(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 201346764 A
(43)公開日： 中華民國 102 (2013) 年 11 月 16 日

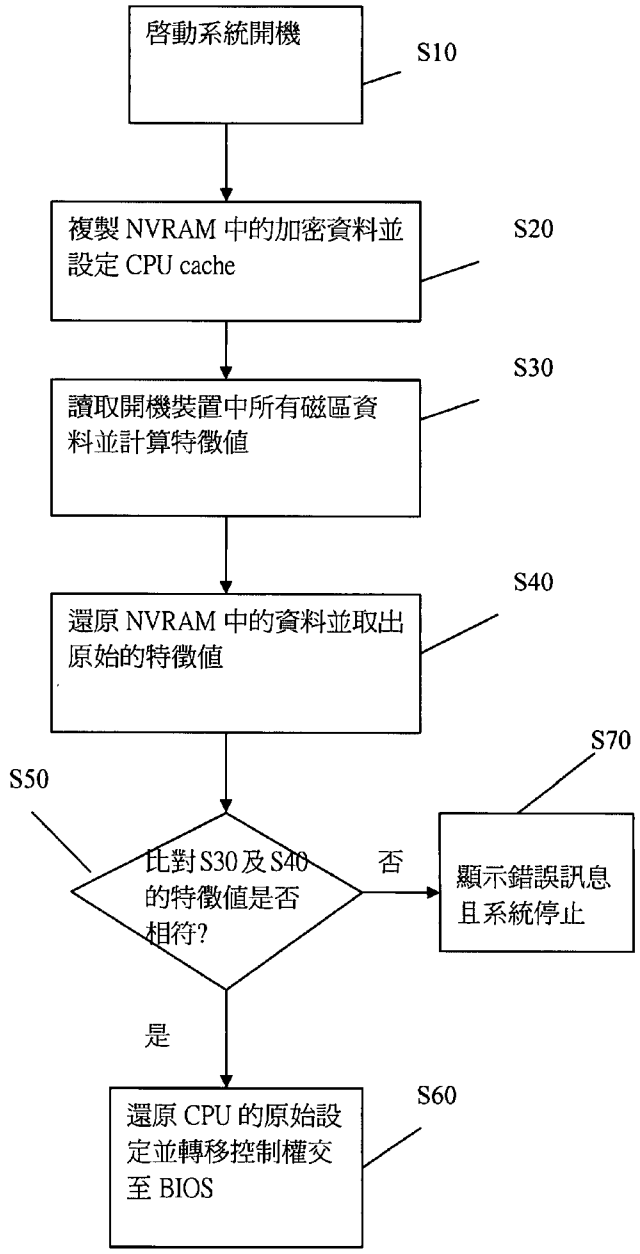
(21)申請案號：101116939 (22)申請日： 中華民國 101 (2012) 年 05 月 11 日
(51)Int. Cl.： *G06F9/445 (2006.01)* *G06F21/57 (2013.01)*
(71)申請人：廣積科技股份有限公司 (中華民國) (TW)
臺北市南港區園區街 3 之 1 號 11 樓
(72)發明人：李家富 (TW)
(74)代理人：洪堯順
申請實體審查：有 申請專利範圍項數：6 項 圖式數：2 共 15 頁

(54)名稱

開機保全軟體方法

(57)摘要

一種開機保全軟體方法，包括：啟動系統開機；將基本輸入輸出系統中快閃記憶體的加密資料複製到執行空間，並設定中央處理器的快取功能；讀取開機裝置中當作開機軟體的所有磁區資料，並利用安全雜湊演算法以計算目前特徵值；藉解密以還原快閃記憶體的出廠原始資料，並取出原始特徵值；以及比對目前特徵值及原始特徵值是否相符，如果相符，則還原中央處理器的原始設定並轉移控制權至基本輸入輸出系統，而如果不相符，則顯示錯誤訊息且系統停止。因此，本發明可防止非原始的作業系統被載入而執行，改善整體系統的安全性。



第一圖

S10：啟動系統開機

S20：複製 NVRAM 中的加密資料並設定 CPU cache

S30：讀取開機裝置中所有磁區資料並計算特徵值

S40：還原 NVRAM 中的資料並取出原始的特徵值

S50：比對 S30 及 S40 的特徵值是否相符

S60：還原 CPU 的原始設定並轉移控制權交至 BIOS

S70：顯示錯誤訊息且系統停止

201346764

發明專利說明書

（本說明書格式、順序，請勿任意更動，※記號部分請勿填寫）

※ 申請案號：101116939

※ 申請日：101. 5. 11　　※IPC 分類：G06F 9/445 2006.01
G06F 21/57 (2013.01)

