公告本

發明專利說明書

101年12月20日修正替換頁

中文說明書替換(101 年 12 月)

（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：094147065

※ 申請日期：94.12.28　　※IPC 分類：G06F 9/54, 9/445 15/163

一、發明名稱：（中文/英文）

保全韌體之更新

SECURE FIRMWARE UPDATE

二、申 請 人：（共 1 人）

姓名或名稱：（中文/英文）

塞席爾商金萊控股有限公司

KINGLITE HOLDINGS INC.

代表人：（中文/英文）

羅素 鮑伍德

BOLTWOOD, RUSSELL

住居所或營業所地址：（中文/英文）

新加坡泰瑪賽克大道 7 號新達城一座 #15-01A

7 TEMASEK BOULEVARD, #15-01A SUNTEC TOWER ONE,

SINGAPORE 038987

國　籍：（中文/英文）

塞席爾島　SEYCHELLES

三、發明人：(共 5 人)

姓　名：(中文/英文)

1. 安德魯　寇特瑞爾
   COTTRELL, ANDREW
2. 吉森卓　貝斯勒
   BETHUR, JITHENDRA
3. 堤摩西　J　瑪奇
   MARKEY, TIMOTHY J.
4. M　席瑞肯
   SRIKANT, M.
5. 拉克斯曼納　席瑞尼瓦森
   SRINIVASAN, LAKSHMANAN

國　籍：(中文/英文)

1. 英國　U.K.
2. 印度　INDIA
3. 美國　U.S.A.
4. 美國　U.S.A.
5. 印度　INDIA

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；2004 年 12 月 29 日；11/026,813

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：

本發明揭示一保全韌體更新方法，其包括接收一韌體之更新影像，例如，包括校正或更新功能性之韌體程式碼。接下來，鑑定該韌體之更新影像及該韌體之更新影像之源。在該韌體之更新影像及該韌體之更新影像之該源已經鑑定之後，當前韌體影像為該韌體之更新影像所替換。若新的韌體影像或韌體更新模組中之任一者未經授權，則記憶體保持鎖定；藉此，防止未經授權之韌體影像快閃至該記憶體中。一電子裝置包括一處理器及一記憶體。該記憶體保存由該處理器執行時使該處理器接收一韌體之更新影像之指令。接下來，該等指令使該處理器鑑定該韌體之更新影像及該影像之源。在該韌體之更新影像及該韌體之更新影像之源已經鑑定之後，該當前韌體影像為該韌體之更新影像所替換。

六、英文發明摘要：

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:

10	電子裝置/膝上型電腦
12	控制器/處理器
13	匯流排
14	非揮發性記憶體/第一記憶體
15	BIOS程式碼
16	第二記憶體/RAM
17	應用程式
18	收發器
19	新的或經更新之韌體影像
20	顯示器控制器
21	顯示裝置
22	I/O控制器
23	鍵盤
24	滑鼠
25	印表機
26	韌體應用模組(FAM)
32	影像資料
33	經格式化之資料

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】

本發明大體而言係關於電子裝置，且更明確地說，係關於保全地更新在電子裝置上執行之韌體。

【先前技術】

電子裝置(例如，膝上型電腦，桌上型電腦，個人數位助理(PAD))，網際網路器具、嵌入式裝置(例如，路由器及機上盒)，無線通信裝置及其它類似裝置及其組合)通常包括一控制器(例如，中央處理單元)及一含有韌體或由控制器執行之其它適當程式碼之非揮發性記憶體或唯讀記憶體(ROM)。當最初將電子裝置加電時，一基於特定ROM之程式碼(例如，基本輸入/輸出系統(BIOS)程式碼)藉由控制器來掌握電子裝置之控制。

BIOS負責初始化且組態各種硬體子系統(例如，顯示器控制器、輸入/輸出(I/O)控制器或其它適當元件或電子裝置中出現或受其控制之系列元件)，且啟動作業系統(OS)開機過程。此等初始化及開機任務通常被稱為開機自我測試(POST)。現在，時新的個人電腦(PC)系統使用一快閃記憶體；藉此，允許更新BIOS。

有時，原始設備製造商(OEM's)或原始裝置製造商(ODM's)發佈校正各種問題之更新資料或將增強(enhancements)添加至BIOS。更新資料係提供為BIOS之先前版本之經校正影像，或進行校正或增強之BIOS之版本。在更新期間，新的BIOS影像(例如)藉由一快閃更新過程來替換原始的BIOS影

像。為了使BIOS可更新，在電子裝置(例如個人電腦)已啟動作業系統後，儲存BIOS影像之快閃記憶體必須保持為一解鎖狀態。由於快閃記憶體或其它適當之記憶體未被鎖定，故可藉由能夠存取記憶體之任何過程來修改記憶體。因為快閃記憶體可更新，所以其亦容易受到惡意或其它不期望之攻擊的損害。

舉例而言，一攻擊者(例如，個人或第三方程式)可(經由一快閃更新過程)將未經授權之韌體插入快閃記憶體中，該快閃記憶體模擬所替換之BIOS之功能性以及執行未經授權之行為，例如，監視使用者之按鍵敲擊或自網際網路下載額外的或未經授權之程式。此韌體大體上不受由現有病毒偵測程式之偵測的影響，此歸因於快閃更新過程之不保全特性。

防止攻擊之習知方法包括提供具有快閃記憶體之電子裝置，該等快閃記憶體支持一經鎖定即不能解瑣直至裝置電力經循環之可鎖定記憶體範圍。電力循環通常發生在電子裝置處於一冷開機過程時。與使用冷開機過程以控制可應用記憶體之鎖定相關之一缺點為，冷開機過程花費一相對長之時間(例如，三分鐘以上)來完成其；從而令使用者失望。

【發明內容】

一保全韌體更新方法包括接收一韌體之更新影像，例如，包括校正或更新功能性之韌體程式碼。接下來，鑑定韌體之更新影像及韌體之更新影像之源。在一示範性實施例中，根據本發明運作之一裝置包括一鎖定記憶體。在基

