200903340

發明專利說明書

（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：961[illegible]8　　906K 19/07

※ 申請日期：96.7.11　　※IPC 分類：[illegible]

一、發明名稱：（中文/英文）

數位資料記憶卡加密之構造及方法

二、申請人：（共 1 人）

姓名或名稱：（中文/英文）

林暉

代表人：（中文/英文）

住居所或營業所地址：（中文/英文）

台北市內湖區堤頂大道 2 段 501 號 6 樓

國　籍：（中文/英文）　中華民國 TW

三、發明人：（共 1 人）

姓　名：（中文/英文）

林暉

國　籍：（中文/英文）

中華民國 TW

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：

☐ 無主張專利法第二十七條第一項國際優先權：

☐ 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。

九、發明說明：

【發明所屬之技術領域】

本發明係關於一種數位資料記憶卡加密之構造及方法，尤指一種將需要取得權利方可取用之數位資料載入記憶卡內，並將其加密之保護管理機制（DRM，Digital Rights Management）。

【先前技術】

由於電腦與數位技術之進步使然，許多創作、著作之內容，（例如電影或音樂內容），其內容皆被轉換成數位影音壓縮檔案，再將該檔案燒錄於 CD、DVD 等影音載體供一般消費者使用。該創作、著作之內容，除電影或音樂外，甚至廣泛延伸至演講、教學錄影、舞台劇等等，皆可以將內容轉換成數位影音壓縮檔案（以下合稱為【數位資料】）。

然而，由於壓縮與複製技術之純熟，前述之數位資料，無論電影或音樂內容，皆容易被形成各種檔案格式，透過各種複製、燒錄等技術予以重製，更由於網路推波助瀾下，成為散佈之媒介而提供更廣面之上傳與下載，使得複製之內容，更無遠弗屆地被傳遞、擴散。從而，數位資料（尤其是音樂或電影）之製作心血以及著作內容，被科技所提供之環境輕易攻破，而毫無防備。也令許多著作人之創作意願低落，對於重視智慧財產權之現今文明社會，不啻為一種極大之發展障礙，因此如何透過科技防護機制對於著作內容形成複製之障礙，以及內容之保護，為許多影音出版、發行業者，甚或演藝人員以及詞曲創作人等高度重視，更符

合我國科學技術基本法以及相關之科技法令之立法美意。

再者，前述之載體，一般而言 CD、DVD 等光碟片目前為市場之主流，但由於其重複使用之技術，除少數可抹寫式之光碟片可以多次重複燒錄外，其重複燒錄之型態並未形成如早期錄音帶之普及性，且由於體積較大之關係，使得目前許多播放器材（如MP3）播放器等，並未能同步使用。而是將該數位資料，由前述之載體，擷取、複製至所謂之 SD 卡等記憶卡使用。

按，目前記憶卡主要是用於數位檔案資料之儲存（目的同磁碟片等）。若能積極使其形成數位資料之載體，同時配合 Secured Digital Card (SD) (安全數位記憶卡)之安全數位特性以及體積小之特性，當可以符合更進一步之形成較佳之數位資料載體，且具有攜帶性高、適用性廣之安全防護機制。尤其目前市面上所流通的 SD 記憶卡，除傳輸速度以及容量已經大幅提升，且技術成熟而導致產品價格可以被廣泛接受。使得記憶卡形成較佳之數位資料載體之條件更為成熟。

雖然目前已經對於網路下載之音樂，藉由個人電腦（PC）播放器中含 DRM 機制(DRM，即所謂的數位版權管理【Digital Right Management】)，可以提供使用者在適當提出對價（付費）情形下可以提供相對應的安全保護機制，使得在資訊上傳送的數位資料可免於被有心人士非法複製與散佈。或者藉由限制下載者身份、次數、有限時間、有限份數內之複製，然而對於載體本身（尤其是記憶卡）並無一個適當之防護機制。

