



(19) 中華民國智慧財產局

(12) 發明說明書公告本

(11) 證書號數：TW I493463 B

(45) 公告日：中華民國 104 (2015) 年 07 月 21 日

(21) 申請案號：102139253

(22) 申請日：中華民國 102 (2013) 年 10 月 30 日

(51) Int. Cl. : G06F9/445 (2006.01)

G06F12/02 (2006.01)

(71) 申請人：系微股份有限公司 (中華民國) INSYDE SOFTWARE CORP. (TW)

臺北市中山區民生東路 2 段 161 號 12 樓

(72) 發明人：陳彥君 (TW)

(74) 代理人：賴經臣；宿希成

(56) 參考文獻：

TW 201131475A

TW 201224752A1

TW 201310344A

US 2013/0227540A1

US 2013/0276128A1

審查人員：林剛煌

申請專利範圍項數：8 項 圖式數：2 共 14 頁

(54) 名稱

電子裝置、通用可延伸韌體介面基本輸入輸出系統之韌體檔案之更新方法、記錄媒體及電腦程式產品

(57) 摘要

一種通用可延伸韌體介面基本輸入輸出系統之韌體檔案之更新方法，其由平台系統來實施，此更新方法包括下列步驟：在作業系統階段，於儲存媒體中將具有多個映象檔之韌體檔案儲存在記憶體中；在開機階段，存取經儲存在記憶體中之韌體檔案；比較韌體檔案之一全域唯一辨識符與通用可延伸韌體介面基本輸入輸出系統之全域唯一辨識符是否相同；以一雜湊演算法運算韌體檔案之所有映象檔以得到運算雜湊值，並比較運算雜湊值與韌體檔案中之雜湊值是否相同；以及將韌體檔案中複數個映象檔來更新複數個相應分割區中之韌體。

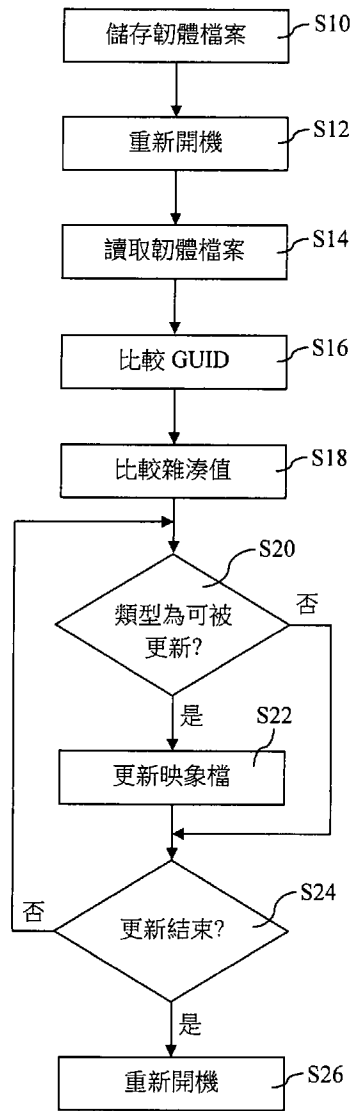


圖 2

發明摘要

公告本

※ 申請案號：102139253

※ 申請日：102/10/30

※IPC 分類：

G06F9/00 (2006.01)

G06F12/00 (2006.01)

【發明名稱】(中文/英文)

電子裝置、通用可延伸韌體介面基本輸入輸出系統之韌體檔案之更新方法、記錄媒體及電腦程式產品

【中文】

一種通用可延伸韌體介面基本輸入輸出系統之韌體檔案之更新方法，其由平台系統來實施，此更新方法包括下列步驟：在作業系統階段，於儲存媒體中將具有多個映象檔之韌體檔案儲存在記憶體中；在開機階段，存取經儲存在記憶體中之韌體檔案；比較韌體檔案之一全域唯一辨識符與通用可延伸韌體介面基本輸入輸出系統之全域唯一辨識符是否相同；以一雜湊演算法運算韌體檔案之所有映象檔以得到運算雜湊值，並比較運算雜湊值與韌體檔案中之雜湊值是否相同；以及將韌體檔案中複數個映象檔來更新複數個相應分割區中之韌體。

