



(19)中華民國智慧財產局

(12)發明說明書公開本 (11)公開編號：TW 201025005 A1

(43)公開日：中華民國 99 (2010) 年 07 月 01 日

(21)申請案號：097151562 (22)申請日：中華民國 97 (2008) 年 12 月 31 日

(51)Int. Cl. : **G06F12/14 (2006.01)**

(71)申請人：合智電子股份有限公司 (中華民國) (TW)
臺北縣中和市中正路 700 號 17 樓之 3

(72)發明人：鄭智文 (TW)

(74)代理人：王雲平；莊志強

申請實體審查：有 申請專利範圍項數：23 項 圖式數：6 共 25 頁

(54)名稱

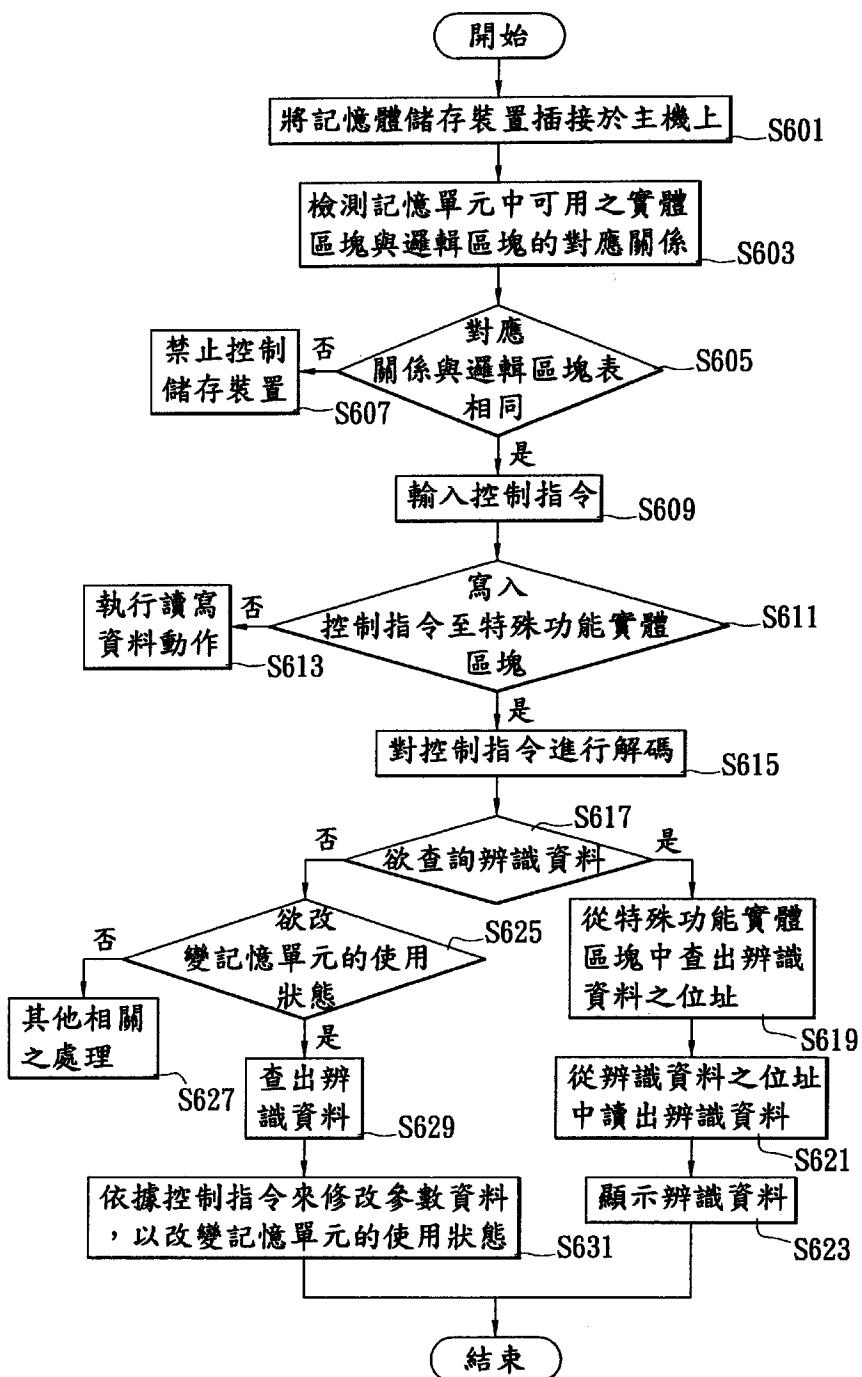
記憶體儲存裝置之辨識方法

RECOGNIZING METHOD OF MEMORY STORAGE DEVICE

(57)摘要

一種記憶體儲存裝置之辨識方法，此記憶體儲存裝置具有一記憶單元，其由連續之複數個實體區塊組成。所述之辨識方法的步驟如下：首先，保留其一之該實體區塊，並將其標記為一特殊功能實體區塊；再來，寫入一控制指令至特殊功能實體區塊；最後，進行一回應程序，其根據該控制指令來顯示或改變該記憶單元之狀態。

S601~S631：各個步驟流程



六、發明說明：

【發明所屬之技術領域】

本發明係關於一種辨識方法，尤指一種記憶體儲存裝置之辨識方法。

【先前技術】

為了提高檔案的可攜性，逐漸發展出可攜式儲存裝置，如記憶卡、USB 隨身碟，以方便隨時隨地儲存資料。請參考第一圖，該圖係為習知之記憶卡之一具體實施例之系統架構示意圖。如第一圖所示，記憶卡 1 中具有一控制單元 11 以及一記憶單元 13。由於快閃記憶體（Flash Memory）具有高儲存密度、低耗電特性、有效的存取效率與合理價格成本等優點，而成為目前記憶單元 13 之主流。控制單元 11 係耦接於記憶單元 13，用以接收主機端(圖中未示)下達之指令來將資料存取於記憶單元 13 中。