一、發明名稱：（中文/英文）

開機保全軟體方法

二、中文發明摘要：

一種開機保全軟體方法，包括：啟動系統開機；將基本輸入輸出系統中快閃記憶體的加密資料複製到執行空間，並設定中央處理器的快取功能；讀取開機裝置中當作開機軟體的所有磁區資料，並利用安全雜湊演算法以計算目前特徵值；藉解密以還原快閃記憶體的出廠原始資料，並取出原始特徵值；以及比對目前特徵值及原始特徵值是否相符，如果相符，則還原中央處理器的原始設定並轉移控制權至基本輸入輸出系統，而如果不相符，則顯示錯誤訊息且系統停止。因此，本發明可防止非原始的作業系統被載入而執行，改善整體系統的安全性。

三、英文發明摘要：

四、指定代表圖：

(一)本案指定代表圖為：第（　一　）圖。

(二)本代表圖之元件符號簡單說明：

S10 啟動系統開機

S20 複製 NVRAM 中的加密資料並設定 CPU cache

S30 讀取開機裝置中所有磁區資料並計算特徵值

S40 還原 NVRAM 中的資料並取出原始的特徵值

S50 比對 S30 及 S40 的特徵值是否相符

S60 還原 CPU 的原始設定並轉移控制權交至 BIOS

S70 顯示錯誤訊息且系統停止

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

無

六、發明說明：

【發明所屬之技術領域】

本發明係有關於一種開機保全軟體方法，尤其是在電腦開機時比對經讀取開機裝置中所有磁區資料而計算的目前特徵值以及經還原快閃記憶體中資料而並取出的原始特徵值。

【先前技術】

一般電腦架構主要包括硬體(Hardware)、作業系統(Operating System，OS)、應用程式(Applications)，其中硬體包括電腦主機、鍵盤、滑鼠、螢幕、儲存設備、印表機、數位相機、掃描器、喇叭、數據機、其他電腦周邊設備等，作業系統包括 Windows(視窗作業系統)、Mac OS(麥金塔作業系統)、Linux(企鵝工作站作業系統)、Windows NT(視窗工作站作業系統)等，而應用程式包括文書處理軟體(比如微軟的 WORD 軟體或 Linux 的 vi 軟體)、瀏覽器軟體(比如微軟的 Internet Explorer 瀏覽器或 google 的 Chrome 瀏覽器)等。

電腦的開機程序包括由基本輸入輸出系統(Basic Input and Output System，BIOS)進行開機自我測試(Power On Self Test，POST)，主要是測試硬體單元的操作是否正常，比如對隨機記憶體(RAM)進行讀寫操作以確定記憶體的記憶功能，接著根據 BIOS 中的設定以決定開機裝置，並載入及執行作業系統，而使用者可在作業系統下，啟動所需的應用程式。

目前的博弈產業主要是使用具電腦架構的博弈機

台，比如吃角子老虎或水果盤拉霸機，但是現有的電腦架構平台在系統運作時，無法確保系統不被惡意侵入並作不當的軟體或硬體修改，以致衍生其他糾紛。尤其，電腦架構平台是在中斷程序 int19h 中執行開機載入程式(bootstrap loader)，且採取完全信任，而僅負責載入開機裝置中的作業系統，且並無任何稽核動作，因此，如果作業系統或是客戶軟體經過惡意修改及破解，便無法利用軟體方式檢測並予以避免，造成防制上的大漏洞。

因此，需要一種開機保全軟體方法，可在開機時檢測開機裝置中的作業系統是否被修改，藉以解決上述習用技術的問題。

【發明內容】

本發明之主要目的在提供一種開機保全軟體方法，用以防止在開機時載入已修改過的作業系統(OS)而達到保全軟體的目的，該開機保全軟體方法包括以下操作步驟：

啟動系統開機，比如按下電腦的電源開關；

將基本輸入輸出系統(BIOS)中非揮發性隨機存取記憶體(Non-Volatile Random Access Memory，NVRAM)所儲存的出廠設定的加密資料複製到執行空間(Work Space)，並設定中央處理器(CPU)為快取(cache)模式以加速處理效能；