【英文】

【代表圖】

【本案指定代表圖】：第（ 2 ）圖。

【本代表圖之符號簡單說明】：

： 無

：

【本案若有化學式時，請揭示最能顯示發明特徵的化學式】：

無

發明專利說明書

(本說明書格式、順序，請勿任意更動)

【發明名稱】(中文/英文)

電子裝置、通用可延伸韌體介面基本輸入輸出系統之韌體檔案之更新方法、記錄媒體及電腦程式產品

【技術領域】

【0001】 本發明有關於一種基本輸入輸出系統，特別有關於一種電子裝置、通用可延伸韌體介面基本輸入輸出系統之韌體檔案之更新方法、記錄媒體及電腦程式產品。

【先前技術】

【0002】 所謂基本輸出入系統(Basic Input Output System, BIOS)是指存放在主機板上之快閃記憶體(Flash Memory)，其中包含了許多例如電腦、平板電腦或智慧型手機等系統平台輸出入的基本副程式、在主機板上為處理軟體與硬體溝通設定，其BIOS的設定與系統平台之硬體具有關連性。例如，如果任意更換系統平台之主機板上的BIOS的話，很可能會造成系統平台無法啟動。

【0003】 BIOS的功能是用來設定與控制中央處理單元(CPU)和各種相關晶片的運作，時脈以及各種標準的周邊裝置作業之設定，例如：印表機、滑鼠、鍵盤、硬碟機與軟碟機。當BIOS啟動系統平台時，其首先會確定所有周邊是否就定位運作，再從硬碟或磁碟機將作業系統載入隨機存取記憶體(DRAM)。有了此BIOS，作業系統與應用程式可藉BIOS承繼輸出入裝置的詳細資料，如網路卡媒介存取控制(Medium

Address Control，MAC位址)、磁碟機容量及位置等，倘若裝置變更，只需透過BIOS的更動，來通知作業系統或應用程式。

【0004】 當對存放有平台系統之韌體或BIOS之韌體之分割區(Partition)進行更新時，習知技術係將儲存在儲存媒體之為檔案形式之一個映象檔(Image File)對相應之分割區(為存放韌體之儲存空間)之韌體進行更新，然而只能一次以一個映象檔對一個分割區來進行韌體(包含BIOS)的更新。因此，習知更新方式對於多個分割區要逐一進行韌體之更新操作係相當繁雜並浪費許多時間，且不符合自動化更新之要求。

【發明內容】

【0005】 有鑑於上述問題，本發明係提供一種電子裝置、通用可延伸韌體介面基本輸入輸出系統(Universal Extensible Firmware Interface Basic Input Output System，UEFI BIOS)之韌體檔案之更新方法、記錄媒體及電腦程式產品，其利用一個具有多個映象檔之韌體檔案來對多個分割區同時進行韌體之更新，因此，更新操作相當簡單並節省時間，且符合自動化更新之要求。

【0006】 本發明之第一態樣係提供一種通用可延伸韌體介面基本輸入輸出系統之韌體檔案之更新方法，其由一平台系統來實施，該更新方法包括下列步驟：

在作業系統階段，於一儲存媒體中將具有多個映象檔之一韌體檔案儲存在一記憶體中；

在開機階段，存取經儲存在該記憶體中之該韌體檔案；

比較該韌體檔案之一全域唯一辨識符與該通用可延伸韌體介面基

本輸入輸出系統之該全域唯一辨識符是否相同；

以一雜湊演算法運算該韌體檔案之所有映象檔以得到一運算雜湊值，並比較該運算雜湊值與該韌體檔案中之一雜湊值是否相同；以及將該韌體檔案中複數個映象檔來更新複數個相應分割區中之韌體。

