



申請日期	90 年 12 月 7 日
案 號	90130438
類 別	G06F 13/00

A4
C4

544579

(以上各欄由本局填註)

發 明 專 利 說 明 書		
一、發明 名稱	中 文	從非揮發性記憶卡、光碟或其它媒體播放音頻、視頻或其它內容之系統、方法及裝置
	英 文	System, method, and device for palying back recorded audio, video or other content form non-volatile memory cards, compact disks, or other media
二、發明人 創作	姓 名	(1) 伯曼·卡瓦米 Qawami, Bahman (2) 法希德·沙貝特-雪希 Sabet-Sharghi, Farshid (3) 張欽澤 Chang, Robert C.
	國 籍	(1) 美國 (2) 美國 (3) 美國
	住、居所	(1) 美國加州聖荷西奇勒尼圓環五八九九號 5899 Killarney Circle, San Jose, CA 95138, U.S.A. (2) 美國加州聖荷西斯諾敦廣場五六三四號 5634 Snowdon Place, San Jose, CA 95138, U.S.A. (3) 美國加州丹維斯坦頓廣場十號 10 Stanton Court, Danville, CA 94506, U.S.A.
三、申請人	姓 名 (名稱)	(1) 桑迪士克股份有限公司 SanDisk Corporation
	國 籍	(1) 美國
	住、居所 (事務所)	(1) 美國加州太陽谷喀斯匹安廣場一四〇號 140 Caspian Court, Sunnyvale, CA 94089, U.S.A.
	代 表 人 姓 名	(1) 查爾斯·凡·歐德 Orden, Charles Van

經濟部智慧財產局員工消費合作社印製

裝

訂

線

(由本局填寫)

承辦人代碼：
大類：
IPC分類：

A6
B6

本案已向：

國(地區) 申請專利，申請日期： 案號： ，☐有 ☐無主張優先權

美國 2000 年 12 月 7 日 60/251,731 ☒有主張優先權

有關微生物已寄存於： ，寄存日期： ，寄存號碼：

(請先閱讀背面之注意事項再填寫本頁各欄)

裝

訂

線

五、發明說明(1)

相互參考

本申請案係與主張優先權之2000年12月7日申請之美國臨時申請案序號60/251,731有關,該臨時申請案之案名為“SECURE SOFTWARE SYSTEM FOR PLAYING BACK RECORDED AUDIO, VIDEO OR OTHER CONTENT FROM NON-VOLATILE MEMORY CARDS, COMPACT DISK OR OTHER MEDIA”,並與美國申請案相關,其案名為“SYSTEM, METHOD, AND DEVICE FOR PLAYING BACK RECORDED AUDIO, VIDEO OR OTHER CONTENT FROM NON-VOLATILE MEMORY CARDS, COMPACT DISKS OR OTHER MEDIA”,美國代理人檔案號M-9913-1,其與本案同日申請並為相同發明人。這些申請案此處一併列入參考。

根據37 CFR 1.52以光碟片作為附件呈送之原始碼含有下述檔案,每一檔案於此一併列入參考:

Sd_security\Sd_oem\Makefile, 11/05/01, 2KB;
Sd_security\Sd_oem\Readme, 11/05/2001, 3KB; Sd_security\Sd_oem\Sd_oem.c,
11/05/2001, 6KB; Sd_security\Sd_oem\Sd_oem.h, 11/05/2001, 1KB;
Sd_security\Sd_oem\Sd_oem.inc, 11/05/2001, 1KB; Sd_security\Sd_oem\Sdtypes.h,
11/05/2001, 3KB; Sd_security\Sd_oem\vssver.scc, 11/05/2001, 1KB;
Sd_security\Security\Ttsampl\Dotest.c, 11/05/2001, 8KB;
Sd_security\Security\Ttsampl\Makefile, 11/05/2001, 4KB;
Sd_security\Security\Ttsampl\Readme, 11/05/2001, 3KB;

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

五、發明說明(2)

Sd_security\Security\Tstsampl\Regress.c, 11/05/2001, 26 KB;
 Sd_security\Security\Tstsampl\Sdls.c, 11/05/2001, 10KB;
 Sd_security\Security\Tstsampl\Sdrn.c, 11/05/2001, 5KB;
 Sd_security\Security\Tstsampl\Securmmc.c, 11/05/2001, 6KB;
 Sd_security\Security\Tstsampl\Tstsampl.inc, 11/05/2001, 1KB;
 Sd_security\Security\Tstsampl\vssver.scc, 11/05/2001, 1KB; Sd_security\Security\Err.h,
 11/05/2001, 1KB; Sd_security\Security\Fsentry.c, 11/05/2001, 7KB;
 Sd_security\Security\keyInfo.h, 11/05/2001, 84KB; Sd_security\Security\Makcfile,
 11/05/2001, 3KB; Sd_security\Security\Readme, 11/05/2001, 4KB;
 Sd_security\Security\Scdrv.c, 11/05/2001, 29 KB; Sd_security\Security\Scdrv.h, 11/05/2001, 5KB;
 Sd_security\Security\Scfs.c, 11/05/2001, 13KB;
 Sd_security\Security\Scfs.h, 11/05/2001, 4KB; Sd_security\Security\Sdsec.h, 11/05/2001,
 5KB; Sd_security\Security\Sdsys.c, 11/05/2001, 2KB; Sd_security\Security\Security.c,
 11/05/2001, 64KB; Sd_security\Security\Smanager.c, 11/05/2001, 7KB;
 Sd_security\Security\Smanager.h, 11/05/2001, 2KB; Sd_security\Security\Ssmapi.c,
 11/05/2001, 3KB; Sd_security\Security\vssver.scc, 11/05/2001,
 1KB; Sdaudlib\HostFunc.c, 11/05/2001, 3KB; Sdaudlib\Inpoutp.c, 11/05/2001, 1KB;
 Sdaudlib\msccprj.scc, 11/05/2001, 1KB; Sdaudlib\plmInfo.h, 11/05/2001, 16KB;
 Sdaudlib\Sd_plm.h, 11/05/2001, 5KB; Sdaudlib\Sd_tkm.h, 11/05/2001, 4KB;
 Sdaudlib\Sd_types.h, 11/05/2001, 2KB; Sdaudlib\Sdapi.h, 11/05/2001, 2KB;
 Sdaudlib\Sdaudapi.c, 11/05/2001, 91KB; Sdaudlib\Sdaudapi.h, 11/05/2001, 8KB;
 Sdaudlib\Sdaudlib.dsp, 11/05/2001, 4KB; Sdaudlib\Sdaudlib.dsw, 11/05/2001, 1KB;
 Sdaudlib\vssver.scc, 11/05/2001, 1KB.

發明背景

發明領域

發明大體上及特別地關於從記憶卡、光碟或其它媒體安全地播放數位音頻、視頻或其它內容。

相關技藝

五、發明說明(3)

網際網路上有著作權的音樂由其它通訊系統或經由零售攤位電子散佈的可能性會受未經授權的音樂重製限制。其它音頻以及視頻內容也有相同情形。內容典型上係以加密形式提供給最終的消費者，且消費者會將加密的內容歸檔於諸如個人電腦記憶體、可攜式播放裝置的記憶體、可寫式光碟(CD)或非揮發性記憶卡。內容供應者會要消除未經授權的內容重製之可能性但又必須採取令人滿意之步驟以使重製數量最少。這包含提供記錄媒體上的內容之保護。此處將說明特定實施例之儲存於非揮發性記憶卡上的內容之保護，但是，相同的內容保護技術可以應用至光碟或其它可記錄媒體。

有數種商業上可取得之適於作為內容資料儲存媒體之非揮發性記憶卡。一者為小巧型快閃(CF)卡，另一者為多媒體卡(MMC)，又有一者為安全(SD)記憶卡，其與MMC卡有緊密關係。所者這三者及其它者均可從加州Sunnyvale之SanDisk公司取得不同的儲存容量，該公司係本發明的受讓人。MMC之實體及電規格載於加州Cupertino的多媒體協會(MMCA)時常更新及出版之「多媒體卡系統規格(The MultiMediaCard System Specification)」。該規格書之2.11及2.2版，日期為1999年6月及2000年1月，於此一併列入參考。MMC產品也分別載於SanDisk公司2000年4月出版之「多媒體卡產品手冊(MultiMediaCard Product Manual)」版本2中，於此一併列入參考。MMC產品某些態樣之

五、發明說明(4)

電操作也說明於讓渡予 SanDisk 公司，Thomas N. Toombs 及 Micky Holtzman 於 1998 年 11 月 4 日申請之序號

09 / 185, 649 及 09 / 186, 064 之專利申請案中。實體的卡結構及其製造方法說明於讓渡給 SanDisk 公司之美國專利號 6,040,622 中。這些申請案及專利一併列入參考。

在平面視圖上，較新的 SD 卡類似於 MMC 卡。它們之間的主要差異在於 SD 卡包含增加的資料接點以便能夠在卡與主機之間更快速地傳送資料。SD 卡的其它接點與 MMC 卡的接點相同，以便設計用以接收 SD 卡之腳座也能接受 MMC 卡。與 SD 卡的電介面又製成爲大部份可以與上述的規格 2.11 版中所述的 MMC 產品背向並容，以便於主機操作要作一些改變以容納此二型的卡。SD 卡的電介面及其操作說明於 2000 年 8 月 17 日申請之專利申請序號 09 / 641, 023 中，此處將其一併列入參考。

發明概述

經過加密的內容難以接取，且具有加密內容之記憶卡或光碟均具有需要特定命令及常式以接取加密及未加密的內容之特定結構。本發明的軟體係一簡單的解決之道，任何原始設備製造商 (OEM) 可以安裝及在具有多種不同型式的微處理器之各種不同型式的裝置上執行。這些裝置從個人電腦至可攜式裝置至汽車音響，並包含任何人可從

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

五、發明說明(5)

其中接取可能加密的內容之任何裝置。可攜式裝置可為可攜式音響播放器或行動電話或可攜式電子記事本(Organizer)或任何微處理器控制的可攜式裝置。儲存媒體可為快閃記憶體或任何型式的可記錄碟片。裝置可具有簡單強力的微處理，帶小或大量記憶體。軟體僅利用及要求小量緩衝器以用於加密之用並設計成即使在具有有限的處理力及記憶體之環境中，仍能有效率地執行。其可由任何型式一般用途的微處理器、或諸如DSP或ASIC等特別用途之微處理器所執行。此外，在計算上需要諸如加密及解密(安全)引擎等部份軟體可由DSP執行，而其它部份軟體可由另一處理器或ASIC執行。

軟體具有音頻、視頻及影像介面以接收用於每一個別型式檔案之命令。這些介面可以組織播放及記錄，包含管理清單及其它便利特徵。因此，不管裝置為何，其僅需發出命令給介面且軟體會從安全媒體讀取及寫入資料，並在音頻、視頻或影像引擎內，以任何習知的音頻、視頻或影像檔案格式，解碼及解壓縮資料。

在難以接取及因而隔離任何未經授權的人員嘗試接取加密鑰以從媒體或裝置重製檔案之隔離的模組中，發生加密及解密。內容僅會小部份地被解密，且動態鑰產生及刪除之方法會使經過解密的鑰曝露之可能性最小。

圖式簡述

圖1係說明用以在安全媒體上讀取及寫入資料之裝置

五、發明說明(6)

。

圖 2 係用以接取安全媒體之裝置。

圖 3 A 係顯示安全媒體的複數個層。

圖 3 B 係顯示安全媒體的記憶胞之實體及邏輯構造。

圖 3 C 係顯示軌構造及軌的元件部份。

圖 4 係顯示分解成組成塊之媒體鑰區塊 (M K B) 影像。

圖 5 係顯示鑑定及解密處理之部份。

圖 6 係顯示鑑定及加密處理。

圖 7 係圖 6 中所示的鑑定鑰交換處理。

圖 8 A 係本發明的軟體之方塊圖。

圖 8 B 係方塊圖，顯示本發明之軟體的模組。

圖 8 C 係藉由所示之相關的 A P I 模組／呼叫，根據本發明之預先播放及播放處理的流程圖概要。

圖 8 D 係圖 8 C 中的音頻內容之初始化相位的解釋流程圖。

圖 8 E 係圖 8 C 的預先播放處理 8 0 5 期間產生的資訊塊。

圖 9 係根據本發明的音軌播放之流程圖概要。

圖 1 0 係圖 4 中所見的 M K B 影像處理之流程圖，圖 9 之步驟。

主要元件對照表

1 1 主電腦裝置

五、發明說明(7)

- 1 3 卡
- 1 5 可攜式裝置
- 1 7 串列匯流排連接
- 1 9 卡寫入器／讀取器
- 2 1 串列匯流排連接
- 2 3 系統匯流排
- 2 5 計算單元
- 2 5 A 非揮發性記憶體
- 2 7 系統記憶體
- 2 9 介面電路
- 3 1 數位訊號處理器
- 3 1 A 隨機存取記憶體
- 3 2 唯讀記憶體
- 3 9 裝置驅動器
- 1 0 5 音頻介面
- 1 1 0 視頻介面
- 1 1 5 影像介面
- 1 3 0 命令派送器
- 1 3 0 A 應用程式介面
- 1 4 0 安全數位音頻引擎
- 1 4 0 A 安全應用程式介面
- 1 4 0 B 非安全應用程式介面
- 1 5 0 安全數位視頻引擎
- 1 5 0 A 安全應用程式介面

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

五、發明說明 (8)

- 1 5 0 B 非安全應用程式介面
- 1 6 0 安全數位影像引擎
- 1 6 0 A 安全應用程式介面
- 1 6 0 B 非安全應用程式介面
- 1 7 0 非安全檔案介面
- 1 7 5 安全數位保全引擎
- 1 8 0 安全管理員
- 1 9 0 裝置驅動器
- 1 9 0 A 安全裝置驅動器介面
- 1 9 0 B 非安全裝置驅動器介面

發明詳述

加密的內容難以接取，且具有加密內容之記憶卡或光碟均具有要求特定命令及常式以接取加密資料及未加密內容之特定結構。本發明的軟體係簡單的解決之道，任何原始設備製造商（OEM）可以安裝及在具有多種不同型式的微處理器之各種不同型式的裝置上執行。這些裝置從個人電腦至可攜式裝置至汽車音響，並包含任何人可從其中接取可能加密的內容之任何裝置。可攜式裝置可為可攜式音響播放器或行動電話或可攜式電子記事本（Organizer）或任何微處理器控制的可攜式裝置。儲存媒體可為快閃記憶體或任何型式的可記錄碟片。裝置可具有簡單強力的微處理，帶小或大量記憶體。軟體僅利用及要求小量緩衝器以用於加密之用並設計成即使在具有有限的處理力及記憶

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

五、發明說明(9)

體之環境中，仍能有效率地執行。其可由任何型式一般用途的微處理器、或諸如DSP或ASIC等特別用途之微處理器所執行。此外，在計算上需要諸如加密及解密（安全）引擎等部份軟體可由DSP執行，而其它部份軟體可由另一處理器或ASIC執行。相互參考一節中提到的原始碼形成本案之一部份，並於此一併列入參考。

參考圖1，其說明舉例說明之系統，於其中對諸如音樂等音頻內容施加內容保護。主電腦裝置11可為所示之位於零售店中散佈音樂或其它內容的個人電腦（PC）、攤位、等等。在本實施例中，使用SD記憶卡13儲存音樂。卡13可插入公用裝置，在此情形中為可攜式裝置（PD）15，其能以電池操作以經由個人耳機播放記錄在卡13上的音樂或其它音頻內容。藉由諸如電腦通用串列匯流排（USB）連接17以將裝置15連接至主機11，當卡13插入裝置15中時，音樂可記錄於卡13上。或者，假使播放裝置15未具有記錄內容於卡13上之能力，或假使其為其它情形所需，則卡寫入器／讀取器19可以經由USB連接21連接至電腦，且卡13插入於其中以記錄音樂於卡上。接著，從寫入器／讀取器19移除卡13並將其入可攜式裝置15以播放記錄於卡上之音頻內容。當主機11包含根據4C實體及SD族的安全及鑑定協定對卡13讀寫資料所需之軟體時，主機11係稱為符合授權的模組（LCM）。

在可攜式公用裝置15的實施例中的電子系統顯示於

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

五、發明說明(10)

圖 2 中。較佳地具有某些非揮發性快閃記憶體 25 A 之計算單元 (MCU) 25、系統記憶體 27 (較佳地為高速隨機存取記憶體 (RAM))、及用於與記憶卡 13 連接之介面電路 29，在操作上經由匯流排 23 連接在一起。USB 連接 17 也可選加地提供給 MCU 25。於需要時也包含數位訊號處理器 (DSP) 31，以將諸如音頻或視頻資料等以壓縮及／或加密形式儲存之內容資料解壓縮及／或解密。DSP 31 也具有其自己的 RAM 記憶體 31 A 作為處理器的一部份。可包含或不包含 DSP 31。此外，假使包含 DSP 處理器，則其可執行 MCU 25 的功能，且因而可免除 MCU 25。唯讀記憶體 (ROM) 32 儲存發明的所有或部份軟體。ROM 32 中的軟體指令及資料會直接從 ROM 32 中被執行或讀取，或是首先隱藏於被包含於裝置電路中的 RAM 記憶體中。