快閃記憶體有許多種類，且其價格亦有大幅度的差異。常見之快閃記憶體包括採用多級單元型記憶體（Multi-level-cell, MLC）製成之高密度記憶體（High density memory）或單級單元型記憶體（Single-level-cell, SLC），製成之低密度記憶體（Low density memory）。相較於低密度記憶體，高密度記憶體單位面積的資料儲存容量可成倍數增加，因而具有大幅提高儲存容量與降低成本的優勢，然其讀寫資料、執行燒錄與抹除（Erase）動作所需的時間卻較長；此外，多級單元製程技術也致使高密度記憶體所能承受的抹寫次數(Erase cycle)較少，如此便連帶影響了採用高密度記憶體的儲存裝置的資料存取速度與使用

壽命。為了避免不肖業者將品質差或價格低的記憶體替換成原廠記憶卡 1 中的記憶單元 13，並大量製造、兜售仿冒品來破壞原廠記憶卡 1 之市場競爭性，業者紛紛提出許多防偽之機制。

目前市面上常見的防偽方式大多係於原廠記憶卡 1 中的記憶單元 13 內儲存含有產品序號的辨識資料，經由特殊軟體來查驗此辨識資料是否合法。然而，有心人士仍很容易破解軟體的運作演算法來得到合法之辨識資料。或是，將辨識資料儲存於記憶單元 13 中特定之位址，並設計硬體到該特定之位址讀取辨識資料來辨別記憶單元 13 的真偽，但有心人士僅需一樣在仿冒品的該特定之位址寫入相同的辨識資料，仍然能大量複製盜用。

又，記憶卡 1 除了用以儲存資料，確保資料的完全保密性是未來的發展重點。目前坊間所提供的資料內容保護技術如 APS、CSS、RPC、DRM、CPRM 及軟體加密等方式都遭到有心人士的破解，而無法提供完善的保密機制。一般的記憶卡 1 僅接受讀取和寫入資料的動作，若要使用其他特殊功能，例如查詢序號、資料防拷等功能，則必須於主機端安裝適合的軟體或驅動程式，以提供相對應之特殊功能。然而，由於每台主機所使用之軟硬體、連接介面皆有出入，因此在主機上安裝軟體和驅動程式時，便存在相容性的問題，進而無法達到跨平台之訴求。且，若每次欲辨識記憶卡 1 時，測試人員皆須事先安裝用以辨識之驅動程式或應用軟體，將拉長測試時間並增加測試程序之不便性。

