

發明專利說明書

中文說明書替換頁(101年11月)15日

(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：097148609

※ 申請日期：97.12.12

※IPC 分類：G06F 12/00 (2006.01)

一、發明名稱：(中文/英文)

用於通用輸出入裝置之安全資料轉移應用之整合

INTEGRATION OF SECURE DATA TRANSFER APPLICATIONS FOR
GENERIC IO DEVICES

二、申請人：(共 1 人)

姓名或名稱：(中文/英文)

美商桑迪士克科技公司

SANDISK TECHNOLOGIES INC.

代表人：(中文/英文)

阿薩 勒 富斯泰科

LE FUSTEC, ASA

住居所或營業所地址：(中文/英文)

美國德克薩斯州布蘭諾市北達拉斯公園路6900號雙城中心

TWO LEGACY TOWN CENTER, 6900 NORTH DALLAS PARKWAY,

PLANO, TEXAS 75024, U.S.A.

國 籍：(中文/英文)

美國 U.S.A.

三、發明人：(共 7 人)

姓 名：(中文/英文)

1. 劉祥貞
LIU, XIAN JUN
2. 羅伯特 C 張
CHANG, ROBERT C.
3. 波 元
YUAN, PO
4. 王貞吉
WANG, JUNZHI
5. 羅 巴利列
BARZILAI, RON
6. 巴曼 卡瓦蜜
QAWAMI, BAHMAN
7. 法西德 沙貝特-沙爾西
SABET-SHARGHI, FARSHID

國 籍：(中文/英文)

1. 中華人民共和國 P.R.C.
2. 美國 U.S.A.
3. 美國 U.S.A.
4. 中華人民共和國 P.R.C.
5. 以色列 ISRAEL
6. 美國 U.S.A.
7. 美國 U.S.A.

四、聲明事項：

☐ 主張專利法第二十二條第二項 ☐ 第一款或 ☐ 第二款規定之事實，其事實發生日期為： 年 月 日。

☒ 申請前已向下列國家（地區）申請專利：

【格式請依：受理國家（地區）、申請日、申請案號 順序註記】

☒ 有主張專利法第二十七條第一項國際優先權：

1. 美國；2007年12月13日；11/956,042

2.

☐ 無主張專利法第二十七條第一項國際優先權：

1.

2.

☐ 主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號 順序註記】

☐ 主張專利法第三十條生物材料：

☐ 須寄存生物材料者：

國內生物材料 【格式請依：寄存機構、日期、號碼 順序註記】

國外生物材料 【格式請依：寄存國家、機構、日期、號碼 順序註記】

☐ 不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。

五、中文發明摘要：

本發明提出用於自一主持數位器具向一可攜式媒體發送一應用指令之技術，其中該指令被構造為一或多個其大小為一第一大小或若干位元組之單元。在沖洗一快取之內容之後，將該指令寫入至該快取，其中該快取被構造為邏輯塊，該等邏輯塊具有一係一大於(就位元組數目而言)該第一大小之第二大小之大小。在寫入該指令(具有一命令部分且可能具有一資料部分)時，將該指令之開始與該快取中之邏輯塊邊界中之一者對準，且藉由虛擬資料填滿該指令，使得其填充一整數數目之快取塊。當在一主持數位器具處接收來自一可攜式裝置之對一指令之一回應時，在接收該回應之前以類似之方式沖洗該快取。然後，儲存該回應以與該快取之一邏輯塊邊界對準。

六、英文發明摘要：

Techniques are presented for sending an application instruction from a hosting digital appliance to a portable medium, where the instruction is structured as one or more units whose size is a first size, or number of bytes. After flushing the contents of a cache, the instruction is written to the cache, where the cache is structured as logical blocks having a size that is a second size that is larger (in terms of number of bytes) than the first size. In writing the instruction (having a command part and, possibly, a data part), the start of the instruction is aligned with one of the logical block boundaries in the cache and the instruction is padded out with dummy data so that it fills an integral number of the cache blocks. When a response from a portable device to an instruction is received at a hosting digital appliance, the cache is similarly flushed prior to receiving the response. The response is then stored to align with a logical block boundary of the cache.

七、指定代表圖：

(一)本案指定代表圖為：第 (1) 圖。

(二)本代表圖之元件符號簡單說明：

(無元件符號說明)

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

(無)

九、發明說明：

【發明所屬之技術領域】

本發明一般而言係關於一起使用可攜式媒體(例如一安全記憶體卡)與數位器具(例如一電話手機)之領域；且更特定而言係關於用於在一數位器具與一與該數位器具通信之可攜式媒體之間轉移指令之技術。

【先前技術】

諸如筆記型或膝上型電腦、個人數位助理(PDA)或行動電話等數位器具通常與可攜式媒體(例如記憶體卡或USB驅動)一起使用。於某些情形中，安全資料係儲存於此等可攜式媒體上。負責在主持器具與媒體之間安全轉移此資料之應用經常使用具有一特定結構之指令。作為轉移過程之部分，主機可快取該指令；但由於該主機之作業系統可能不知曉該指令之結構，且因該主機之快取結構可能不與該指令之結構相容，因此可能無法成功轉移該指令連同任何相關聯資料。

【發明內容】

根據一個態樣，提供用於自一主持數位器具向一可攜式媒體發送一應用指令之技術，其中該指令被構造為一或多個其大小為一第一大小或若干位元組之單元。在沖洗一快取之內容之後，將該指令寫入至該快取，其中該快取被構造為邏輯塊，該等邏輯塊具有一係一大於(按照位元組數目)該第一大小之第二大小之大小。在寫入該指令(其具有一命令部分且可能具有一資料部分)時，將該指令之開始