【0007】 本發明之第二態樣係提供一種內儲一程式之記錄媒體，當一平台系統於該記錄媒體載入該程式並執行後，可完成本發明之第一態樣之更新方法。

【0008】 本發明之第三態樣係提供一種內儲一程式之電腦程式產品，當一平台系統於電腦程式產品載入該程式並執行後，可完成本發明之第一態樣之更新方法。

【0009】 本發明之第四態樣係提供一種電子裝置，其包括：
一儲存媒體，其用以儲存一韌體檔案，該韌體檔案包括複數映象檔、一全域唯一辨識符以及以一運算雜湊值，其中該運算雜湊值利用一雜湊演算法運算上述映象檔取得；以及

一運算處理裝置，其用以從該儲存裝置中將該韌體檔案儲存在一記憶體中，並利用該全域唯一辨識符判斷是否為更新一通用可延伸韌體介面基本輸入輸出系統之韌體。

【圖式簡單說明】

【0010】

圖1為本發明之韌體檔案之資料格式之示意圖；以及

圖2為本發明之UEFI BIOS之韌體檔案之更新方法之流程圖。

【實施方式】

【0011】 為使熟習本發明所屬技術領域之一般技藝者能更進一步了解本發明，下文特列舉本發明之較佳實施例，並配合所附圖式，詳細說明本發明的構成內容及所欲達成之功效。

【0012】 習知而未繪示之例如電腦、平板電腦或智慧型手機等作為電子裝置之系統平台包含有CPU(即運算處理裝置)、UEFI BIOS、記憶體及儲存媒體(例如硬碟)等以執行本發明之UEFI BIOS之韌體檔案之更新方法。

【0013】 圖1為本發明之韌體檔案之資料格式之示意圖。在圖1中，儲存於儲存媒體中之韌體檔案之檔案名稱為FileShell.efi，韌體檔案的資料格式包含簽章(Signature)之欄位、全域唯一辨識符(Globally Unique Identifier, GUID)之欄位、保留大小(Reserved Size)之欄位及存放韌體二進制資料(Firmware Binary)之緩衝區(Buffer)。

【0014】 簽章之欄位作為用以搜尋韌體檔案中之多個映象檔之起始點。GUID之欄位作為辨識韌體檔案是否為更新UEFI BIOS之檔案。保留大小之欄位係記錄緩衝區的最大容量大小。緩衝區所存放之韌體二進制資料包含封裝標頭(Package Header)之欄位、多個檔案資訊之欄位、存放多個映象檔之區域及雜湊值之欄位。在本實施例中以三個映象檔為例，但不侷限為此數量。

【0015】 封裝標頭之欄位係記錄映象檔之資訊。封裝標頭之欄位包含類型(Type)之欄位、數量之欄位、演算法之欄位及輸出長度之欄位。檔案資訊之欄位係記錄每個映象檔之資訊。檔案資訊之欄位包含

檔案名稱之欄位、偏移之欄位及大小之欄位。映象檔的內容係驅動程式之二進制資料。雜湊值之欄位是作為驗證映象檔是否正確。

【0016】 類型之欄位係記錄每一個映象檔為可被更新或不可被更新。數量之欄位係記錄韌體檔案中之映象檔的數目。演算法之欄位係記錄演算法之類型。輸出長度之欄位係記錄所輸出之雜湊值的長度。檔案名稱之欄位係記錄每個映象檔之簽章。偏移之欄位係記錄每個映象檔之偏移量。大小之欄位係記錄每個映象檔之檔案大小。

【0017】 圖2為本發明之UEFI BIOS之韌體檔案之更新方法之流程圖。在圖2中，當系統平台之韌體或UEFI BIOS之韌體要進行更新時，在作業系統階段，由系統平台執行用以更新多個韌體之應用程式，而由CPU將在儲存媒體中具有多個映象檔之韌體檔案(如圖1所示之檔案FileShell.efi)儲存在記憶體中(步驟S10)，該韌體檔案中之資料格式如圖1所示。接著，所執行之應用程式執行一暖開機，使系統平台重新開機以進入開機階段(步驟S12)。

【0018】 在開機階段，由系統平台存取經儲存在記憶體中之韌體檔案，並搜尋在韌體檔案中之簽章(記錄於韌體檔案的簽章之欄位中)以作為存取韌體檔案之起始點(步驟S14)。

