I298591

公告本

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：93134289

※申請日期：93.11.10　　※IPC 分類：H04L 9/06 (2006.01)

一、發明名稱：（中文/英文）

保密可執行編碼之系統及方法

System and method for securing executable code

二、申請人：（共 1 人）

姓名或名稱：（中文/英文）（簽章）ID ：

美國博通公司/ Broadcom Corporation

□ 指定　　為應受送達人

代表人：（中文/英文）（簽章）狄・韓德森／Dee Henderson

住居所或營業所地址：（中文/英文）

美國加州爾灣市奧爾頓公園路 16215 號 92618-7013

16215 Alton Parkway, Irvine, California U.S.A., 92618-7013

國　籍：（中文/英文）美國／U.S.A.

電話/傳真/手機：

E-MAIL：

三、發明人：（共 1 人）

1. 姓　名：（中文/英文）　　ID ：

馬克・布林／Mark Buer

國　籍：（中文/英文）

美國／U.S.A.

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　2003 年 11 月 10 日　60/518,323

2) 美國　2004 年 6 月 30 日　10/879,349

☐ 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】

本發明係關於資訊保密,尤其係關於一種保密處理。

【先前技術】

眾所皆知，計算平臺內之保密處理是一個問題。特別係可執行編碼之任何無意或非期望之改變，都會產生可怕之運行結果。例如，惡意編碼可被（例如，特洛依木馬）插入至可執行編碼中，從而使處理器執行非期望和/或無法預測之操作。換言之，敵對用戶可以改變指令次序，從而由出故障之處理器來執行操作。此時，其結果可能也是非期望的。其他威脅可能不是惡意的。例如，記憶體硬體故障可能會改變可執行編碼。顯然，其會影響處理器之運行及其結果。

另外，保密係與可編程邏輯電路其自身相關之問題。可執行編碼其本身可能會洩漏了原本應視為是必須秘密而保存之資訊。對可執行編碼之揭露會對敏感資料產生非期望之損害。一般而言，可執行編碼在存儲時、以及在記憶體與處理器或它超快取記憶體之間傳送時，容易被損壞。

考慮到這種已知之威脅及脆弱性，需要一種可克服以上情況之系統及方法，從而使處理器只執行所需要之操作，並保持其程式之機密性。

【發明內容】

本發明的目的在於，提供可執行編碼之保密存儲及這種編碼從記憶體到處理器之保密傳送。本發明包括編碼加密版本之

存儲。在存儲裝置（如快閃記憶體）中重加密之前，可根據需要解密並解壓該編碼。然後將重加密之可執行編碼寫入外記憶體。當需要可執行編碼之超快取記憶體線時，執行一取出動作並對其進行截取。在截取過程中，對所述超快取記憶體線進行解密。然後將得到之明文(plain text)超快取記憶體線存儲於一與處理器相關聯之指令超快取記憶體中。

為瞭解決本發明的目的，本發明提供一種用於保密執行處理器指令之系統，所述系統包括：

一第一記憶體，其包含起動代碼及利用第一密鑰加密之圖像；

一保密嵌入式處理器系統，其包括：

一處理器；

一與所述處理器通訊之指令超快取記憶體；

一與所述指令超快取記憶體通訊之記憶體控制器；及

一與所述指令超快取記憶體通訊之保密控制器；及

一第二記憶體，它位於所述保密嵌入式處理器系統的外部，並與所述第一記憶體、記憶體控制器和保密控制器通訊，其中，所述用第一密鑰加密之圖像被傳輸至所述第二記憶體，被所述保密控制器解密，並由所述保密控制器使用第二密鑰再加密，用所述第二密鑰加密之圖像之一超快取記憶體線從所述第二記憶體被讀取，再用所述第二密鑰進行解密，然後存儲於

所述指令超快取記憶體中，以被所述處理器執行。

較佳的實施例是，所述保密控制器包括使用三重資料加密標準（3DES,Triple Data Encryption Standard）演算法及所述第一密鑰對所述被加密圖像進行解密之邏輯電路。