與該快取中之邏輯塊邊界中之一者對準且藉由虛擬資料填滿該指令，使得其填充一整數數目之快取塊。

根據另一態樣，當在一主持數位器具處接收來自一可攜式裝置之對一指令之一回應時，在接收該回應之前以類似之方式沖洗該快取。然後儲存該回應以與該快取之一邏輯塊邊界對準。

本發明之各種態樣、優點、特徵及實施例包含於下文對本發明實例性實例之闡述中，應結合附圖來閱讀該闡述。本文所提及之所有專利、專利申請案、論文、其他公開案、文檔及物項之全部內容均以引用方式併入本文中以用於所有目的。至於所併入之公開案、文檔或物項中之任一者與本申請案之間之術語之定義或使用中之任何不一致或衝突，應以本申請案之定義或使用為準。

【實施方式】

引言

當在一可攜式媒體(例如一記憶體卡)與一主持數位器具(例如行動電話手機)之間轉移內容時，一主機之作業系統將經常針對該內容使用一快取機制。此快取通常將具有一結構，在該結構中該快取在邏輯上被分割為具有一特定大小之多個塊。被轉移之內容(無論係資料或一指令(一命令，且可能係某些相關聯之資料))亦可以一特定方式構造為一或多個具有某一大小之區段。當該內容係呈具有一個大小之單元(舉例而言，如512位元組之區段)之結構且該快取被構造為具有另一大小之單元(舉例而言，呈2 KB之塊)

時，該快取機制可與該內容之結構性要求抵觸。

此在應對安全內容及安全可攜式儲存媒體(例如以名稱 TrustedFlash 出售之可攜式儲存媒體)之情形中尤其正確。於此等情形中，處置主機與可攜式媒體之間之轉移之一主機作業系統之較基礎位準將把指令視作僅如此多之資料，而不知曉任何嵌入該指令中之命令，且如此將該指令儲存於快取中。美國專利第 7,237,046 號及美國專利申請案第 10/899,260 號且尤其美國專利申請案第 11/298,349 號及第 11/299,186 號中闡述了此等指令之實例及其使用。在此等配置下，主機之作業系統可將指令視作欲被寫入至媒體上之一特定位址之資料；但當在媒體上接收時，此指令將被解釋為(舉例而言)用以在該媒體上之不同位址處儲存資料之一寫入命令。若該主機然後試圖針對此資料發出一讀取命令，則如該主機之作業系統所見之位址將不對應於如在該媒體上所解釋之實際位址；且由於該主機然後可依賴被認為是資料之快取複本，因此其將錯誤地使用此所快取之資料。

本文所闡述之技術廣泛適用於主要與一主持數位器具一起使用之可攜式媒體(例如記憶體卡)及其自身包含非揮發性記憶體(例如嵌入式快閃)之數位器具兩者。此等數位器具之實例包含桌上型、筆記型或膝上型平板電腦、個人數位助理(PDA)、行動電話手機、各種媒體播放器(例如 MP3 播放器、DVD 播放器)、遊戲控制臺、數位記錄裝置(例如數位相機)及其他。可自本發明之受讓人 SanDisk 公司購得

適合之可攜式媒體，其中包含以商品名稱TrustedFlash、CompactFlash (CF)、Multi-Media Card(MMC)、Secure Digital (SD)MicroSD及Memory Stick PRO出售之可攜式媒體。此等記憶體卡可經由對大多數卡而言不同之配合連接器以可移除之方式與數位器具連接。快閃驅動(如以商品名稱Cruzer出售之彼等快閃驅動出售之快閃驅動)含有一根據通用串行匯流排(USB)標準之插頭，因此可被直接插入至具有一USB插座之任何數位器具中。TrustedFlash卡及其他安全卡(SIM、SMMC、SD等)允許安全儲存許可證及相關聯之內容兩者。以下論述亦將經常參考諸如快閃等非揮發性記憶體，但本文所給出之技術並不受此限制且更一般而言適用於用於可攜式裝置及嵌入式記憶體兩者之其他非揮發性記憶體結構(舉例而言，例如美國專利申請案10/841,379所闡述)。儘管本文所給出之教示並不受此限制，但當出於論述之目的而參考一特定實施例時，下文將經常參考一與一記憶體卡(例如TrustedFlash種類之記憶體卡)一起使用之行動電話手機之具體實例，該記憶體卡具有其結構係基於一區段之指令。

為避免主機快取之此等可能性困難，可將與安全轉移相關聯之軟體改變為知曉運行時間命令大小；相關聯之應用工具箱需要與應用整合；自應用向平臺作業系統(OS)發送之指令(其中包含寫入及讀取命令)以一快取塊大小對準之區段開始；且該寫入、讀取緩衝器大小應係快取塊大小對準。

在技術上，為允許自安全內容媒體至數位器具使用者之快速傳播，用於此等平臺與對應安全內容工具箱之整合係重要。由於大多數安全內容技術及程式碼大小之特殊要求考量，對應之應用工具箱通常需要被整合至一手機或其他主持裝置之作業系統(OS)中，使得該等應用可調用由該工具箱提供之應用程式化介面(API)來存取媒體。然而，對於某些標準化或開放平臺(比如Linux及WIPI)，實施此解決方案可相當複雜，此乃因不容易具有支援安全內容媒體所需之平臺修改。

為克服此限制，每一平臺將提供應用存取通用IO裝置之一方式；倘若係一TrustedFlash卡，則此係SD IO裝置。在此假定之情形中，該等應用可藉由將對應工具箱整合至該等應用中來使用所提供之IO存取與安全內容媒體通信。只要該IO裝置對應用而言可存取，則此可用於任何平臺，尤其係有益於彼等未經修改之平臺。此解決方案之主要困難係應對最可能用於每一平臺之快取機制。以下部分闡述此快取機制之性質及其經緩衝IO與較早版本之安全內容轉移韌體之間的衝突。

具有當前安全轉移韌體之經緩衝IO之問題

如上所述，諸多命令及資料轉移過程依賴於指令之一特定結構。舉例而言，當前的TrustedFlash韌體係經界定以經由基於區段(512位元組)之指令來與手機或其他主機通信。每一指令之區段數目係經預定。此對於僅具有經緩衝IO之平臺可導致一主要IO問題。由於主持平臺之快取機