【發明內容】

有鑒於先前技術中對於記憶卡未能有一充分之加密以及防護，因此對於各種需要取得權利，方能取用之數位資料之智慧財產權以及隱私未能達到充分保護。

因此，本發明特針對先前技術提出一記憶卡加密之構造及方法，解決先前問題之技術手段，本發明係關於一種數位資料記憶卡加密之構造及方法，係將一記憶卡內之記憶體除本身具有一讀取控制端（Controller）以及一保護區（Protection Area）外，另分割為一硬碟分割表區（Partition Table Area）以及一檔案區（File Area），並利用一應用程式介面（API，Application Programming Interface），於前開各區選擇其任何一區，寫入一受保護儲存裝置識別碼(PSID)，而當記憶卡內之檔案區（File Area）載有權利物件（Right Object）（需要具有權利取得之數位資料）時，對於各種讀取器讀取時，可以利用該受保護儲存裝置識別碼(PSID)為辨識讀取之加密機制，增加記憶卡數位資料的保護管理機制（DRM，Digital Rights Management）之安全性。因此在記憶卡內共有４個區域：即讀取控制端（Controller）、保護區（Protection Area）、硬碟分割表區（Partition Table Area）以及檔案區（File Area），而欲將(PSID)(Portable Storage ID)置入該記憶卡可以選擇以下數種方式：

一、若要將受保護儲存裝置識別碼(PSID)(Portable Storage ID)放入記憶卡記憶體內之讀取控制端（Controller），即可使用一般記憶卡讀取器(例如 SD Reader)與針對記憶卡記憶體內

之讀取控制端（Controller）所發展之 API 即可，此種較為安全。

二、若要將受保護儲存裝置識別碼(PSID)放入記憶卡之保護區（Protection Area），則可以用特殊治具進行記憶卡保護區（Protection Area）大小之切割，亦可使用一般 SD Reader 與針對記憶卡記憶體內之保護區（Protection Area）所發展之 API。

三、若要將受保護儲存裝置識別碼(PSID)放入硬碟分割表區（Partition Table Area），則使用者使用 Windows 或其他 OS 進行 Format 後即可產生此區。

四、若要將受保護儲存裝置識別碼(PSID)放入檔案區（File Area），則使用者使用 Windows 或其他 OS 進行 Format 後即可產生此區。

【實施方式】

以下透過圖式說明本發明之內容、特點與實施例，俾使 貴審查委員對於本案有更進一步之了解。

請參閱第一圖所示，本發明係關於一種數位資料記憶卡加密構造，包括：

一記憶卡（１），該記憶卡（１）內部設置一記憶體（１１），而該記憶體（１１）除本身設置有一配合讀取器之讀取控制端（Controller）（１１１）以及一保護區（Protection Area）（１１２）外，另分割為一硬碟分割表區（Partition Table Area）（１

１３）以及一檔案區（File Area）（１１４），並以應用程式介面（API，Application Programming Interface），於前開各區選擇任何一區寫入一受保護儲存裝置識別碼(PSID)（１１５），而當記憶卡（１）內之檔案區（File Area）（１１４）載有權利物件（Right Object）（１１６）（需要具有權利取得之數位資料）時，對於各種讀取器讀取時，可以利用該受保護儲存裝置識別碼(PSID)（１１５）為辨識讀取之加密機制，增加記憶卡（１）數位資料的保護管理機制（DRM，Digital Rights Management）之安全性。

配合第二圖所示，記憶卡（１）讀取控制端（Controller）（１１１）廠商對於 API 應嚴守秘密，否則其他人即可使用此 API 來得到本發明中置於記憶體（１１）內之受保護儲存裝置識別碼(PSID)（１１５），例如設於保護區（Protection Area）（１１２）之程式與受保護儲存裝置識別碼(PSID)（１１５）。

然而，為求更進一確保該記憶卡（１）之受保護儲存裝置識別碼(PSID)（１１５），本發明可以將該記憶卡（１）設置為一種 PSD(Personal Storage Disc)，透過一體成型之將 USB 功能與記憶卡整合為一體，讓使用者可以不需要透過讀卡機及傳輸線，便可經由電腦的 USB 介面傳輸資料，也可以免除有心人士利用輕易拆解記憶卡（１）而取得該內部之記憶體，甚至破解。