【0019】 為了確保韌體檔案的映像檔與欲更新之韌體一致，由系統平台之CPU比較韌體檔案之GUID(記錄於韌體檔案的GUID之欄位中)與UEFI BIOS之GUID是否相同，若韌體檔案之GUID與UEFI BIOS之GUID相同，則進行下述韌體的更新；若韌體檔案之GUID與UEFI BIOS之GUID不相同，則不進行韌體的更新(步驟S16)。

【0020】 為了確保儲存在記憶體中之韌體檔案在儲存媒體中存取的过程中正確無誤，由系統平台以一雜湊演算法(例如SHA-256演算法)運算韌體檔案之所有映象檔之二進制資料以得到一運算雜湊值，並比較該運算雜湊值與韌體檔案中之雜湊值(記錄於韌體檔案的雜湊值之欄位中)是否相同，若運算雜湊值與雜湊值相同，則進行下述韌體的更新；若運算雜湊值與雜湊值不相同，則不進行韌體的更新(步驟S18)。

【0021】 接著，由系統平台將韌體檔案中映象檔來更新相應分割區中之韌體，而該更新韌體之步驟進一步包括下述步驟。

【0022】 由系統平台檢查韌體檔案中目前欲對相應分割區中之韌體進行更新之映象檔(例如映象檔1)之相應之一類型(記錄於韌體檔案的類型之欄位中)，以判斷該類型是否為可被更新(步驟S20)，若該類型為可被更新，則由系統平台將韌體檔案中之映象檔1來更新相應分割區中之韌體(步驟S22)。

【0023】 若該類型為不可被更新或者目前進行更新之映象檔已更新結束，由系統平台判斷韌體檔案中所有映象檔是否已對所有相應分割區中之韌體進行更新結束(步驟S24)，若韌體檔案中不是所有映象檔已更新結束，則進行到步驟S20，由系統平台檢查韌體檔案中下一個欲對相應分割區中之韌體進行更新之映象檔(例如映象檔2)之相應之類型；若韌體檔案中所有映象檔已更新結束，則由系統平台執行暖開機，以進入開機階段(步驟S26)。

【0024】 本發明之上述UEFI BIOS之韌體檔案之更新方法可以一程式型態來完成，並可將該程式儲存於一記錄媒體，當電腦於該記錄

媒體載入該程式並執行後，便可完成如上述說明及圖式中所示之方法步驟。

【0025】 同樣地，本發明之上述UEFI BIOS之韌體檔案之更新方法可以一電腦程式產品來完成，當電腦例如從網路下載該電腦程式產品並執行後，便可完成如上述說明及圖式中所示之方法步驟。

【0026】 本發明係提供一種電子裝置、通用可延伸韌體介面基本輸入輸出系統之韌體檔案之更新方法、記錄媒體及電腦程式產品，其優點係利用一個具有多個映象檔之韌體檔案來對多個分割區同時進行韌體之更新，因此，更新操作相當簡單並節省時間，且符合自動化更新之要求。

【0027】 雖然本發明已參照較佳具體例及舉例性附圖敘述如上，惟其應不被視為係限制性者。熟悉本技藝者對其形態及具體例之內容做各種修改、省略及變化，均不離開本發明之申請專利範圍之所主張範圍。