讀取開機裝置中所有磁區的資料，並利用安全雜湊演算法(Secure Hash Algorithm，SHA-1)以計算雜湊值(hash value)，當作目前特徵值；

藉解密處理以還原 NVRAM 中的加密資料，並取出其中

出廠設定的安全雜湊演算法(SHA-1)雜湊值，用以當作原始特徵值；以及

比對目前特徵值及原始特徵值是否相符，如果相符，則還原 CPU 的原始設定並轉移控制權至 BIOS，而如果不相符，則顯示錯誤訊息且系統停止。

因此，本發明開機保全軟體方法可防止非原始的作業系統被載入而執行，改善整體系統的安全性，尤其適合於需要高度保全的博弈機台，藉以確實防止執行經惡意修改或破解的作業系統或是客戶軟體。

【實施方式】

以下配合圖式及元件符號對本發明之實施方式做更詳細的說明，俾使熟習該項技藝者在研讀本說明書後能據以實施。

參閱第一圖，本發明開機保全軟體方法的示意圖。如第一圖所示，首先，本發明的開機保全軟體方法包括步驟 S10，啟動系統開機，比如按下電腦的電源開關(Power On Switch)。接著進入步驟 S20，在程式核心未啟動前，先予以收集系統相關資訊，並準備執行時期所需的環境，同時將基本輸入輸出系統(BIOS)中非揮發性隨機存取記憶體(NVRAM)所儲存的出廠設定的加密資料複製到執行空間(Work Space)，而 NVRAM 可為快閃記憶體(flash memory)或電氣抹除可程式化唯讀記憶體(EEPROM)。

在步驟 S30 中，讀取該開機裝置中所有磁區的資料，比如透過中斷向量 int13h 以讀取開機裝置中的所有資料，並利用安全雜湊演算法(SHA-1)進行總和校檢

5

(checksum)處理，以計算相對應的雜湊值(hash value)，當作目前特徵值，其中開機裝置是由基本輸入輸出系統設定。並在步驟S40中，藉解密處理以還原非揮發性隨機存取記憶體中的加密資料，因為非揮發性隨機存取記憶體中的所有資料均已使用高級加密標準(Advanced Encryption Standard，AES128)加密，並進而取出其中出廠設定的安全雜湊演算法(SHA-1)雜湊值，用以當作原始特徵值。

上述AES128的高級加密標準是由美國國家標準與技術研究院（NIST）於2001年11月26日發佈於FIPS PUB 197，並在2002年5月26日成為有效的標準，其中高級加密標準的區塊長度固定為128 位元，而密鑰長度則可以是128、192或256位元，之後，高級加密標準已然成為對稱密鑰加密中最流行的演算法之一。

由於步驟S30及步驟S40中雜湊值的計算相當花費中央處理器(CPU)的資源，因此可進一步在步驟S20中設定中央處理器為快取(cache)模式，藉以加速處理效能。

之後，進入步驟S50，比對步驟S30的目前特徵值以及步驟S40的原始特徵值是否相符，如果相符，則進入步驟S60，而如果不相符，則進入步驟S70。

在步驟S60中，還原中央處理器的原始設定，比如取消快取模式的設定，並轉移控制權至基本輸入輸出系統。此外，步驟S60可進一步包括消除步驟S30及步驟S40中計算目前特徵值以及原始特徵值時所產生的資料，以防止被惡意利用。在步驟S70中，顯示錯誤訊息且系統停止，其中錯誤訊息係用通知使用者開機異常，因為開機裝置中的資料已被修改，並同時停止運作以保護整體系

統。

此外，如第二圖所示，為進一步執行客戶使用授權驗證程序，以提供更加安全的保全功能，可將客戶使用授權驗證程序儲存於開機裝置中，並在步驟S50比對目前特徵值以及原始特徵值為相符時，於進入步驟S60之前，先進入步驟S52，載入並執行開機裝置中的客戶使用授權驗證程序，檢查相關模組是否經過惡意修改，以避免非法使用，接著在步驟S54中，判斷相關模組是否通過客戶使用授權驗證程序，如果通過驗證程序，則進入步驟S60，否則步驟S70。由於其餘步驟係相同於第一圖的實施例，在此不再贅述。

本發明開機保全軟體方法的特點在於，利用系統載入作業系統之前，對儲存於開機裝置的所有資料進行以得到目前特徵值，並與非揮發性隨機存取記憶體中所設定的原始特徵值進行比對處理，如果與不相符，則判定為異常，可能是開機裝置的資料已被更動或修改，進而停止系統運作，以提供保全功能，並可防止執行經惡意修改或破解的作業系統或是客戶軟體。