較佳的實施例是，所述系統進一步包括一密鑰管理模組，其包括：

以加密形式接收所述第一密鑰之邏輯電路；

使用會話密鑰(session key)對所述被加密之第一密鑰進行解密之邏輯電路；以及

將所述第一密鑰轉發至所述保密控制器之邏輯電路。

較佳的實施例是，所述保密控制器包括：使用高級加密標準（AES, Advanced Encryption Standard）演算法重加密所述圖像之邏輯電路；以及使用所述 AES 演算法解密所述超快取記憶體線之邏輯電路。

較佳的實施例是，所述用於重加密所述圖像之邏輯電路包括實現所述 AES 演算法之密碼分組鏈結（CBC, cipher block chaining）模式之邏輯電路；及所述用於解密所述超快取記憶體線之邏輯電路中，包括實現所述 AES 演算法之 CBC 模式之邏輯電路。

較佳的實施例是，所述用於重加密該圖像之邏輯電路中，包括實現所述 AES 演算法之 CBC 模式之解密模式之邏輯電

路；及所述用於解密所述超快取記憶體線之邏輯電路包括實現所述 AES 演算法之 CBC 模式之加密模式之邏輯電路。

較佳的實施例是，所述用於重加密所述圖像之邏輯電路中，使用所述第二記憶體之一位址作爲所述 AES 演算法之初始化向量（IV, initialization vector），其中所述位址對應於所述超快取記憶體線在所述第二記憶體中之位置；及所述用於解密所述超快取記憶體線之邏輯電路中，使用所述位址作爲所述初始化向量。

另一方面，本發明提供一種提供處理器指令保密執行之方法，其包括：

a. 啓動處理器，以將加密編碼載入至外部記憶體中；

b. 使用圖像密鑰對所述加密編碼中之解壓縮部分進行解密，以產生解密解壓縮碼之第一部分；

c. 執行所述解密解壓縮碼之第一部分；

d. 使用所述圖像密鑰對所述加密編碼之壓縮部分進行解密，以產生一圖像；

e. 鑒別所述圖像；

f. 解壓縮該圖像從而使其佔據外部記憶體之一部分，起點位於第一地址並且終點位於終端地址；及

g. 執行所述圖像之保密執行。

較佳的實施例是，其中使用三重資料加密標準（3DES）

演算法執行所述解密步驟 b 及 d。

較佳的實施例是，在執行步驟 a 之前，所述方法進一步包括以下步驟：

h．確定所述圖像密鑰是否失效，僅於所述圖像密鑰還沒有失效之條件下，才執行所述步驟 a—g。

較佳的實施例是，在執行步驟 a 之前，所述方法進一步包括以下步驟：

h．產生加密編碼。

較佳的實施例是，所述步驟 h 中包括：

i．壓縮所述圖像；

ii．對所述圖像進行散列處理以產生一散列值；

iii．加密所述圖像；

iv．存儲所述加密編碼。

較佳的實施例是，所述步驟 h.ii.中，使用保密散列演算法 1（SHA-1）對所述圖像進行散列處理。

較佳的實施例是，所述步驟 h.iii.中，使用三重資料加密標準（3DES）演算法加密圖像。

較佳的實施例是，所述步驟 h.iv.中，將加密編碼存儲於快閃記憶體中。

較佳的實施例是，該步驟 a 包括：

i. 將處理器的狀態重定；

ii.載入圖像密鑰；

iii.將加密編碼傳輸入外部記憶體；及

iv.將處理器切換至保密模式。

較佳的實施例是，所述外部記憶體包括雙倍資料傳輸率同步動態隨機存取記憶體（DDR-SDRAM）。

較佳的實施例是，所述步驟 a.iv.中包括：

清除處理器之狀態；

A． 將與處理器相關聯之一指令超快取記憶體設置爲無效狀態；及

將圖像之執行限制於外部記憶體之一部分。

較佳的實施例是，所述步驟 g 包括：

i. 分別加密圖像之每一個超快取記憶體線；

ii. 取出一加密超快取記憶體線；

iii. 截取所述取出過程；

iv. 解密所取出之加密超快取記憶體線；

v. 確定解密超快取記憶體線是否有效；

vi. 若解密超快取記憶體線無效，捕獲該解密超快取記憶體線；及

vii. 若解密超快取記憶體線有效，執行所述解密超快取記憶體線。

較佳的實施例是，所述步驟 g.i.中，包括使用高級加密標準（AES）加密每一個超快取記憶體線，所述步驟 g.iv.中，包

括使用 AES 演算法解密所取出之加密超快取記憶體線。

較佳的實施例是，所述 AES 演算法使用於密碼分組鏈結（CBC）模式。

較佳的實施例是，所述步驟 g.i.中，包括使用 AES 演算法解密模式來加密每個超快取記憶體線，所述步驟 g.iv.中，使用 AES 演算法之加密模式解密取出之加密超快取記憶體線。

