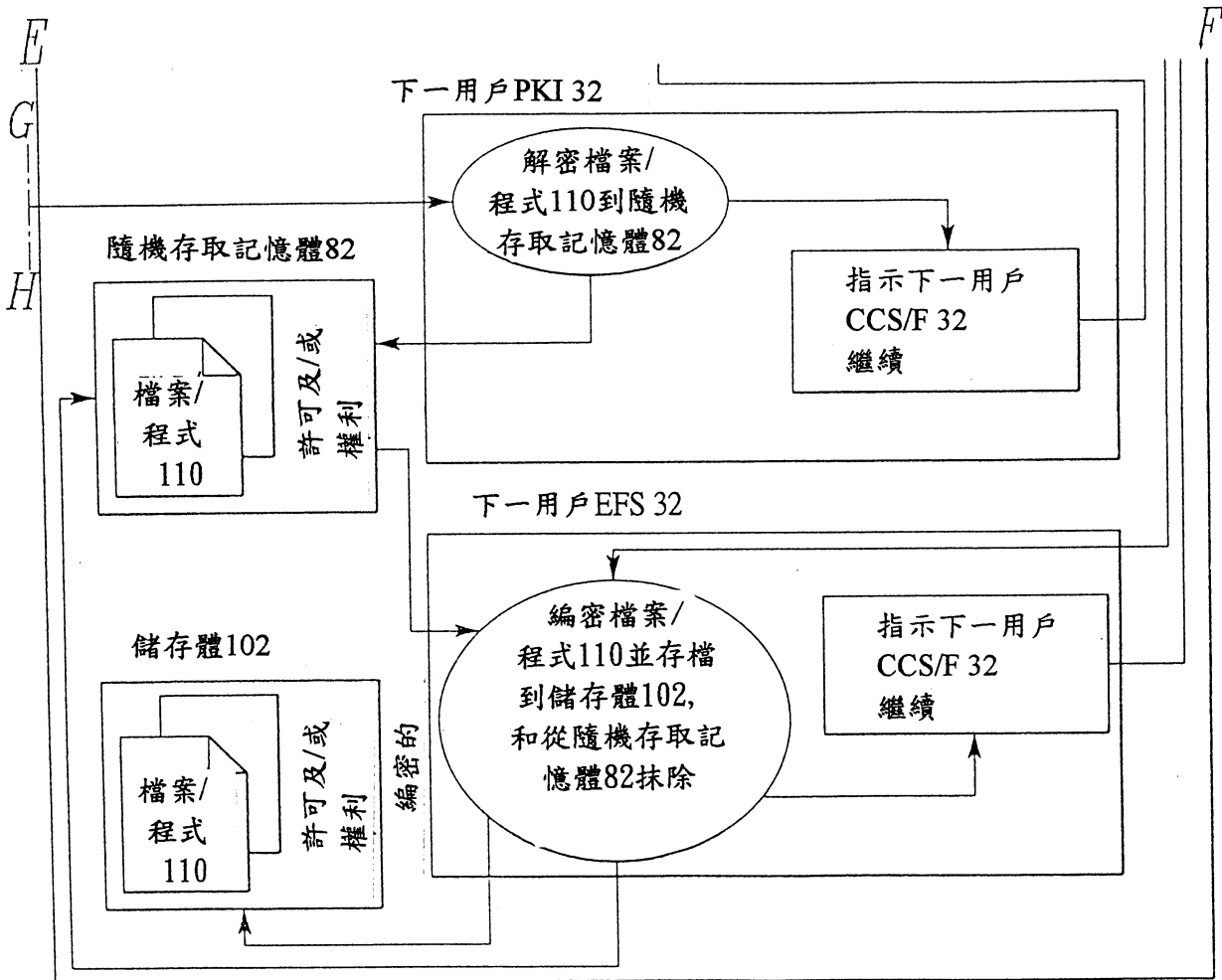


圖 4d

89年9月2日 修正
 89年9月2日 補正

9月2日

修正

申請日期：89.7.22

9103051

類別：G06F1/00

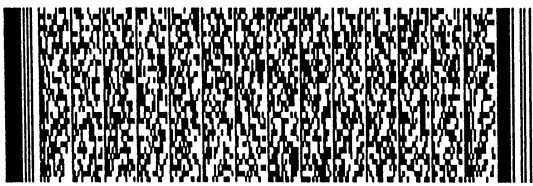
公告本

(以上各欄由本局填註)