制，發送至媒體上之TrustedFlash韌體之指令可不基於區段，以致破壞TrustedFlash通信頻道。舉例而言，一TrustedFlash CREATE ACR命令係一單區段寫入指令。當一應用向平臺OS發送一單區段寫入時，可將此寫入命令改變為一具有多個區段之寫入命令，且在此命令到達媒體上之安全轉移韌體之後，亦可改變開始寫入位置。

以下係寫入命令之一常見情景：

- 應用要求在第m個區段位置上向裝置寫入n個區段。
- OS將檢查快取以尋找相關記憶體位置；若其不存在，則OS將自卡(包含所需要之位置)上之一位置讀取資料，且然後將其儲存於該快取上。
- 該OS將更新相關區段。
- 該OS可以或可不立刻將資料沖洗回至該卡。

圖1係一闡述如主機所見之寫入命令之此常見行為之流程圖。應再次注意，儘管應用可將指令視作一至作業系統之可能具有附接之資料之命令，但僅將其解釋為資料。

圖1在101處以應用要求向裝置寫入開始。在103處檢查快取以確定一相關位置是否已存在於該快取中；若存在("Y"路徑)，則在105處將資料寫入至該快取之相關位置。若未發現一相關快取位置(出自103之"N"路徑)，則然後在107處確定n(欲寫入之區段數目)是否係快取塊大小對準及m(用於該寫入之位置)是否係快取塊大小對準，且若如此，則該過程再次去往105。出自107之NO路徑通向109，在109處按照需要調整開始寫入位置或緩衝器大小緩衝

器。舉例而言，以其中快取塊之大小為2 KB且主持應用發送具有總共 $n=5$ 個區段且其開始於第七區段($m=7$)之指令資料之情形為例。該主機會將該開始改變為始於第五區段且將資料之總區段改變為8個。在去往105之前，109然後繼續去往111，在111處自裝置讀取與快取塊大小對準之相關資料。最後，若被迫，則OS可立刻將該資料沖洗回至該卡。作為此快取機制之結果，TrustedFlash韌體可能不能夠理解自該等應用發送之任何命令。

在實踐中，某些平臺支援直接IO，而其他平臺僅提供經緩衝之IO。另外，快取演算法可因各平臺而異。因此，一通用解決方案相當較佳地用於與安全轉移應用之工具箱之整合。以下論述基於TrustedFlash之實例提供此一經整合之解決方案，無論主機平臺使用直接IO或經緩衝IO，該解決方案均起作用。下文將此解決方案提供為包含四個組成部分：系統整合之結構；韌體之修改；及解決用於寫入及用於讀取之快取之方法。

將安全轉移工具箱整合至應用中

由於一平臺保持不變以用於應用存取安全內容卡，因此對應之工具箱將需要整合至主機應用中，使得該等主機應用可調用工具箱API向TrustedFlash卡發送(比如)TrustedFlash命令。簡言之，該工具箱提供供應用存取安全媒體之完整API封包。此封包提供與安全系統相關之諸多功能，例如系統作業、帳戶作業、儲存作業及數位權利管理(DRM)作業。

該等應用將直接調用工具箱之API，且然後該工具箱將藉由使用平臺OS所提供之裝置作業方法來與對應之安全媒體通話。舉例而言，在Linux中，此方法係打開()、讀取()、寫入()及關閉()。根據每一個別平臺，於平臺I/O裝置作業中實施工具箱與平臺之間之此膠層。

圖2給出該結構之一方塊圖。在主機側上，所顯示之層在頂部包含各種客戶應用201，其下係平臺之作業系統及檔案系統203，且然後係用於與可攜式媒體250通信之平臺塊裝置驅動器205。因此，工具箱207將位於客戶應用層201與作業系統及檔案系統層之間。如圖2中所示，元件中可包含於工具箱中之元件係：數位權利管理(DRM)、資料保護、客戶API、儲存、帳戶、系統及效用塊，以及安全管理器、安全檔案系統、協定驅動器及平臺I/O裝置作業子層。

安全韌體之修改

如上文所論述，安全資料協定中所使用之指令經常基於具有一特定數目之位元之單元。舉例而言，用於在一主機與媒體上之TrustedFlash韌體之間通信之TrustedFlash指令係基於區段。在韌體載入期間預定每一指令之區段數目。圖3及圖4之表格顯示如在TrustedFlash說明書中找到之TrustedFlash命令結構。

如圖3中所示且如美國專利申請案第11/298,349號及第11/299,186號中所展示，實例性指令由一保持命令之第一區段(512位元組)組成。此命令塊後跟任何相關聯之資料區

段，其同樣構造為區段。舉例而言，一用於資料之N個區段之寫入指令將由N+1個區段組成，其中一第一區段用於後跟資料區段之寫入命令。對於無資料之命令(例如一狀態請求)，將僅係該命令塊之一個區段。諸如一讀取命令之資料等任何回應將由以下最後部分之讀取過程處理。圖4之表格圖解闡釋TrustedFlash協定中之實例性命令塊結構之某些細節。

圖5示意性圖解闡釋在一基於一第一大小之單元之指令被寫入至一基於一不同大小之邏輯塊之快取中時在先前技術配置下可發生之未對準類別。對於此實例，指令501被認為係由5個區段大小之單元構成，其中第一區段501a係命令部分且存在相關聯資料之四個區段501b。快取503係按照2 KB(或更精確地係2048位元組)塊之結構。(情形將通常係：快取中所使用塊之大小將係一標準區段之某一倍數。)若無下文所論述之配置類別，則可在如圖5中所示之快取中之一任意位置處快取該指令，同時伴有上述所得問題。

為使媒體韌體理解來自具有經緩衝IO之平臺之命令，當前韌體較佳知曉每一命令之動態命令大小。為完成此，可引入一個欄位以添加至該命令塊中以規定當前發送命令之總大小。舉例而言，在圖4之表格中，可將一用於虛擬區段計數之新欄位添加至開始於位元組36之命令區段之第二部分中。預定之命令長度將被視作預設值，且此欄位將在運行時間中告知此命令之實際大小。若此欄位係0，則將