Intel、IBM、Matsushita Electric Industrial Co., Ltd. 及 Toshiba 聯合建立可記錄媒體上的內容保護規格 (4 C 實體)。與此處特別相關的是下述二個 4 C 實體公告，它們一併列入參考：Content Protection for Recordable Media Specification, Introduction and Common Cryptographic Elements” 校正版 0.94, 2000 年 10 月，“Content Protection for Recordable Media Specification, SD Memory Card Book,” 修正版 0.95, 2001 年 5 月，及 “C2 Block Cipher Specification,” 修正版 0.9, 2000 年 1 月，以及 “Content

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

五、發明說明 (11)

Protection for Recordable Media Specification, DVD Book, " 修正版 0.95, 2001 年 5 月。Matsushita Electric Industrial Co., Ltd. (MEI)、SanDisk 公司及 Toshiba 公司建立在 S D 記憶卡上實施這些 4 C 實體規格之其它細部規格 (S D 族) 。

參考圖 3 A , 記憶卡 3 被視為具有四個不同層。這些層也出現於其它型式之安全媒體中。

在其最基本的一級中, 資料記錄於以簇集配置於記憶卡 1 3 的實體層 1 3 d 上之記憶胞中。資料假使為有版權的材料或其它值得加密者, 則會被加密或安全化。用以將安全內容加密及解密之鑰也會被加密及儲存於實體層的安全區中。

本發明的軟體在裝置內執行, 允許裝置儲存及取還加密資訊, 製造商 (O E M) 無須程式化特定的指令以接取含有加密資料及鑰之記憶胞。其含有傳送加密資料至裝置之方法、在裝置內將資料解密之方法、及應裝置請求以解壓縮和播放音頻、視頻及影像檔案之方法。簡而言之, 裝置僅需要傳送諸如「播放軌」等命令。軟體將接收命令, 取還儲存於記憶胞中的加密資料, 取還加密鑰、組織及解密資料、將其解壓縮及格式化, 並播放歌曲。

邏輯層 1 3 c 含有用於實體層 1 3 d 的記憶胞及簇之組織結構。二層 1 3 c 及 1 3 d 含有及邏輯地結構化卡

1 3 的記憶體。當卡 1 3 為安全卡時, 安全層 1 3 b 會控制及限制容納於下方的層中之安全資料之接取。

五、發明說明(12)

應用層 1 3 a 係記憶卡 1 3 與接取儲存在卡中的內容之裝置通訊的部份。其經由裝置介面或接點 3 9 以達成此功能。記憶卡 1 3 較佳地包含控制器，控制器與卡的所有層 1 3 a - d 之控制一起管理應用層 1 3 的卡及功能之操作。

根據上述說明書及對應於圖 3 A 之層 1 3 c 及 1 3 d，記錄媒體的實體及邏輯結構顯示於圖 3 B 中。卡包含記憶胞陣列 3 3 及記憶體控制器 3 5。使用者資料、命令及狀態訊號會於電路 3 7 上，在控制器 3 5 與記憶陣列 3 3 之間通訊。控制器 3 5 會與連接至腳座的主裝置通訊，卡係經由卡上的序列電接點 3 9 而插入於插座中。

陣列 3 3 的記憶胞分成四個非重疊的胞區，它們個別地用以儲存不同型式的資料。在此情形中，最大的儲存容量區 4 1 係設計成儲存使用者資料、加密的音頻、視頻或其它資料。使用者資料可以包含也可以不用包含未經加密的資料。記憶體的系統區 4 3 儲存卡製造商的 6 4 位元媒體識別標記 (Idmedia)、4 C 實體提供的 1 6 媒體鑰區 (M K B)，每一 M K B 具有 4 k 位元組的最大尺寸，所有這些資料均由卡製造商預先記錄。1 6 M K B 之一被指定為用於音頻使用者資料，另一者用於視頻使用者資料，又另一者用於影像資料、等等。系統區 4 3 係防寫區，可從卡的外部讀取。隱藏區 4 5 載有對應於儲存在系統區 4 3 中的 1 6 個不同的媒體鑰區 (M K B) 之 1 6 個預先記錄的媒體獨特鑰 (K m u)。隱藏區 4 5 係僅能由記憶

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

五、發明說明 (13)

卡本身接取之保護區。保護區 4 7 係僅在成功的明確相互鑑定發生之後才可接取之讀／寫區。被隨機拾訊之標題鑰 (K t) 及重製控制資訊 (C C I) 以加密形式儲存於保護區 4 7 中。儲存於使用者資料區 4 1 中之每一件 (檔案) 內容會以獨特的標題鑰加密，標題鑰亦以加密形式儲存於保護區 4 7 中。儲存在保護區 4 7 中的標題鑰及 C C I 會由媒體獨有的鑰一起連鎖及加密，媒體獨有的鑰對於每一記憶卡及而言是特有的並儲存於其隱藏區 4 5 中。

使用者資料區 4 1 A 的檔案系統典型上為一般 F A T 檔案系統。F A T 系統說明記那些憶簇構成那些軌及軌的不同副組成。使用者資料區 4 1 內的音頻或視頻軌道包括如圖 3 C 所示的多個檔案。音頻檔案稱為音頻物件 (A O B)，而圖像檔案稱為圖像物件 (P O B)。軌可包括二者。舉例而言，軌 3 0 0 由 A O B 3 0 4 及 A O B 3 0 8 構成，而軌 3 0 4 由 A O B 3 0 6 構成，而最後軌 x x x 係由 A O B x x x 及 P O B x x x 構成。每一 A O B 或 P O B 也會向下分成副組成。A O B 3 0 4 顯示成向下分成 A O B 區 3 1 2，它們係分成具有表面 3 1 8 之 A O B 元件 3 1 6。每一元件可儲存於記憶卡 1 3 的一或更多記憶體簇中。A O B 元件分成最低元件層，A O B 框 3 2 0。取決於內容的編碼及壓縮，每二秒可能包括不同數目的框。時間搜尋表 (TMSRT) 具有關於框數目的資訊及對應於「每二秒」播放之資料大小。當音頻或視頻軌及組成 A O B 的元件和框被接取以便快速正轉及

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

五、發明說明 (14)

倒轉時，使用此資訊。而且，如同稍後參考圖 9 及 10 之說明所述般，雖然從小於一至十秒的內容會被一次解密，但是，標題鑰 (K 1) 僅在用於接取此「每二秒」的內容時才為解密狀態。詳細內容，請參考前述併入參考之

C P R M 規格、S D 記憶卡手冊。

當儲存於卡記憶體的系統區 4 3 中時，媒體鑰區 (M K B) 包含相鄰記錄序列，一此種記錄顯示於圖 4 中。整個 M K B 影像 4 9 係 6 4 K 位元組。其會分成 1 2 8 塊，每塊 5 1 2 位元組，含有所有或部份第一記錄並於圖中以 M K B 塊 5 0 標示之塊 1 會被放大以顯示其組成部份。塊 5 0 也包含多重記錄。第一欄 5 1 含有記錄型式，第二欄 5 3 含有總記錄長度，其餘欄 5 5 含有鍵本身。記錄型式及長度欄 5 1 和 5 3 中的資料未被加密。M K B 的每一記錄總長度係 4 位元組的倍數。如同圖 5 的區 5 7 所示，M K B 鍵記錄會由使用記憶卡以讀取或程式化儲存在卡上的內容資料之可攜式裝置 (P D)、符合授權模組 (L C M) 或其它裝置中儲存的裝置鑰解密。裝置鑰 K d 1、K d 2、K d 3、… 會由裝置製造商寫入至公用裝置的記憶體中，舉例而言，公用裝置的記憶體如圖 2 的可攜式音頻播放器之 M C U 2 5 內的非揮發性快閃記憶體。裝置鑰會被提供給 4 C 實體之裝置製造商，並維持保密。儲存於給定的公用裝置中之裝置鑰的數目取決於裝置的型式。

執行圖 5 的處理之公用裝置 (P D、L C M 或其它裝

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

五、發明說明(15)

置)會計算媒體鑰 K_m 作為區57解密的部份,將參考圖9及10,進一步說明。通常以此方式處理從插入的記憶卡之系統區讀取之 MKB 的每一記錄(圖4),最近算出的 K_m 值會被當作區57的秘密媒體鑰輸出。如圖5之區59所示,此媒體鑰 K_m 及媒體標記 $Idmedia$ 係藉由使用C2單向功能以合併,而產生媒體獨特鑰 K_{mu} 。此處理的其它細節可參考先前列入參考之4C實體文獻。

圖6係顯示當記錄音頻內容至圖3之具有記憶空間分配的記憶卡13或從其中播放音頻內容時,所發生的所有鑑定及加密處理。發生於個人電腦或其它LCM63中的處理顯示為用於記錄音頻或其它內容至卡13。同樣地,可攜式音頻或其它公用裝置65之處理顯示為用於從卡13讀取記錄的內容。包含於二者中的係參考圖5說明之處理,處理區57及59係公用裝置65的部份,而對應的處理區57'及59'係內容記錄系統63之部份。

關於記錄內容之一部份,任意指定的標題鑰 K_1 會於加密模組69所使用的線67輸入以將線71處的音頻或其它內容輸入之一檔案(件)加密。經過加密的檔案接著儲存於記憶卡13的使用者資料區41中。為了使鑰可用於解密記錄的內容,如前所述,標題鑰(K_t)的加密版會被儲存於受保護的卡記憶體區47。標題鑰(K_t)的加密版本也會儲存於系統記憶體27、MCU25之RAM記憶體25A,或是DSP31的RAM記憶體31A。將經過加密的標題鑰(K_t)儲存於裝置的記憶

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

五、發明說明 (16)

體中可免除接取受保護的卡記憶體區 4 7。由於這種功能相對於每一次讀取要接取保護區 4 7，可以節省可觀的時間及處理容力，所以，其是很重要的。稍後將參考圖 9 以說明此點。標題鑰 K t 及重製控制資訊 C C I 會由 L C M 模組 6 3 中一序列加密模組 7 5、7 7 及 7 9、以及記憶卡 6 1 上的模組 8 1 加密。媒體獨有鑰 K m u 會由模組 7 7 使用。鑑定鑰交換 (A K E) 模組 8 3 會結合模組 5 9' 算出及儲存於卡 6 1 的隱藏區 4 5 中之媒體獨有鑰 K m u，以產生由模組 7 9 及 8 1 使用的任務鑰 K s。為了使公用裝置 6 5 將記錄之加密內容解密，由相同代號但加上分號 (') 所標示之對應模組係用於執行加密處理的反處理。

圖 7 係顯示用於接取記憶卡的保護區 4 7 之技術，其利用卡與某些 L C M 或公用裝置之間的鑑定及鑰交換 (A K E) 挑戰－回應協定。當此鑑定成功時，卡及其它模組或裝置會共用安全共同任務鑰 K s。上述處理及協定的其它細節可參考先前列入參考之 4 C 實體文獻。

圖 8 A 及 8 B 顯示用以在可攜式裝置或 L C M 中執行以便以上述處理接取經過加密的資訊之軟體系統實施例。SanDisk 軟體，S W 1 0 0 係完全一啓動即用的軟體，使得 O E M 音樂播放器及記錄器能夠輕易地支援包含安全數位 (S D) 記憶卡之安全媒體。S W 1 0 0 顯示於可攜式裝置 1 5 之內以便接取 S D 卡 1 3。S W 1 0 0 也可安裝於諸如個人電腦等任何符合授權的模組中。如圖 8 A 所示

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

五、發明說明 (17)

，在其最高層，S W 1 0 0 會接收來自裝置 1 5（特別是裝置的使用者介面 1 5）之呼叫，從安全數位卡 1 3 取還加密內容，及將解密的內容歸還給裝置。如此，僅需要簡單的呼叫，即可執行很多複雜的處理。取還儲存於卡

1 3 的記憶區中之加密資料、及接著將內容解密及格式化的複雜處理係由 S W 1 0 0 處理。

執行 S D 記憶卡的鑑定區之接取會要求使用如上所述之 O E M 必須從 4 C 實體授權之安全裝置鑰。保護這些鑰值及限制它們在 S D K S W 內的曝露係軟體設計的中心考量之一。以堅固及安全的介面方法，在單一內部模組內隔離這些鑰（及諸如任務鑰等其它所造成的值）並使得諸如 S D 記憶卡裝置驅動器等安全媒體能夠取決於這些值而執行操作。再度使用 S D 記憶卡以說明發明；但是，發明可以用於諸如 C D 或卡中、甚至是遠方儲存裝置中的其它安全記憶體上。

圖 8 B 係更詳細地顯示 S W 1 0 0 之層結構。音頻介面 1 0 5、視頻介面 1 1 0、及影像介面 1 1 5 係通訊至裝置的點。這些裝置提供單點通訊給裝置並通常從裝置接收簡單命令，以致於裝置不須涉入從安全媒體取得加密資料、接著解密及處理資料之交介功能。所有這些複雜的處理係由 S W 1 0 0 處理。介面 1 0 5、1 1 0、及 1 1 5 也會管理播放支配，舉例而言，管理播放清單及諸如歌曲之藝術家和不同的播放清單等影像相關性。應用程式介面（A P I）1 3 0 A 位於命令派送器（C D）

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

五、發明說明 (18)

1 3 0 內。C D 1 3 0 及 A P I 1 3 0 A 會從介面 1 0 5、1 1 0、及 1 1 5 接收命令，將資訊轉送至介面，及以所有必要的加密、解密、及壓縮演繹法，將發生於 S W 1 0 0 中的所有處理組織化，所有處理係指與儲存於安全媒體上的內容之播放及記錄有關的裝置 1 5 之處理。

在收到來自 C D 1 3 0 的指令時，S D 音頻引擎 (S D A E) 1 4 0、S D 視頻引擎 (S D V E) 1 5 0、及 S D 影像引擎 (S D I E) 1 6 0 分別地處理位於安全媒體上音頻、視頻、及影像內容。此意指 S D A E 1 4 0 可以處理用於影像夾之任何習知的格式，舉例而言，視窗 (Windows) 媒體檔案或真實網路檔案 M P E G 或任何其它習知型式的視頻檔案。最後，S D I E 1 6 0 可以處理諸如 T I F、G I F、J P E G、位元映射 (bitmap)、等任何習知型式的影像檔案。處理的內容會被加密或不被加密。經由 S A P I 1 4 0 A、1 5 0 A、及 1 6 0 A 接取被加密之內容。這些 S A P I 會與 SanDisk 安全管理員 (S S M) 1 8 0 通訊。所有必須處理安全內容之命令會通過 S S M 1 8 0。稍後更詳細說明之安全數位保全引擎 (S D S E) 1 7 5 處理所有加密及解密處理。用以鑑定媒體及將內容解密之鑰會包含於 S D S E 1 7 5 內並由其獨占地處理。經由 N S A P I 1 4 0 B、1 5 0 B、及 1 6 0 B，接取位於卡上之未經加密的內容。這些 N S A P I 會與非安全檔案介面 (N S F I) 1 7 0 通訊

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

五、發明說明 (19)

以便接取媒體上未經加密的內容。

爲了讀取或寫入資料於儲存媒體中，NSFI 170及SDSE 175會與裝置驅動器190通訊。在SD卡的實施例中之裝置驅動器190會管理及驅動往來於SD卡13的裝置介面39的接點之訊號。裝置驅動器190將修改成不同裝置或媒體的特定型式之裝置介面39。在記憶卡裝置的情形中，驅動器190會管理及驅動往來於裝置15上的接點之訊號。在光媒體的情形中，裝置驅動器190會管理及驅動往來於包含光學拾訊單元等不同硬體元件之訊號。或者，在硬碟機(hdd)的情形中，裝置驅動器190將管理及驅動所需的hdd訊號。裝置驅動器190含有安全裝置驅動器介面(SDDI)190A，及非安全裝置驅動器介面(NSDDI)190B。SDDI 190A及NSDDI 190B在裝置驅動器190之內彼此隔離。SDDI 190A會與SDSE 175獨占地通訊，而NSDDI 190B會與NSFI 170獨占地通訊。

SD－音頻安全設計的中心之裝置鑰及其它值係容納於一限定的安全軟體模組SD安全引擎(SDSE)175內。這些值的所有操作僅限定於此模組。值絕不會進出SDSE 175以上的軟體層。所有用於關於這些鑰的安全服務之請求會由屏蔽此安全模組之SSM 180控制及監視。在安全模組之下，SD記憶卡裝置驅動器190會執行安全接取。經由僅爲安全模組所知之私有驅

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

五、發明說明 (20)

動器安全介面 (安全裝置驅動器介面 (S D D I)

1 9 0 A) , 請求這些驅動器服務。 S D S E 1 7 5 使用此介面 1 9 0 A 以執行諸如 Get Media Key Block (M K B) 等特別安全命令。非安全裝置驅動器介面 (N S D D I) 1 9 0 B 也會利用裝置驅動器 1 9 0 以接取卡 1 3 的使用者區 4 1 中任何未加密的檔案。

S W 1 0 0 架構的安全性在於其鑰的安全性。由於會增加危及鑰的可能性及因而危及加密內容, 所以, 秘密的「軟鑰」未長期地儲存在暫時安全區中。 S W 1 0 0 利用 S D S E 1 7 5 內的設計, 動態產生所需的鑰 (或「軟鑰」) 及當未立即需要這些特定鑰時將它們刪除。