本發明所使用之該記憶體（１１）可以為一種快閃記憶體（Flash Memory），亦可以為一種電性可擦除式唯讀記憶體 EEPROM（(Electrically Erasable Programmable Read-Only Memory)。

一、若要將受保護儲存裝置識別碼(PSID)(Portable Storage ID)（１１５）放入記憶卡（１）記憶體（１１）內之讀取控制端（Controller）（１１１），即可使用一般記憶卡讀取器(例如 SD Reader)與針對記憶卡記憶體內之讀取控制端（Controller)所發展之 API 即可讀取或寫入，此種較為安全。

二、若要將受保護儲存裝置識別碼(PSID（１１５）放入記憶卡（１）之保護區（Protection Area）（１１２），則可以用特殊治具進行記憶卡保護區（Protection Area）（１１２）大小之切割，亦可使用一般 SD Reader 與針對記憶卡記憶體內之保護區（Protection Area）所發展之 API 即可讀取或寫入。

三、若要將受保護儲存裝置識別碼(PSID)（１１５）放入硬碟分割表區（Partition Table Area）（１１３），則使用者使用 Windows 或其他 OS 進行 Format 後即可產生此區。

四、若要將受保護儲存裝置識別碼(PSID)（１１５）放入檔案區（File Area）（１１４），則使用者使用 Windows 或其他 OS 進行 Format 後即可產生此區。

無論受保護儲存裝置識別碼(PSID)（１１５）存在何區，該權利物件（Right Object）（１１６）皆需要取得權利，方能取用之數位資料）。當各種裝置如個人電腦（PC）、手機或各種播放裝置（合稱為讀取器）欲讀取對應之權利物件（Right Object）（１１６）檔案時，讀取控制端（Controller）（１１１）會使用存在讀取控制端(Controller)（１１１）之軔體或保護區(Protection Area)（１１６）之程式來進行權利物件（Right Object）（１１６）檔

案解密並由解密之權利物件（Right Object）（１１６）檔案中求得對應之受保護儲存裝置識別碼(PSID)（１１５），再與儲存在保護區（Protection Area）（１１２）（以保護區為例，但不限於保護區）之受保護儲存裝置識別碼(PSID)（１１５）作比對，若比對成功方將權利物件（Right Object）（１１６）檔案提供予播放裝置。若比對不成功則告知播放裝置檔案不可讀取。

進一步說明第二圖之意義，當讀取控制端（Controller）（１１１）接受讀取器指令而進行資料讀取時，首先會進行特定副檔名（例如但不限於 ROM），當確定為保護區（Protection Area）（１１２）之變數所形成之副檔名之後，若是，則循由電性可擦除式唯讀記憶體 EEPROM（Electrically Erasable Programmable Read-Only Memory）（亦可為快閃記憶體（Flash Memory）），例如／但不限於其保護區（Protection Area）（１１２）儲存之加密 PSID（１１５），並且取出該副檔名下某一位元資料，然後執行存在於該讀取控制端（Controller）（１１１）之記憶卡韌體，或存在於保護區（Protection Area）（１１２）內之內碼（CODE）。然後判斷取出之位元資料是否符合受保護儲存裝置識別碼(PSID)（１１５），若是，則執行原來讀取器得以讀取之路徑與資料；若不是，則依不正常回報 bus protocal（匯流排協定）。

本發明對於數位版權管理機制（DRM，Digital Rights Management）提供一種數位資料的保護管理機制，除音樂、影像甚至視訊的數位資料，皆可以達到有效保護，保障數位資料使用的授權取用，以及不被第三者非法存取，避免不必要的數位資產

損失。

綜上所述，本發明確實符合產業利用性，且未於申請前見於刊物或公開使用，亦未為公眾所知悉，且具有非顯而易知性，符合可專利之要件，爰依法提出專利申請。

惟上述所陳，為本發明產業上一較佳實施例，舉凡依本發明申請專利範圍所作之均等變化，皆屬本案訴求標的之範疇。

【圖式簡單說明】

第一圖係本發明之記憶卡架構示意圖

第二圖係本發明之操作流程圖

【主要元件符號說明】

（１）：記憶卡

（１１）：記憶體

（１１１）：讀取控制端

（１１２）：保護區

（１１３）：硬碟分割表區

（１１４）：檔案區

（１１５）：受保護儲存裝置識別碼(PSID)