本輸入輸出系統或相應裝置之其它核心系統軟體(CSS)內提供一韌體應用模組以調用一經授權之韌體更新模組，該韌體更新模組鑑定新的或經更新的韌體影像及韌體之更新影像之源。執行解鎖記憶體且鑑定韌體之更新影像及韌體之更新影像之源的狀態。在韌體之更新影像及韌體之更新影像之源已經鑑定之後，當前韌體影像(例如)藉由重新快閃記憶體而為韌體之更新影像所替換。在一S3恢復模式下執行記憶體解鎖。若新的韌體之更新影像或韌體之更新影像之源中之任一者未經授權，則記憶體保持鎖定；藉此，防止未經授權之韌體影像快閃至記憶體中。

S3恢復模式係指裝置之電力管理狀態之改變，例如，自S3狀態變至S0狀態。稱為待命之S3狀態係一中間省電狀態，裝置之元件中之一些(例如，中央處理單元)掉電以節約能源。S0狀態係指裝置之正常全功率狀態。當裝置處於S3狀態時，保存系統記憶體之內容以允許裝置快速地進入S0狀態。藉由在S3狀態期間實施快閃記憶體更新，確保更新之保全及鑑定，且避免伴隨習知冷開機過程之等待時間。

一電子裝置包括一處理器及一耦接至該處理器之記憶體。該記憶體包括由該處理器執行時使該處理器接收一韌體之更新影像(例如，校正當前韌體影像中出現的一些功能性或增加當前韌體影像之增強的一新的韌體影像或一經更新之韌體影像)的指令。接著，處理器鑑定韌體之更新影像及韌體之更新影像之源，以確保經更新之韌體影像係有效的且係由一可信源提供。在一示範性實施例中，電子裝置

包括一鎖定記憶體，例如，一快閃記憶體或保存裝置韌體之其它非揮發性記憶體。該等指令使該處理器解鎖該記憶體且起始韌體之更新影像及韌體源鑑定過程。在鑑定韌體之更新影像及韌體之更新影像之源之後，該等指令使該處理器(例如)藉由重新快閃非揮發性記憶體而以韌體之更新影像替換當前韌體影像。在完成更新後，鎖定記憶體；藉此，防止未經授權之韌體影像存取經更新之韌體影像。

本發明提供之一優勢為裝置之保全性得到保持，因為當更新之韌體影像及更新之韌體影像之源皆來自經授權或可信源時，僅替換或更新韌體。

本發明提供之另一個優勢為韌體更新之效率得到改良，因為不必執行一冷開機過程。

【實施方式】

圖1為一示範性電子裝置10的示意性方塊圖，例如，一桌上型電腦，一膝上型電腦，平板PC，個人數位助理(PDA)，網際網路器具，嵌入式裝置(例如，路由器及機上盒)，無線通信裝置(例如，行動電話)或併有根據本發明之保全韌體更新功能性之其它適當裝置及其組合。出於說明而非限制之目的，該電子裝置10係表示為一膝上型電腦，其包括至少一處理器或其它適當控制器12，一第一記憶體14(例如，NVRAM、ROM、快閃記憶體或其它適當之非揮發性記憶體)，一第二記憶體16(例如，RAM或其它適當之揮發性記憶體)，一收發器18，一顯示器控制器20及一輸入/輸出(I/O)控制器22。第一記憶體14、第二記憶體16、收發器18、顯

示器控制器20及I/O控制器22係完全全部互連，且經由一匯流排13在各種其它元件(例如，硬體子系統)與處理器12之間傳送資料及指令。

處理器12可包括一用於執行計算之算術邏輯單元(ALU)，用於資料及指令之臨時儲存的一或多個暫存器，及一用於控制膝上型電腦10之運作的控制器。在一實施例中，處理器12包括由Intel公司製造之x86、Pentium™及PentiumPro™微處理器或由Advanced Micro Devices銷售之K-6微處理器中之任一者。進一步實例包括由Cyrix Corp.銷售之6X86MX微處理器，由Motorola銷售之680X0處理器，或由International Business Machines銷售之Power PC™處理器。另外，各種其它處理器中之任一種(包括來自Sun Microsystems、MIPS、NEC、Cyrix及其它之彼等處理器)可用於實施處理器12。處理器12不限於微處理器，而是可具有其它形式，諸如微控制器、數位訊號處理器(DSP)、專用硬體(例如，特殊應用積體電路(ASIC))、狀態機或分佈於一網路上之一或多個處理器上執行之軟體。

舉例而言，匯流排13可實施為含有位址、指令及/或資料資訊之傳送且為其作準備之一或多個線路，一包括含有位址、指令及/或資料資訊之一或多個經調變之訊號的載波，或用於傳送訊號或其組合之任何適當媒體或架構。出於說明而非限制之目的，匯流排13可實施為一周邊元件互連(PCI)匯流排，一通用串列匯流排(USB)介面或其它適當之匯流排或通信架構。

第一記憶體14可由一非揮發性記憶體(例如，一唯讀記憶體(ROM)、快閃記憶體)、複數個記憶體裝置、諸如一網路上之伺服器之分散式記憶體、或能夠將電訊號保存於其中之其它適當裝置來實施。第一記憶體14包括其專用於基本輸入/輸出系統(BIOS)程式碼15之部分，該程式碼可用於在一最初通電或恢復操作期間初始化且組態膝上型電腦10之硬體及其它子系統(例如，顯示器控制器20、I/O控制器22)。另外，該BIOS程式碼15包括當由處理器12執行時使處理器12執行根據本發明之保全韌體更新功能性之指令。第一記憶體14之內容得以在膝上型電腦10之斷電或掉電期間保存。

另外，BIOS 15可儲存在一處理器可讀媒體中或藉由一嵌入於一載波中之電腦資料訊號經由一傳輸媒體或其它適當通信鏈路來傳輸。處理器可讀媒體可包括可儲存或傳送資訊之任何媒體，例如，一電子電路、一半導體記憶體裝置、一ROM、一快閃記憶體、一可擦可程式化唯讀記憶體(EPROM)、一軟碟、一緊密光碟-唯讀記憶體(CD-ROM)、一光碟、一光纖媒體、一射頻(RF)鏈路或其它適當媒體。該電腦資料訊號可包括可經由一傳輸媒體(例如，電子網路通道、光纖、空氣、電磁波、RF鏈路或其它適當傳輸媒體或其組合)傳播之任何訊號。該等碼段可經由電腦網路(例如，網際網路、一企業內部網、LAN、WAN或其它適當網路或其組合)下載。