現在更詳細地說明 S W 1 0 0 的操作。 S W 1 0 0 , 特別是命令分送器 1 3 0 / A P I 1 3 0 A 具有一些 A P I 常式, 這些常式可被叫出以執行某功能。雖然有很多常式, 但是這些常式中僅有 2 2 個會由裝置 1 5 從外部接取。這些常式係由也稱為命令之呼叫所接取。為了取得記憶卡 (或其它媒體) 1 3 中的內容, 裝置僅需傳送 2 2 個呼叫之一且內容會被取還, 於需要時被解密, 並被解碼。舉例而言, 在音頻的情形中, 裝置僅需傳送「播放」呼叫, 音樂即會開始。

下述列出的 A P I 允許應用程式與符合安全數位 (S D) 標準交介。雖然以 S D 標準顯示發明的實施, 但是, 本發明可以用於很多不同標準。

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

五、發明說明(21)

表 1 —— A P I 常式／呼叫

呼叫/API 常式	呼叫名稱/API 常式(如同附送的原始碼中所見般)
1. 初始化音頻系統	SdIntiAudioSystem
2. 安裝媒體(於需要時)	SdMountAudio
3. 解除安裝音頻(於需要時)	SdUnMountAudio
4. 檢查可資利用的空間	SdDriveFreeSpace
5. 退出媒體	SdEjectCard
6. 取得播放清單數目	SdGetPlayListCount
7. 取得播放清單	SdGetPlayLists
8. 取得軌道標題	SdGetTrackTitle
9. 取得軌道資訊	SdGetTrackInfo
10. 開啓軌道	SdOpenTrack
11. 播放軌道	SdPlayTrack
12. 至下一軌道	SdNextTrack
13. 停止播放	SdStopPlay
14. 暫停播放	SdPauseTrack
15. 恢復播放	SdResumeTrack
16. 重設播放清單	SdResetPlayList
17. 快速正轉/倒轉播放(+/-)	SdForward
18. 將軌道索引號加至播放清單	SdAddTKItoPLM
19. 從播放清單刪除索引號	SdDelTKItoPLM
20. 從軌道管理員刪除軌道索引號	SdDelTKItoTMG
21. 將 MP3 轉換成內部播放格式	SdConvertMP3ToSA1
22. 將 AAC 轉換成內部播放格式	SdConvertAACToSA1

(請先閱讀背面之注意事項再填寫本頁)

D 裝

五、發明說明 (22)

現在，將詳述可由裝置 1 5 呼叫的主要 A P I 常式。將參考圖 8 A — 8 E。

從圖 8 C 可知，有預先播放處理 8 0 5 及播放處理 8 1 0。在圖 8 C 的處理期間產生圖 8 E 的區塊。當由裝置 1 5 的使用者介面呼叫時，執行相關的 A P I 模組。在音頻播放的情形中，對模組的呼叫會由裝置 1 5 的使用者介面傳送至圖 8 B 中所見的音頻介面 1 0 5。執行列於流程圖中的功能之主呼叫／模組標示於右方。這些模組中的很多模組執行其它內部及外部接取模組，且清單並非意指耗用性，而是意指先前併入參考之光碟上的軟體碼之參考並形成本申請案之一部份。更詳細的說明，請參考軟體碼。

裝置在步驟 8 0 3 中首先被啟動電源，在此步驟之後，預先播放處理 8 0 5 開始。預先播放具有二主要階段：電源啟動初始化階段 8 0 5 . 1 0 及音頻內容初始化階段 8 0 5 . 2 0。將參考圖 8 D，進一步詳細地說明音頻內容初始化階段。

一般而言，在先前播放處理 8 0 5 中，裝置及媒體會被初始化且某些資訊會從媒體中讀取並被儲存於裝置 1 5 的 R A M 記憶體的緩衝器中。如同先前從圖 2 中可見般，此 R A M 記憶體可為系統記憶體 2 7、D S P 3 1 的 R A M 記憶體 3 1 A、或 M C U 2 5 的 R A M 記憶體 2 5 A。在步驟 8 0 5 A 中，S W 1 0 0 將會取得媒體的驅動號數。在某些應用軟體中，會有多於一的記憶卡或

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

五、發明說明 (23)

碟片由裝置 1 5 接取。在此步驟中，其將取得所有的驅動號數以便每一驅動器上的內容可以被適當地接取。此可由 A P I 常式 SdInit-AudioSystem 完成，並可由裝置 1 5 呼叫或由 S W 1 0 0 內部地呼叫以作為先前播放常式的一部份。S W 1 0 0 接著初始化 S W 1 0 0 內的 S S M 1 8 0 及 S D S E 1 7 5。在任何編碼鑰及來自媒體的內容被處理之前，這是需要的。S W 1 0 0 也將初始化卡 1 3 中的播放清單及軌道管理員。

在步驟 8 0 5 B 中，S W 1 0 0 將初始化及鑑定媒體。在此處所述之 S D 卡的情形中，將執行圖 5 - 7 的 M K B 處理。在步驟 8 0 5 A 期間，也可執行此 M K B 處理，且假使先前被執行，則其將不會於步驟 8 0 5 B 中再度被執行。此處理的進一步細節，請參考圖 5 - 7 及先前併入參考之 4 C 文獻。也將參考圖 1 0，更詳細地討論此處理。在步驟 8 0 5 B 中，將從卡 1 3 中重製資訊值，且資訊值會被儲存於裝置 1 3 的 R A M 記憶體中之圖 8 E 的媒體資訊塊 8 5 0 的區域中。這將由 A P I 常式 SdMountAudio 完成，並可由裝置 1 5 呼叫或由 S W 1 0 0 內部呼叫作為預先播放常式的一部份。因此，用於播放一般資訊的值 (pTGInfo)、媒體的有效號數 (SanDis)、驅動號數 (drivenum)、媒體的安全系統 (security) 及媒體的安裝狀態 (mounted) 將分別填充於它們個別的區域中。當被任何數目之 A P I 呼叫所呼叫而不用從卡 1 3 讀取這些區域時，它們會從裝置 1 5 的 R A M 中被順序地讀取。

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

五、發明說明 (24)

在電源啓動初始化 8 0 5 . 1 0 完成之後，音頻內容初始化 8 0 5 . 2 0 開始。一般而言，在音頻內容初始化 8 0 5 . 2 0 期間，個別軌及多個音頻軌（播放清單）的加密音頻內容之資訊指定區及排序會從卡（或其它媒體）1 3 中重製至裝置 1 5 的 R A M 中的小緩衝器中。圖 8 E 中的區塊所示之此資訊因而在裝置內可被快速地及輕易地接取且於後續的播放處理 8 1 0 期間無須從卡 1 3 中固定地讀出或更新至卡 1 3 中。

將參考圖 8 D，更詳細說明音頻初始化階段 8 0 5 . 2 0。此階段會產生一些結構，作為記憶卡（或其它媒體）1 3 上加密內容之本區地圖或導引。

在步驟 8 0 5 C 中，裝置 1 5 會呼叫 A P I 模組 SdGetPlayListCount。此呼叫及所有下述呼叫通常會從裝置 1 5 的使用者介面之軟體傳送至 S W 1 0 0 的介面模組之一。在此音頻播放說明中，呼叫會從使用者介面傳送至音頻介面 1 0 5。在視頻播放的情形中，呼叫會被傳送至視頻介面 1 1 0，且在影像再生的情形中，呼叫會被傳送至影像介面 1 1 5。呼叫接著會被轉送至含有 A P I 1 3 0 A 內的 A I P 模組之命令分送器 1 3 0。

在步驟 8 0 5 D 中，SdGetPlayListCount 藉由從卡 1 3 重製資訊至裝置 1 5 的 R A M 記憶體中，填入用於播放清單資訊塊 8 0 6' 之值。其藉由參考媒體資訊塊 8 5 0，以選取適當的授權驅動器。所有授權的驅動器之播放清單之總數會被重製至裝置 1 5 的 R A M 中。

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

五、發明說明 (25)

在步驟 8 0 5 E 中，裝置 1 5 呼叫 A P I 模組 SdGetPlaylist。

在步驟 8 0 5 F 中，SdGetPlaylist 藉由將資訊從卡 1 3 重製至裝置 1 5 的 R A M 記憶體中，填入用於播放清單資訊塊 8 6 0 之值。其將藉由參考媒體資訊塊 8 5 0 以選取播放清單資訊所在之適當的授權驅動器。被選取的或內定的播放清單之總播放時間為毫秒 (pListTime)，播放清單中的軌道數目 (tracksInPlist)，對應於目前播放清單之索引號 (index)、播放清單名稱字串長度 (Length)、及播放清單名稱 (pListName) 將會填入於它們的播放清單資訊塊 8 6 0 的個別區域中。

在步驟 8 0 5 G 中，裝置 1 5 會呼叫 A P I 模組 SdGetTrackInfo。

在步驟 8 0 5 H 中，SdGetTrackInfo 藉由將資訊從卡 1 3 重製至裝置 1 5 的 R A M 中，填入用於軌道資訊塊 8 7 0 的值。其將藉由參考媒體資訊塊 8 5 0 以選取播放清單資訊所在之適當的授權驅動器。其將藉由參考播放清單資訊塊 8 6 0 以選取每一播放清單內的軌道。包含軌道中相關軌道單元 (T K I) 之以毫秒計之總軌道時間 (trackTime)、包含相關 T K I 之以位元組計的總軌道尺寸 (bytesize)、軌道中 T K I 的數目 (tkisInTrack)、軌道數 (tracknum)、對應於目前軌道之索引號數 (index)、及來自媒體之軌道資訊 (trkInformation) 將填入於它們個別的區域中。

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (26)

在步驟 8 0 5 I 中，裝置 1 5 會呼叫 A P I 模組 SdOpenTrack。

在步驟 8 0 5 J 中，SdOpenTrack 會藉由將資訊從卡 1 3 重製至裝置 1 5 的 R A M 中而填入用於 Track Gen Info 塊 8 8 0 的一些值。其藉由參考媒體資訊塊 8 5 0 以選取適當的驅動器，並藉由參考播放清單資訊塊 8 6 0 及軌道資訊塊 8 7 0，以選取適當的播放清單及軌道內的軌道、選取毫秒計之播放清單的總播放時間 (pListTime)、目前播放號數 (plistnum)、擬播放的軌道號數 (tracknum)、用於軌道之第一 A O B (firstAOB)、及解密的 A O B (currentAOB)。

在步驟 8 0 5 K 中，SdOpenTrack 藉由將資訊從卡 1 3 重製至裝置 1 5 的 R A M 中，以填入軌道索引號資訊塊 8 7 5。其將藉由參考媒體資訊塊 8 5 0 及播放清單資訊塊 8 6 0 以選取播放清單資訊所處之授權的驅動器，並藉由參考播放清單資訊塊 8 6 0 及軌道資訊塊 8 7 0 以選取適當的播放清單內之適當軌道。

在產生軌道資訊塊 8 7 0 之後，在步驟 8 0 5 L 中，SdOpenTrack 藉由將資訊從卡 1 3 重製至裝置 1 5 的 R A M 中，以填入軌道一般資訊塊 8 8 0 的其餘值。下述值將被填入它們的塊 8 8 0 之個別區域中：用於媒體之鑑定號 (SanDisk)、操作命令 (C M D)、諸如 M P 3、A A C、或 W M A 等音頻格式 (audioformat)、碼取樣頻率 (sampfreq)、諸如音樂、書影像等應用屬性 (appAttrib)、

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

五、發明說明 (27)

以位元組計之音頻物件的尺寸 (尺寸 A O B) 、用於軌道之最後 A O B 塊 (lastAOB) 、用於軌道之 A O B 的總數 (countAOB) 、 A O B 塊中的同步位置之目前位置 — 這是什麼 & 其作什麼 (WHAT IS THIS & WHAT DOES IT DO????) — (同步字) 也稱為表頭、A O B 內的搜尋位置 A O B (seekposAOB) 、以毫秒計之軌道消耗時間 (trkElapsedTime) 、以毫秒計之軌道的總播放時間 (trkTotalTime) 、包含相關 T K I 之以位元組計的總軌道大小 (bytesize) 、以毫秒計之每一元件的播放時間 (elementplaytime) 、順向搜尋時間 (feTime) 、至一軌道之時間 (fwNext) 、播放清單中的軌道號數 (tracksInPlist) 、目前元件的大小 (elementsize) 、目前元件內的偏移 (element offset) 、 A O B 中的目前元件 (currentelement) 、 A O B 中的元件總數 (totalelements) 、及 A O B 的檔案處理 (f d A O B) 。在發明的不同實施例中，步驟 8 0 5 J 將完全填充軌道一般資訊塊 8 8 0 的，而步驟 8 0 5 K 將被免除。軌道索引號資計塊 8 7 5 係軌道一般資訊塊 8 8 0 的子集合並設計成節省空間及處理時間。意指，假使其正好瀏覽資訊時，會由裝置 1 5 的使用者介面參考。一旦使用者介面選取特定軌道播放，則軌道一般資訊塊 8 8 0 將會被填充，包含含於塊 8 7 5 中的資訊之子集合。

SdOpenTrack 可由裝置 1 5 呼叫或由 S W 1 0 0 內部地呼叫作為預先播放常式的一部份。

使區塊及區塊的資訊包含於裝置的記憶體中係一優點

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

五、發明說明 (28)

，這是因為即使在播放處理中發生任何故障，也無須重設媒體，亦即，執行電源啟動初始化 8 0 5 . 1 0 的步驟

8 0 5 A 或 8 0 5 B 。而且，通常不需要從卡 1 3 讀取播放所需的資訊。由於區塊 8 5 0 、 8 6 0 、 8 7 0 、

8 7 5 、及 8 8 0 中的資訊會作為包含於下一框中的內容之指標，所以，區塊中的資訊可被用以接取下一內容（音頻、視頻、等等）。如同先前參考圖 3 C 所述般，圖 8 E 的區塊詳載構成音頻或視頻軌道之檔案、元件及框的記憶卡 1 3 內之區域係位於記憶卡 1 3 之內。

步驟 8 0 5 的預先播放處理可由一些呼叫（在表 1 中括號中的號碼標示呼叫）觸發。如同圖 8 C 所示，將會觸發音頻內容初始化 8 0 5 . 2 0 之外部呼叫係：SdOpenTrack 、 SdGetPlaylistCount 、 SdGetPlaylist 、及 SdGetTrackInfo 。 SdOpenTrack(10) 係由 SdNextTrack(12)、SdStopPlay(13)、及 SdResetPlaylist(16)內部呼叫。A P I 模組 SdGetPlaylistCount、SdGetPlaylist 及 SdGetTrackInfo 也可由 SdOpenTrack 內部呼叫。一般而言，其會因諸如顯示軌道時間、倒轉、快速正轉、改變播放清單、改變圖形使用者介面顯示、或刪除軌道等裝置功能而被裝置 1 5 呼叫。一旦預先播放處理 8 0 5 完成，則播放處理 8 1 0 開始。

在播放處理 8 1 0 中，會初始化、停止、或暫停一或更多音頻或視頻軌道的播放之呼叫會由步驟 8 1 0 A 中的圖 8 B 之音頻介面 1 0 5 、視頻介面 1 1 0 、或影像介面 1 1 5 接收。在圖 8 C 中可見這些呼叫係在播放處理

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

五、發明說明 (29)

8 1 0 之後，為 SdPlayTrack、SdNextTrack、SdStopPlay、SdPauseTrack、SdResumeTrack、SdResetPlayList、SdForward、SdAddTKItOPLM、SdDelTKItOPLM、SdDelTKItOTMG、SdConvertMP3ToSA1、及 SdConvertAACToSA1。

無論多少 A P I 模組內部地或裝置呼叫時被執行，總是需要二主要模組以播放音頻軌道。這些模組是 SdOpenTrack(10) 及 SdPlayTrack(11)。SdOpenTrack(10) 及 SdPlayTrack(11) 將讀取軌道一般資訊塊 8 8 0 中的資訊以便接取記憶卡 1 3 的簇記憶區中加密的內容。

SdOpenTrack(10) 會由 SdNextTrack(12)、SdStopPlay(13)、及 SdResetPlaylist(16) 內部呼叫。一般而言，其會因諸如顯示軌道時間、倒轉、快速正轉、改變播放清單、改變圖形使用者介面顯示、或刪除軌道等裝置功能而由裝置 1 5 呼叫。

SdPlayTrack(11) 係播放音樂或影像軌道之核心 A P I。當使用者要播放目前的軌道、下一軌道時、或當使用者要在軌道內倒轉或快速正轉時，其通常由裝置使用。其會由諸如 SdNextTrack(12)、SdResumeTrack(15)、及 SdForward(17) 等其它 A P I 呼叫。SdPlayTrack 找出用於選取的軌道之 A O B、檢查音頻格式 (M P 3、A A C、或 W M A 等等)、及將軌道解碼。

參考圖 8 B、9、及 1 0，現在說明圖 8 C 的步驟

8 1 0，加密軌道之播放。

假使需要加密的內容時，則命令會發給／來自要求

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

五、發明說明 (30)

O E M 的 4 C 授權裝置鑰被使用之裝置 1 5 及 S W 1 0 0 。所有這些鑰的處理僅限於容納於 S S M 1 8 0 下方的 S D S E 1 7 5 模組。假使請求非安全性或未加密內容時，N S F I 1 7 0 及 N S A P I 1 4 0 B 、 1 5 0 B 、 及 1 6 0 B 和 N S D D 1 9 0 B 將接取內容。

當 S S M 1 8 0 接收用於安全服務的請求時，其會藉由傳送命令請求分封給 S D S E 1 7 5 內的 process_security 功能而執行它。鑰值絕不會包含於請求分封內或曝露於 S D S E 1 7 5 上的軟體層。