較佳的實施例是，每個超快取記憶體線之 AES 演算法之初始化向量（IV）爲超快取記憶體線在外部記憶體中之地址。

【實施方式】

現參照附圖描述本發明之最佳實施例，其標號表示相同或功能相似之元件。在附圖中，每個標號最左側之一位對應於第一次使用標號之附圖。對於其中所描述之具體配置及設備，應理解僅係出於示意之目的。本領域之技術人員可在不脫離本發明之宗旨及範圍之條件下，使用其他配置及設備。對於本領域之技術人員而言，本發明顯然也可以用於多種裝置、系統及應用程式。

Ⅰ. 概述

現參照附圖描述本發明之最佳實施例，其標號表示相同或功能相似之元件。在附圖中，每個標號最左側之一位對應於第一次使用標號之附圖。對於其中所描述之具體配置及設備，應理解僅係出於示意之目的。本領域之技術人員可在不脫離本發明之宗旨及範圍之條件下，使用其他配置及設備。對於本領域

之技術人員而言，本發明顯然也可以用於多種裝置、系統及應用程式。

II. 系統

本發明提供一種與記憶體模組進行通訊之保密嵌入式處理器系統。第一圖爲本發明之一種實施例。圖中，保密嵌入式處理器系統 105 與外部記憶體模組 160 及快閃記憶體模組 175 相連接。快閃記憶體模組 175 以壓縮及加密之形式存儲可執行編碼（在下文中稱爲圖像）。由如下之詳細描述可知，在啓動過程中，加密壓縮之圖像被傳輸至外部記憶體 160。然後，該圖像被解密、解壓縮，再被重加密並存儲於外部記憶體 160 之中。

對於將被處理器 110 執行之指令，每次從外部記憶體 160 中取出其一個超快取記憶體線。然而，該取出之過程會被記憶體控制器 150 所截取。在將取出之超快取記憶體線載入至指令超快取記憶體 130 之前，由保密控制器 140 將其解密。

如圖所示，在保密嵌入式處理器系統 105 中設有一密鑰管理模組 170，其爲保密控制器 140 提供密鑰管理服務。在本發明之一種實施例中，還可提供一外部介面 180，以實現快閃記憶體 175 與系統 105 間之相互連接。還可提供一周邊零件連接（PCI）介面 185，以實現與保密嵌入式處理器系統 105 之通訊。PCI 介面 185、外部介面 180、密鑰管理模組 170、保密控

制器 140 及處理器 110 通過諸如匯流排之基礎結構 145 相互連接。

第二圖更詳細地示出了快閃記憶體 175。第二圖揭示了當圖像駐留於快閃記憶體 175 內時之圖像結構。該圖像包括一段啓動碼 210。接下來是兩個碼塊 220、230。 用第一加密密鑰，這裏稱爲圖像密鑰，對該兩個碼塊共同加密。在本發明之一種實施例中，使用三重資料加密標準（3DES）演算法對這些碼塊進行加密。在圖示實施例中，碼塊 220 包括用於解密剩餘碼塊 230 所需之邏輯。應該注意，在圖示實施例中，碼塊 230 係壓縮的。碼塊 240 代表由碼塊 210、220 及 230 所得到之鑒別碼(authentication data)。碼塊並不是圖像本身之一部分。在圖示實施例中，所述鑒別過程係一散列訊息鑒別碼（HMAC）過程。

第三圖示出了當圖像被解密並解壓縮後，駐留於外部記憶體 160 時之圖像結構。如圖所示，塊 330 中佔據記憶體之 10KB 存儲容量。該存儲間隔之初始地址爲 310。該間隔之終端地址爲 320。在本發明之一種實施例中，該初始地址 310 及終端地址 320 被轉發到記憶體控制器 150。以起動保密檢驗之作用，從而不允許執行這些邊界以外之指令。