本發明的另一特點在於，可進一步執行特定的客戶使用授權驗證程序，檢查相關模組是否經過惡意修改，以避免相關模組被非法使用，大幅改善博奕機台的保全功能。

以上所述者僅為用以解釋本發明之較佳實施例，並非企圖據以對本發明做任何形式上之限制，是以，凡有在相同之發明精神下所作有關本發明之任何修飾或變更，皆仍應包括在本發明意圖保護之範疇。

【圖式簡單說明】

第一圖顯示本發明開機保全軟體方法的操作示意圖。

第二圖顯示本發明另一實施例開機保全軟體方法的操作示意圖。

【主要元件符號說明】

S10 啟動系統開機

S20 複製 NVRAM 中的加密資料並設定 CPU cache

S30 讀取開機裝置中所有磁區資料並計算特徵值

S40 還原 NVRAM 中的資料並取出原始的特徵值

S50 比對 S30 及 S40 的特徵值是否相符

S52 載入並執行客戶使用授權驗證程序

S54 判斷是否通過客戶使用授權驗證程序

S60 還原 CPU 的原始設定並轉移控制權交至 BIOS

S70 顯示錯誤訊息且系統停止

七、申請專利範圍：

1. 一種開機保全軟體方法，係用以防止在開機時載入已修改過的作業系統(OS)而達到保全軟體的目的，該開機保全軟體方法包括以下操作步驟：

啟動系統開機；

將基本輸入輸出系統(BIOS)中非揮發性隨機存取記憶體所儲存的出廠設定的加密資料複製到執行空間；

讀取該開機裝置中所有磁區的資料，並利用安全雜湊演算法(SHA-1)以計算相對應的雜湊值(hash value)，當作目前特徵值，其中開機裝置是由基本輸入輸出系統設定；

藉解密處理以還原非揮發性隨機存取記憶體中的加密資料，並取出其中出廠設定的安全雜湊演算法(SHA-1)雜湊值，用以當作原始特徵值；以及

比對目前特徵值及原始特徵值是否相符，如果相符，則還原中央處理器的原始設定並轉移控制權至基本輸入輸出系統，而如果不相符，則顯示錯誤訊息且系統停止。

2. 一種開機保全軟體方法，係用以防止在開機時載入已修改過的作業系統(OS)而達到保全軟體的目的，該開機保全軟體方法包括以下操作步驟：

啟動系統開機；

將基本輸入輸出系統(BIOS)中非揮發性隨機存取記憶體所儲存的出廠設定的加密資料複製到執行空間；

讀取該開機裝置中所有磁區的資料，並利用安全雜湊演算

法(SHA-1)以計算相對應的雜湊值(hash value)，當作目前特徵值，其中開機裝置是由基本輸入輸出系統設定；

藉解密處理以還原非揮發性隨機存取記憶體中的加密資料，並取出其中出廠設定的安全雜湊演算法(SHA-1)雜湊值，用以當作原始特徵值；以及

比對目前特徵值及原始特徵值是否相符，如果不相符，則顯示相關錯誤訊息且系統停止，而如果相符，則載入並執行開機裝置中的客戶使用授權驗證程序，檢查相關模組是否經過惡意修改，並判斷相關模組是否通過客戶使用授權驗證程序，如果未通過驗證程序，則相關顯示錯誤訊息且系統停止，而如果通過驗證程序，則還原中央處理器的原始設定並轉移控制權至基本輸入輸出系統。