第二記憶體16為一快速存取記憶體，例如，一隨機存取

記憶體(RAM)，其保存應用程式17，例如，文字處理、記帳、電子郵件、MP3程式、瀏覽器及其它適當程式或其組合，此等應用程式係經由匯流排13傳輸至處理器12以用於執行。當膝上型電腦10處於全功率(S0)或待命(S3)模式時，保存RAM 16之內容，但在斷電或掉電狀態期間不保存該等內容。雖然第二記憶體16被描述為一快速存取揮發性記憶體，但是一般技術者應認識且瞭解，其它記憶體組態(例如，一網路上分佈之記憶體)可用來替換RAM 16，且該等替換實施例涵蓋且屬於本發明之精神及本發明之範疇。

收發器18可包括任何適當元件，例如，一天線、數據機或能夠發送或接收資訊(例如，一將施加至膝上型電腦10之新的或經更新之韌體影像19)之無線裝置。

顯示器控制器20自處理器12或一相應影像/圖形子系統(未圖示)接收影像資料32且提供經格式化資料33以在一相應顯示裝置21(例如，一陰極射線管(CRT)、平板、電腦監控器或能夠呈現影像及/或資料之其它適當裝置)上顯示其。經格式化之資料33亦可保存在RAM 16中以用於隨後顯示或處理。

I/O控制器22經組態以控制複數個輸入裝置(例如，一鍵盤23、滑鼠24、雷射或光指標、操縱桿或其它周邊輸入裝置)與複數個輸出裝置(例如，一印表機25)之間的資訊傳輸。

在應用中，僅當新的或經更新之韌體影像19經授權且新的或經鑑定之韌體影像19之源為一經授權或可信任方時，本發明才允許新的或經更新之韌體影像19替換保存在非揮

發性記憶體14中之當前韌體(例如，BIOS 15)。藉由提供此雙層保全，大體上減少或消除了對非揮發性記憶體14及一部分係由非揮發性記憶體14形成之大型裝置之未經授權存取。當膝上型電腦10運行時，非揮發性記憶體14處於一鎖定狀態。當膝上型電腦10處於S3狀態時，更新非揮發性記憶體14僅回應於一S3恢復模式狀況發生。稱為待命之S3狀態為一中間省電狀態，膝上型電腦10之該等元件中之一些(例如，處理器12)在此狀態下掉電以節約能源。S0狀態係指膝上型電腦10之正常全功率狀態。當膝上型電腦10處於S3狀態時，保存第二或系統(例如，RAM)記憶體16之內容以允許膝上型電腦10快速進入S0狀態。

圖2為韌體應用模組(FAM) 26的表示，該韌體應用模組形成BIOS 15(圖1)或韌體程式碼之部分，且其經組態以提供根據本發明之保全快閃更新功能性。運行時，處理器12藉由調用FAM 26來起始並控制非揮發性記憶體14之更新。FAM 26包括一判定將快閃至記憶體14中之新的韌體影像19之授權的鑑定韌體更新模組(FUM)42。舉例而言，在一示範性實施例中，授權係藉由一RSA密鑰對(例如，公用密鑰/私人密鑰)鑑定技術來判定。在應用中，一OEM產生一RSA密鑰對，接著將該密鑰對之公用組份包覆在一二元模組中，且其包括與該新產生之韌體影像之部分相同的部分，其接著經散列以建立一無符號之公用密鑰容器。該私人密鑰接著用於標記公用密鑰容器；藉此，建立一經數位標記之容器。此數位簽名係授權新的或更新之韌體影像19之簽名。若公

用及私人密鑰匹配，則新的或經更新之韌體影像19經授權；否則，韌體之更新影像19未經授權。若新的韌體之更新影像19及韌體之更新影像19之源皆未經授權，則否定更新且非揮發性記憶體14保持鎖定。若新的韌體之更新影像19及該韌體之更新影像之源皆經授權，則非揮發性記憶體14被解鎖且接著如相對於圖3-5所論述的，以韌體之更新影像19重新快閃其。非揮發性記憶體14接著返回至其鎖定狀態。

舉例而言，新的或經更新之韌體影像19包括將寫入至膝上型電腦之非揮發性記憶體中且保存在其中之新的韌體程式碼19a，及用於鑑定新的韌體程式碼19a且有助於快閃(記憶體)更新過程之執行之新的韌體影像憑證19b。在一示範性實施例中，該等韌體影像憑證19b係保存在一包括(例如)新的韌體程式碼之一SHA-1散列法之有符號的容器中。舉例而言，使用一般技術者熟知之RSA演算法以一保全私人密鑰來密碼標記該容器。RSA演算法指定一分別用於加密/標記及解密/驗證之公用及私人密鑰。通常，RSA處理與一相應PKI相關。因此，本發明使用一嵌入調用應用程式中之密碼標記之程式碼模組19b來執行快閃更新過程。此為該更新過程提供一附加的保全等級；藉此，大體上減少或消除攻擊或防止記憶體更新處理之能力。

圖3為一說明實施根據本發明之保全韌體更新方法100時由膝上型電腦執行之操作的流程圖。下列步驟係藉由及/或結合膝上型電腦之BIOS或核心系統軟體來執行。在步驟102

中，膝上型電腦接收一請求一韌體更新之命令。舉例而言，此可藉由使用者輸入一更新系統韌體之命令，一內部產生之訊號或中斷請求一更新命令訊號或自一遠端位置接收之一更新命令訊號來完成。

在步驟104中，將新的或經更新之韌體影像及鑑定資訊(例如，新的韌體影像憑證)載至揮發性記憶體中且將其初始化。舉例而言，此可藉由以下方式來完成：膝上型電腦接收新的或經更新之韌體影像及新的或經更新之韌體影像憑證且將韌體影像及憑證置於保全快閃應用程式目錄中。

在步驟106中，使膝上型電腦處於一S3暫止狀態。舉例而言，此可藉由在DOS快閃應用程式中明確地搜尋且程式化ACPI暫存器或使用視窗快閃應用程式中之視窗S3 API來完成。當進入S3狀態時，解鎖非揮發性記憶體且將新的或經更新之韌體影像傳輸至膝上型電腦以用於非揮發性記憶體(例如，快閃記憶體)的隨後重新快閃。