當由 S D S E 1 7 5 內部地需求時，能裝置鑰會經由功能呼叫而被取還至 O E M 供應的資料庫內。S D S E 1 7 5 的資料庫 security.lib 含有下述 A P I ，這些 A P I 係設計用以減少位於系統安全區中解密鑰之時間：

- 1) SEC_AKE API;
- 2) SEC_ENC_TKEY API;
- 3) SEC_DEC_TKEY API;
- 4) SEC_GETCCI API;
- 5) SEC_UPDATECCI API。

S W 1 0 0 的功能及結構說明於本申請案的文中，特別地，A P I 1 - 5 的功能顯示於圖 9 的流程圖中。A P I 顯示為跟隨於它們實施之對應功能之後。這些 A P I 以及 S W 1 0 0 實施的進一步細節見於本案附件之源始碼中。

一旦取得時，裝置鑰會與來自 S D 記憶卡之媒體鑰區

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

五、發明說明 (31)

(M K B) 合併以形成「媒體鑰」。此值會保持於 S D S E 1 7 5 之內以用於處理後續請求。注意，但是「專有媒體鑰」(K m u) 絕不會保持在 S D S E 1 7 5 之內。此值係形成所有安全接取之基礎，其總是以即時為基礎被計算（且絕不會被快取）以作為額外的安全防護。於下詳細說明 S D S E 1 7 5 內的鑰處理。

加密處理一般設計成停止未經授權重製安全媒體上的內容。發明有很多態樣以達成此目的。首先，諸如歌曲等整個檔案絕不會一次被解密並儲存於易受攻擊的記憶體中。可攜式裝置會分配緩衝器，且 S D S E 1 7 5 一次讀取成塊的加密內容、將其解密、然後一再地寫於相同的緩衝器上直到檔案結束為止。

如同圖 6 及 7 所示般，媒體專有鑰 (K m u) 及標題鑰 (K t) 最後被用於將內容解密。有很多方式保護標題鑰。一方式係將鑰儲存於裝置 1 5 非常安全的區域中，另一方式係每當加密的緩衝器被讀取及解密時，從卡 1 3 的保護區 4 7 讀取標題鑰。

回至圖 9，在步驟 2 0 5 中，M K B 影像如同圖 4 所示為 6 4 仟位元組，如圖 6 所示，其會被讀取以處理媒體鑰 (K m) 而產生媒體獨有鑰 (K m u)。此步驟進一步詳述於圖 1 0 中，稍後說明之。在步驟 2 0 5 中裝置及媒體的相互認證完成之後，進行 A K E 處理以造成任務鑰 (K s)，任務鑰 (K s) 係在步驟 2 1 0 中僅能於任務期間被使用（只要裝置開啓或是處於主動狀態）。再度參考

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

五、發明說明 (32)

圖 6，以瞭解 A K E 處理。在步驟 2 1 3 中，刪除媒體專有鑰 (K m u)。在步驟 2 1 5 中，使用任務鑰 (K s) 以將儲存於記憶卡 1 3 的保護區 4 7 中之雙重加密的標題鑰 E (E (K t)) 解密。結果係單一加密的標題鑰 (E (K t))。在步驟 2 2 0 中，加密的標題鑰 (E (K t)) 會被儲存於裝置 1 5 的記憶體中。(E (K t)) 可儲存於系統記憶體 2 7、M C U 2 5 的 R A M 記憶體 2 5 A、或 D S P 3 1 的 R A M 記憶體 3 1 A 中。標題鑰 K t 係特定用於每一標題，在音頻領域中稱為軌道並顯示於用以說明發明之圖 9 上。在長的古典歌曲之情形中，每一軌道由多個檔案構成。對於大的影像夾而言，標題可能包括很多檔案。因此，對於軌道之加密內容的所有後續讀取及解密而言，由於標題鑰係儲存於本地記憶體中，所以，無須從記憶卡中取還標題鑰，並可節省寶貴的時間及計算資源，同時，標題鑰可因安全目的而維持加密。

在步驟 2 2 5 中，軌道的一部份會被播放。此部份可能是在包括軌道之任何檔案中。在步驟 2 2 5 a 中，再度計算媒體專有鑰 (K m u)。在步驟 2 2 5 b 中，儲存於本地記憶體中的加密標題鑰會被解密。然後，在步驟 2 2 5 c 中，標題鑰會被用以將含有來自記憶卡 1 3 的使用者區 4 1 的內容之裝置 1 5 的緩衝器之內容解密。緊接在緩衝器被解密之後，標題鑰會於步驟 2 2 5 中被刪除且媒體專有鑰會於步驟 2 2 5 e 中被刪除。步驟 2 2 5 d 及 2 2 5 e 的次序並不重要，重要的是此二鑰僅於讀取軌道

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

五、發明說明 (33)

的一部份時曝露。此部份可為從播放（解密、解壓縮、及解碼）內容、音頻、或其它之數分之一秒至約十秒。較佳的是其為二秒。用以讀取部份之時間係取決於很多因素，包含裝置的處理速度及緩衝器大小。如前所述般，S W 1 0 0 可由M C U 2 5 或D S P 3 1 執行並儲存於裝置 1 5 的任一記憶體 2 7、2 5 A、3 1 A、或 3 2 中，因此，處理時間會變化。這一直重覆直到軌道的所有部份如同步驟 2 3 0 所示般被讀取為止。一旦所有的部份被讀取時，假使繼續播放，則如同步驟 2 3 5 所示般，系統會移動至下一軌道。舉例而言，此可能為假使使用者選擇播放整個播放清單之情形。

當軌道的所有部份被讀取且下一軌道的讀取要開始時，處理將會再度於步驟 2 1 5 開始並從卡 1 3 的保護區 4 7 取還下一雙重加密標題鑰。此通常為使用者設定裝置作動以播放包含多個軌道之整個播放清單之情形。假使任務結束（亦即，裝置 1 5 開啓或關閉），則必須產生新的任務鑰且處理將於步驟 2 1 0 初始化。假使移除或重新插入記憶卡時，將必須重新鑑定裝置及媒體且處理將於步驟 2 0 5 再度開始以讀取軌道。

圖 1 0 係說明上述圖 9 之步驟 2 0 5 的處理媒體鑰塊之操作。如圖 4 所示，M K B 影像 4 9 係 6 4 仟位元組長。一次讀取整個影像 4 9 以計算 M K B 是沒效率的，會需要大的 R A M 及長的處理時間。本系統會減少 R A M 的需求並減少處理時間。M K B 影像 4 9 會分成塊 1 至 1 2 8

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

五、發明說明 (34)

。每一塊係 5 1 2 位元組且包含四個不同型式的 M K B 記錄之一：驗證媒體鑰記錄 (V M K R)，為 0 x 8 1；計算媒體鑰記錄 (C M K R)，為 0 x 0 1；有條件地計算媒體鑰記錄 (C C M K R)，為 0 x 8 2；或是結束媒體鑰記錄 (E M K R)，為 0 x 0 2。這些記錄係說明於上述 4 C 實體的可記錄媒體 (C P R M) 規格之內容保護中。

在本實施例中，塊長度及緩衝器長度相同。但是，緩衝器長度及塊長度均為 2 5 6 位元組至 4 0 9 6 位元組之範圍。每一記錄會被檢查以根據記錄型式執行特定操作且儲存某些資料以便稍後用於取得媒體鑰。每當記錄被識別時，記錄長度會加至緩衝器偏移的總長度。以總長度除以塊長度，計算塊號數。塊號數係選取的塊資料之媒體鑰塊之索引。總長度的其餘部份係選取的塊資料之偏移。列及行會被用以計算加密的媒體鑰及有條件的加密媒體鑰在何處。這些加密鑰會被儲存且電子碼簿模式 (Electronic Codebook Mode) 演繹法中的解密 C 2 密碼會被執行以取得媒體鑰。此媒體鑰接著被驗證以作為正確的最後媒體鑰 (K m)。

每一 M K B 塊所需之用於從與記錄數目有關的 M K B 取得媒體鑰 (K m) 之讀取次數 T 顯示如下：

$$\text{記錄數目} < T < (\text{記錄數目} * 2)$$

T：接取 M K B 塊所需之次數

五、發明說明 (35)

每一記錄具有不同的長度及資料值。每一記錄的資訊可以在二讀取內取得。由於有四個記錄，所以，在4與8讀取之間，將需要處理MKB塊及取得記錄。

因此，讀取數目T為：

$$4 < T < 8$$

假設要耗掉N ms以接取512位元組的MKB資料。則將耗費(128*N)ms以接取整個64K MKB影像以從第一方法取得媒體鑰。第二方法對於最壞的情形僅耗費(8*N)ms以取得媒體鑰。因此，使用此設計，可節省相當可觀的時間。平均而言，為取得媒體鑰(Km)，讀取次數在4至6之範圍，且所需時間成比例地小於上述。

圖9的步驟205，此處於圖10中展開，其會被執行直至在步驟205.75中產生最終媒體鑰或媒體於步驟205.80中被拒絕為止。並非所有的128塊需要被讀取，且非每塊所有的512位元組需要被讀取以計算媒體鑰。處理MKB資料係需要一次請求資料塊之操作，其指向該特定塊內之所需區域及計算取得的值。並非所有的MKB資料都需要。圖10中所述的演繹法將提供數學計算以正確地算出需要什麼MKB資料塊，什麼記錄應被處理及加密資料位於何處。

在步驟205.5中，緩衝器指標器設定於資料緩衝器且緩衝器偏移被清除。接著，在步驟205.10中，

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

五、發明說明 (36)

檢查塊號以看看其是否等於或大於最大塊號。假使是，則於步驟 2 0 5 . 1 5 中歸還錯誤。假使為否，則塊號將被增量且於步驟 2 0 5 . 2 0 中新資料會被載入緩衝器中。然後，緩衝器偏移會於步驟 2 0 5 . 2 5 中被更新。因此，指標器可以被設定至正確位置（塊號加上偏移）。在步驟 2 0 5 . 3 0 中，緩衝器指標器會被設定至緩衝器偏移。在步驟 2 0 5 . 4 0 中，緩衝器會從指標器所處之偏移開始被讀取。系統接著判斷其正讀取何種型式的記錄。如同步驟 2 0 5 . 4 0 所見般，系統將首先檢查何種型式的記錄正被讀取，及何種型式的記錄與該記錄相關連。後續之動作將視記錄的型式及長度而不同。每一記錄的記錄長度將被用以決定緩衝器指標器於讀取後續的記錄時應位於何處。此由步驟 2 0 5 . 4 9 反映，更新緩衝器偏移及將緩衝器指標器設定在新偏移。

假使如同步驟 2 0 5 . 4 2 所示，記錄為 C M K R，則系統會於步驟 2 0 5 . 4 9 中更新緩衝器塊號數及對加密媒體鑰所處之正確的 M K B 位置的偏移。因此，系統將取得加密媒體鑰所處之偏移、前進至特定的 M K B 塊號數、分配緩衝器（1 6 區塊 x 5 1 2 位元組）、及前進至每一區塊內的偏移以讀取加密的媒體鑰。然後，系統於步驟 2 0 5 . 5 0 中使用從裝置 1 5 供應的裝置鑰（K d）以將媒體鑰解密（計算）。一旦計算出媒體鑰，則下一步驟係驗證媒體鑰。

假使記錄係於步驟 2 0 5 . 4 4 中被驗證為 V M K R

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

五、發明說明 (37)

，則先前在步驟 2 0 5 . 5 0 第一次嘗試、或是步驟 2 0 5 . 6 5 中後續嘗試算出的媒體鑰將於步驟 2 0 5 . 5 5 中與參考媒體鑰 (K m) 相比。爲了執行此點，參考媒體鑰將首先被儲存於本地。假使鑰相同，則發還以 1 6 進位 D E A D B E E F 表示之通行證，且系統無需有條件地計算媒體鑰。爲了算出從何處開始讀取下一記錄，V M K R 的記錄長度會被用以移動緩衝器指標器至下一記錄。假使其不相同，則當 C C M K R 記錄在步驟 2 0 5 . 4 6 中被讀取時，其會再度被計算。當此記錄被讀取時，在步驟 2 0 5 . 4 9 中設定緩衝器指標器以在更新的緩衝器偏移處讀取之後，再次計算媒體鑰，接著，當 V M K R 被讀取時，其將接著被驗證。C C M K R 被計算的最多次數會由系統設定且較佳地爲一。

第一次計算發生於 C M K R 被發現時。假使其被成功地計算出來，如同 V M K R 被發現時驗證處理被初始化期間所決定般，則將不需有條件地計算媒體鑰 (K m)。假使驗證不成功，則當 C C M K R 被發現時，則媒體鑰將再度被計算及再被驗證。此意指有二次機會以計算媒體鑰。最後，假使如同步驟 2 0 5 . 4 8 中驗證般記錄爲 E M K R，則在步驟 2 0 5 . 7 5 中，系統將驗證記錄結束時有效的媒體鑰 (K m) 存在，在步驟 2 0 5 . 4 9 中將緩衝器指標器設定於用於此型記錄之適當偏移處之後，產生最終的媒體鑰 (K m)。但是，假使有效的媒體鑰未於步驟 2 0 5 . 7 0 中被歸還，則媒體將於步驟

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

五、發明說明 (38)

2 0 5 . 8 0 中被拒絕。假使最終媒體鑰於步驟 2 0 5 . 7 0 中被歸還，則如同步驟 2 0 5 . 8 5 所示般，處理將於圖 9 的步驟 2 1 0 繼續。

S D S E 1 7 5 內的功能會藉由使用裝置驅動器 1 9 0 的安全裝置驅動器介面 (S D D I) 1 9 0 A 以執行諸如 G e t M K B 等安全接取。此相同的裝置驅動器 S D D I 1 9 0 A 也會使用 S D S E 1 7 5 內其能直接呼叫的功能。舉例而言，在發出鑑定區讀取之前，S D D I 1 9 0 a 必須首先呼叫 S D S E 1 7 5 內的 sec_ake 功能。sec_ake 功能將接著回呼 S D S I 1 9 0 A。此「雙向呼叫關係」便於 S D S E 1 7 5 內的裝置鑰之隔離，其係 S D - 音頻標準的 S W 1 0 0 之實施所獨有。

由於 S D S E 1 7 5 處理所有的鑰導向處理，且當某些 S D 命令由音頻介面 1 0 5、視頻介面 1 1 0、或影像介面 1 1 5 接收時需要這些值，所以，裝置驅動器必須使用其直接呼叫的 S D S E 1 7 5 內之功能。當執行功能時，S D S E 模組 1 7 5 必須接著回呼裝置驅動器 1 9 0 的私有安全介面 S D D I 1 9 0 A 中。此「雙向呼叫關係」允許在 S D S E 1 7 5 與裝置驅動器 1 9 0 之間交織請求，因而使得鑰值能被隔離於安全模組內。

軟體層的 S D S E 1 7 5 藉由初始化安全驅動器請求分封及呼叫通過請求分封指標器之安全驅動器介面進入點，經由私有介面，請求安全裝置驅動器服務。

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

五、發明說明 (39)

提供下述表格，以使併入參考之附件原始碼更加清楚。

請求分封 (sdapi.h 中所界定) 係由資料型 SSMSEVER 組成，其定義如下：

表 2

變數	變數名稱
Typedef struct mySecuredDrv	
{	
Data buffer	UCHAR *buffer
Number of data blocks	UINT16 noBlocks
Application unique Number	UINT16 mkb ID
Start address	UINT16 lba
Security flag	INT16 securityFlag
Drive number	INT16 driveNo
Command index	INT16 opCode
}	

命令索引 (INT 16 opCode) 持有用於被請求的服務之命令。支援的命令包含：

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

五、發明說明 (40)

表 3

命令	函數碼常式
Device identify	#define SDDRV_IDENT 0
Security identify	#define SDDRV_SECIDENT 1
Secure read	#define SDDRV_SECRD 2
Secure write	#define SDDRV_SECWR 3
Secure erase	#define SDDRV_SECERASE 4
Read MKB	#define SDDRV_RDMKB 5
Get MID	#define SDDRV_GETMID 6
Set challenge	#define SDDRV_SETCHALGE 7
Get challenge	#define SDDRV_GETCHALGE 8
Set response	#define SDDRV_SETRESP 9
Get response	#define SDDRV_GETRESP 10
Change size of protected area	#define SDDRV_CHANGESA 11

安全裝置驅動器服務請求從 S D S E 1 7 5 模組發出。舉例而言，產生挑戰 1 功能送出如下所述之挑戰 1：

表 4－產生挑戰 1

命令	運算
Call security routine	SDSECURITYDRV mySecDrv
Set drive number	mySecDrv.driveNo = (INT16)drv
Set memory address within media	mySecDrv.lba = 0
Number of data blocks	mySecDrv.noBlocks = 1
Set challenge	mySecDrv.opCode = SDDRV_SETCHALGE
Send challenge 1	mySecDrv.buffer = Chlg1
Call to device driver	scDDHandler(&mySecDrv)

由於所有的鑰操作被侷限於 S D S E 1 7 5，所以，S S D I 1 9 0 A 必須依賴 S D S E 1 7 5 功能以執行鑑定鑰交換 (A K E) 或用於將透過匯流排傳送的資料解密 (注意，使用從每一 A K E 產生的「任務鑰」，將透過匯流排傳送的所有資料首先加密)。

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

五、發明說明 (41)