【發明內容】

因此，本發明之目的係在於提供一種記憶體儲存裝置之辨識方法，其利用存取一存放辨識資料的位址來對儲存裝置進行控制，以改善習知技術之問題。

本發明係揭示一種記憶體儲存裝置之辨識方法，此記憶體儲存裝置具有一記憶單元，其由連續之複數個實體區塊組成。所述之辨識方法的步驟如下：首先，保留其一之該實體區塊，並將其標記為一特殊功能實體區塊；再來，寫入一控制指令至特殊功能實體區塊；最後，進行一回應程序，其根據該控制指令來顯示或改變該記憶單元之狀態。

藉由前述技術方案，本發明係將辨識資料事先儲存在特定位址，利用直接存取該特定位址來對儲存裝置進行相對應之控制，如此能在跨平台、免安裝驅動程式之情況下，達到辨識儲存裝置之真偽的目的，以及提供一個更安全的資料保護機制。

以上之概述與接下來的詳細說明及附圖，皆是為了能進一步說明本發明為達成預定目的所採取之方式、手段及功效。而有關本發明的其他目的及優點，將在後續的說明及圖式中加以闡述。

【實施方式】

本發明所提出之記憶體儲存裝置之辨識方法，係於儲存裝置出廠前，將辨識資料事先儲存於記憶體之特定位址，藉由控制器直接對該特定位址下達讀取或寫入的指令來獲得辨識資料或控制儲存裝置的使用狀態，以避免安裝額外的驅動程式來對儲存裝置執行特殊之額外功能，進而達到跨平台之優點。

本發明之主要技術特徵在於在記憶體儲存裝置中產生一檔案，並藉由讀寫該檔案的方式辨識或控制記憶體儲存裝置之狀態，以下就僅提出必要之內部系統架構及其動作流程，然而，熟悉該項技藝者得知，除了以下所提及之構件，記憶體儲存裝置中當然包括其他的必要元件，因此，不應以本實施例揭露者為限。

首先，請參閱第二圖，該圖係為本發明所揭示之記憶體儲存裝置之一具體實施例之系統架構示意圖。如第二圖所示，一記憶體儲存裝置 21（以下簡稱儲存裝置）係應用於一數位系統 2 中，配合執行寫入與讀取資料。數位系統 2 中，儲存裝置 21 係可插接於主機 23，接受主機 23 所下達的指令運作。具體來說，主機 23 係為一計算機系統，其選自於行動裝置(Mobile Device)、個人電腦(PC)、筆記型電腦/Desktop)、平板電腦(Tablet PC)、伺服器或個人數位助理器(PDA)之其一；而儲存裝置 21 則為計算機系統之一周邊裝置，其可為記憶卡、隨身碟、MP3 或固態硬碟。

儲存裝置 21 包括有一控制單元 211 以及一記憶單元 213。控制單元 211 係耦接於主機 23 與記憶單元 213 之間，用以接收主機 23 所下達之一控制指令，所述之控制指令可為一寫入指令或一讀取指令，寫入指令是將對應一邏輯區塊位址的資料寫入記憶單元 213 中，而讀取指令則是將對應一邏輯區塊位址的資料從記憶單元 213 中讀取出來。記憶單元 213 為一快閃記憶體(Flash Memory)，其由單級單元記憶體(SLC)、相變化記憶體(PCM)、自由鐵電式隨機存取記憶體(FeRAM)、磁性隨機存取記憶體(MRAM)或多級單元記憶體(MLC)之群組組合之一構成。