在步驟107中，做出關於是應恢復還是繼續S3狀態之判定。舉例而言，此可藉由檢查一專用暫存器之狀態來達到，或BIOS ACPI POST程式碼藉由檢查ACPI表做出是否恢復S3之判定。若不恢復S3狀態，則該方法繼續至鎖定非揮發性記憶體之步驟108。舉例而言，此可藉由一實施閉鎖演算法(flash lock-down algorithm)之完善PNPNVS模組來完成。此演算法本身是快閃部分規格且係由賣主提供。若繼續S3狀態，則該方法繼續至步驟109。

在步驟109中，做出關於FAM之資料交換區域是否經填充

之判定。在應用中，該資料交換區域位於SMM中且係經由32位元之SMI調度器由SFLS API來存取。舉例而言，此可藉由FAM以至該韌體影像及其憑證及該韌體影像及其憑證之指標填充一引數封包(argument packet)及調用SFLS API之Put函數來完成。S3恢復處置器中之BIOS接著調用SFLS之Get函數以檢查該等指標是否經填充。若未填充該資料交換區域，則該方法繼續至鎖定非揮發性記憶體之步驟114。否則，該方法繼續至步驟110。

在步驟110中，做出關於新的韌體是否已經鑑定之判定。舉例而言，此係藉由提取該簽名(例如，新的韌體更新憑證)區塊及以BIOS中嵌入之公用密鑰來驗證(例如，解密)加密之新的韌體影像且接著重新散列該韌體影像及與容器中儲存之散列進行比較來完成。若新的韌體之更新影像已經鑑定，則該方法繼續至重新快閃記憶體之步驟112；藉此以該新的經鑑定之韌體之更新影像替換舊的韌體。否則，該方法繼續至鎖定非揮發性記憶體之步驟114。

圖4為說明載入及初始化新的韌體之更新影像及新的韌體鑑定憑證時執行之操作的流程圖。在步驟142中，將該新的韌體影像、新的韌體影像憑證、該韌體更新模組及該等韌體模組更新憑證載至記憶體中。

在步驟144中，將該韌體更新模組、韌體更新模組憑證、新的或經更新之韌體影像及新的或經更新之韌體影像憑證寫入該韌體應用模組之資料交換區域。在已填充該資料交換區域後，該過程繼續至使膝上型電腦處於一暫止(例如，

S3模式)狀態之步驟106(圖3)。藉由在S3模式期間實施記憶體更新，確保更新之保全及鑑定，以及避免伴隨習知冷開機過程之等待時間。

圖5為說明判定該新的或經更新之韌體鑑定過程是否已成功時執行之操作的流程圖。在步驟158中，自該韌體應用模組之資料交換區域讀取該韌體更新模組、韌體更新模組憑證、新的或經更新之韌體影像及該等新的或經更新之韌體影像憑證。

在步驟160中，鑑定該等韌體更新模組憑證及新的或經更新之韌體影像憑證。舉例而言，此係藉由提取該韌體影像憑證區塊或模組及利用嵌入之公用密鑰解密該等憑證來完成。若解密成功，則驗證成功或完成；否則，驗證不成功。在完成驗證之後，將控制傳輸至韌體更新模組，其接著在步驟112(圖3)中開始重新快閃該非揮發性記憶體之過程。

出於說明及描述之目的，已提供本發明之前述詳細描述。雖然已參看該等附式於本文中詳細描述了本發明之一示範性實施例，但應瞭解，本發明不限於所揭示之該(該等)精確實施例，且根據上述教示，本發明之各種改變及修改係可能的。因此，本發明之範疇將由附加於此之申請專利範圍界定。

【圖式簡單說明】

圖1為實施根據本發明之保全快閃更新功能性之一示範性電子裝置的示意性方塊圖；

圖2為經組態以在根據本發明之電子裝置執行時提供保

全快閃更新功能之程式碼的表示；及

圖3-5為說明根據本發明在實施該保全韌體更新功能性時，由電子裝置執行之操作的流程圖。

【主要元件符號說明】

10	膝上型電腦/電子裝置
12	控制器/處理器
13	匯流排
14	非揮發性記憶體/第一記憶體
15	BIOS程式碼
16	第二記憶體/RAM
17	應用程式
18	收發器
19	新的或經更新之韌體影像
19a	新的韌體程式碼
19b	新的韌體影像憑證
20	顯示器控制器
21	顯示裝置
22	I/O控制器
23	鍵盤
24	滑鼠
25	印表機
26	韌體應用模組(FAM)
32	影像資料
33	經格式化之資料
42	鑑定韌體更新模組(FUM)

十、申請專利範圍：

1. 一種用於更新一具有一非揮發性記憶體之電子裝置之方法，其包含：

接收一韌體更新影像，該韌體更新影像具有一第一公用加密密鑰(first public encryption key)及一第二公用加密密鑰，該第一公用加密密鑰對應於一第一私人加密密鑰(first private encryption key)，以形成一第一加密密鑰對，該第二公用加密密鑰對應於一第二私人加密密鑰，以形成一第二加密密鑰對，且該第一加密密鑰對不同於該第二加密密鑰對；

利用經過該第一加密密鑰對密碼標記(cryptographically signed)的一碼模組(code module)來鑑定該韌體更新影像之來源；

利用該第二加密密鑰對來鑑定該韌體更新影像；及

若該韌體更新影像之來源經該第一加密密鑰對鑑定且該韌體更新影像經該第二加密密鑰對鑑定，則以該韌體更新影像取代一現有韌體影像；

其中該碼模組經嵌入於一應用程式中，該應用程式係用於以該韌體更新影像取代該現有韌體影像。

2. 如請求項1之方法，其進一步包括將該韌體更新影像寫入至該非揮發性記憶體之一資料交換區域(data exchange area)。

3. 如請求項1之方法，其中該韌體更新影像覆寫(overwrite)一基本輸入/輸出系統(BIOS)軟體之至少一部分公用公

用。

4. 如請求項1之方法，其中該韌體更新影像覆寫一核心系統軟體(CSS)之至少一部分。

5. 如請求項1之，其中以該韌體更新影像取代該現有韌體影像的步驟發生在一中間省電狀態中。

6. 如請求項1之方法，其中以該韌體更新影像取代該現有韌體影像的步驟不必執行一冷開機。

7. 如請求項1之方法，其進一步包括：在該取代該現有韌體影像的步驟之前，解鎖該非揮發性記憶體包含該韌體影像之至少一部分；及在該取代該現有韌體影像的步驟之後，鎖定該非揮發性記憶體包含該韌體影像之至少該部分。