第四圖係從外部記憶體 160 中取出指令時之流程。當圖像被解密後，使用第二密鑰將圖像重加密以形成重加密圖像

410。然後基於超快取記憶體線取出所述重加密圖像 410。出於解密之目的，由解密邏輯電路 440 找到並讀取超快取記憶體線 420。在圖示實施例中，超快取記憶體線 420 之地址 430 用於初始化解密過程。在本發明之一種實施例中，重加密過程按密碼分組鏈結（CBC）模式，使用高級加密標準（AES）演算法。此外，在本發明之一種實施例中，重加密過程在解密模式中可使用 AES/CBC 過程。結果，在該實施例中，解密過程 440 實際上使用 AES 之加密模式。然後將得到之明文超快取記憶體線 450 轉發到指令超快取記憶體 130。最終由處理器 110 執行該明文超快取記憶體線 450。

第一圖所示，密鑰管理模組 170 處理一部分與加密密鑰之保護相關之管理及保密功能。特別地，在本發明之一種實施例中，保密嵌入式處理器系統 105 以加密形式接收圖像密鑰。密鑰管理模組 170 使用會話密鑰(session key)將加密圖像密鑰解密。從而使保密控制器 140 如上所述那樣使用所得到之明文圖像密鑰。

此外，可將一時間限制與所述圖像密鑰相關聯，從而只能在給定之持續時間內或者某特定之時間點使用該圖像密鑰。在該時間點過後，該密鑰不能夠再使用，而稱其爲失效。在本發明之一種實施例中，保密控制器 140 在使用該密鑰之前會校驗圖像密鑰是否已經失效。當然，也可以在密鑰管理模組 170 中

執行該校驗。

Ⅲ. 方法

第五圖係當圖像被存儲於快閃記憶體中時，其初始壓縮及加密過程。該過程開始於步驟 510。在步驟 520 中，將圖像壓縮。在步驟 530 中，對圖像進行散列處理以產生 HMAC。在本發明之一種實施例中，其使用保密散列演算法 1（SHA-1）。在步驟 540 中，使用圖像密鑰將壓縮圖像加密。如上所述，可使用 3DES 演算法執行該加密。在步驟 550 中，將得到之壓縮加密圖像存儲在快閃記憶體中。本過程於步驟 560 而結束。

第六圖係保密地存取及執行圖像之總體過程。本過程開始於步驟 610。在步驟 620 中，處理器經歷其啓動操作。在步驟 630 中，使用圖像密鑰對圖像之未解壓縮部分進行解密。在步驟 640 中，執行該解壓縮碼。所述編碼之解壓縮碼部分中之邏輯用於對剩餘圖像進行解密。在步驟 650 中，使用圖像密鑰對圖像之剩餘部分進行解密。在步驟 660 中，鑒別所述圖像。如上所述，可使用 SHA-1 演算法執行鑒別。在步驟 670 中，將圖像解壓縮。在步驟 680 中，開始保密執行。本過程於步驟 690 而結束。

第七圖更詳細地示出處理器之啓動步驟（即第六圖之步驟 620）。本過程開始於步驟 710。在步驟 720 中，將裝置狀態重定。在步驟 730 中，出於順序加密處理之目的，載入加密編碼。

在步驟 740 中，將圖像從快閃記憶體移動至外部記憶體。在本發明之一種實施例中，可使用雙倍資料傳輸率同步動態隨機存取記憶體（DDR-SDRAM）實現外部記憶體。在步驟 750 中，將系統切換至保密模式。本過程於步驟 760 而結束。

第八圖更詳細地示出切換至保密模式之步驟(即第七圖之步驟 750)。本過程開始於步驟 810。在步驟 820 中，清除處理器狀態。在步驟 830 中，將與處理器相關聯之指令及資料超快取記憶體設爲無效狀態。其可防止任何恰好駐留於這些緩存內之資訊被處理器所執行。在步驟 840 中，將圖像之上方及下方之地址邊界轉發至記憶體控制器，從而將執行限制在低於 DDR-SRAM 之 n 千位元組。本過程於步驟 850 而結束。