【符號說明】

無

申請專利範圍

1. 一種通用可延伸韌體介面基本輸入輸出系統之韌體檔案之更新方

法，其由一平台系統來實施，該更新方法包括下列步驟：

在作業系統階段，於一儲存媒體中將具有多個映象檔之一韌體檔案儲存在一記憶體中；

在開機階段，存取經儲存在該記憶體中之該韌體檔案；

比較該韌體檔案之一全域唯一辨識符與該通用可延伸韌體介面基本輸入輸出系統之該全域唯一辨識符是否相同；

以一雜湊演算法運算在該記憶體中之該韌體檔案之所有映象檔以得到一運算雜湊值，並比較該運算雜湊值與在該記憶體中之該韌體檔案中之一雜湊值是否相同；

將在該記憶體中之該韌體檔案中複數個映象檔來更新複數個相應分割區中之韌體；

檢查在該記憶體中之該韌體檔案中一個映象檔之相應之一類型，以判斷該類型是否為可被更新；

以該類型為可被更新之該一個映象檔來更新一個相應分割區中之韌體；

判斷在該記憶體中之該韌體檔案中所有之映象檔是否已更新結束；以及

執行一暖開機，以進入開機階段。

2. 如申請專利範圍第 1 項之更新方法，在存取經儲存在該記憶體中之

該韌體檔案之步驟前進一步包括下列步驟：

在作業系統階段，執行一暖開機，以進入開機階段。

3. 如申請專利範圍第 1 項之更新方法，其中，在存取經儲存在該記憶體中之該韌體檔案之步驟中，搜尋在該記憶體中之該韌體檔案中之一簽章。
4. 一種內儲一程式之記錄媒體，當一平台系統於該記錄媒體載入該程式並執行後，可完成申請專利範圍第 1 至 3 項中任一項之更新方法。
5. 一種內儲一程式之電腦程式產品，當一平台系統於電腦程式產品載入該程式並執行後，可完成申請專利範圍第 1 至 3 項中任一項之更新方法。
6. 一種電子裝置，其包括：
 - 一儲存媒體，其用以儲存一韌體檔案，該韌體檔案包括複數映象檔、一全域唯一辨識符以及以一運算雜湊值，其中該運算雜湊值利用一雜湊演算法運算上述映象檔取得；以及
 - 一運算處理裝置，其用以從該儲存裝置中將該韌體檔案儲存在一記憶體中，並利用該全域唯一辨識符判斷是否為更新一通用可延伸韌體介面基本輸入輸出系統之韌體；其中在該記憶體中之該韌體檔案更包括一簽章資訊、一封裝標頭以及複數檔案資訊，其中，該簽章資訊用以搜尋該映象檔之起始點，該封裝標頭用以記錄該映象檔之資訊，且每個檔案資訊用以記錄對應之該映象檔的資訊。
7. 如申請專利範圍第 6 項之電子裝置，其中，該封裝標頭包含每一個映象檔之一可被更新或不可被更新的資訊、該映象檔之一數目資