發明專利說明書

574641

一、發明名稱	中文	用以操縱電腦檔案及/或程式之系統及方法
	英文	A SYSTEM AND METHOD FOR MANIPULATING A COMPUTER FILE AND/OR PROGRAM
二、發明人	姓名(中文)	1. 亞塞 R. 海爾
	姓名(英文)	1. ARTHUR R. HAIR
	國籍	1. 美國
	住、居所	1. 美國賓州聖克萊爾市亞利森路1518號
三、申請人	姓名(名稱)(中文)	1. 美商聲光聯合公司
	姓名(名稱)(英文)	1. SIGHTSOUND.COM INCORPORATED
	國籍	1. 美國
	住、居所(事務所)	1. 美國賓州利伯諾市400區華聖頓路733號
	代表人姓名(中文)	1. 亞塞 R. 海爾
	代表人姓名(英文)	1. ARTHUR R. HAIR

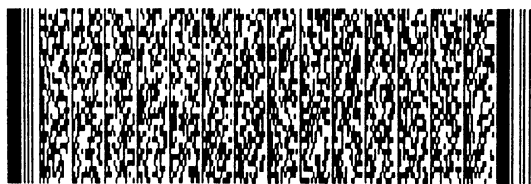


五、發明說明 (13)

圖4是一電腦程式流程圖，其可用在進行本發明的指導，以自動地啟動用戶裝置11的作業系統61之功能，來：從儲存體101解密一電腦檔案及/或程式110，並儲存其一份電子副本、及儲存相關的許可及/或權利，在隨機存取記憶體81中；和透過連接到通訊裝置120的收發器71之使用編密並傳送一電腦檔案及/或程式110及與其相關的許可及/或權利，到下一用戶裝置12；然後從隨機存取記憶體81抹去該電腦檔案及/或程式110的任何電子副本；和，然後在該電腦檔案及/或程式110從儲存體101移動到儲存體102的情況中，從儲存體101抹去該電腦檔案及/或程式110的任何電子副本。圖4是一電腦程式流程圖，其也可用在進行本發明的指導，以自動地啟動用戶裝置12的作業系統62之功能，來：透過連接到通訊裝置120的收發器72之使用，從來自用戶裝置11的傳輸，接收和解密一電腦檔案及/或程式110及其相關的許可及/或權利，並儲存其一份電子副本在隨機存取記憶體82中；使用該相關的許可及/或權利從隨機存取記憶體82將該電腦檔案及/或程式110編密並存檔到儲存體102，然後並從隨機存取記憶體82抹除該電腦檔案及/或程式110的任何電子副本。

發明詳述

現在參考圖式，其中同樣的參考號碼指示相似的或完全相同之零件的幾個視面，特別是對圖1和2，顯示了用來操縱一電腦檔案及/或程式的一種系統。此系統包含一伺服器裝置10，能夠存取一未編密的電腦檔案及/或程式，且其



五、發明說明 (15)

置11有一機制，用來由伺服器裝置要求未編密的電腦檔案及/或程式。

控制用戶軟體及/或韌體31最好引起未編密的電腦檔案及/或程式和許可及/或權利的編密以供儲存。最好，用戶裝置11有一作業系統，且控制用戶軟體及/或韌體31指示作業系統在需要的時間重建使用者干涉。伺服器裝置最好有一伺服器公用鍵基礎40，其使用編密的通訊協定來編密許可及/或權利和未編密的電腦檔案及/或程式。

最好，用戶裝置11有一用戶公用鍵基礎41，其使用編密的通訊協定從許可及/或權利和編密的電腦檔案及/或程式的傳輸中解密。用戶裝置11最好包括一編密檔案系統51，其編密未編密的電腦檔案及/或程式和許可及/或權利，並允許手動選擇未編密的電腦檔案及/或程式以供編密或解密。最好，用戶公用鍵基礎41有一編密及/或解密鍵，且此編密檔案系統51使用用戶公用鍵基礎41所利用的編密及/或解密鍵。