第九圖更詳細地示出保密執行之步驟（第六圖之步驟 680)。本過程開始於步驟 910。在步驟 915 中，使用基於每個超快取記憶體線之會話密鑰對圖像進行加密。在本發明之一種實施例中，本步驟於 CBC 模式之下使用 AES 演算法。此外，還可以此加密過程中使用 AES 之解密配置。其提供整個圖像加密過程中之錯誤校驗。在步驟 920 中，將加密圖像寫入外部記憶體。在步驟 925 中，取出一指令超高速超快取記憶體線，所述指令超快取記憶體線係在位址邊界內而被取出。在步驟 930 中，所述取出被記憶體控制器所截取。在步驟 935 中，由保密控制器對該超快取記憶體線進行解密。如果加密過程按解

密模式使用 AES/ CBC 演算法，那麼解密步驟 935 實際上會使用 AES/ CBC 之加密模式。在步驟 935 對超快取記憶體線進行解密之後，會在步驟 940 中確定得到之指令是否有效。如果無效，則於步驟 945 捕獲該指令。否則，該指令準備在步驟 955 中執行。在步驟 960 中，將確定是否有需要取出並執行之附加指令，或者確定本過程是否中止。如果本過程已中止，則過程在步驟 950 結束。否則過程返回步驟 925，以取出附加之超快取記憶體線。

圖 10 係本發明之另一種方法。本過程開始於步驟 1005。在步驟 1010 中，從單板唯讀記憶體（ROM）發起啓動過程。在步驟 1015 中，將啓動編碼提交至保密模組。在步驟 1020 中，散列該啓動碼。在本步驟中，保密模組會保持該散列值。在步驟 1025 中，開始執行啓動碼。在步驟 1030 中，散列該壓縮碼，從而使保密模組保持其所取得之快取值。在步驟 1035 中，標記該散列值。在步驟 1040 中，將加密圖像傳輸至外部記憶體。如上所述，在本發明之一種實施例中，外部記憶體可用 DDR-SRAM 實現。在步驟 1045 中，使用圖像密鑰解密所述解壓縮碼。在步驟 1050 中，執行該解壓縮碼。在步驟 1055 中，用圖像密鑰將剩餘圖像解密。在步驟 1060 中，根據需要對剩餘圖像進行解密。本過程於步驟 1065 而結束。

IV. 結論

綜上所述，本發明符合發明專利要件，爰依法提出專利申請。惟，以上所述者僅為本發明之較佳實施例，舉凡熟悉本案技藝之人士，在援依本案發明精神所作之等效修飾或變化，皆應包含於以下之申請專利範圍內。