當執行 A K E 時， S D S E 1 7 5 必須傳送命令給 S D 記憶卡 1 3，因此，其必須接著呼叫 S D D I 1 9 0 A。此呼叫關係概述於圖 7 中，其說明處理鑑定區的讀取所需之步驟。

注意， S D S E 1 7 5 內的 sec_ake 功能，當由安全 S D D I 1 9 0 A 呼叫時，經由私有驅動器介面，對安全裝置驅動器執行四個回呼。這四個請求包含：

SDDRV_SETCALGE、SDDR_GETCALGE、SDDRV_SETRESP、及 SDDRV_GETRESP。這將使得安全模組能夠執行圖 7 中所示之必要的設定挑戰／取得挑戰、設定回應／取得回應。所造成的任務鑰會儲存於安全模組內。當安全裝置驅動器回呼 S D S E 1 7 5 的 bus_decrypt 功能以從 S D D I 1 9 0 A 取得資訊時，這會被用以將資料解密。

本發明的系統及方法在很多方面均較習知技藝有利。本發明提供原始設備製造商隨開即用解決之道，不需知道儲存媒體的記憶結構即可接取加密內容。解密處理本身是非常複雜。此外，簡單地讀寫記憶卡本質上且本身是複雜的。製造商所需作的是傳送諸如「播放」或「下一軌道」等簡單命令並將來自任何記憶裝置之解密內容歸還。

在非常隔離的及保護的軟體層中，操作裝置鑰及所造成的任務鑰。這些絕對不會曝露在較上層中。即使較低的裝置驅動器層也不會被授予直接接取鑰之權。當產生媒體鑰時，從 O E M 供應資料庫中取還裝置鑰。此鑰會被固持

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

五、發明說明(42)

在安全引擎內，但是，絕對不儲存安全設計心臟之媒體獨有鑰（K_{mu}）。安全引擎的私有介面使得安全引擎能夠取得記憶卡之低階接取並使所有的安全有關之鑰（舉例而言，裝置鑰、媒體鑰、任務鑰）之曝露侷限於安全引擎內。

「雙向呼叫關係」允許安全引擎及安全裝置驅動器交織使用彼此的服務。

雖然已顯示及說明本發明的特別實施例及其優點，但是，在不悖離後附申請專利範圍中所界定的發明之精神及範圍下，可以作不同的改變、取代、及變更。舉例而言，雖然顯示使用SD記憶卡以說明發明的作用，但是，發明也可用於任何具有加密內容之媒體。其也可由任何型式的裝置使用。此外，可從固定式或可移式、或固態型或旋轉型等任何型式的記憶裝置，將加密的內容解密。內容不限於音頻或視頻，也可為任何值得加密之內容。

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

四、中文發明摘要(發明之名稱：)

從非揮發性記憶卡、光碟或其它媒體播放音頻、視頻或其它內容之系統、方法及裝置

一種用於原始設備製造商之安全套裝軟體，能在電子裝置中執行以便從諸如記憶卡、光碟或硬碟等記憶儲存裝置中，接取及動態地解密加密的音頻視頻或其它內容，以致於裝置的使用者介面僅需傳送簡單的命令且解密的內容被輸出。

(請先閱讀背面之注意事項再填寫本頁各欄)

裝

訂

英文發明摘要(發明之名稱：)

**SYSTEM, METHOD, AND DEVICE FOR PLAYING BACK RECORDED
AUDIO, VIDEO OR OTHER CONTENT FROM NON-VOLATILE MEMORY
CARDS, COMPACT DISKS, OR OTHER MEDIA**

A secure software package for original equipment manufacturers to run in electronic devices in order to access and dynamically decrypt encrypted audio video or other content from a memory storage device such as a memory card, optical or hard disk such that the user interface of the device need only send simple commands and the decrypted content is output.

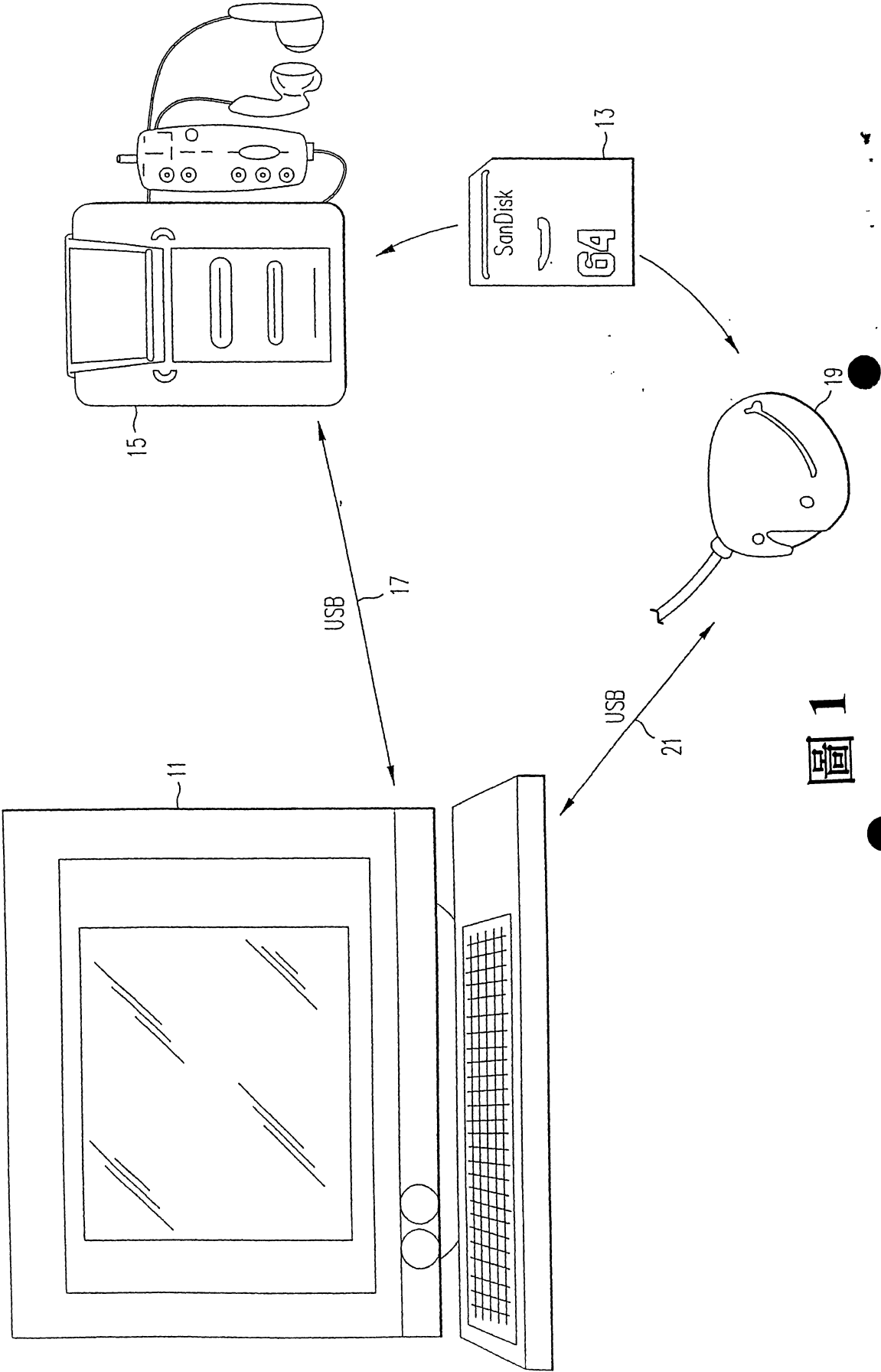


圖 1

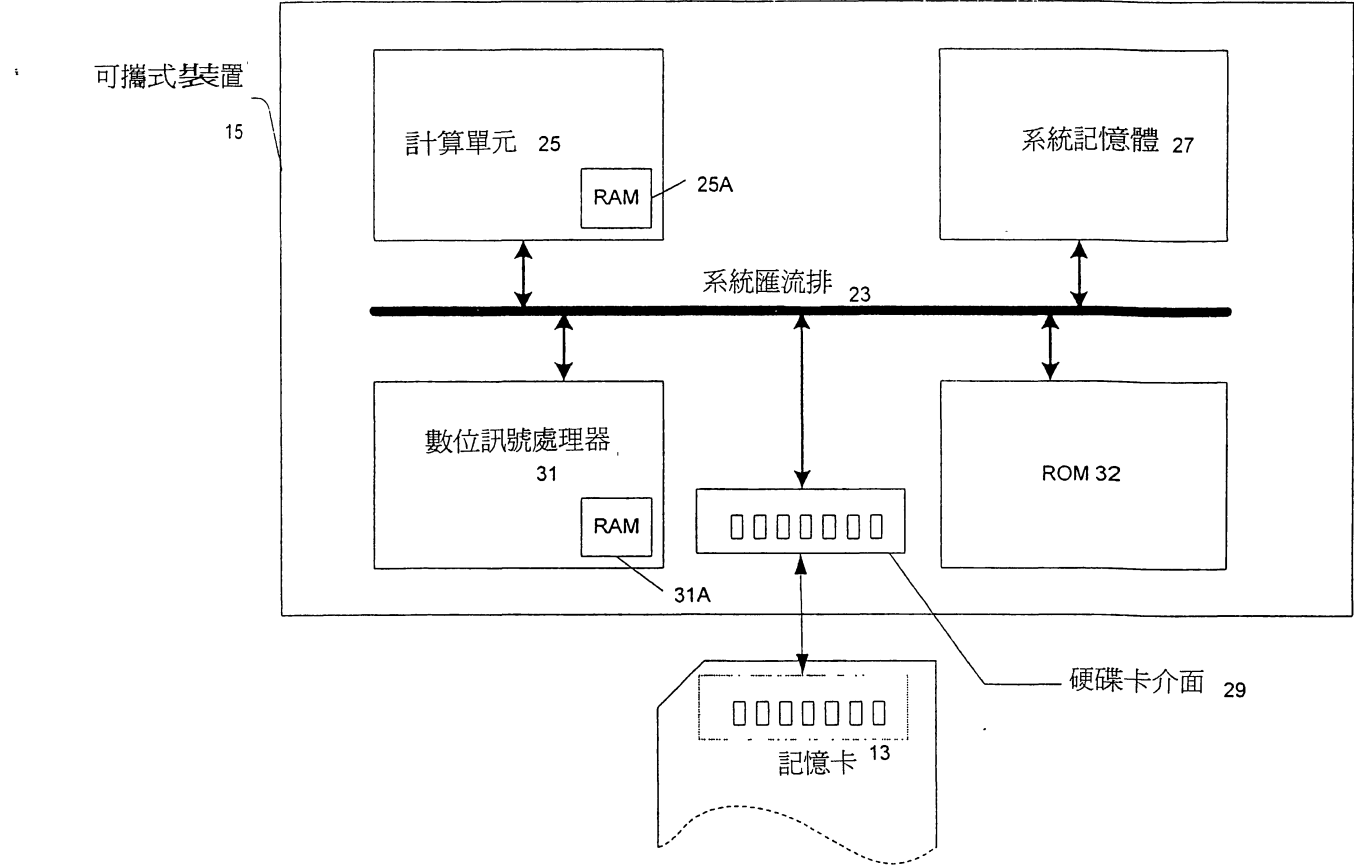
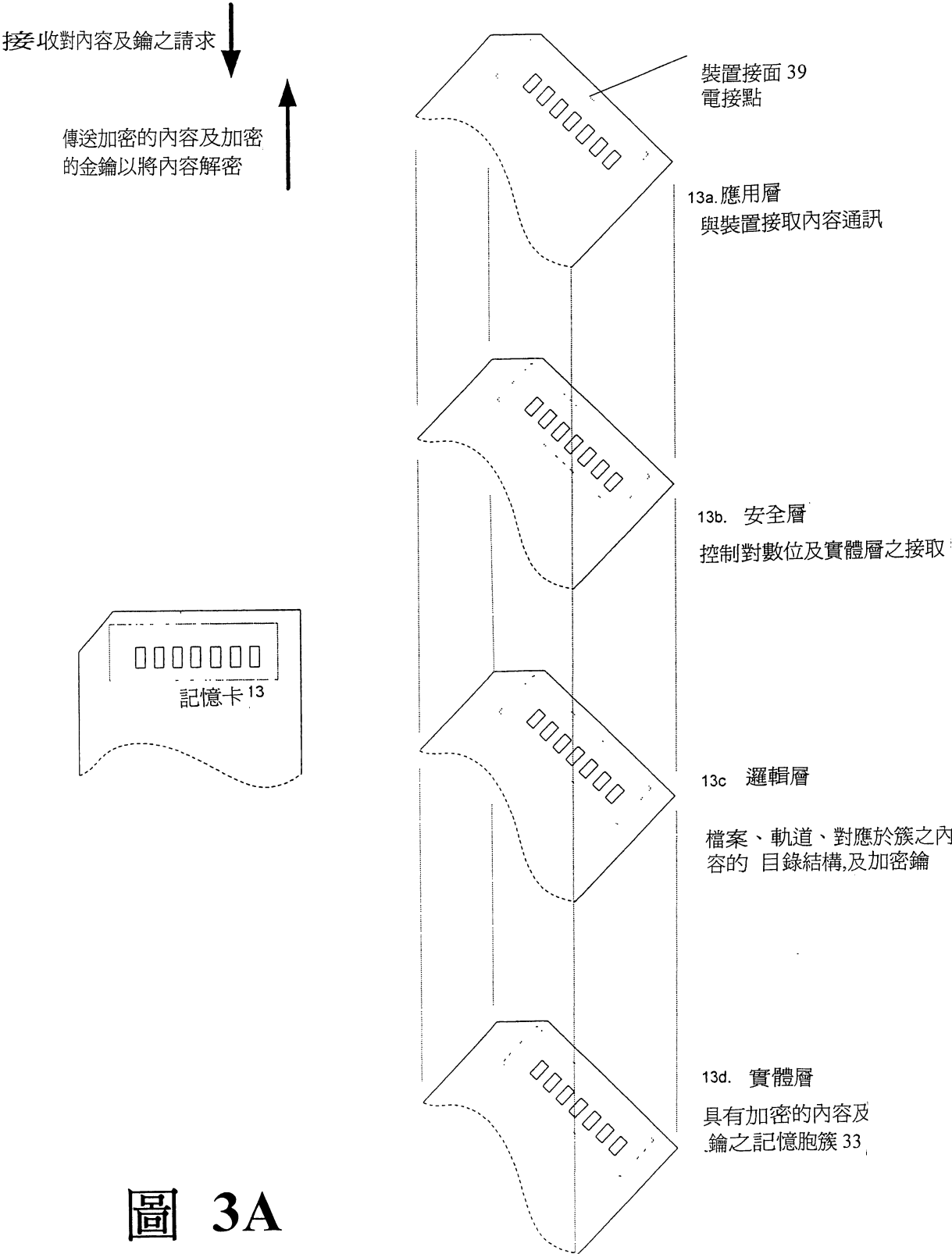