使用該等預設值。

當一平臺OS正在使用經緩衝IO時，可如下文所述改變讀取及寫入兩者之行為。以下兩個部分闡述應對關於寫入(當向媒體發送一指令時)及讀取(當返回一回應時)之快取之方式。簡言之，圖6中圖解闡釋了此過程，其與圖5編號類似，除了如圖6中所示該指令現在與該快取中之一邏輯塊邊界對準且然後如陰影線區607所示填滿任何被部分地填充之快取塊。

用於經緩衝IO之直接寫入命令之方法

安全轉移韌體係媒體(例如TrustedFlash)卡內用以處置命令之代理。較佳地將來自主機之安全轉移命令立即發送至該卡。因此，若平臺OS不向該卡發送一寫入命令卻改為將資料放入緩衝器中，則媒體將無法取得該命令及回應於該命令。另外，對於藉由被要求在一特定位置處之命令塊(如藉由必須係整個命令之第一區段之TrustedFlash命令塊)構造之指令，寫入命令之序列必須遵循適當(例如TrustedFlash)協定；在命令完成之前之命令序列中之任何額外讀取或寫入(包含取得命令狀態)將導致韌體之問題，使得該命令將不會成功。下文係逐個解決此等問題之方法。

以下係迫使OS沖洗寫入命令之方法：

- 關閉裝置
- 重新打開該裝置

某些平臺可提供一用於寫入之沖洗功能，於此情形中可使

用對應之命令。在缺乏此一命令之其他情形中或在沖洗可能不起作用時，可在邏輯上關閉並重新打開媒體。為確保該寫入命令被沖洗至卡中，關閉-重新打開總是起作用。

一般而言，當將一卡插入至主機時，該主機將初始化並安裝媒體/卡。為存取該媒體之內容，其將打開該媒體。其被認為係"邏輯"打開。建立相關資料、表格、快取等等。在此之後，你可瀏覽目錄或打開"檔案"以用於讀取/寫入作業。藉由"關閉"該媒體，所有快取內容、表格或資料被清除或失效。舉例而言，Linux作業系統包含一打開()命令及一關閉()命令。該關閉()命令關閉該媒體之一檔案描述符，使得其不再指代任何檔案且可使用。移除該檔案描述符上所保持之任何與該過程相關聯並涵屬於該過程之記錄鎖定。為在邏輯上重新打開該裝置，一打開()調用將產生一新打開檔案描述。 (Linux程式員手冊中進一步闡述此等情形。)

另一問題係寫入位置、寫入緩衝器大小及命令序列之潛在改變。為避免此等改變，工具箱將以以下方式向媒體發送一命令：

- 知曉特定平臺之快取塊大小
- 設定寫入命令之開始區段與快取塊大小對準
- 使緩衝器與該快取塊大小對準，從而給出發送命令之正確大小。

藉此方式，由於一切事物均係快取塊大小對準，因此OS不需要調整此寫入命令，且由於該緩衝器大小係塊大小對

準，因此OS不需要自卡讀取資料。因此，來自主機之寫入命令將不會被修改。若一平臺支援直接IO，則此方法藉由簡單地將塊大小設定為512位元組而仍可適用。

圖7之流程圖闡述寫入命令之此方法。該流程在701處以媒體之原始狀態係打開而開始。然後，在703處藉由在邏輯上關閉該裝置且然後將其重新打開來沖洗快取。另一選擇係，若作業系統具有一用以沖洗快取之特定命令，則可改為使用該特定命令。

然後，在塊705處將指令放置於該經沖洗之快取中。如圖6中所示，儲存指令601(包含命令塊601a且在此實例中四個資料區段)，使得其與快取603中之一邏輯邊界對準。若此使任何快取塊僅部分地被填充，則填滿此等快取塊以將該指令維持為該快取中一整數數目之邏輯塊。在此實例中，由於該快取中之每一邏輯塊可保持4個區段且該指令具有5個區段，因此當連續地快取該指令時，該指令之最後區段僅佔用一快取塊之部分。607處之陰影線代表所添加之充填，使得主機之作業系統認為該指令係由完整快取塊形成且如此對待該指令。

返回至圖7，如塊705中所示，此過程可包含命令塊由實際指令或命令之總大小填充且讀取回與快取之邏輯塊大小對準之開始區段。然後填充資料，其中包含用以填滿一完整快取塊之任何虛擬區段。然後可檢查開始寫入區段以確認該指令之塊對準。在塊707處，然後可將用以向媒體發送此指令之寫入命令發送至平臺之作業系統，在該作業系

統處寫入過程現在將以與快取之塊邊界及大小對準之邏輯塊位址(LBA)開始。

應對用於IO讀取之快取之方法

自主機接收一指令之後，媒體可能需要回應該主機，例如藉由一狀態或藉由資料回應於一讀取請求。由於快取，無論應用何時發送一讀取命令，若相關位置資料係在快取中，則OS可僅去往該快取以讀取回該資料。因此，不將實際韌體回應返回至該應用。

為應對此問題，可以以下方式使用快取旁路：

- 每一 TrustedFalsh 命令之讀取相關開始邏輯塊位址(LBA)針對每一讀取改變。

- 兩個讀取命令之間之開始讀取LBA之差應大於快取塊大小。

- 開始讀取LBA應與快取塊大小對準。

- 關閉並重新打開裝置以確保OS針對應用沖洗讀取。

若一平臺支援直接IO，則此方法藉由簡單地將快取塊大小設定為512位元組而仍可適用。圖8之流程圖闡述讀取命令之此方法。

圖8顯示一用於允許媒體回應於一來自主機之指令之實例性實施例。通常而言，此讀取過程將緊跟上一部分中所闡述之寫入過程，其中無其他命令被插入該寫入指令與該讀取命令之間。在塊801處，該流程再次以原始裝置狀態係打開而開始。