8. 一種電子裝置，其包含：

一處理器；

一非揮發性記憶體；及

一耦接至該處理器之RAM記憶體，該RAM記憶體保存指令，該等指令在由該處理器執行時使該處理器執行以下步驟：

接收一韌體更新影像，該韌體更新影像具有一第一公用加密密鑰及一第二公用加密密鑰，該第一公用加密密鑰對應於一第一私人加密密鑰，以形成一第一加密密鑰對，該第二公用加密密鑰對應於一第二私人加密密鑰，以形成一第二加密密鑰對，且該第一加密密鑰對不同於該第二加密密鑰對；

利用經過該第一加密密鑰對密碼標記的一碼模組來鑑定該韌體更新影像之來源；

利用該第二加密密鑰對來鑑定該韌體更新影像；及

若該韌體更新影像之來源經該第一加密密鑰對鑑定且該韌體更新影像經該第二加密密鑰對鑑定，則以該韌體更新影像取代一現有韌體影像；

其中該碼模組經嵌入於一應用程式中，該應用程式係用於以該韌體更新影像取代該現有韌體影像。

9. 如請求項8之電子裝置，其中該非揮發性記憶體及該RAM記憶體保存指令，當該等指令由該處理器執行時，之至少一者使該處理器進一步執行以下步驟：將該韌體更新影像寫入至該非揮發性記憶體之一資料交換區域。

10. 如請求項8之電子裝置，其中該韌體更新影像覆寫一基本輸入/輸出系統(BIOS)軟體之至少一部分。

11. 如請求項8之電子裝置，其中該韌體更新影像覆寫一核心系統軟體(CSS)之至少一部分。

12. 如請求項8之電子裝置，其中以該韌體更新影像取代該現有韌體影像的步驟發生在一中間省電狀態中。

13. 如請求項8之電子裝置，其中以該韌體更新影像取代該現有韌體影像的步驟不必執行一冷開機。

14. 如請求項8之電子裝置，其中該非揮發性記憶體及該RAM記憶體之至少一者保存指令，當該等指令由該處理器執行時，使該處理器進一步執行以下步驟：在該取代該現有韌體影像的步驟之前，解鎖該非揮發性記憶體包含該

韌體影像之至少一部分；及在該取代該現有韌體影像的步驟之後，鎖定該非揮發性記憶體包含該韌體影像之至少該部分公用公用。

15. 一種更新一具有一非揮發性記憶體之電子裝置之方法，其包含：

接收一韌體更新影像，該韌體更新影像具有一第一公用加密密鑰及一第二公用加密密鑰，該第一公用加密密鑰對應於一第一私人加密密鑰，以形成一第一加密密鑰對，該第二公用加密密鑰對應於一第二私人加密密鑰，以形成一第二加密密鑰對，且該第一加密密鑰對不同於該第二加密密鑰對；

將該韌體更新影像寫入至該非揮發性記憶體之一資料交換區域；

利用經過該第一加密密鑰對密碼標記的一碼模組來鑑定該韌體更新影像之來源；

利用該第二加密密鑰對來鑑定該韌體更新影像；及

若該韌體更新影像之來源經該第一加密密鑰對鑑定且該韌體更新影像經該第二加密密鑰對鑑定，則以該韌體更新影像取代一現有韌體影像；

其中該碼模組經嵌入於一應用程式中，該應用程式係用於以該韌體更新影像取代該現有韌體影像。

16. 如請求項15之方法，其中該韌體更新影像覆寫一基本輸入/輸出系統(BIOS)軟體之至少一部分公用公用。

17. 如請求項15之方法，其中該韌體更新影像覆寫一核心系

統軟體(CSS)之至少一部分。

18. 如請求項15之方法，其中以該韌體更新影像取代該現有韌體影像的步驟發生在一中間省電狀態中。

19. 如請求項15之方法，其中以該韌體更新影像取代該現有韌體影像的步驟不必執行一冷開機。

20. 如請求項15之方法，其進一步包括：在該取代該現有韌體影像的步驟之前，解鎖該非揮發性記憶體包含該韌體影像之至少一部分；及在該取代該現有韌體影像的步驟之後，鎖定該非揮發性記憶體包含該韌體影像之至少該部分。