【圖式簡單說明】

第一圖係本發明之原理方塊圖，其示出了本發明一實施例之總體結構和內容；

第二圖係本發明一種實施例中可執行編碼在快閃記憶體內於加密及壓縮形式時之示意圖；

第三圖係本發明一種實施例中包含有解密及解壓縮之可執行編碼之外部記憶體之示意圖；

第四圖係本發明一種實施例之取出過程，其中將編碼之超快取記憶體線解密並轉發送至指令超快取記憶體；

第五圖係本發明一種實施例之加密圖像之產生的流程圖；

第六圖係本發明一種實施例存取並使用加密圖像之總體流程圖；

第七圖係本發明一種實施例之處理器啓動過程之詳細流程圖；

第八圖係本發明一種實施例中切換至保密模式之流程圖；

第九圖係本發明一種實施例中保密執行過程之流程圖；

第十圖係本發明方法之一簡化版本之流程圖。

【主要元件符號說明】

保密嵌入式處理器系統　105　處理器　110

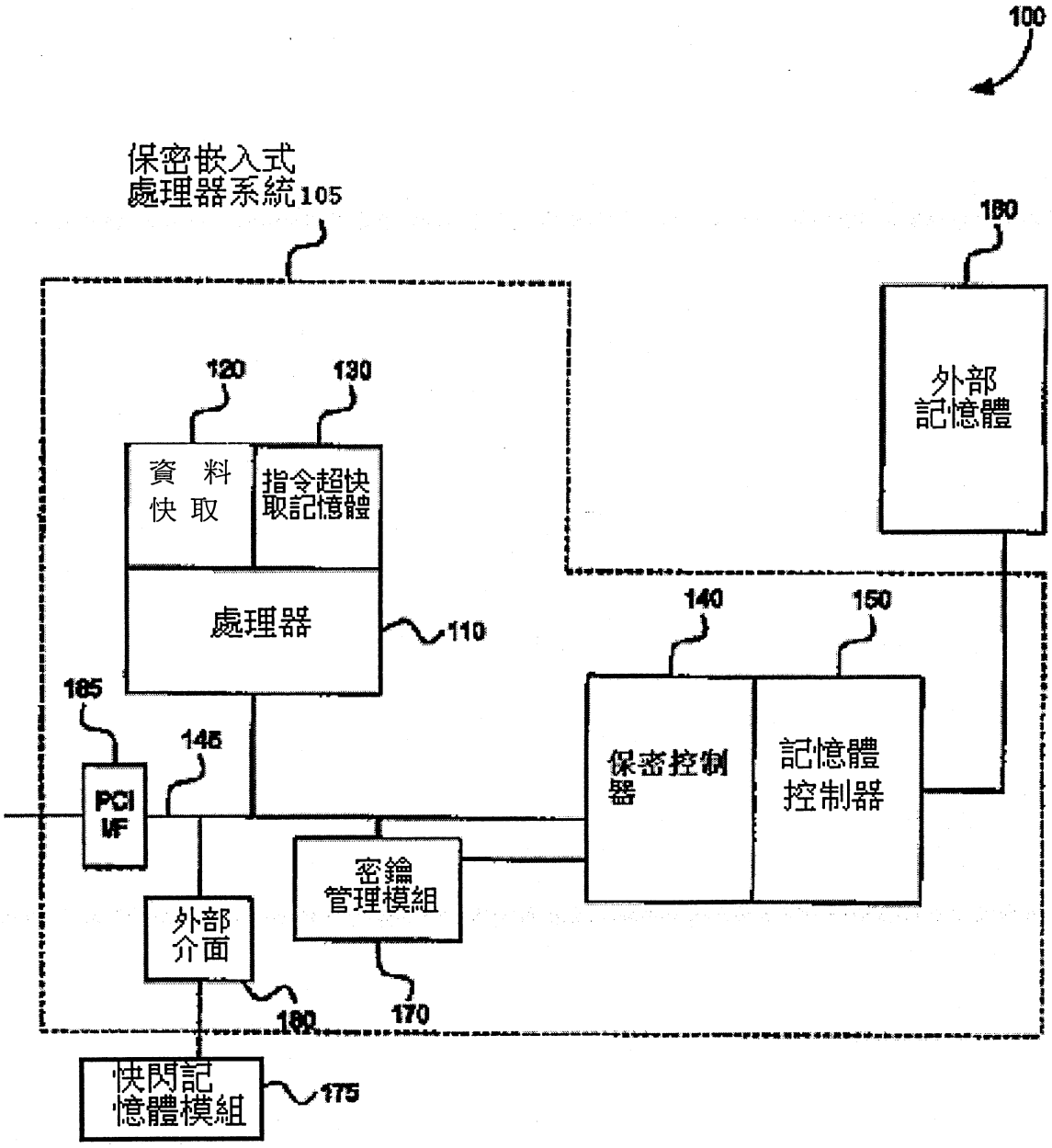
指令超快取記憶體	130	保密控制器	140
基礎結構	145	記憶體控制器	150
外部記憶體	160	密鑰管理模組	170
快閃記憶體模組	175	外部介面	180
周邊零件連接（PCI）介面	185	啓動碼	210
碼塊	220、230、240	初始地址爲	310
終端位址爲	320	塊	330
重加密圖像	410	超快取記憶體線	420
地址	430	解密邏輯電路	440