（１１６）：權利物件

五、中文發明摘要：

本發明係關於一種數位資料記憶卡加密之構造及方法，主體係於一記憶卡內設置一記憶體，而該記憶體本身設置有一配合讀取器之讀取控制端（Controller）以及一保護區（Protection Area）外，另外分割為一硬碟分割表區（Partition Table Area）以及一檔案區（File Area），並以應用程式介面（API，Application Programming Interface），於前開各區選擇其任何一區，寫入一受保護儲存裝置識別碼(PSID，Portable Storage ID)，而當記憶卡內之檔案區（File Area）載有權利物件（Right Object）（需要具有權利取得之數位資料）時，對於各種讀取器讀取時，可以利用該受保護儲存裝置識別碼(PSID 為辨識讀取之加密機制，增加記憶卡數位資料的保護管理機制（DRM，Digital Rights Management）之安全性。

六、英文發明摘要：

十、申請專利範圍：

1、一種數位資料記憶卡加密之方法，係於一記憶卡內設置一記憶體，而該記憶體本身設置有一配合讀取器之讀取控制端（Controller）以及一保護區（Protection Area）外，另外分割為一硬碟分割表區（Partition Table Area）以及一檔案區（File Area），並以應用程式介面（API，Application Programming Interface），選擇其一區，寫入一受保護儲存裝置識別碼(PSID，Portable Storage ID)，而當記憶卡內之檔案區（File Area）載有權利物件（Right Object）時，對於各種讀取器讀取時，可以利用該受保護儲存裝置識別碼(PSID 為辨識讀取之加密機制，增加記憶卡數位資料的保護管理機制（DRM，Digital Rights Management）之安全性。

2、如申請專利範圍第 1 項所述之數位資料記憶卡加密之方法，其特徵在於該記憶體為一種選自於快閃記憶體（FLASH）、電性可擦除式唯讀記憶體 EEPROM (Electrically Erasable Programmable Read-Only Memory)。