十一、圖式：

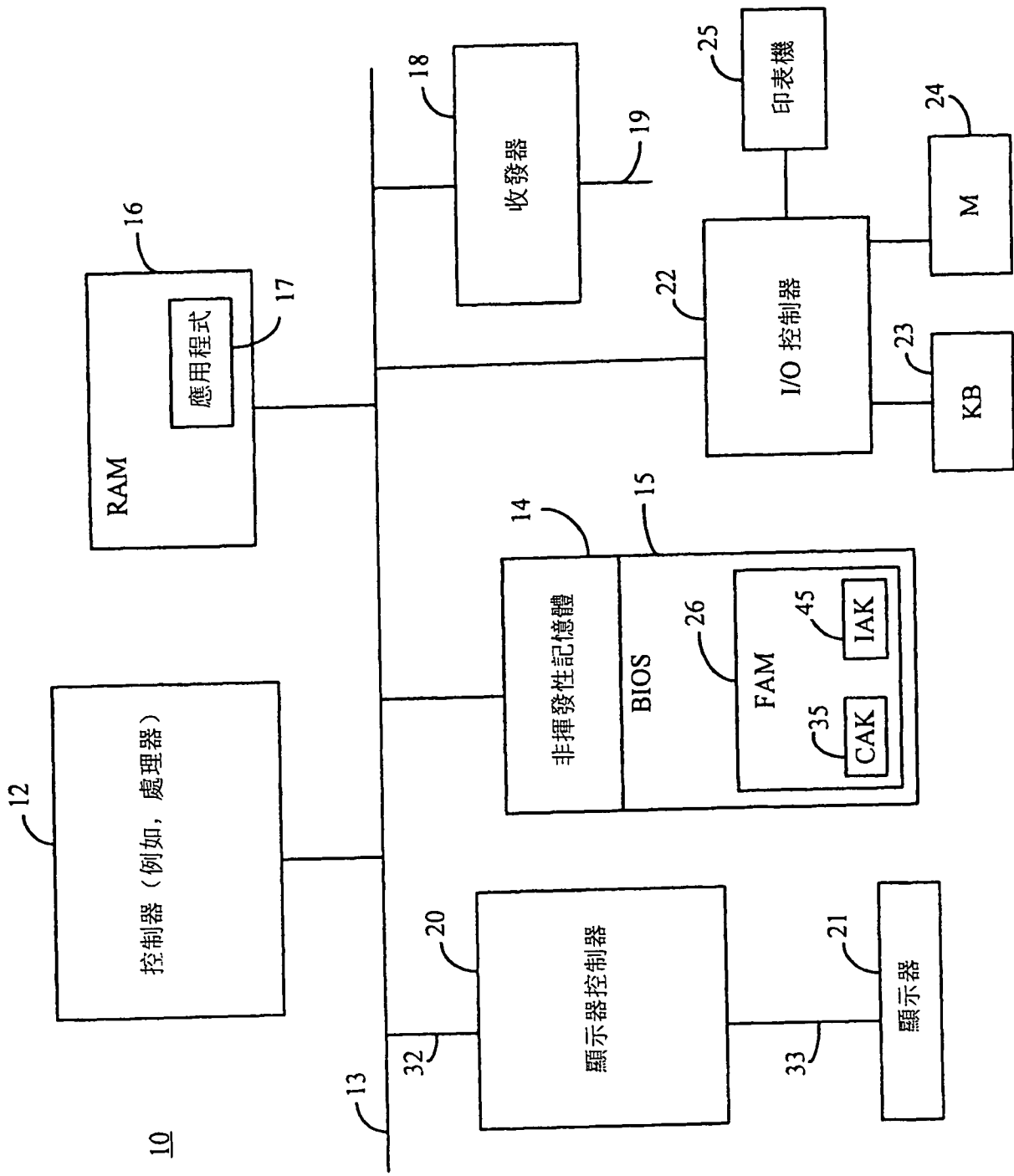
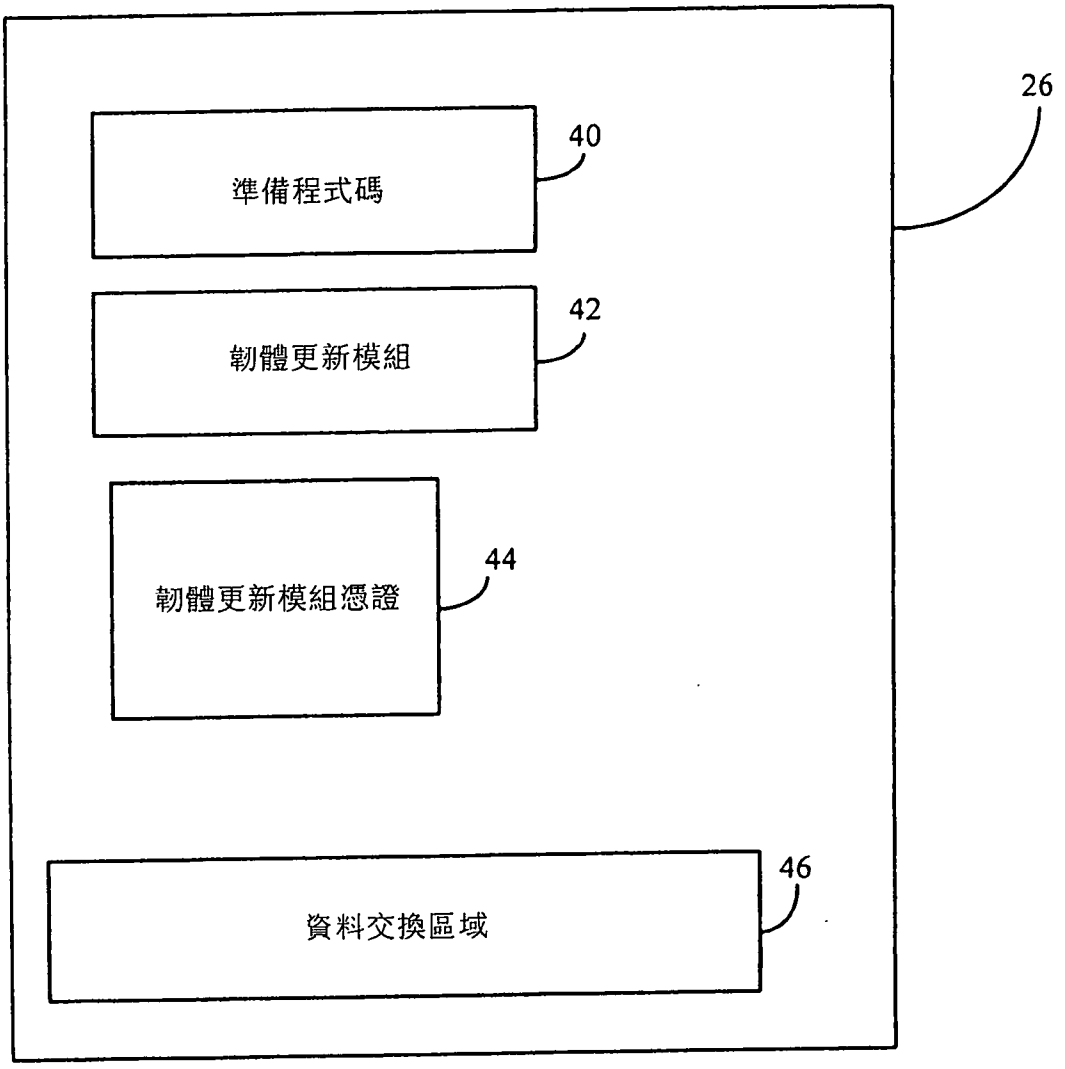