接著，請參考第三圖，該圖係為本發明所揭示之記憶單元之一具體實施例之示意圖。其中相關之系統架構請一併參考第二圖。如第三圖所示，記憶單元 213 定義連續複數個實體區塊 PBA_0 、 PBA_1 、 PBA_2 ……，當中包括了無法記錄資料之至少一損壞區塊(圖中以 X 來表示之)。每一記憶體儲存裝置 21 在出廠時，控制單元 211 會掃描整個記憶單元 213，記錄並收集所有的損壞區塊之位址，以產生一壞塊索引表 4，如第四圖所示，損壞之實體區塊 PBA_{j-1} 、 PBA_q ……會依序記錄於壞塊索引表 4 中。控制單元 211 亦根據壞塊索引表 4 之內容來將可用之該實體區塊轉換成一邏輯區塊表 5，如第五圖所示，邏輯區塊表 5 中定義連續複數個邏輯區塊 LBA_0 、 LBA_1 、 LBA_2 ……，當中記錄了可用之實體區塊以及邏輯區塊之對應關係。資料可依序存取於該等邏輯區塊，並藉由控制單元 211 將資料實際存取於邏輯區塊所對應之實體區塊中。由於每個儲存裝置 21 中的損壞區塊之數量及位置皆不相同，故業者能事先儲存壞塊索引表 4 以及邏輯區塊表 5 於每一個新出廠之記憶體儲存裝置 21 中，以對其進行辨識。

於本發明之一具體實施例中，使用者每次將儲存裝置 21 插接於主機 23 時，控制單元 211 會檢測記憶單元 213 中實體區塊以及邏輯區塊的對應關係是否與邏輯區塊表 5 相同，若相同，即可進一步使用儲存裝置 21 來存取資料；否則便禁止一切對儲存裝置 21 的存取動作。

以上方式僅係能判斷儲存裝置 21 之真偽，為了更進一步辨識其詳細資訊，記憶單元 213 中特別儲存一辨識資料，其包括有記憶體製造廠商資訊及其製造日期、實體區

塊大小之資訊、可用之該實體區塊大小之資訊、損壞區塊大小之資訊、該壞塊索引表 4 或參數資料之群組組合之一。舉例來說，辨識資料的態樣可為”ABC, 081025, 500, 400, {5, 10, 15, ...}, 101”，其中 ABC 表示廠商名稱，081025 表示製造日期，500 表示實體區塊大小，400 表示可用之實體區塊大小，{5, 10, 15, ...} 表示損壞區塊之索引值，101 表示記憶單元 213 之使用狀態之參數資料。

請再參閱第三圖，本發明特別保留其一之實體區塊，將其標記為一特殊功能實體區塊 PBA_i ，用以記錄辨識資料的儲存位址。特殊功能實體區塊係為主機 23 端與儲存裝置 21 直接溝通之中介腳色，其中儲存之內容係不允許被任意改變。其中，特殊功能實體區塊 PBA_i 以及儲存辨識資料的實體區塊可以係於儲存裝置 21 出廠時預設之實體區塊，亦可係根據壞塊索引表 4 之內容而決定的。

一具體實施例中，以設計特殊功能實體區塊 PBA_i 為預設之實體區塊，且鎖定由第一之損壞區塊之下一個實體區塊(即實體區塊 PBA_j)來儲存辨識資料為例，當使用者欲辨識儲存裝置 21 時，從主機 23 端下達一控制指令，主機 23 便於預設之邏輯區塊 LBA_i 寫入該控制指令。控制單元 211 接收從主機 23 傳來的控制指令後，依據邏輯區塊表 5 得知該控制指令係欲對邏輯區塊 LBA_i 所對應之特殊功能實體區塊 PBA_i 進行寫入動作，於是便對該控制指令進行解碼，以提供特殊功能。

假設該控制指令係欲詢問辨識資料，則控制單元 211 會從特殊功能實體區塊 PBA_i 中查出辨識資料的儲存位址，進而從實體區塊 PBA_j 中讀出辨識資料，使用者便能從

辨識資料之內容來辨識儲存裝置 21。倘若儲存裝置 21 為仿冒品，則由主機 23 端寫入的邏輯區塊 LBA_i 所對應的實體區塊就不一定是特殊功能實體區塊 PBA_i (因為特殊功能實體區塊 PBA_i 之前有其他損壞區塊)，因此無法正確獲得辨識資料的儲存位址；即使主機 23 寫入之邏輯區塊 LBA_i 所對應的實體區塊剛好是特殊功能實體區塊 PBA_i ，進而查出辨識資料之內容，然而控制單元 211 會再更進一步確認辨識資料所在之實體區塊 PBA_j 之前一個實體區塊是否是記憶單元 213 的第一個損壞區塊，若是，則證明了辨識資料的可靠性，且此時的辨識資料的內容可允許被修改來改變記憶單元 213 之使用狀態。