3、如申請專利範圍第 1 項所述之數位資料記憶卡加密之方法，該應用程式介面（API）係使用讀取控制端（Controller）置入該記憶體之保護區。

4、如申請專利範圍第1項所述之數位資料記憶卡加密之方法，該應用程式介面（API）係使用微軟視窗作業系統（Windows）置入硬碟分割表區。

5、如申請專利範圍第1項所述之數位資料記憶卡加密之方法，該應用程式介面（API）係使用微軟視窗作業系統（Windows）置入快閃記憶體之檔案區。

6、如申請專利範圍第1項所述之數位資料記憶卡加密之方法，其特徵在於該記憶卡為PSD(Personal Storage Disc)一體成型。

7、一種數位資料記憶卡加密之構造，該記憶卡包括一記憶體，而該記憶體設置：

一讀取控制端（Controller）：

一保護區（Protection Area）：

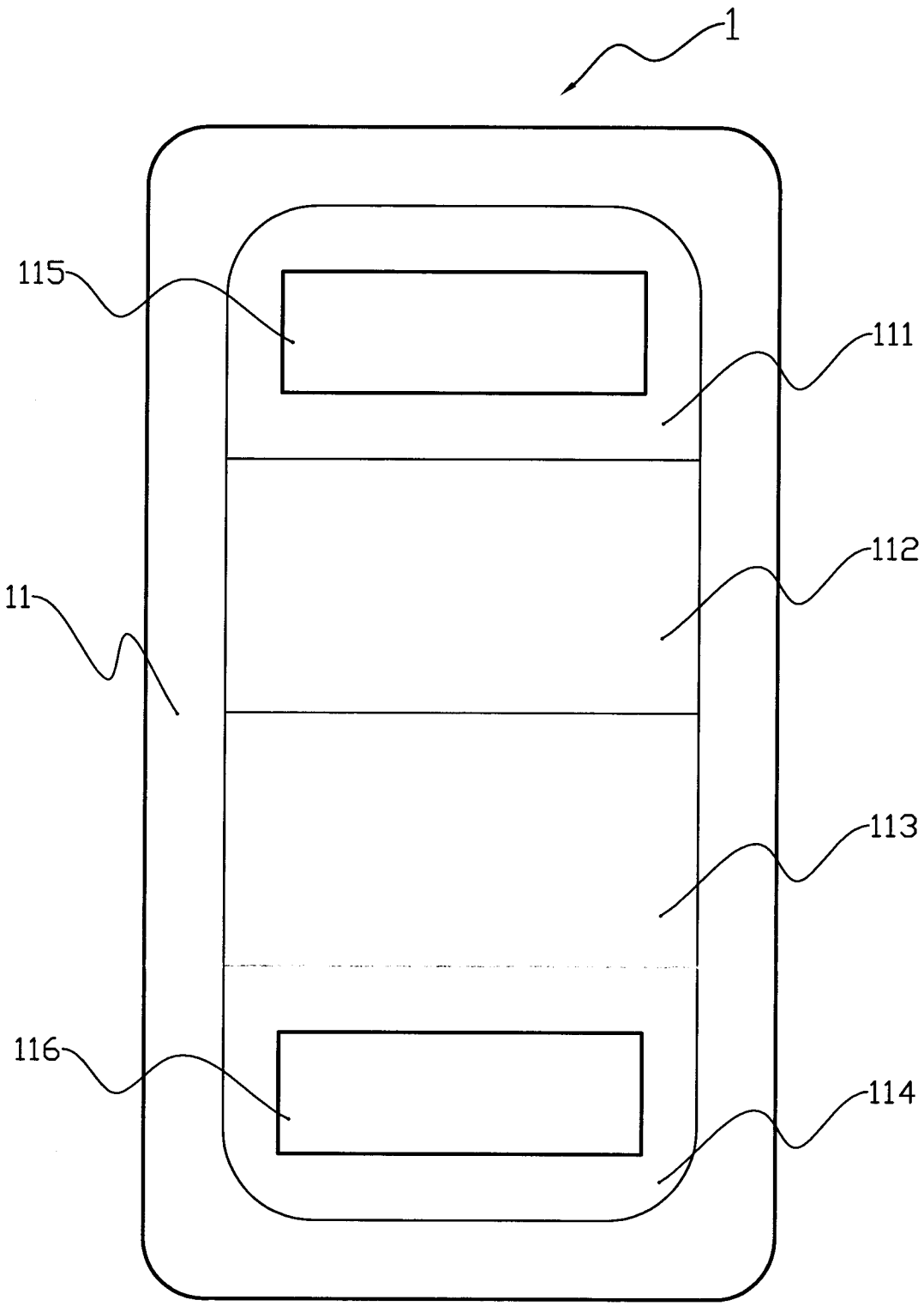
一硬碟分割表區（Partition Table Area），以及一檔案區（File Area）；

以應用程式介面（API，Application Programming Interface），於前開各區選擇其一，寫入一受保護儲存裝置識別碼(PSID，Portable Storage ID)。