10
控制器（例如，處理器）
12
RAM
16
應用程式
17
13
32
顯示器控制器
20
33
顯示器
21
非揮發性記憶體
14
BIOS
15
FAM
26
IAK
45
CAK
35
收發器
18
19
I/O 控制器
22
印表機
25
M
24
KB
23

圖 1


26
40
準備程式碼
42
韌體更新模組
44
韌體更新模組憑證
46
資料交換區域

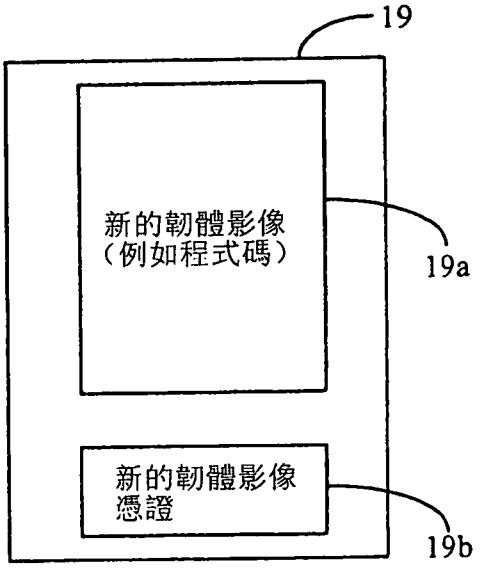
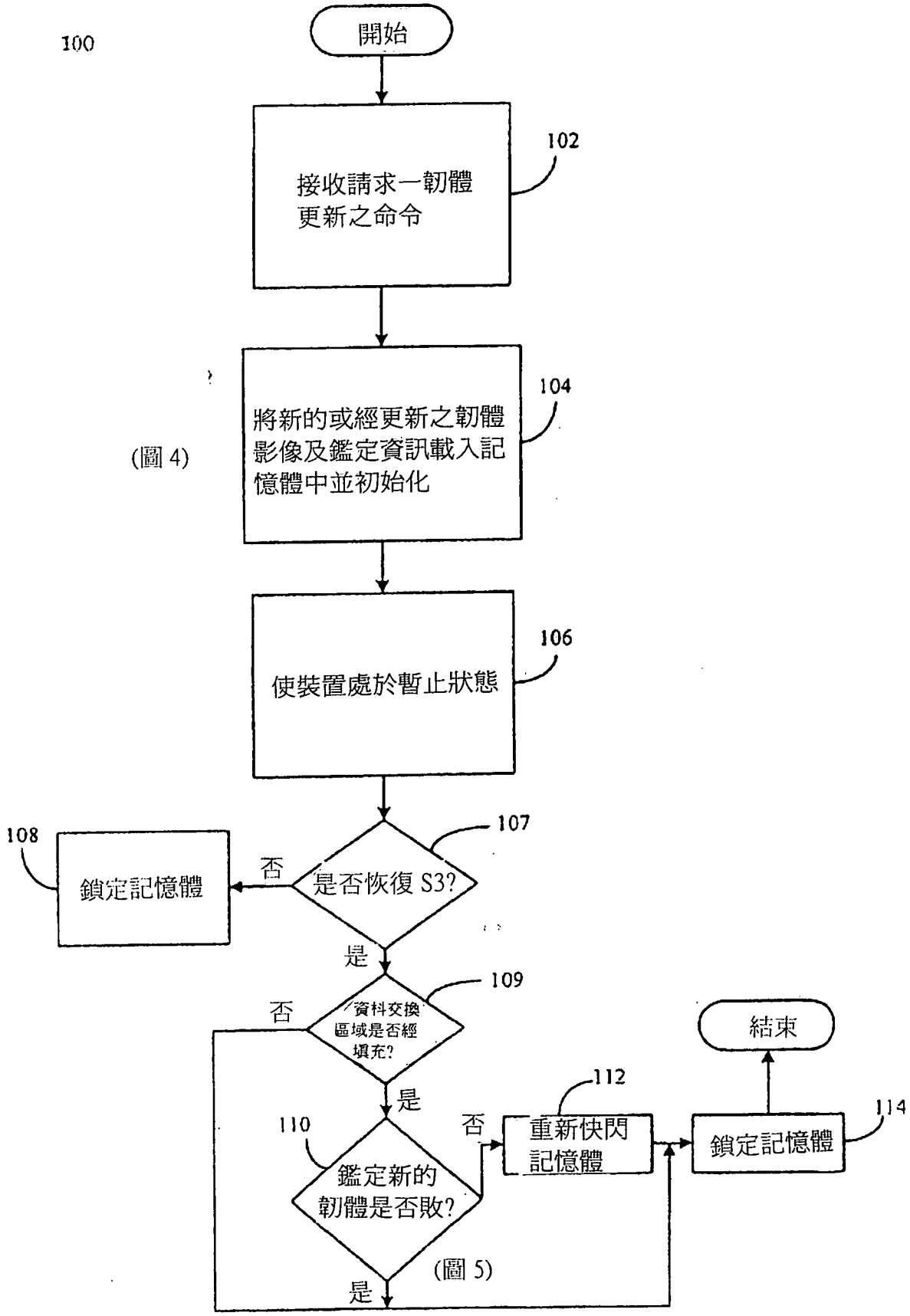

19
新的韌體影像
（例如程式碼）
19a
新的韌體影像
憑證
19b

圖 2


100
開始
接收請求一韌體更新之命令
102
將新的或經更新之韌體影像及鑑定資訊載入記憶體中並初始化
104
使裝置處於暫止狀態
106
是否恢復 S3?
107
否
鎖定記憶體
108
是
資料交換區域是否經填充?
109
否
是
鑑定新的韌體是否敗?
110
否
重新快閃記憶體
112
鎖定記憶體
114
是
結束

(圖 4)

(圖 5)