3. 依據申請專利範圍第 1 項或第 2 項所述之開機保全軟體方法，其中該啟動系統開機係包括按下電腦的電源開關。

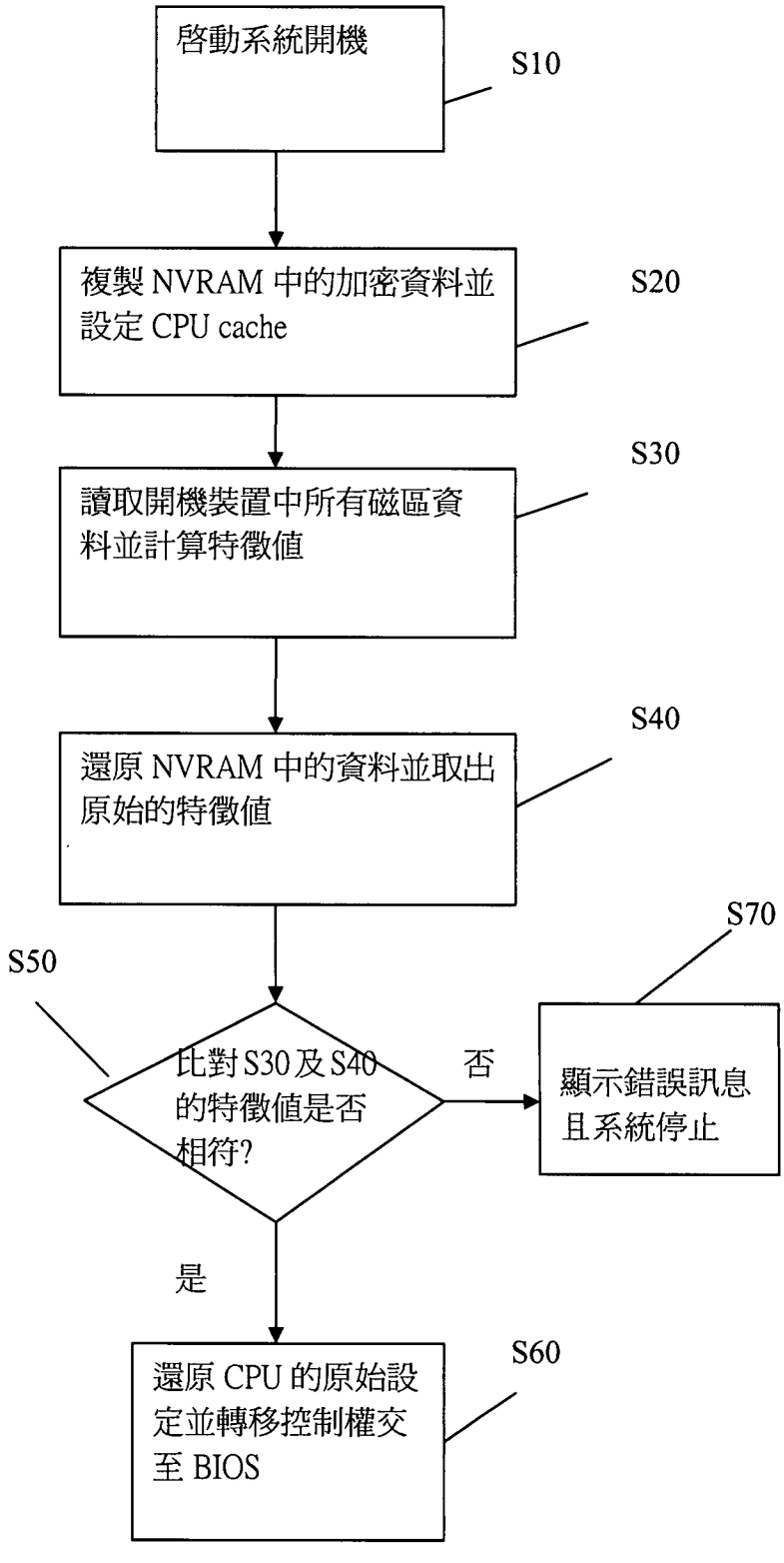
4. 依據申請專利範圍第 1 項或第 2 項所述之開機保全軟體方法，其中該非揮發性隨機存取記憶體為快閃記憶體(flash memory)或電氣抹除可程式化唯讀記憶體(EEPROM)。