訊、該雜湊演算法類型之資訊及該雜湊值之一長度資訊。

8. 如申請專利範圍第 6 項之電子裝置，其中，每個檔案資訊包含一檔案名稱資訊、一檔案偏移資訊及一檔案大小資訊。

圖式

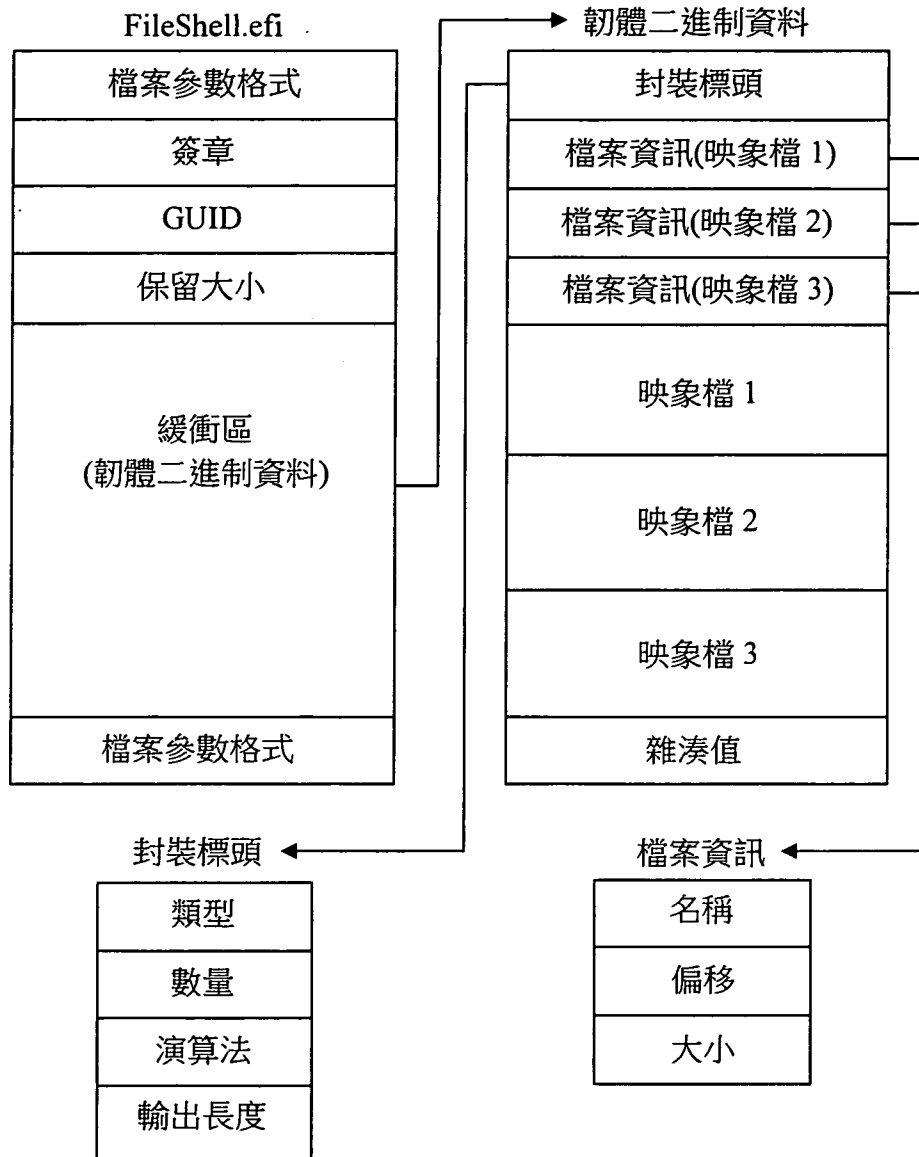


圖 1

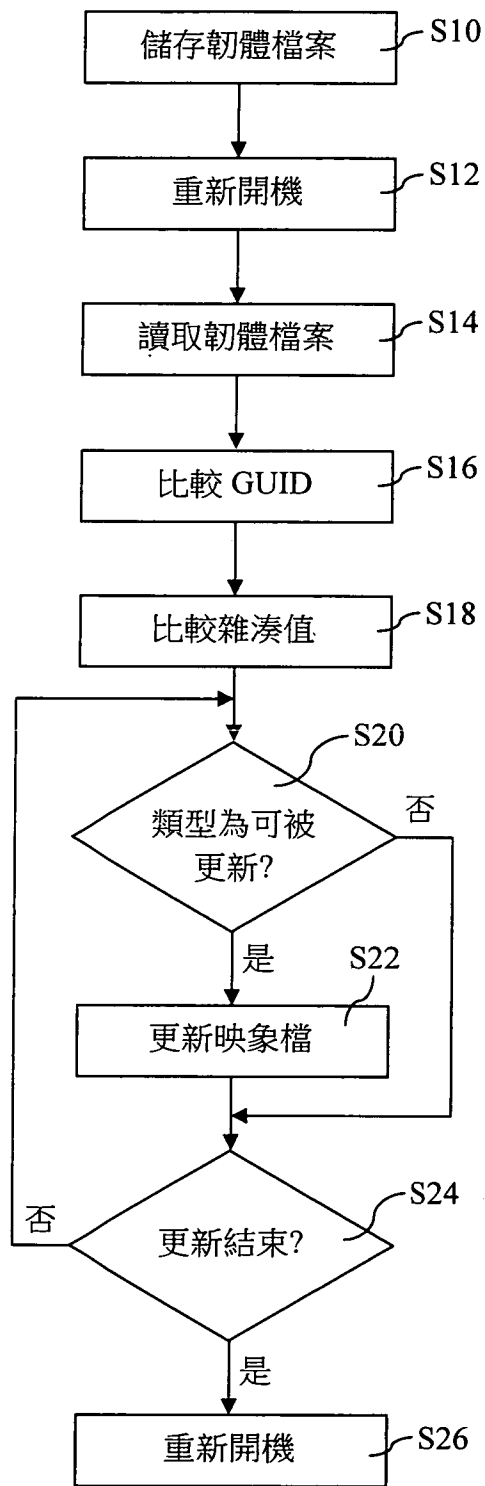


圖 2