在803處，如在703處以一關閉及然後打開沖洗快取，或

若可用，則以一命令沖洗該快取。由於該快取現在係空白，此防止作業系統僅返回所快取之材料而不是來自媒體之實際回應。在805處，檢查對準以明瞭當將所接收之回應放置於該快取中時，該回應將與該快取之邏輯塊結構對準。最後，將讀取命令發送至平臺之作業系統。

一旦已做了此等準備，驅動器然後可將讀取指令發送至媒體，該媒體然後將返回回應。如上所述，此可包含實際安全使用者資料(即，如所見之係安全轉移系統之資料)或一諸如一狀態等非資料回應。然後快取與快取之邏輯塊邊界對準之回應。亦可添加然後安全轉移應用將忽略之充填以填滿一整數數目之快取塊。

儘管本文已參考特定實施例闡述了本發明，但該闡述僅係本發明之應用之一實例且不應被視作一限制。因此，所揭示實施例之特徵之各種修正及組合歸屬於以下申請專利範圍所涵蓋之本發明之範圍內。

【圖式簡單說明】

可藉由查閱以下圖式來更好地理解本發明之各種態樣及特徵，圖式中：

圖1係一用於一藉由快取之寫入過程之共同序列之一流程圖；

圖2係一應用系統圖；

圖3顯示一命令結構之一實例；

圖4係一顯示一命令結構之一實例之表格；

圖5圖解闡釋一指令之快取，例如圖3中所示，其中該指

令不與一快取邊界對齊；

圖6圖解闡釋一指令之快取，例如圖3中所示，其中該指令與一快取邊界對準且被填滿；

圖7圖解闡釋一將一指令放置於快取中之方法；及

圖8圖解闡釋一將一回應放置於主機之快取中之方法。

【主要元件符號說明】

201	客戶應用
203	作業系統及檔案系統
205	塊裝置驅動器
207	工具箱
250	可攜式媒體
501	指令
501a	區段
501b	區段
503	快取
601	指令
601a	命令塊
603	快取
607	陰影線區

十、申請專利範圍：

1. 一種自一主持數位器具向與其連接之一可拆離(detachable)之非揮發性記憶體系統發送一應用指令之方法，該非揮發性記憶體系統包括一或多個非揮發性記憶體電路及待由其執行該應用指令之一控制器電路，其中該應用指令係經構造為一或多個其大小係一第一數目之位元組之單元，該方法包括：

沖洗(flushing)該主持數位器具上之一快取之內容；

隨後將該應用指令寫入至該主持數位器具上之該快取，其中該主持數位器具上之該快取係經構造為複數個其大小係一第二數目之位元組之邏輯塊，該第二數目係大於該第一數目，該寫入包含：

將該應用指令之開始與該等邏輯塊之一邊界對準；及

藉由虛擬資料充填該應用指令以具有一係該第二數目之位元組之一整數倍數之大小；及

隨後自該主持數位器具上之該快取將應用指令發送
至該非揮發性之記憶體系統。

2. 如請求項1之方法，其中該第二數目係該第一數目之一整數倍數。
3. 如請求項1之方法，其中該等單元之該大小係一區段。
4. 如請求項1之方法，其中該應用指令包含一命令部分及資料部分。
5. 如請求項4之方法，其中該命令係一用於將該資料部分儲存於該非揮發性記憶體系統中之寫入命令。

6. 如請求項4之方法，其中該命令部分在大小上係該等單元中之一者且該資料部分在大小上係該等單元中之一或多者。
7. 如請求項1之方法，其中該應用指令不包含一資料部分。
8. 如請求項7之方法，其中該應用指令包括一讀取資料命令。
9. 如請求項8之方法，其進一步包括：

回應於該應用指令，將來自該非揮發性記憶體系統之資料返回至該主持數位器具。
10. 如請求項9之方法，其進一步包括：

將該所返回之資料儲存於該主持數位器具上之該快取中，包含將該資料之開始與該等邏輯塊之一邊界對準。
11. 如請求項7之方法，其進一步包括：

將一對該應用指令之回應儲存於該主持數位器具上之該快取中，其中對該應用指令之該回應係經構造為一或多個其大小係該第一數目之位元組之單元且該儲存包含將該回應之開始與該等邏輯塊之一邊界對準。
12. 如請求項1之方法，其中沖洗該主持數位器具上之該快取之該等內容包括：

由該主持數位器具關閉該非揮發性記憶體系統；及
隨後由該主持數位器具打開該非揮發性記憶體系統。
13. 一種在一主持數位器具處接收對於該主持數位器具所發出之一應用指令之一回應之方法，該回應係來自與該主

持數位器具連接之一可拆離之非揮發性記憶體系統之一控制器電路，其中該非揮發性記憶體系統包括一或多個非揮發性記憶體電路及該控制器電路，且其中該回應係經構造為一或多個其大小係一第一數目之位元組之單元，該方法包括：