5. 依據申請專利範圍第 1 項或第 2 項所述之開機保全軟體方法，進一步包括：

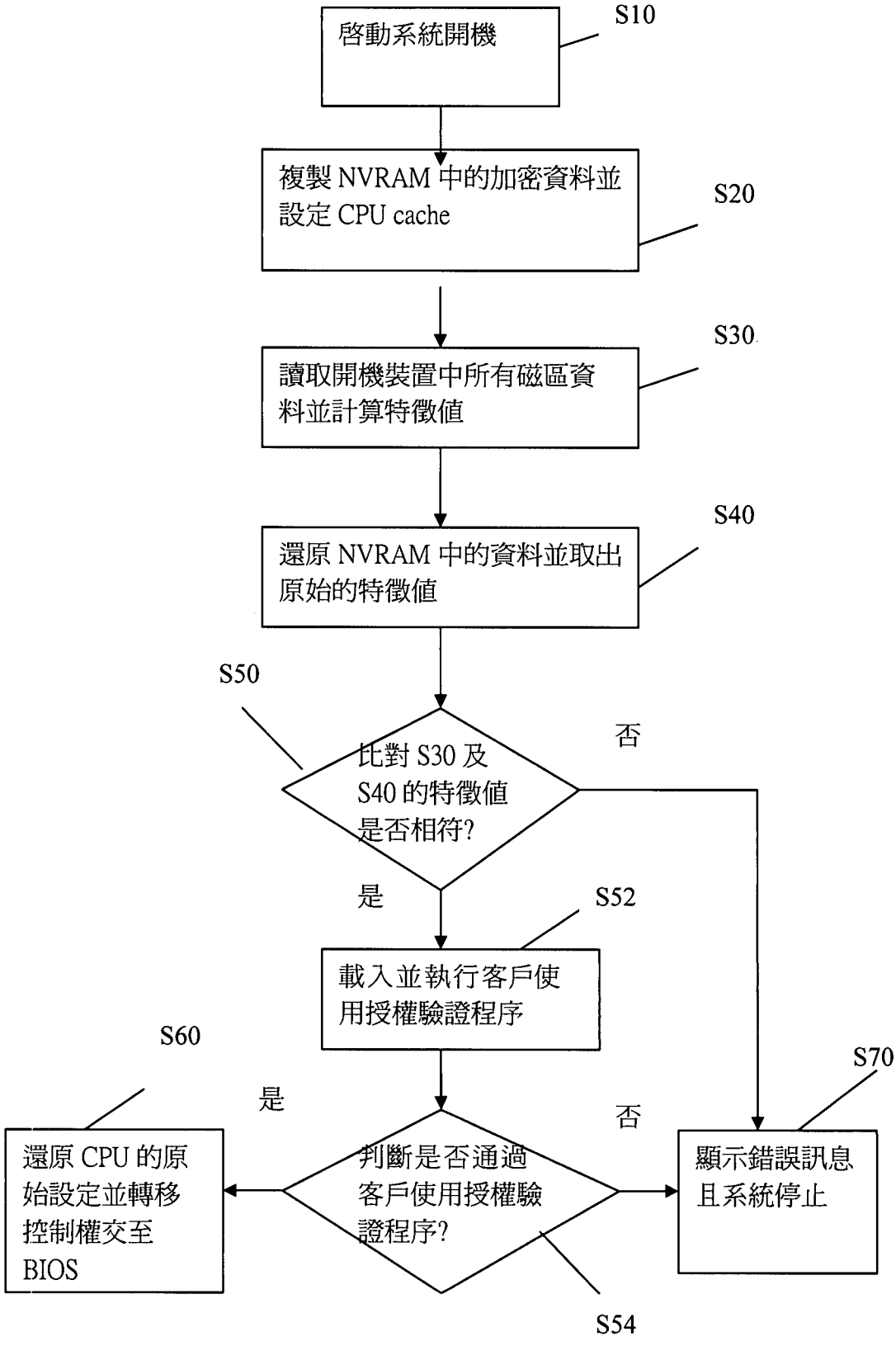
設定中央處理器為快取(cache)模式，以加速處理效能。

6. 依據申請專利範圍第 1 項或第 2 項所述之開機保全軟體方法，進一步包括在還原中央處理器的原始設定時，消除計算目前特徵值及原始特徵值所產生的資料。

八、圖式：


啓動系統開機
S10
複製 NVRAM 中的加密資料並設定 CPU cache
S20
讀取開機裝置中所有磁區資料並計算特徵值
S30
還原 NVRAM 中的資料並取出原始的特徵值
S40
S50
比對S30及S40的特徵值是否相符?
否
S70
顯示錯誤訊息且系統停止
是
還原 CPU 的原始設定並轉移控制權交至 BIOS
S60

第一圖


啓動系統開機
S10
複製 NVRAM 中的加密資料並設定 CPU cache
S20
讀取開機裝置中所有磁區資料並計算特徵值
S30
還原 NVRAM 中的資料並取出原始的特徵值
S40
S50
比對 S30 及 S40 的特徵值是否相符?
否
是
S52
載入並執行客戶使用授權驗證程序
S60
是
否
S70
還原 CPU 的原始設定並轉移控制權交至 BIOS
判斷是否通過客戶使用授權驗證程序?
顯示錯誤訊息且系統停止
S54

第二圖