圖 2



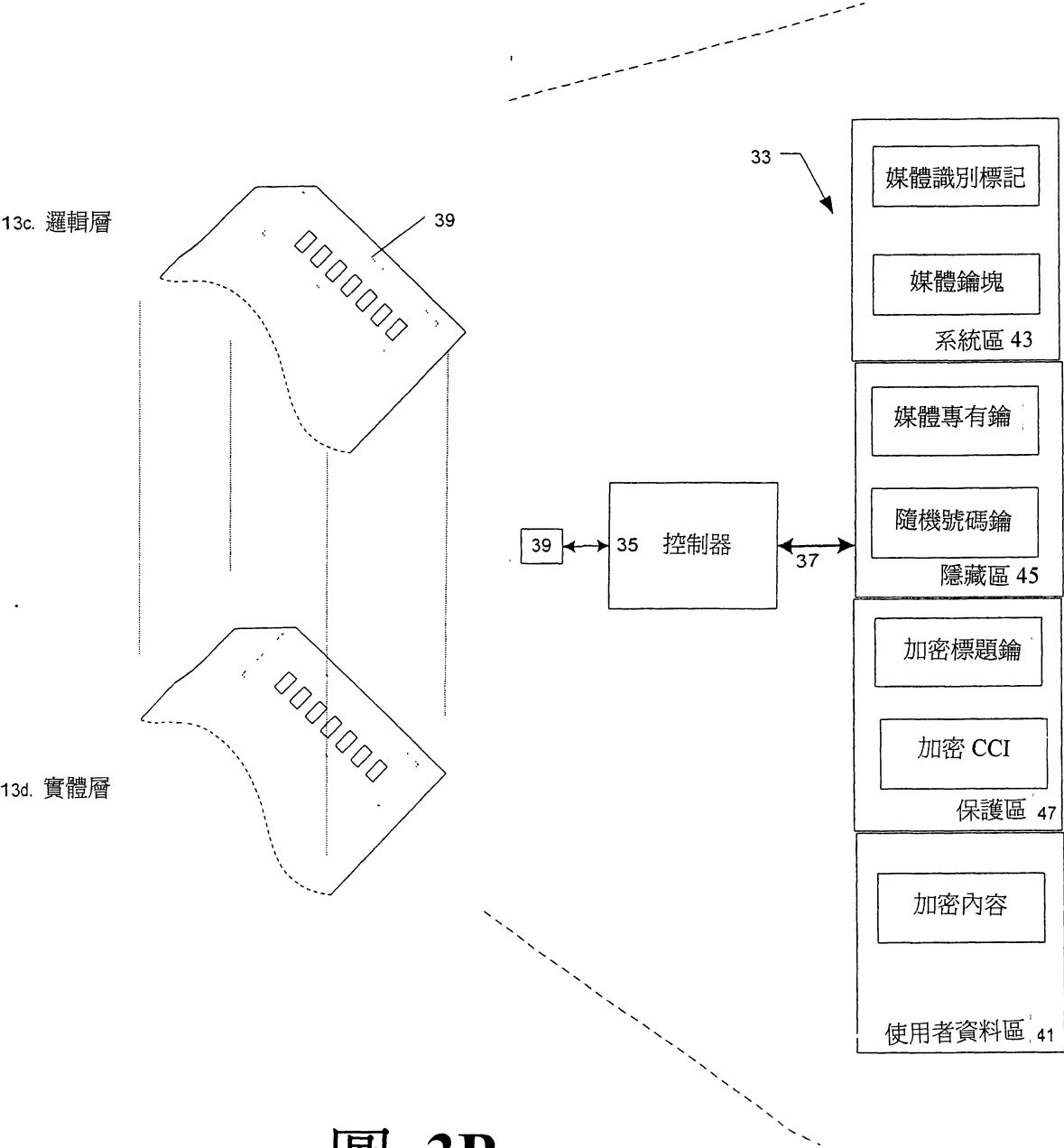


圖 3B

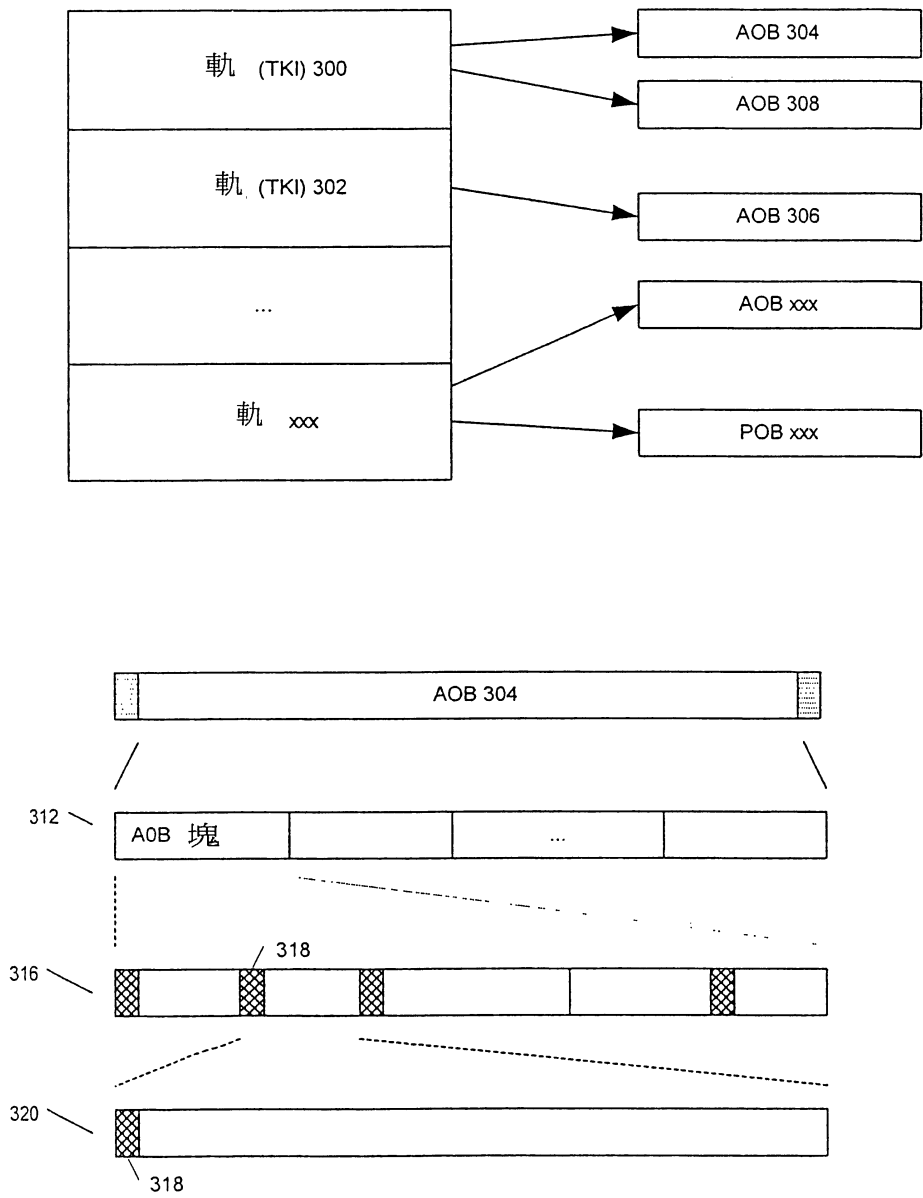


圖 3C

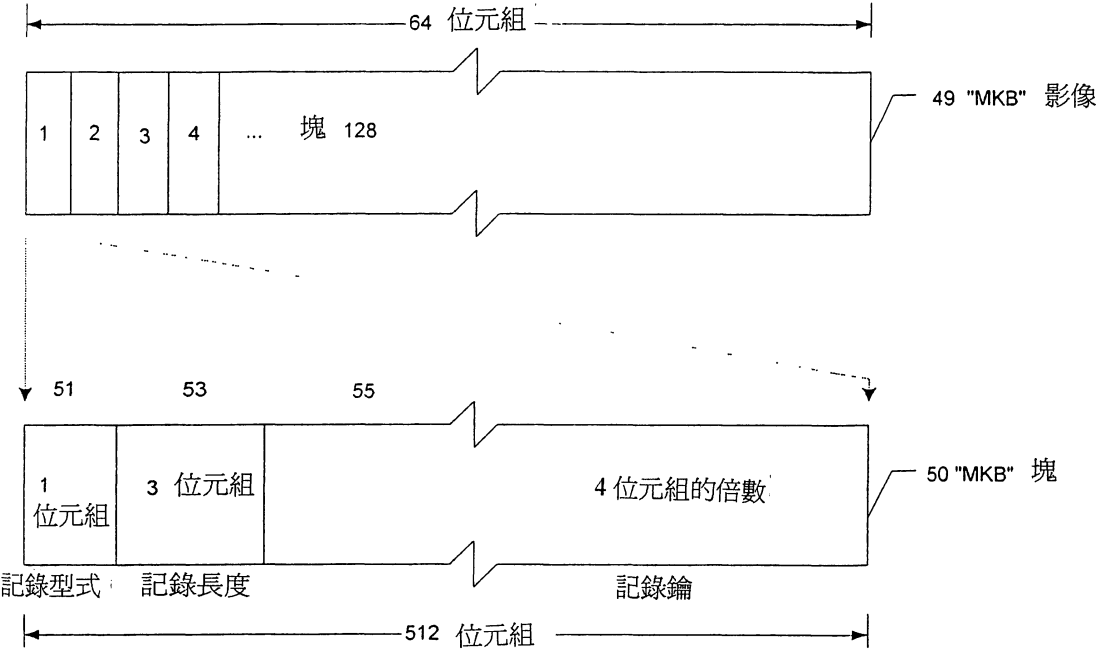


圖 4

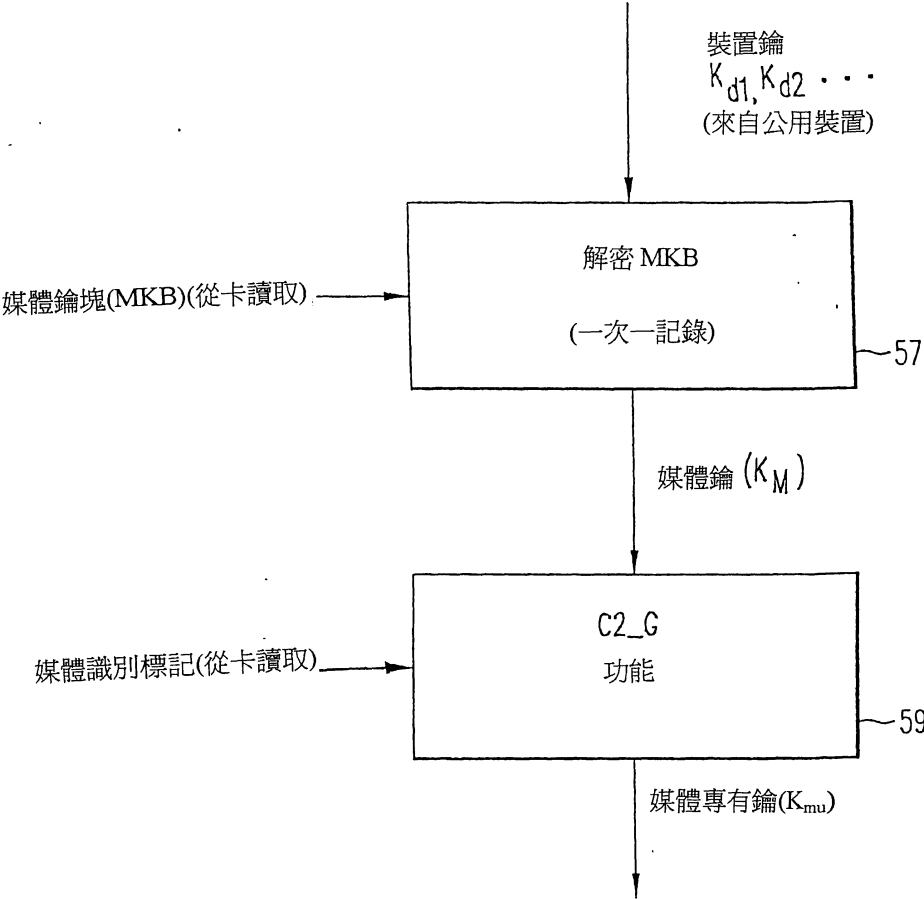
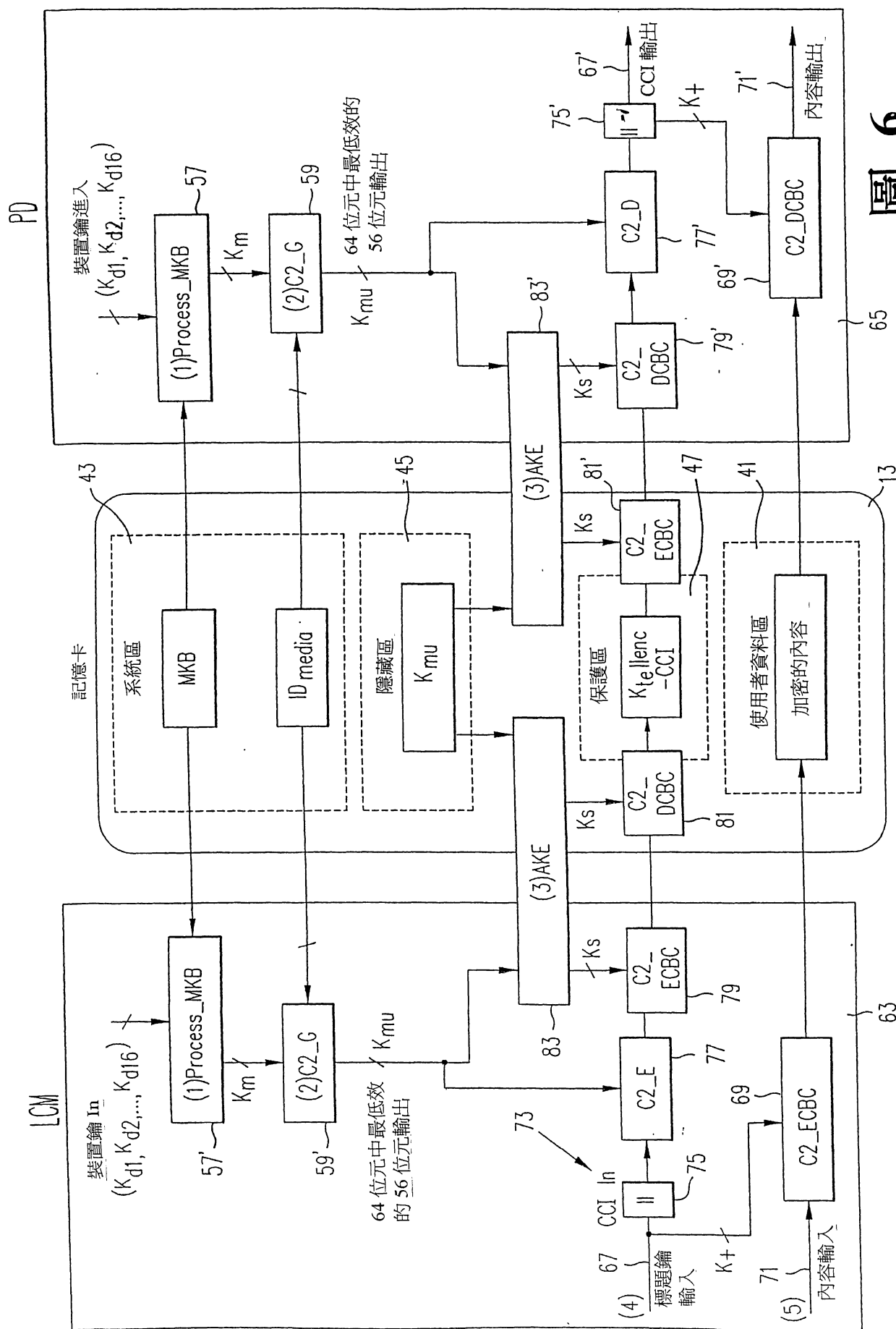
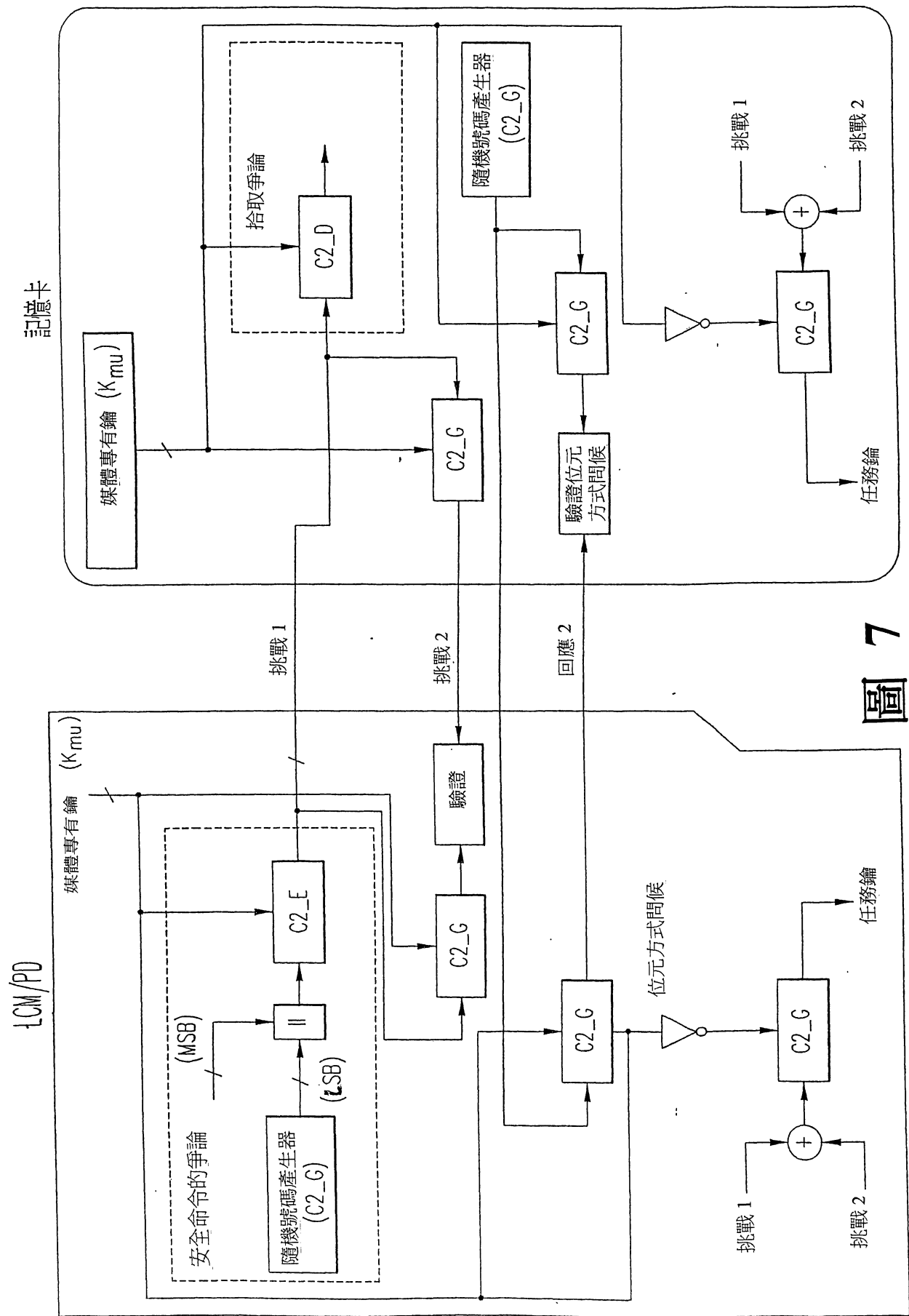