自該主持數位器具向該非揮發性記憶體系統發出該應用指令；

沖洗該主持數位器具上之一快取之內容，其中該主持數位器具上之該快取係經構造為複數個其大小係一第二數目之位元組之邏輯塊，該第二數目係大於該第一數目；

隨後接收來自該控制器電路對該主持數位器具上之該應用指令之該回應；及

將來自該控制器電路之該回應儲存於該主持數位器具上之該快取中，該儲存包含：

將該回應之開始與該等邏輯塊之一邊界對準。

14. 如請求項13之方法，其中該第二數目係該第一數目之一整數倍數。

15. 如請求項13之方法，其中該儲存進一步包含：

藉由虛擬資料充填該回應以具有一係該第二數目之位元組之一整數倍數之大小。

16. 如請求項13之方法，其中該應用指令包含一讀取命令且該回應包含資料。

17. 如請求項13之方法，其中該回應係一狀態。

18. 如請求項13之方法，其中沖洗該主持數位器具上之該快
取之該等內容包括：

由該主持數位器具關閉該非揮發性記憶體系統；及

隨後由該主持數位器具打開該非揮發性記憶體系統。

19. 如請求項13之方法，其中該等單元之該大小係一區段。

十一、圖式：

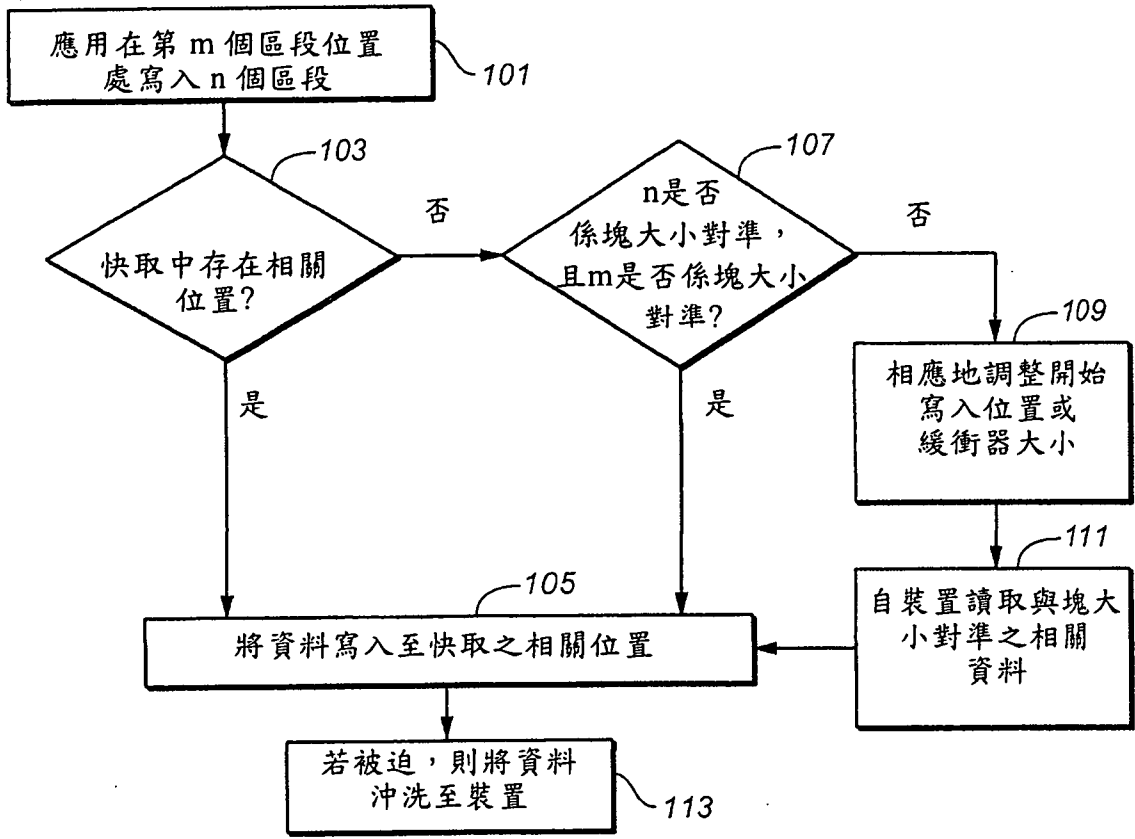


圖1

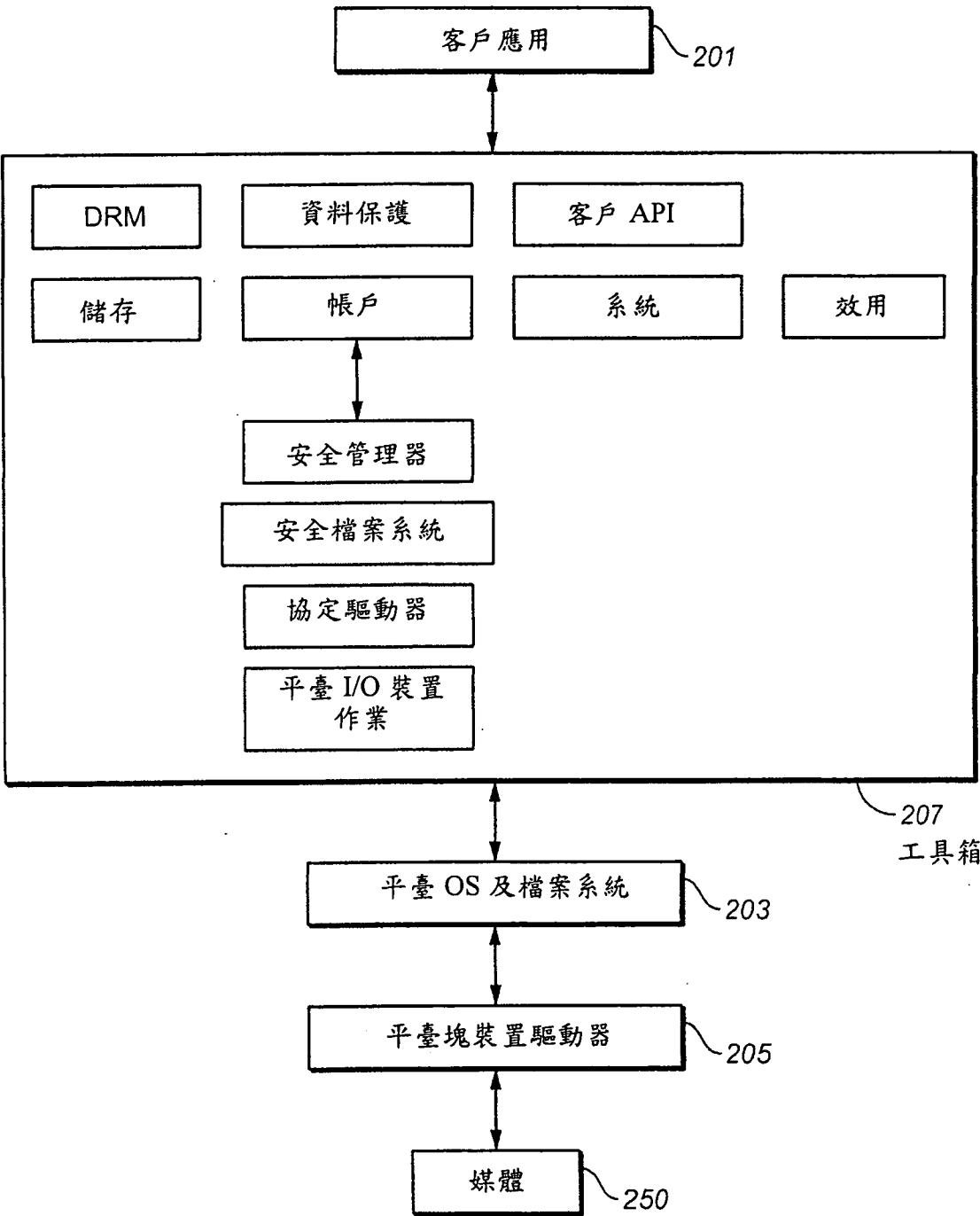


圖2

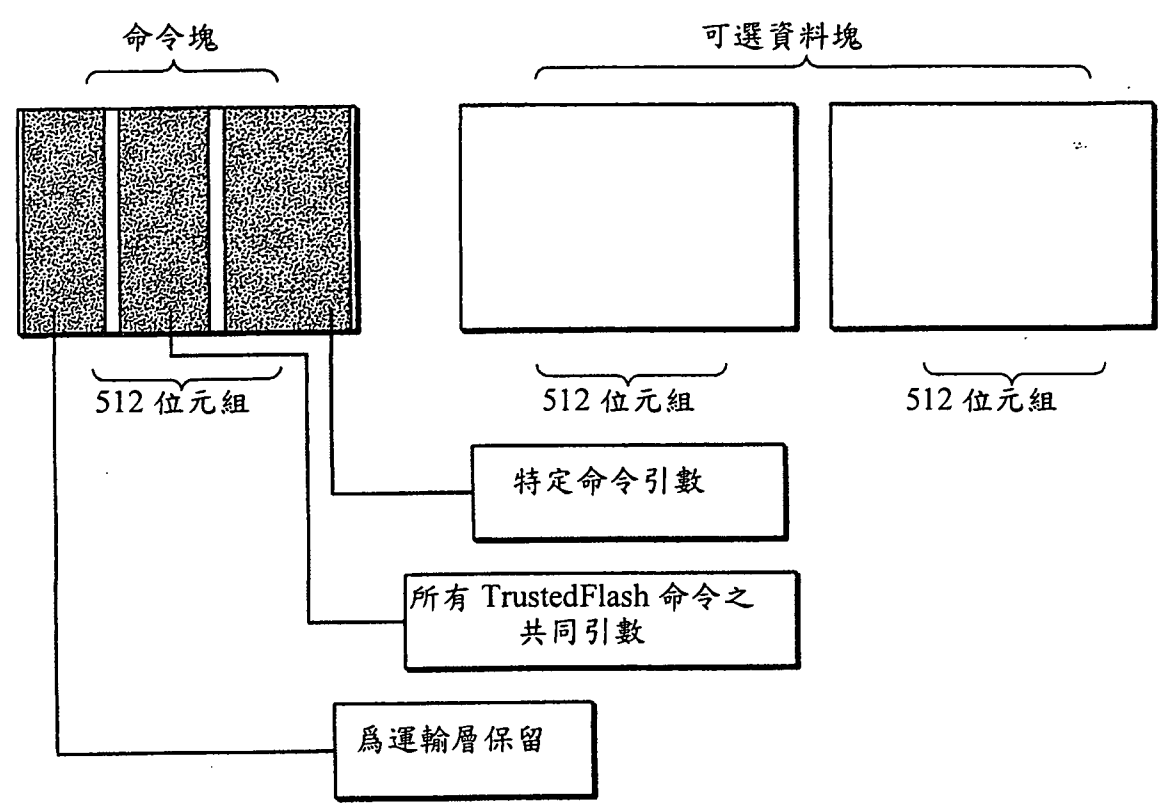


圖 3

位元組 偏移量	引數 長度	引數名稱	引數類型	註解
0-35	36	為卡運輸層保留	未界定	
36	40	所有 TrustedFlash 命令 之共同引數		此區段係為 TrustedFlash 安全 程序、版本控制及其他共同引 數保留(可包含用於虛擬區段 計數之欄位)
76	436	命令特定引數		根據不同命令功能度, 特定引 數區段用於特定命令