而所述之控制指令除了可查詢辨識資訊之功能外，亦可對記憶單元 213 進行一鎖檔程序以及一解鎖程序。假設控制指令係欲將鎖住記憶單元 213 中的所有檔案，則控制單元 211 藉由上述步驟找到辨識資料後，會進行鎖檔程序，即修改辨識資料中的參數資料，例如將”101”改成”010”，以禁止對記憶單元 213 內儲存之檔案進行刪除、複製、寫入、讀取或顯示之動作；同樣地，若控制指令係欲將開放記憶單元 213 中的所有檔案，則控制單元 211 藉由上述步驟找到辨識資料後，會進行解鎖程序，即修改辨識資料中的參數資料，例如將”010”改成”101”，以開放對記憶單元 213 內儲存之檔案進行刪除、複製、寫入、讀取或顯示之動作。如此一來，每當使用者對記憶單元 213 中的檔案進行處理時，控制單元 211 會根據參數資料的設定來決定是否能對檔案進行相關之處理。

於本發明之一具體實施例中，獲得辨識資料的方法除

了上述提出將特殊功能實體區塊 PBA_i 設定為預設之實體區塊，且鎖定由第一之損壞區塊之下一個實體區塊(即實體區塊 PBA_j)來儲存辨識資料，亦可使用其他設計來達成。例如，將特殊功能實體區塊 PBA_i 設定為第一之損壞區塊之下一個實體區塊；或將特殊功能實體區塊 PBA_i 設定為複數個之損壞區塊之索引值加總之值的實體區塊，意即若前三個損壞區塊係為 PBA_1 、 PBA_2 、 PBA_6 ，則指定實體區塊 $PBA_9(1+2+6)$ 為特殊功能實體區塊 PBA_i ；或設定辨識資料儲存於複數個之損壞區塊之索引值加總之值的實體區塊中。因此，凡是根據壞塊索引表之內容而決定辨識資料所儲存之位址的各種演算法設計，皆屬本發明提出之技術特徵，故不應以本發明揭露者為限。

最後，請參閱第六圖，該圖係為本發明所揭示記憶體儲存裝置之辨識方法之一具體實施例之步驟流程圖。其中相關之系統架構請同時參閱第二~五圖。如第六圖所示，所述之辨識方法為以下步驟：

首先，將記憶體儲存裝置 21 插接於主機 23(步驟 S601)；控制單元 211 隨即對記憶單元 213 進行掃描，以檢測記憶單元 213 中可用之實體區塊與邏輯區塊的對應關係(步驟 S603)；接著便判斷檢測出了對應關係是否與原本就存在記憶單元 213 中的邏輯區塊表 5 中的內容相符(步驟 S605)，若否，則表示記憶單元 213 係為仿冒的，故禁止一切對儲存裝置的控制行為(步驟 S607)；若是，則表示記憶單元 213 係為原廠製造。

再來，使用者可於主機 23 端輸入一控制指令(步驟 S609)，意即寫入控制指令於邏輯區塊 LBA_i 中；控制單元

211 接收到主機 23 傳來之控制指令後，會經由邏輯區塊表 5 來轉換邏輯區塊 LBA_i 所對應之實體區塊位址，以判斷是否欲將控制指令寫至特殊功能實體區塊 PBA_i (步驟 S611)；若否，則表示該控制指令僅係執行一般讀寫動作，控制單元 211 便根據控制指令將資料存取於邏輯區塊 LBA_i 所對應之實體區塊位址(步驟 S613)；若係將控制指令寫入特殊功能實體區塊 PBA_i ，則表示欲執行讀寫動作以外之特殊功能，控制單元 211 隨即對控制指令進行解碼(步驟 S615)，以依據控制指令來進行相對應之一回應程序，進而執行顯示或改變記憶單元 213 之使用狀態之處理。

控制指令經解碼後，控制單元 211 便判斷該控制指令是否符合欲查詢儲存裝置 21 的辨識資料之指令格式(步驟 S617)；若是，則從特殊功能實體區塊 PBA_i 中查出辨識資料之儲存位址(步驟 S619)，進而從辨識資料之儲存位址中讀出辨識資料(步驟 S621)；主機 23 端接收到辨識資料後，便顯示辨識資料之內容(步驟 S623)，於是使用者可從辨識資料中查出儲存裝置 21 的產品型號及其使用狀態等資訊。