五、中文發明摘要：

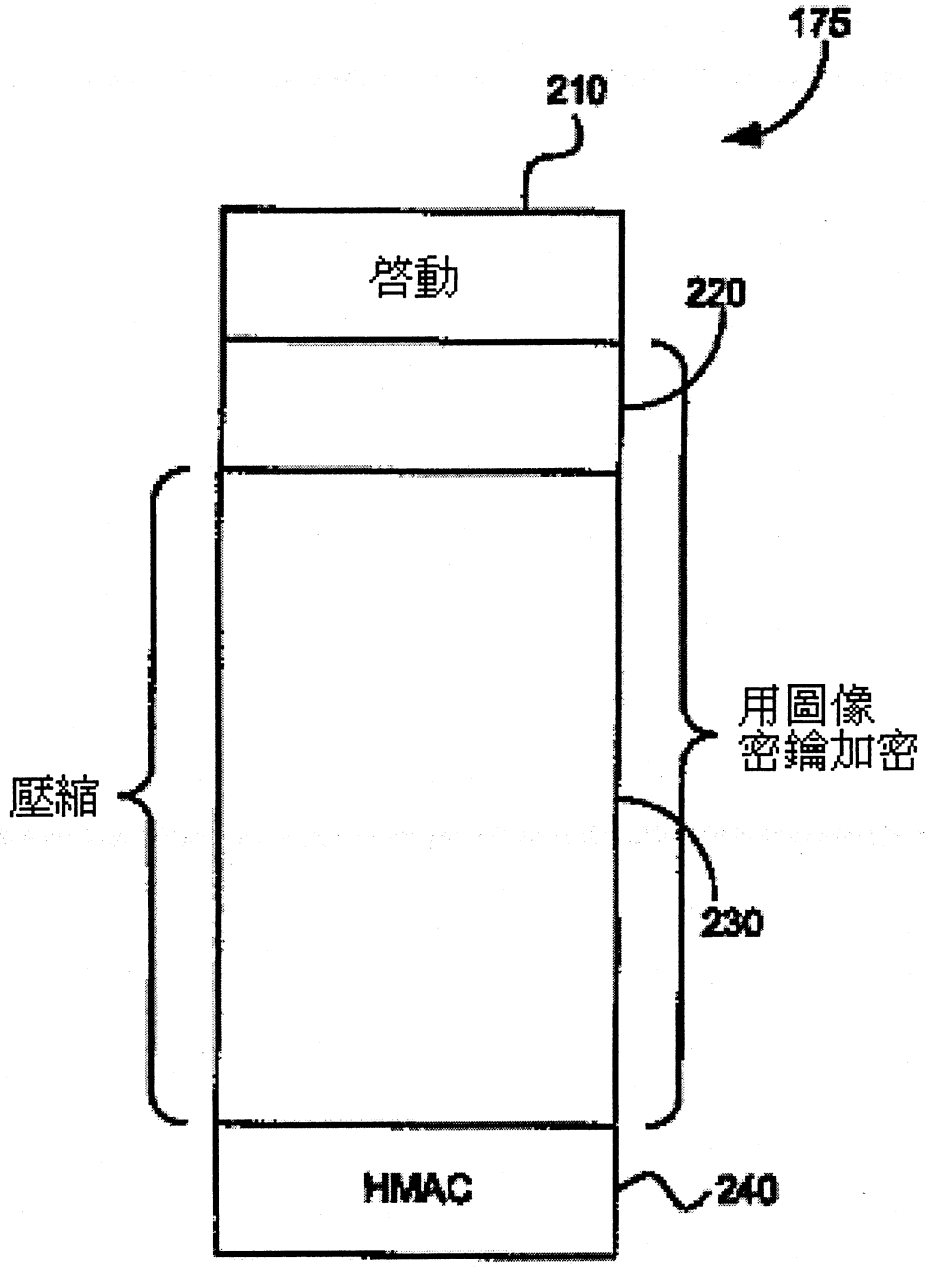
本發明係關於一種用於對可執行編碼進行保密存儲、及將這種編碼從記憶體保密傳送至處理器之系統及方法。所述方法包括存儲所述編碼之加密版本。在存儲裝置中重加密之前，根據需要解密並解壓該編碼。然後將重加密之可執行編碼寫入外記憶體。當需要所述可執行編碼之超快取記憶體線時，執行一取出動作，但對其進行截取。在截取過程中，對所述超快取記憶體線進行解密。然後將所得到之明文超快取記憶體線存儲在與處理器相關聯之指令超快取記憶體中。