圖 4

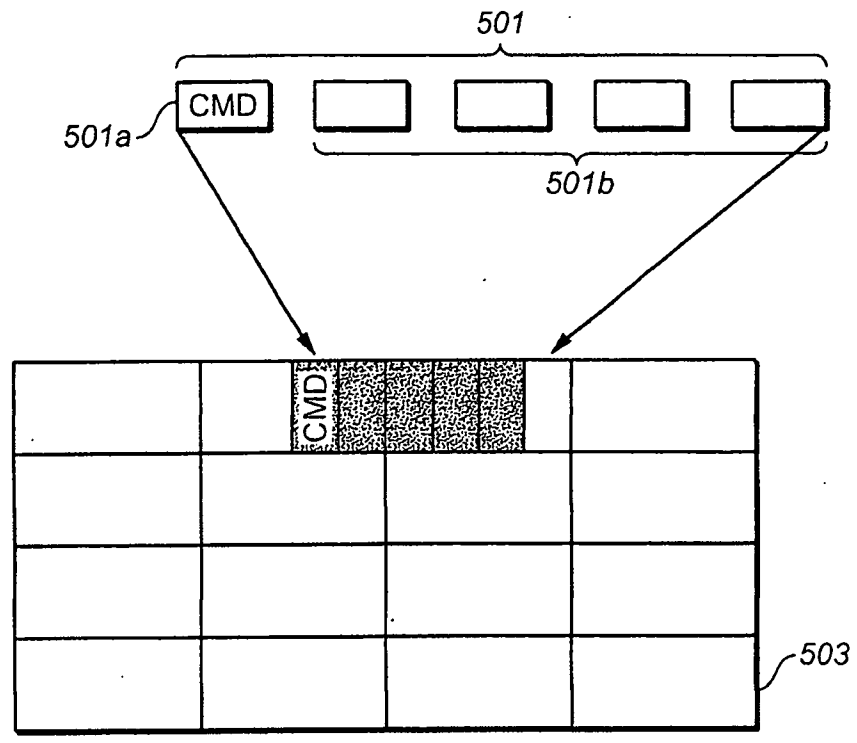


圖 5

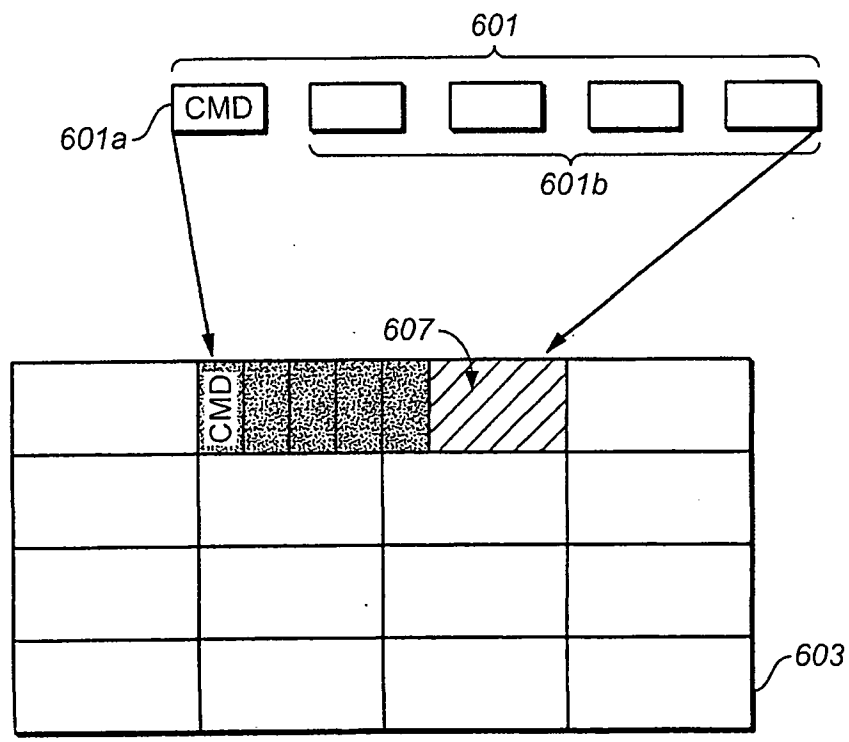


圖 6

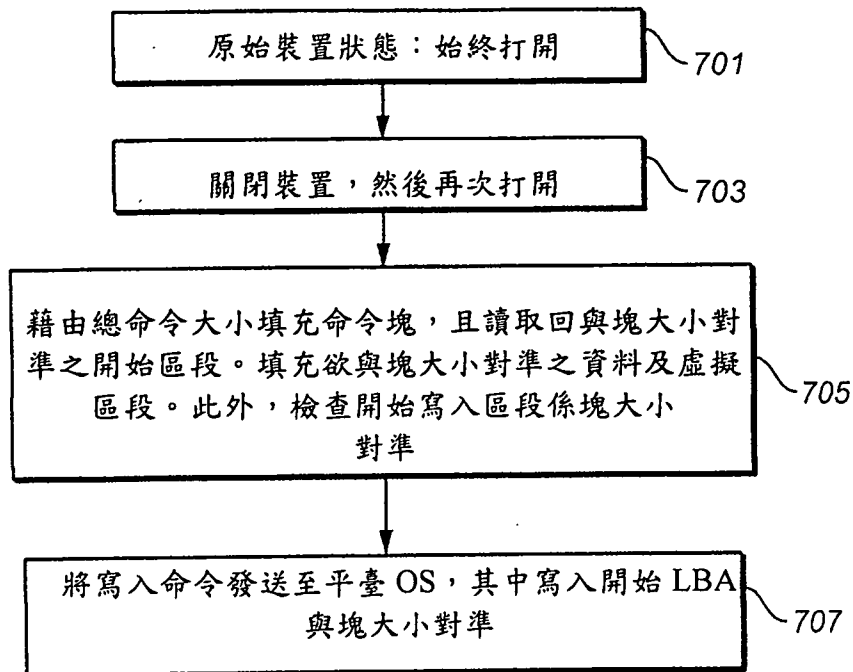


圖 7

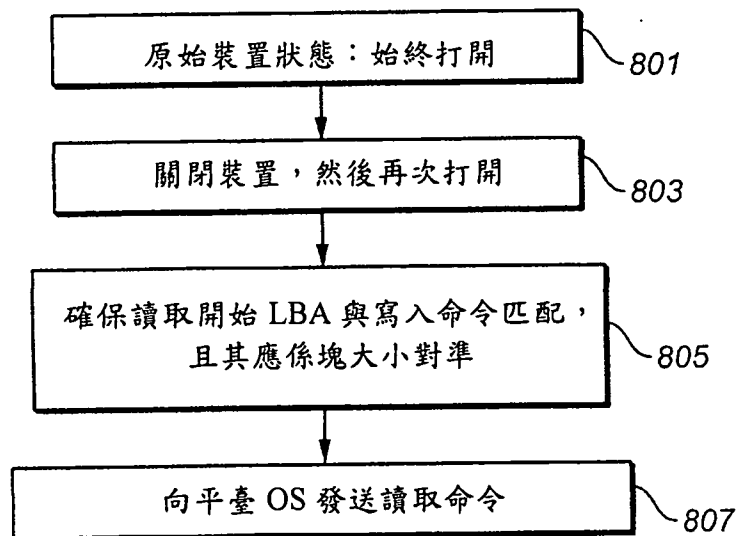


圖 8