若步驟 S617 的判斷為否，則控制單元 211 會再判斷該控制指令是否符合欲改變記憶單元 213 的使用狀態之指令格式(步驟 S625)；若否，則執行其他對應於該控制指令之相關之處理(步驟 S627)，或可能該控制指令並不符合控制單元 211 所定義之指令格式，便不予以理會該控制指令；若步驟 S625 之判斷為是，則進行如步驟 S619~S621 之步驟來查出辨識資料(步驟 S629)，並依據控制指令來修改辨識資料中的參數資料，以改變記憶單元 213 的使用狀態(步驟 S631)，於是使用者可任意改變記憶單元 213 中的檔案

之使用權限，進而達到防刪、防寫、防讀等資料保護功能。

值得一提的是，在步驟 S613 中，控制單元 211 係依據參數資料的設定來決定記憶單元 213 的使用權限，若此時的記憶單元未被鎖住，使用者才能進行資料讀寫程序。而在步驟 S619 之後，控制單元 211 亦可進一步檢測辨識資料的儲存位址之前一個實體區塊是否係為第一個損壞之實體區塊，若是，才允許顯示辨識資料或修改參數資料。

藉由以上實例詳述，當可知悉本發明之記憶體儲存裝置之辨識方法，係在記憶體的特定位址事先儲存用以辨識或變更權限之辨識資料，透過直接讀寫該特定位址來查詢儲存裝置的辨識資料或對其進行修改，進而達到其他控制機制。藉由本發明提出之技術手段，可達到以下優點：

1. 藉由檔案讀寫的方式來傳遞指令與資料，毋須搭配特殊的讀取裝置，即可在任何作業系統以及沒有安裝驅動程式的情況下，進行對儲存裝置硬體的控制，如此提供跨平台的優勢，並且不受限於系統使用權限。
2. 由於每個記憶單元所具有之損壞之實體區塊的位置和數量皆不相同，故利用損壞區塊的分布情形來表示每一儲存裝置的唯一識別碼，如此可防止有心人士將仿冒品取代原廠之記憶單元。
3. 依據每個記憶單元的損壞區塊之分布情形來決定辨識資料的儲存位址，如此在修改和查詢辨識資料時，能先驗證該辨識資料之位址是否與損壞區塊之分布情形相符，如此提供一個更安全的資料保護機制。
4. 最後，在使用上，使用者可設定在儲存裝置插入任一

主機後，必須輸入密碼才能讀取資料，而之後對記憶單元的控制亦需輸入相對應之指令，如此輕易達到防軟/硬體複製、防非法讀寫等功能。

惟，以上所述，僅為本發明的具體實施例之詳細說明及圖式而已，並非用以限制本發明，本發明之所有範圍應以下述之申請專利範圍為準，任何熟悉該項技藝者在本發明之領域內，可輕易思及之變化或修飾皆可涵蓋在以下本案所界定之專利範圍。

【圖式簡單說明】

第一圖係為習知之記憶體儲存裝置之一具體實施例之系統架構示意圖；

第二圖係為本發明所揭示之記憶體儲存裝置之一具體實施例之系統架構示意圖；

第三圖係為本發明所揭示之記憶單元之一具體實施例之示意圖；

第四圖係為本發明所揭示之壞塊索引表之一具體實施例之示意圖；

第五圖係為本發明所揭示之邏輯區塊表之一具體實施例之示意圖；以及

第六圖係為本發明所揭示記憶體儲存裝置之辨識方法之一具體實施例之步驟流程圖。

【主要元件符號說明】

習知

1：記憶卡

201025005

11：控制單元

13：記憶單元

本發明

2：數位系統

21：記憶體儲存裝置

211：控制單元

213：記憶單元

23：主機

PBA₀、PBA₁、PBA₂、PBA_{j-1}、PBA_j、PBA_q：實體區塊

PBA_i：特殊功能實體區塊

4：壞塊索引表

5：邏輯區塊表

LBA₀、LBA₁、LBA₂、LBA_i：邏輯區塊

S601~S631：各個步驟流程