圖 5



回



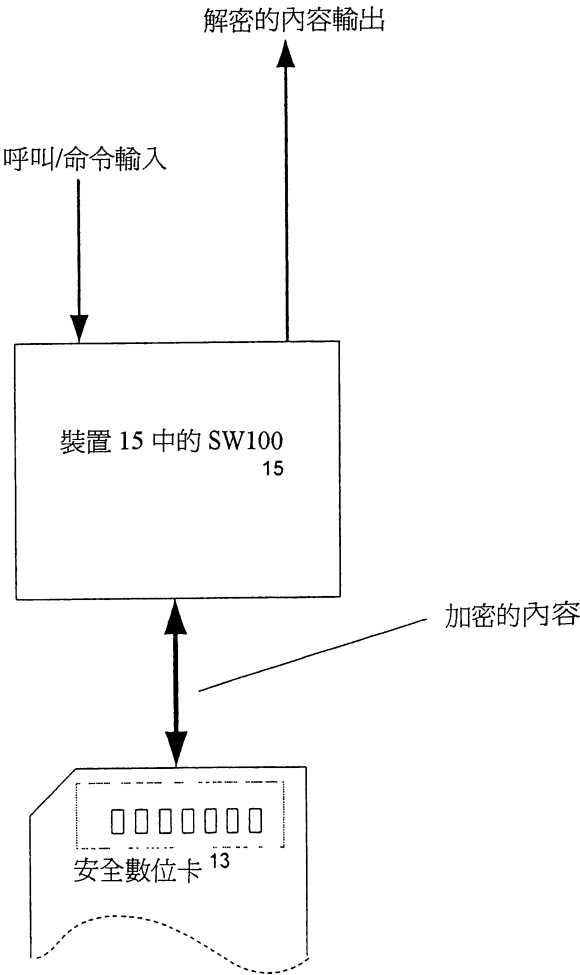


圖 8A

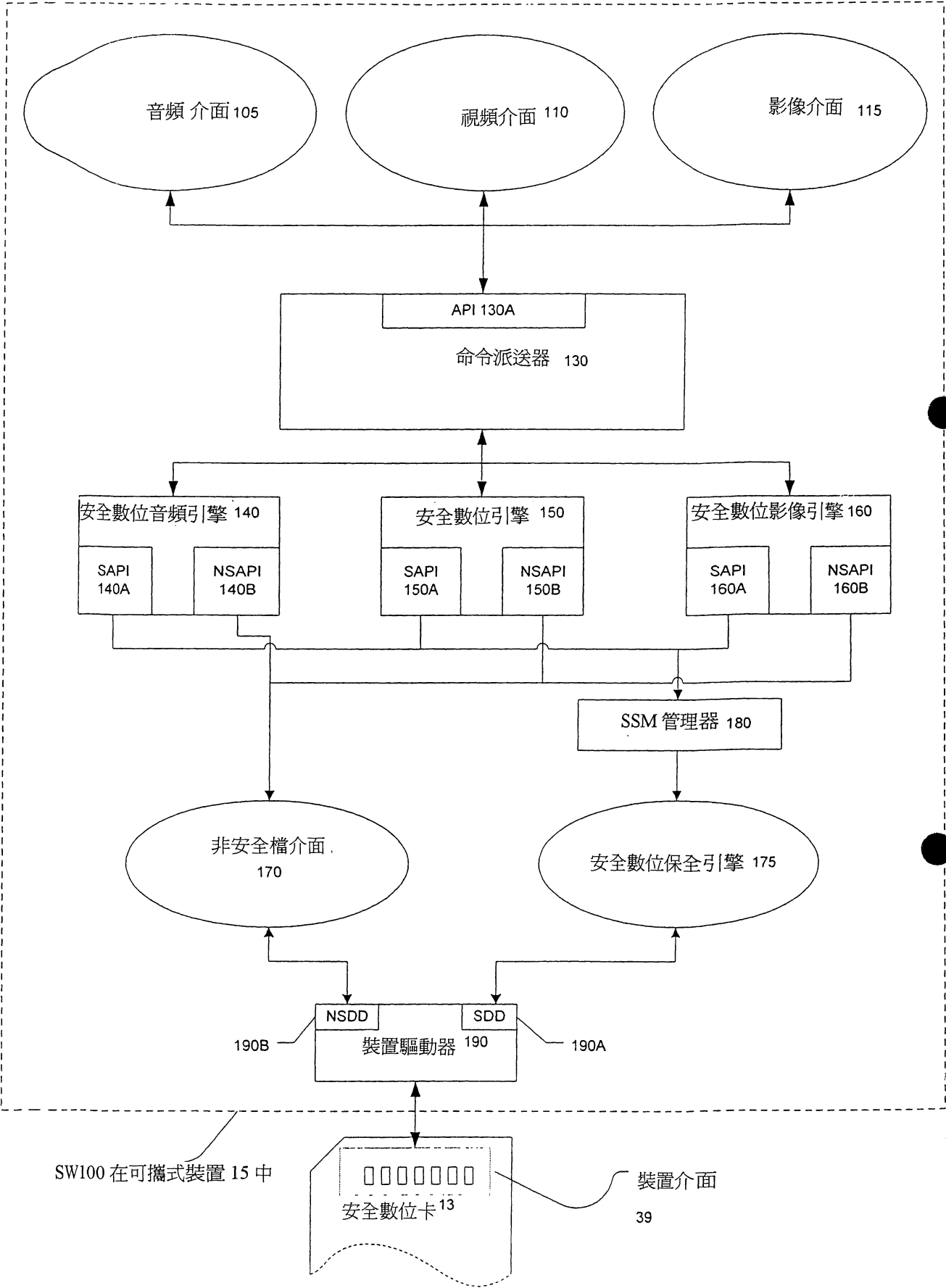


圖 8B

SW100 碼中相關的 API 模組/呼叫

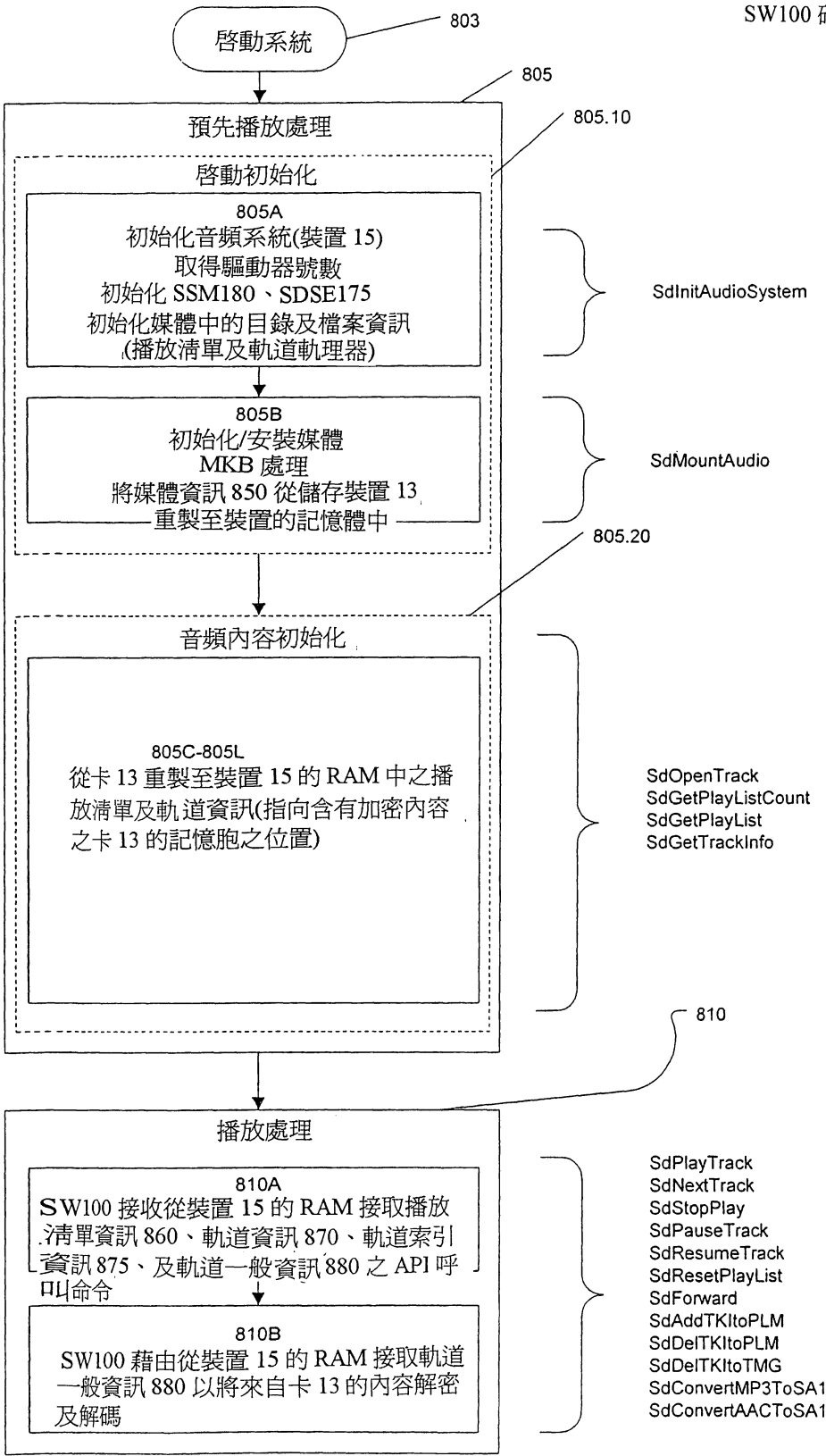


圖 8C

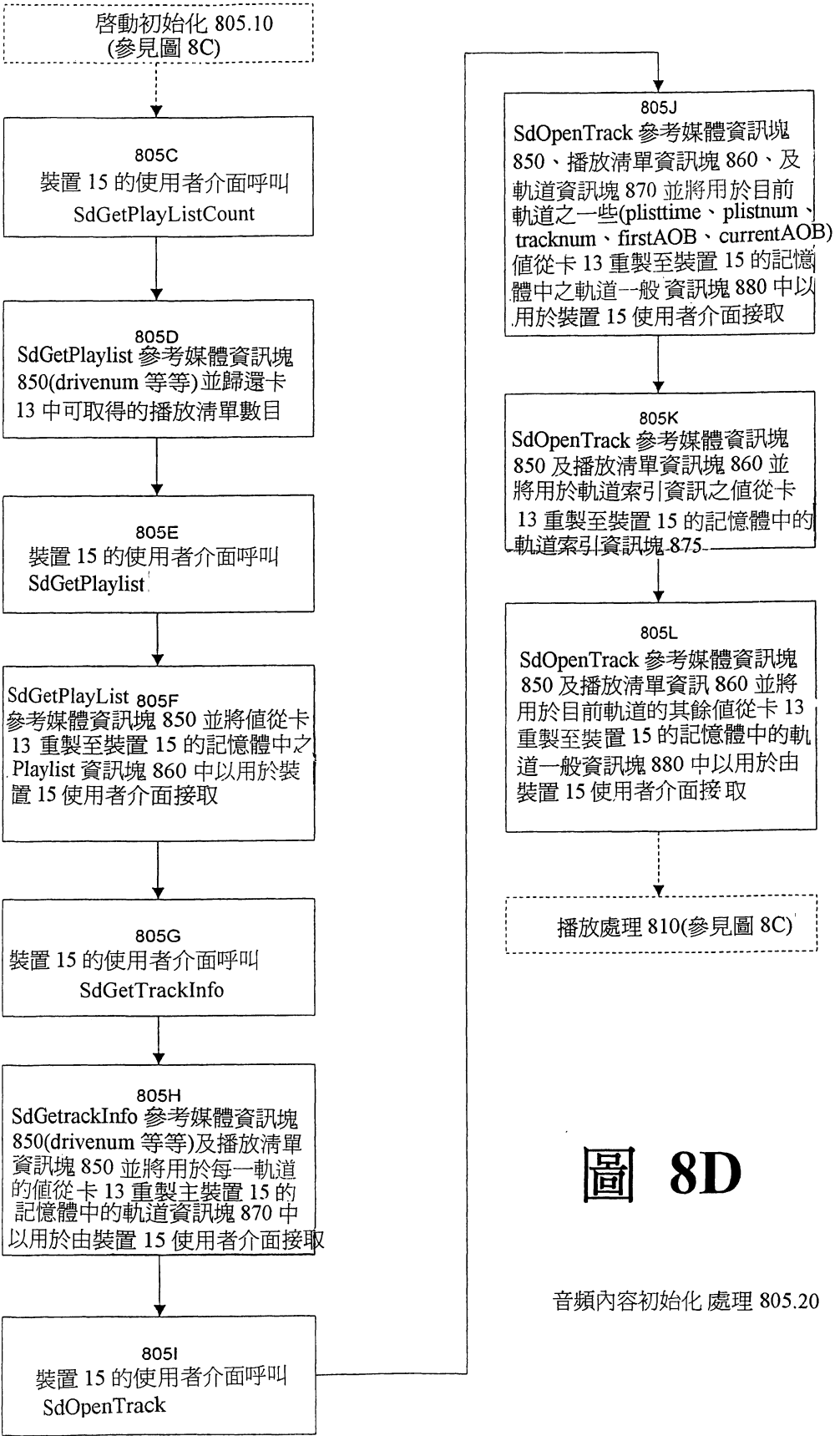
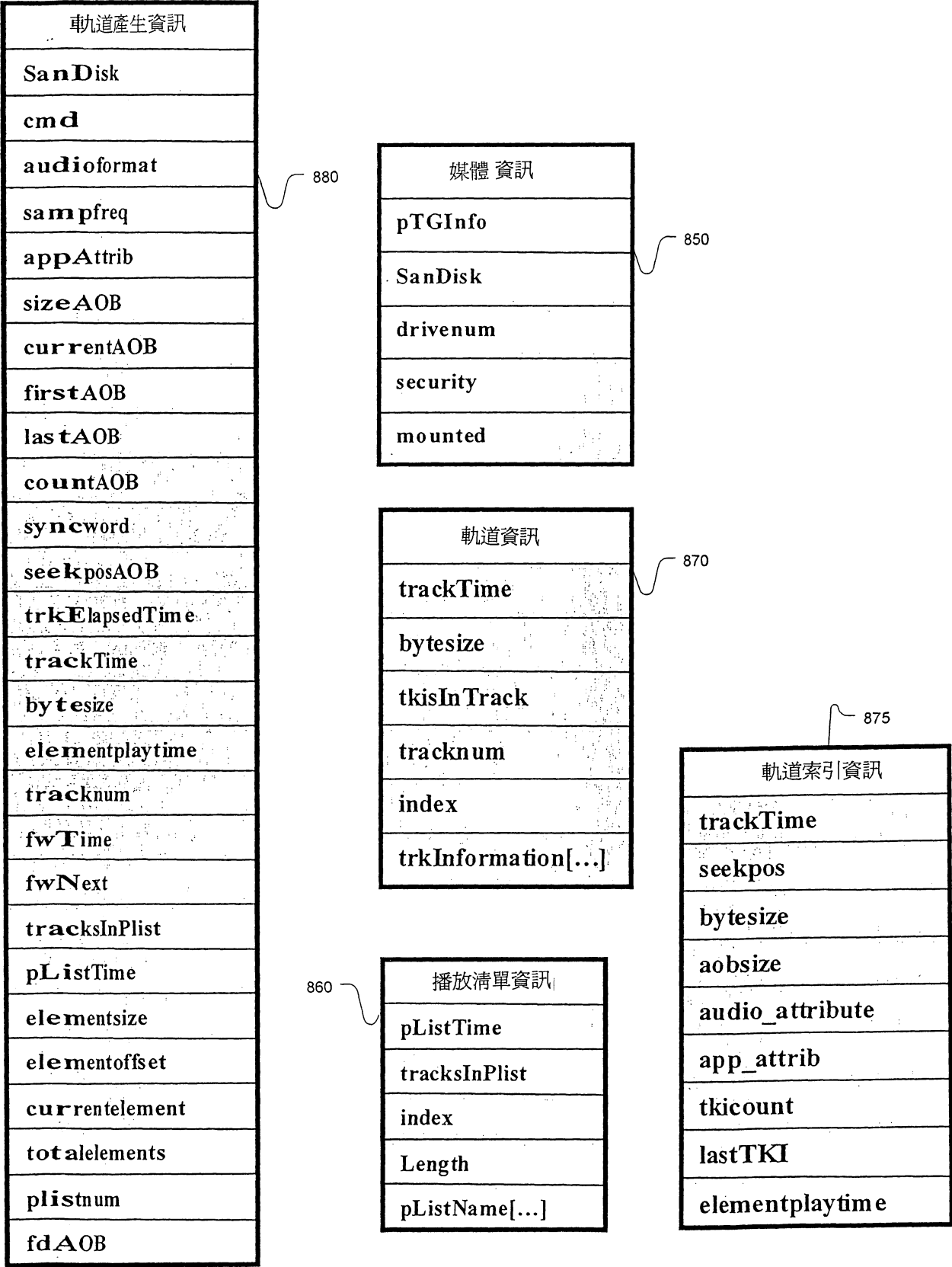