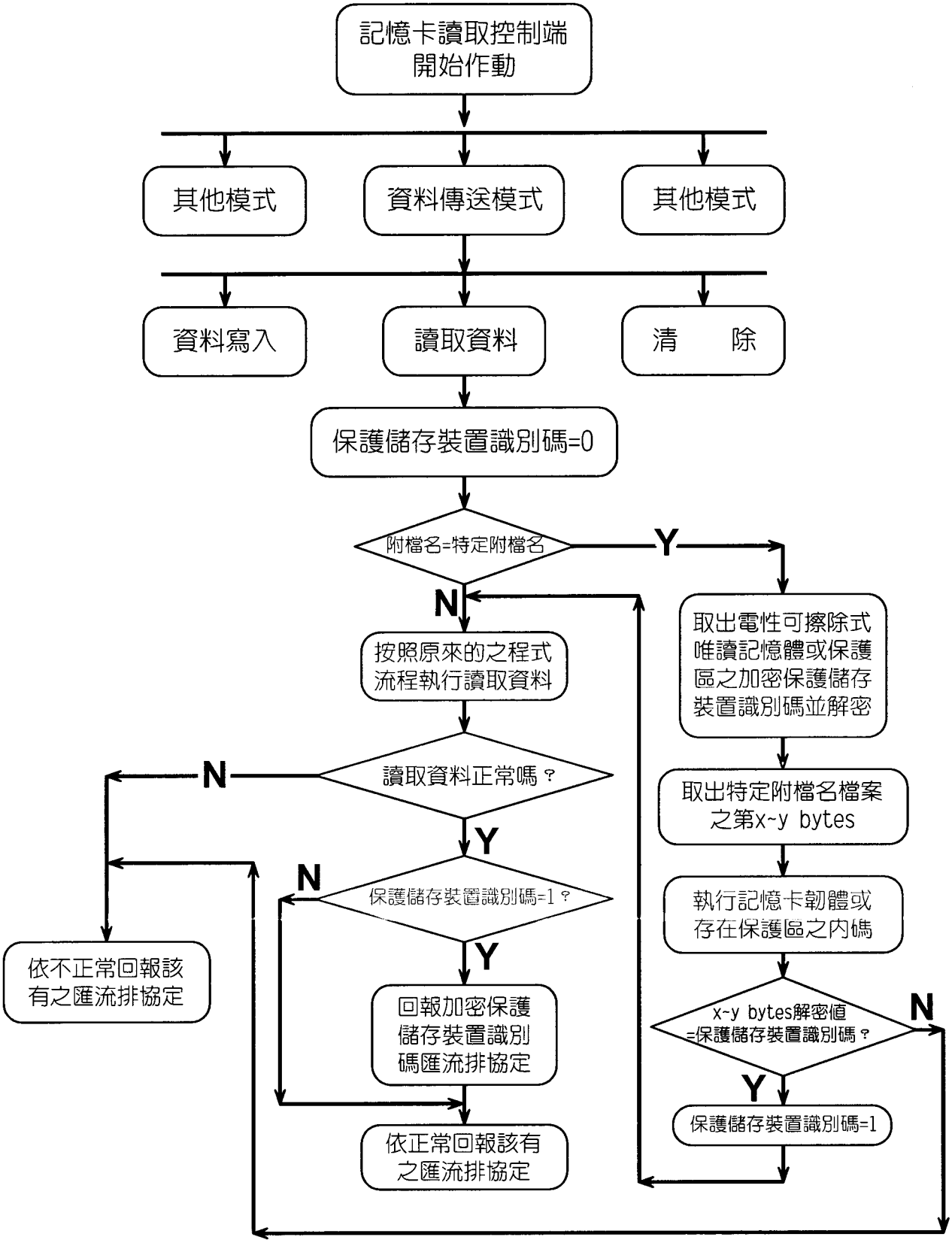
8、如申請專利範圍第7項所述之數位資料記憶卡加密之構造，其特徵在於該記憶體為一種選自於快閃記憶體（FLASH）、電性可擦除式唯讀記憶體 EEPROM

（(Electrically Erasable Programmable Read-Only Memory)。

9、如申請專利範圍第7項所述之數位資料記憶卡加密之構造，其特徵在於該記憶卡為PSD(Personal Storage Disc)一體成型。



第一圖


記憶卡讀取控制端
開始作動
其他模式
資料傳送模式
其他模式
資料寫入
讀取資料
清　除
保護儲存裝置識別碼=0
附檔名=特定附檔名
Y
N
取出電性可擦除式
唯讀記憶體或保護
區之加密保護儲存
裝置識別碼並解密
按照原來的之程式
流程執行讀取資料
讀取資料正常嗎？
N
Y
取出特定附檔名檔案
之第x~y bytes
保護儲存裝置識別碼=1？
N
Y
執行記憶卡韌體或
存在保護區之內碼
依不正常回報該
有之匯流排協定
回報加密保護
儲存裝置識別
碼匯流排協定
x~y bytes解密值
=保護儲存裝置識別碼？
N
Y
保護儲存裝置識別碼=1
依正常回報該有
之匯流排協定

第二圖

七、指定代表圖：

(一)本案指定代表圖為：第（二）圖。

(二)本代表圖之元件符號簡單說明:

無

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