此系統最好包括一下一用戶裝置12，透過連接器連接到用戶裝置11。最好，控制用戶軟體及/或韌體31透過第二連接器移動或複製編密的電腦檔案及/或程式到下一用戶裝置12，該用戶裝置11有一控制下一用戶軟體及/或韌體，其解密所收到之編密的電腦檔案及/或程式和編密的許可及/或權利，並在下一用戶裝置12接收編密的電腦檔案及/或程式時，暫時地中止下一用戶裝置12的使用者干涉。最好，連接器包括一通訊鏈結，伺服器裝置包括一連接



六、申請專利範圍

1. 一種用以操縱一電腦檔案之系統，包含：

一伺服器裝置，能夠存取一未編密的電腦檔案，且其可編密未編密的電腦檔案成為一編密的電腦檔案，和傳遞它；

一連接器，連接到電腦檔案於其上傳播的伺服器裝置，和連接到伺服器裝置對其傳遞編密的電腦檔案者；和

一用戶裝置，其接收編密的電腦檔案，並解密編密的電腦檔案回到未編密的電腦檔案，該用戶裝置在編密的電腦檔案接收期間，不允許對編密的電腦檔案的干涉，該伺服器裝置與用戶裝置係獨立、分開和不同，且該用戶裝置係連接至該連接器。

2. 如申請專利範圍第1項之系統，其中該伺服器裝置指派許可或權利給未編密的電腦檔案，其識別在用戶裝置收到編密的電腦檔案之後、或用戶裝置解密了編密的電腦檔案回到未編密的電腦檔案之後，用戶裝置可如何處置未編密的或編密的電腦檔案。

3. 如申請專利範圍第2項之系統，其中該伺服器裝置編密許可或權利，並將它們透過連接器傳遞到用戶裝置，該用戶裝置解密未編密的許可或權利。

4. 如申請專利範圍第3項之系統，其中伺服器裝置包括控制伺服器軟體或韌體，其引起未編密的電腦檔案和許可或權利的編密，並指示用戶裝置在當用戶裝置接收編密的電腦檔案和編密的許可或權利時，暫時中止使用者干涉。

5. 如申請專利範圍第4項之系統，其中用戶裝置包括控制用戶軟體或韌體，其引起編密的電腦檔案的解密。



六、申請專利範圍

6. 如申請專利範圍第5項之系統，其中用戶裝置有一種機制，用來從伺服器裝置請求未編密的電腦檔案。

7. 如申請專利範圍第6項之系統，其中控制用戶軟體或韌體引起未編密的電腦檔案、和許可或權利的編密以供儲存。

8. 如申請專利範圍第7項之系統，其中用戶裝置有一作業系統，且控制器用戶軟體或韌體指示作業系統在一需要的時間重建使用者干涉。

9. 如申請專利範圍第8項之系統，其中伺服器裝置有一伺服器公用鍵基礎，其使用編密的通訊協定編密許可或權利和未編密的電腦檔案。

10. 如申請專利範圍第9項之系統，其中用戶裝置有一用戶公用鍵基礎，其使用編密的通訊協定從傳輸中解密許可或權利和編密的電腦檔案。

11. 如申請專利範圍第10項之系統，其中用戶裝置包括一編密檔案系統，其編密未編密的電腦檔案和許可或權利，並允許手動選擇未編密的電腦檔案供編密或解密。

12. 如申請專利範圍第11項之系統，其中用戶公用鍵基礎有一編密或解密鍵，且編密檔案系統使用用戶公用鍵基礎所利用的編密或解密鍵。

13. 如申請專利範圍第12項之系統，包括一用戶裝置，透過連接器連接到用戶裝置。

14. 如申請專利範圍第13項之系統，其中控制用戶軟體或韌體經由第二連接器移動或複製編密的電腦檔案到下一



六、申請專利範圍

用戶裝置，該用戶裝置具有控制下一用戶軟體或韌體，其解密所收到之編密的電腦檔案和編密的許可或權利，且在下一用戶裝置接收編密的電腦檔案時，暫時中止下一用戶裝置的使用者干涉。

15. 如申請專利範圍第14項之系統，其中連接器包括一通訊鏈結，伺服器裝置包括一連接到通訊鏈結的發射器，用來傳遞編密的電腦檔案和未編密的許可或權利到通訊鏈結，而用戶裝置包括一連接到通訊鏈結的接收器，其從通訊鏈結接收編密的電腦檔案和編密的許可或權利。