圖 8D

音頻內容初始化 處理 805.20



預先播放結構

圖 8E

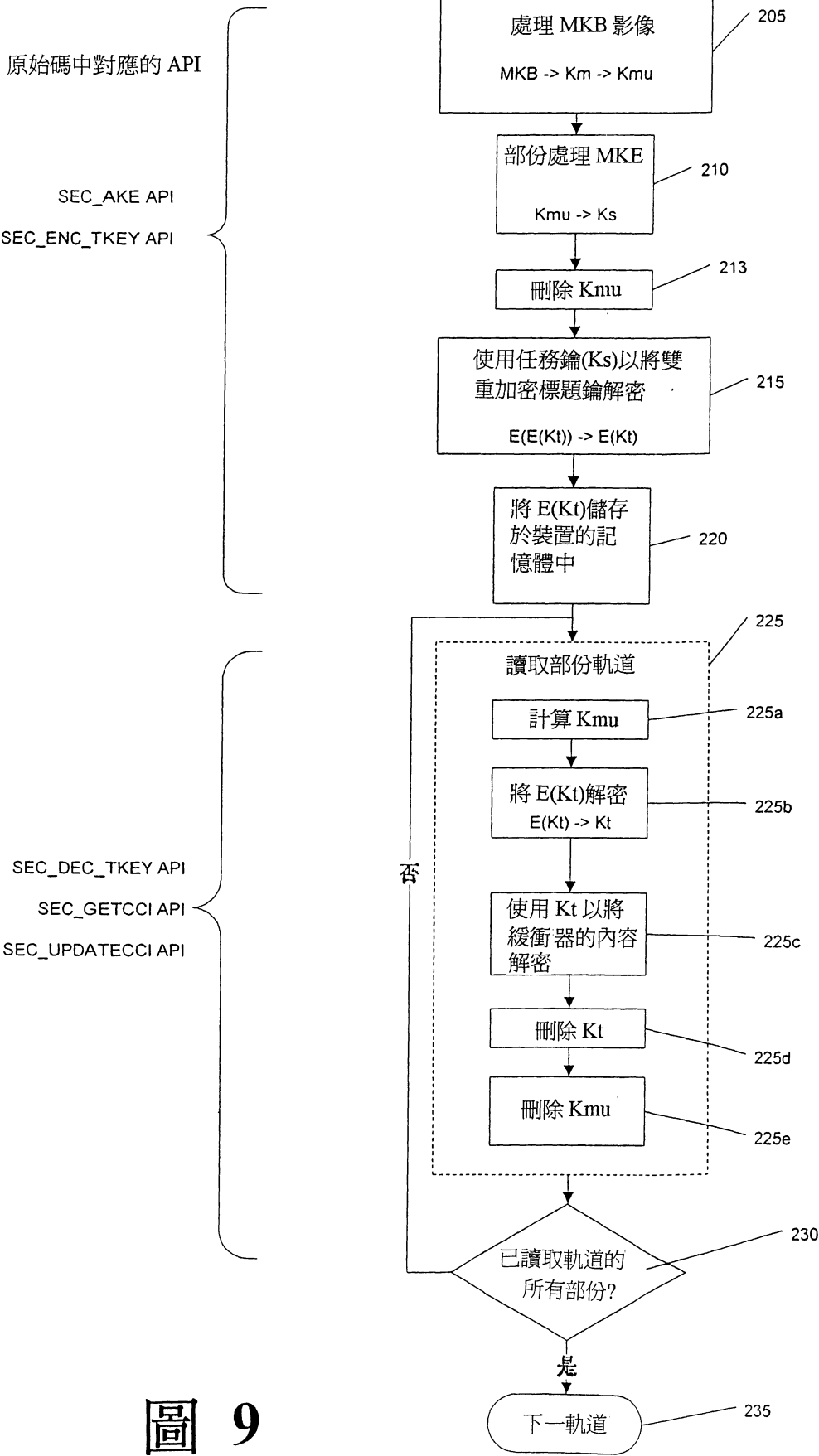


圖 9

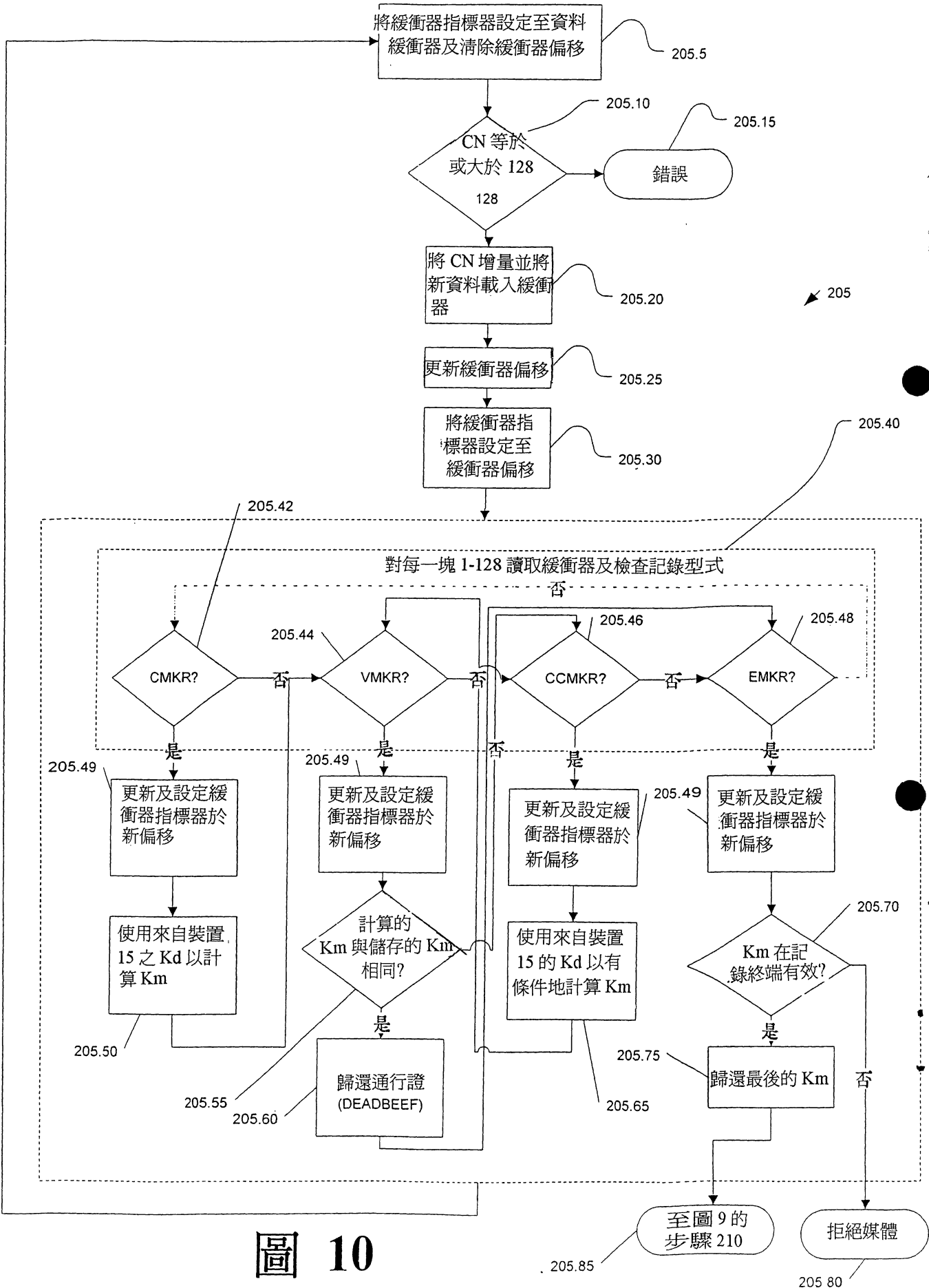


圖 10

六、申請專利範圍

附件 2A：第 90130438 號專利申請案
修正後無劃線之中文申請專利範圍替換本
民國 92 年 4 月 11 日呈

1. 一種具有軟體程式之電腦可讀取記錄媒體，用於裝置的原始設備製造商製造的音頻或視頻裝置中，該裝置係用於播放記憶卡中加密的音頻或視頻內容，該軟體程式配置成：

接收來自裝置的使用者介面之命令，該命令包含播放命令；

將來自記憶卡之加密的音頻或視頻內容解密，以致於原始設備製造商僅需傳送來自裝置的使用者介面之播放命令給該軟體程式且解密的音頻或視頻將會被播放。

2. 如申請專利範圍第 1 項之具有軟體程式之電腦可讀取記錄媒體，其中軟體程式又配置成：

將加密內容的位置資訊重製至音頻視頻裝置的記憶體中；

從音頻視頻裝置的記憶體中接取位置資訊；

找出具有接取位置資訊之記憶卡內的加密內容。

3. 如申請專利範圍第 1 項之具有軟體程式之電腦可讀取記錄媒體，其中，將音頻或視頻解密包括：

將一或更多加密鑰從記憶卡的保護區重製至裝置的記憶體緩衝器中；

將加密的音頻或視頻內容從記憶卡拷重製至裝置的記憶體緩衝器中；

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

六、申請專利範圍

將一或更多重製的加密鑰解密；

以一或更多解密鑰，將重製的加密音頻或視頻內容解密。

4．如申請專利範圍第3項之具有軟體程式之電腦可讀取記錄媒體，又包括音頻或視頻內容解密之後立即刪除一或更多解密鑰。

5．如申請專利範圍第4項之具有軟體程式之電腦可讀取記錄媒體，其中，在一或更多解密鑰被刪除之前，以一或更多解密鑰，將約小於一至十秒的內容一次解密。

6．如申請專利範圍第4項之具有軟體程式之電腦可讀取記錄媒體，其中，在一或更多解密鑰被刪除之前，以一或更多解密鑰，將約二秒的內容一次解密。

7．如申請專利範圍第1項之具有軟體程式之電腦可讀取記錄媒體，其中，將音頻或視頻內容解密，包括：

(a) 計算媒體專有鑰；接著

(b) 以媒體專有鑰，將儲存於裝置的記憶體中之標題鑰解密；接著

(c) 將框組解密；接著

(d) 刪除解密的標題鑰；

(e) 將媒體專有鑰刪除；及

(f) 重覆(a)至(e)，直到完成整個軌道為止。

8．一種具有微處理器、隨機存取記憶體及由微處理器執行的軟體之可攜式裝置，該裝置配置成：

接收來自可攜式裝置的使用者介面之命令組，該命令

裝

訂

線

六、申請專利範圍

組 包含播放命令；

於收到命令時，取還可移式儲存媒體中的加密資料；

將加密資料儲存於裝置的記憶體中；

將資料解密；及

輸出解密的音頻或視頻內容，以致於裝置僅需傳送來自對軟體程式的使用者介面之命令組中的命令，以便輸出解密的音頻或視頻內容。

9．如申請專利範圍第8項之可攜式裝置，其中約二秒的加密資料會儲存於裝置的記憶體中，且隨後在被刪除前被解密。

10．如申請專利範圍第8項之可攜式裝置，其中可移式儲存媒體係固態記憶卡。

11．如申請專利範圍第8項之可攜式裝置，其中可移式儲存媒體係光碟。

12．如申請專利範圍第8項之可攜式裝置，其中裝置的軟體又配置成以AAC、MP3或WMA格式解壓縮及解碼音頻內容。

13．如申請專利範圍第8項之可攜式裝置，其中裝置的軟體又配置成：

將播放清單資訊及軌道資訊從可移式儲存媒體重製至裝置的記憶體，及

根據裝置的記憶體內之播放清單及軌道資訊，尋找要取還的加密資料。

14．如申請專利範圍第13項之可攜式裝置，其中

六、申請專利範圍

軌道資訊包括下述以用於每一軌道：

由軌道所包含之音頻物件的數目；

由軌道所包含之第一音頻物件；

由軌道所包含之最後音頻物件；

正解密之目前音頻物件；

目前音頻物件之偏移。

15. 如申請專利範圍第14項之可攜式裝置，其中軌道資訊又包括：

以位元組計之軌道尺寸；

軌道的總播放時間；

軌道的消逝時間；

音頻物件內的目前元件號數；

要播放之軌道的目前元件；

目前元件的偏移；

音頻物件中元件的總數。

16. 一種以裝置播放儲存於安全媒體中加密的音頻或視頻內容之方法，該方法包括：

預先播放處理，包括：

將一或更多組關於待播放的軌道之資訊重製至裝置的記憶體中；

播放處理，包括：

從使用者介面接收一或更多命令以初始化播放；

從裝置的記憶體接取一或更多組資訊；

根據以重製至隨機存取記憶體之資訊中的一或更多組

六、申請專利範圍

資訊為基礎之順序，將加密內容從安全媒體重製至裝置的記憶體；

依據以該一或更多組資訊的資訊為基礎之順序，將來自安全媒體的加密資訊解密。

17. 如申請專利範圍第16項之方法，其中幾乎小於一至五秒的加密內容會一次被重製及解密。

18. 如申請專利範圍第16項之方法，其中一或更多組資訊包括播放清單及軌道資訊。

19. 如申請專利範圍第16項之方法，其中一或更多組資訊指定那一清單要播放、清單內那一軌道要播放。

20. 如申請專利範圍第19項之方法，其中該一或更多組資訊又包括軌道內那一音頻物件要播放、以及音頻物件位於安全媒體內的何處。

21. 如申請專利範圍第20項之方法，其中該一或更多組資訊又包括音頻物件內那一元件要播放、以及元件內那一框要播放。

22. 如申請專利範圍第16項之方法，其中該預先播放處理又包括授權該安全媒體。

23. 一種使可攜式裝置能夠接取記憶儲存裝置上的加密音樂之系統，包括：

一或更多應用程式介面，配置成：

接收來自可攜式裝置的使用者介面之多個命令；及

傳送命令給隔離的安全引擎，隔離的安全引擎配置成：

：

六、申請專利範圍

接收來自應用程式介面之命令；

將加密鑰及加密內容從記憶儲存裝置重製至可攜式裝置的

記憶體；

將鑰解密；

使用解密鑰，將內容解密；接著

刪除解密鑰。

24. 一種允許裝置以命令組容易地從記憶卡接取加密的資料之方法，該裝置具有處理器及隨機存取記憶體，該方法包括：

從記憶卡接收播放清單資訊及儲存資訊於裝置的隨機存取記憶體；

從記憶卡取還軌道資訊及將軌道資訊儲存於裝置的隨機存取記憶體中；

從裝置接收選自該命令組之命令，該命令從隨機存取記憶體接取播放清單資訊、及軌道資訊；

藉由取還儲存於記憶卡內的加密資料以執行該命令並根據該接取到的資訊以將資料解密。

25. 如申請專利範圍第24項之方法，其中播放清單資訊包括：

播放清單的名稱；

播放清單字串長度；

播放清單的播放時間；

播放清單所包括的軌道；及



六、申請專利範圍

對應於播放清單之索引。

26. 如申請專利範圍第24項之方法，其中軌道資訊包括：

軌道號數；

對應於軌道號數之索引；

軌道中的軌道單元數目；及

軌道的播放時間。

27. 如申請專利範圍第24項之方法，其中軌道資訊包括：

軌道的格式型式；

軌道的取樣頻率；

以位元組計的軌道尺寸；及

正解密之目前軌道。

28. 如申請專利範圍第27項之方法，其中一般軌道資訊又包括：

軌道所包括的音頻物件之數目；

軌道所包括的第一音頻物件；

軌道所包括的最後音頻物件；

正解密的目前音頻物件；及

目前音頻物件的偏移。

29. 如申請專利範圍第27項之方法，其中將資料解密包括：

將一或更多加密鍵從記憶卡的保護區重製至裝置的記憶體緩衝器；

六、申請專利範圍

將加密的音頻或視頻內容從記憶卡重製至裝置的記憶體緩衝器；

將一或更多重製的加密鑰解密；

以一或更多解密的鑰，將重製的加密音頻或視頻內容解密。

30．如申請專利範圍第27項之方法，其中將資料解密包括：

(a)計算媒體專有鑰；隨後

(b)以媒體專有鑰，將儲存於裝置的記憶體中之標題鑰解密；隨後

(c)將框組解密；隨後

(d)刪除解密的標題鑰；

(e)刪除媒體專有鑰；及

(f)重覆(a)至(e)直到整個軌道完成為止。

31．一種使得裝置能夠接取安全媒體上的內容之軟體系統，包括：

一或更多使用者介面模組，用於從裝置接收命令；

應用程式介面，用於從使用者介面模組接收命令及管理來自安全媒體之加密的及未加密的內容之取還和儲存；

安全引擎，用於將從安全媒體送至裝置的記憶體之加密的內容及加密的鑰解密，該解密的鑰用以將加密內容解密，及其中

一或更多軌道包含於第一加密資料區段中，及

加密內容包含於第二加密資料區段中，及

六、申請專利範圍

安全引擎會緩衝及解密部份第一資料區段、緩衝及解密第二資料區段、及接著在解密之前將解密的一或更多鑰刪除，以致於解密的鑰處於解密的狀態一段時間，該段時間係其用以解密小於一至約5秒的內容所耗費的時間。

3 2 . 如申請專利範圍第3 1 項之軟體系統，其中鑰處於解密的狀態一段時間，該段時間係其用以解密及處理約2秒的內容所耗費的時間。

3 3 . 如申請專利範圍第3 2 項之軟體系統，其中內容係以A A C、M P 3、或W M A格式編碼。

3 4 . 如申請專利範圍第3 1 項之軟體系統，其中被緩衝及解密之部份第一資料區段約5 1 2位元組。