圖 3

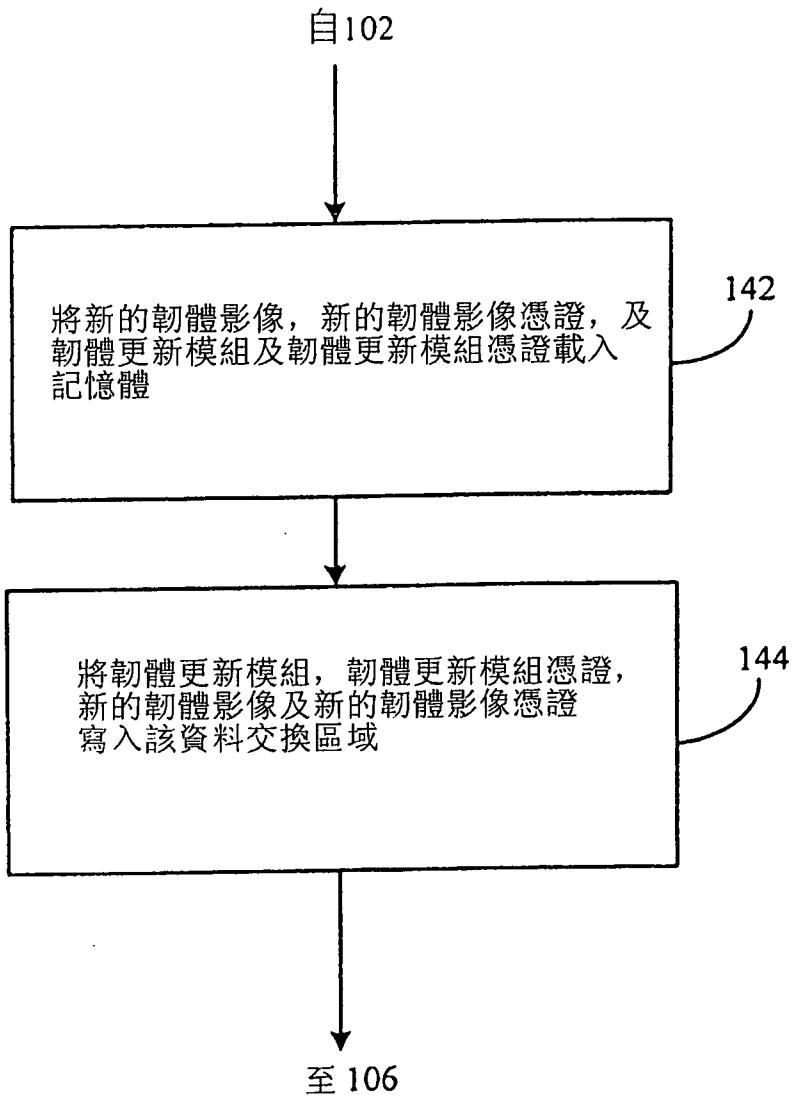

自102
將新的韌體影像，新的韌體影像憑證，及韌體更新模組及韌體更新模組憑證載入記憶體
142
將韌體更新模組，韌體更新模組憑證，新的韌體影像及新的韌體影像憑證寫入該資料交換區域
144
至106

圖 4

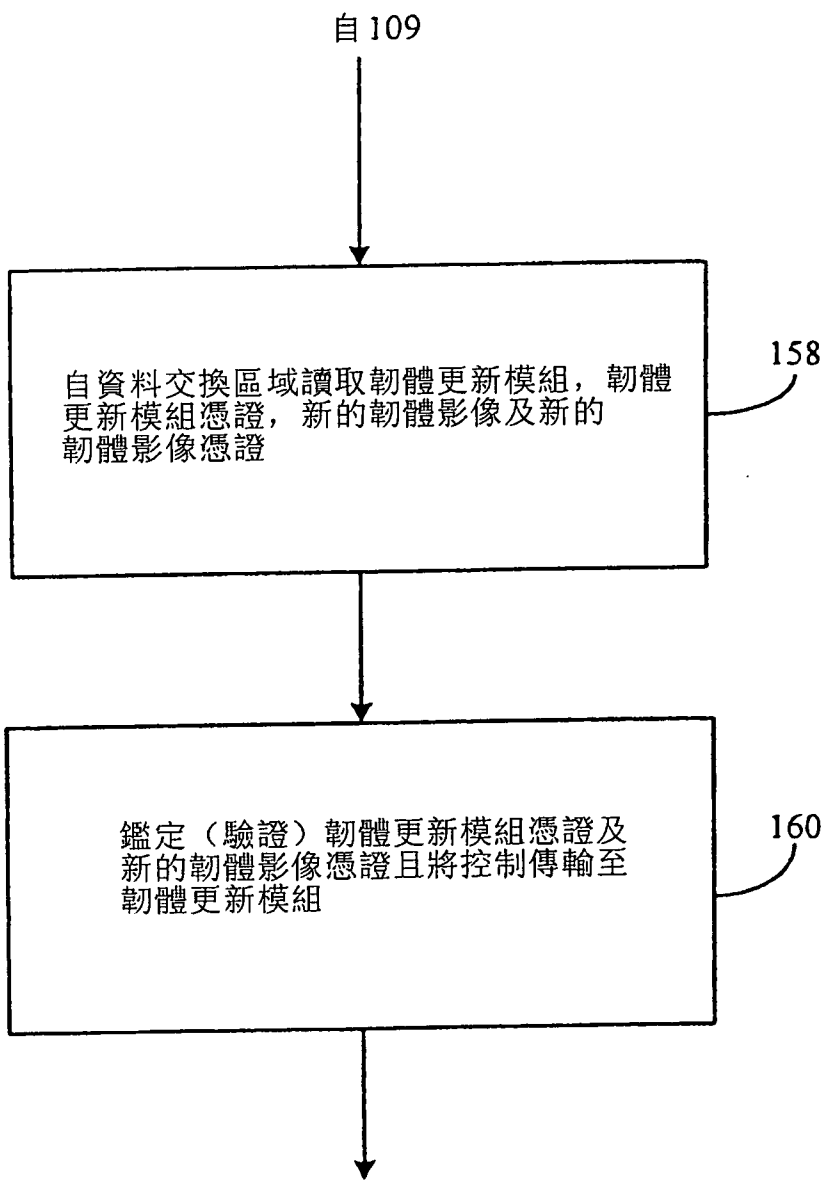

自 109
自資料交換區域讀取韌體更新模組，韌體更新模組憑證，新的韌體影像及新的韌體影像憑證
158
鑑定（驗證）韌體更新模組憑證及新的韌體影像憑證且將控制傳輸至韌體更新模組
160
至 112

圖 5