16. 如申請專利範圍第15項之系統，其中第一和第二連接器是網際網路或其他通訊網路的一部份。

17. 一種用以操縱一電腦檔案之方法，包含以下步驟：

在用戶裝置處中止用戶裝置的使用者之干涉；

在伺服器裝置處編密一未編密的電腦檔案，

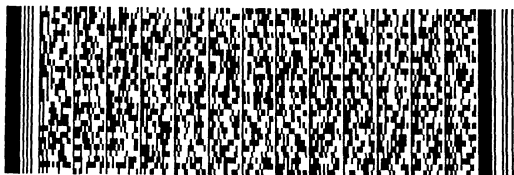
以形成一編密的電腦檔案；

沿著一連接到用戶裝置和伺服器裝置的連接器，傳遞編密的電腦檔案到用戶裝置；和

重建使用者對用戶裝置的干涉。

18. 如申請專利範圍第17項之方法，包括在傳遞步驟之前，有編密未編密的電腦檔案之許可或權利、和沿著連接器從伺服器裝置傳遞編密的許可或權利到用戶裝置的步驟。

19. 如申請專利範圍第18項之方法，包括在編密未編密的電腦檔案的步驟之前，有由用戶裝置請求伺服器裝置的



六、申請專利範圍

未編密的電腦檔案之步驟。

20. 如申請專利範圍第19項之方法，包括在請求步驟之後，有複製一主要的未編密的電腦檔案，以形成未編密的電腦檔案的步驟。

21. 如申請專利範圍第20項之方法，包括在重建步驟之前，有在用戶裝置解密編密的電腦檔案以回到未編密的電腦檔案的步驟。

22. 如申請專利範圍第21項之方法，包括在解密步驟之後，有在用戶裝置編密未編密的電腦檔案和許可或權利、和儲存編密的電腦檔案和編密的許可或權利在用戶裝置中的步驟。

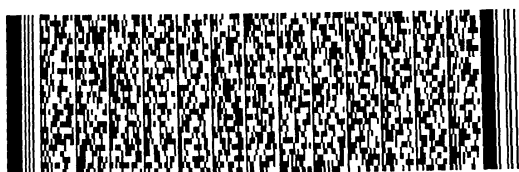
23. 如申請專利範圍第22項之方法，包括在儲存步驟之後，有傳遞編密的電腦檔案到由一第二連接器連接到用戶裝置的下一用戶裝置之步驟。

24. 一種用以操縱一電腦程式之系統，包含：

一伺服裝置，能夠存取一未編密的電腦程式，且其可編密未編密的電腦程式成為一編密的電腦程式，和傳遞它；

一連接器，連接到電腦程式於其上傳播的伺服裝置，和連接到伺服裝置對其傳遞編密的電腦程式者；和

一用戶裝置，其接收編密的電腦程式，並解密編密的電腦程式回到未編密的電腦程式，該用戶裝置在編密的電腦程式接收期間，不允許對編密的電腦程式的干涉，該伺服裝置與用戶裝置係獨立、分開和不同，且該用戶裝置係



六、申請專利範圍

連接至該連接器。

25. 如申請專利範圍第24項之系統，其中該伺服器裝置指派許可或權利給未編密的電腦程式，其識別在用戶裝置收到編密的電腦程式之後、或用戶裝置解密了編密的電腦程式回到未編密的電腦程式之後，用戶裝置可如何處置未編密的或編密的電腦程式。

26. 如申請專利範圍第25項之系統，其中該伺服器裝置編密許可或權利，並將它們透過連接器傳遞到用戶裝置，該用戶裝置解密未編密的許可或權利。

27. 如申請專利範圍第26項之系統，其中伺服裝置包括控制伺服器軟體或韌體，其引起未編密的電腦程式和許可或權利的編密，並指示用戶裝置在當用戶裝置接收編密的電腦程式和編密的許可或權利時，暫時中止使用者干涉。

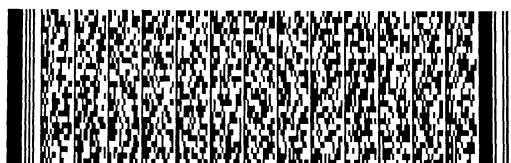
28. 如申請專利範圍第27項之系統，其中用戶裝置包括控制用戶軟體或韌體，其引起編密的電腦程式的解密。

29. 如申請專利範圍第28項之系統，其中用戶裝置有一種機制，用來從伺服器裝置請求未編密的電腦程式。

30. 如申請專利範圍第29項之系統，其中控制用戶軟體或韌體引起未編密的電腦程式、和許可或權利的編密以供儲存。

31. 如申請專利範圍第30項之系統，其中用戶裝置有一作業系統，且控制器用戶軟體或韌體指示作業系統在一需要的時間重建使用者干涉。

32. 如申請專利範圍第31項之系統，其中伺服器裝置有



六、申請專利範圍

一伺服器公用鍵基礎，其使用編密的通訊協定編密許可或權利和未編密的電腦程式。

33. 如申請專利範圍第32項之系統，其中用戶裝置有一用戶公用鍵基礎，其使用編密的通訊協定從傳輸中解密許可或權利和編密的電腦程式。

34. 如申請專利範圍第33項之系統，其中用戶裝置包括一編密檔案系統，其編密未編密的電腦程式和許可或權利，並允許手動選擇未編密的電腦程式供編密或解密。

35. 如申請專利範圍第34項之系統，其中用戶公用鍵基礎有一編密或解密鍵，且編密檔案系統使用用戶公用鍵基礎所利用的編密或解密鍵。

36. 如申請專利範圍第35項之系統，包括一用戶裝置，透過連接器連接到用戶裝置。

37. 如申請專利範圍第36項之系統，其中控制用戶軟體或韌體經由第二連接器移動或複製編密的電腦程式到下一用戶裝置，該用戶裝置具有控制下一用戶軟體或韌體，其解密所收到之編密的電腦程式和編密的許可或權利，且在下一用戶裝置接收編密的電腦程式時，暫時中止下一用戶裝置的使用者干涉。

38. 如申請專利範圍第37項之系統，其中連接器包括一通訊鏈結，伺服器裝置包括一連接到通訊鏈結的發射器，用來傳遞編密的電腦程式和未編密的許可或權利到通訊鏈結，而用戶裝置包括一連接到通訊鏈結的接收器，其從通訊鏈結接收編密的電腦程式和編密的許可或權利。



六、申請專利範圍

39. 如申請專利範圍第38項之系統，其中第一和第二連接器是網際網路或其他通訊網路的一部份。

40. 一種用以操縱一電腦程式的方法，包含以下步驟：

在用戶裝置處中止用戶裝置的使用者之干涉；

在伺服器裝置處編密一未編密的電腦程式，以形成一編密的電腦程式；

沿著一連接到用戶裝置和伺服器裝置的連接器，傳遞編密的電腦程式到用戶裝置；和

重建使用者對用戶裝置的干涉。

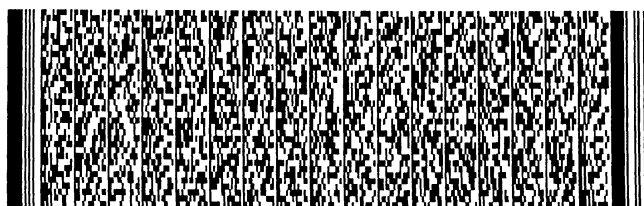
41. 如申請專利範圍第40項之方法，包括在傳遞步驟之前，有編密未編密的電腦程式之許可或權利、和沿著連接器從伺服器裝置傳遞編密的許可或權利到用戶裝置的步驟。

42. 如申請專利範圍第41項之方法，包括在編密未編密的電腦程式的步驟之前，有由用戶裝置請求伺服器裝置的未編密的電腦程式之步驟。

43. 如申請專利範圍第42項之方法，包括在請求步驟之後，有複製一主要的未編密的電腦程式，以形成未編密的電腦程式的步驟。

44. 如申請專利範圍第43項之方法，包括在重建步驟之前，有在用戶裝置解密編密的電腦程式以回到未編密的電腦程式的步驟。

45. 如申請專利範圍第44項之方法，包括在解密步驟之後，有在用戶裝置編密未編密的電腦程式和許可或權利、



六、申請專利範圍

和儲存編密的電腦程式和編密的許可或權利在用戶裝置中的步驟。

46. 如申請專利範圍第45項之方法，包括在儲存步驟之後，有傳遞編密的電腦程式到由一第二連接器連接到用戶裝置的下一用戶裝置之步驟。