六、英文發明摘要：

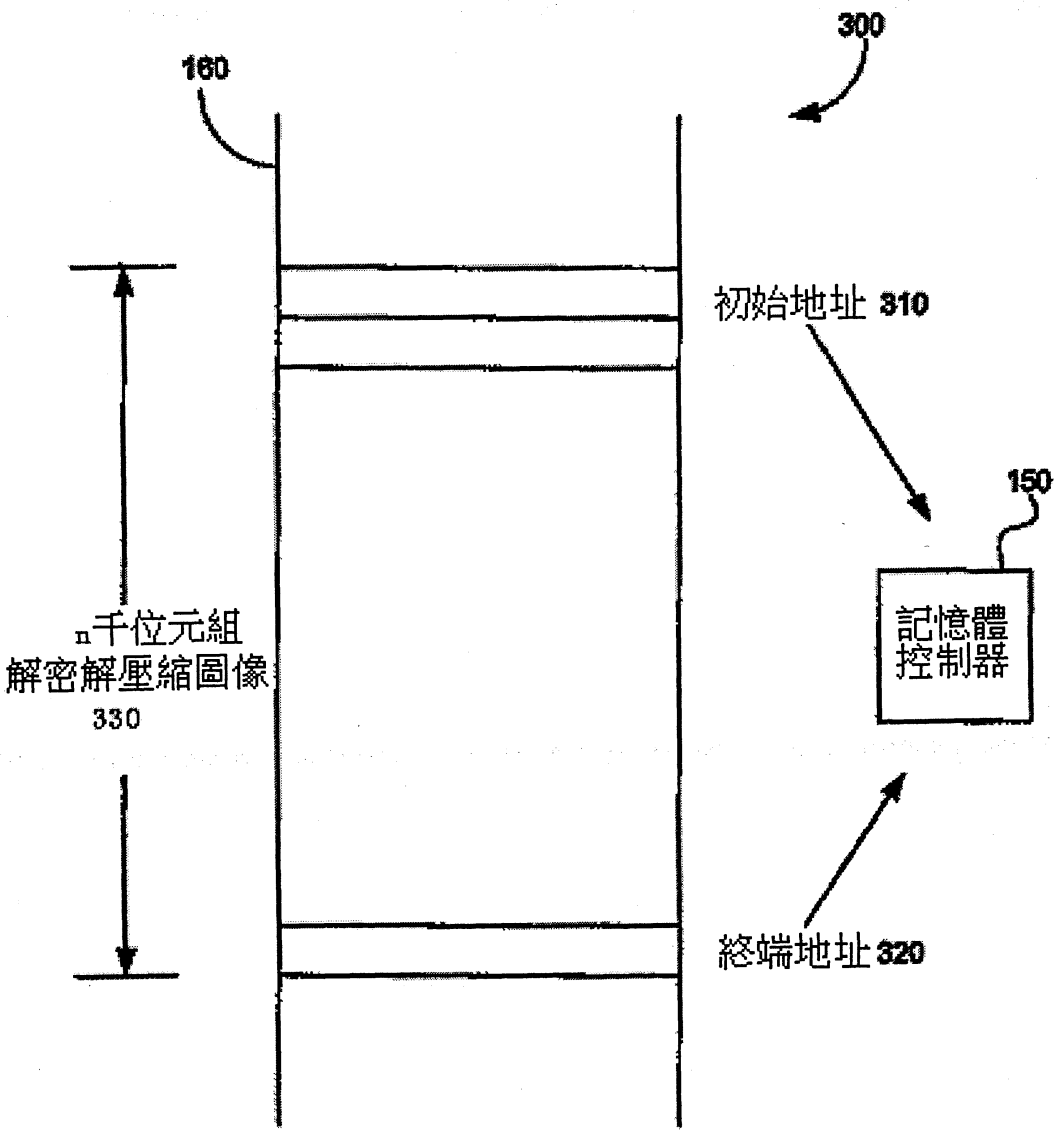
A system and method for the secure storage of executable code and the secure movement of such code from memory to a processor. The method includes the storage of an encrypted version of the code. The code is then decrypted and decompressed as necessary, before re-encryption in storage. The re-encrypted executable code is then written to external memory. As a cache line of executable code is required, a fetch is performed but intercepted. In the interception, the cache line is decrypted. The plain text cache line is then stored in an instruction cache associated with a processor.


100
保密嵌入式
處理器系統105
180
外部
記憶體
120
130
資料
快取
指令超快
取記憶體
處理器
110
140
150
保密控制
器
記憶體
控制器
185
145
PCI
I/F
密鑰
管理模組
外部
介面
160
170
快閃記
憶體模組
175

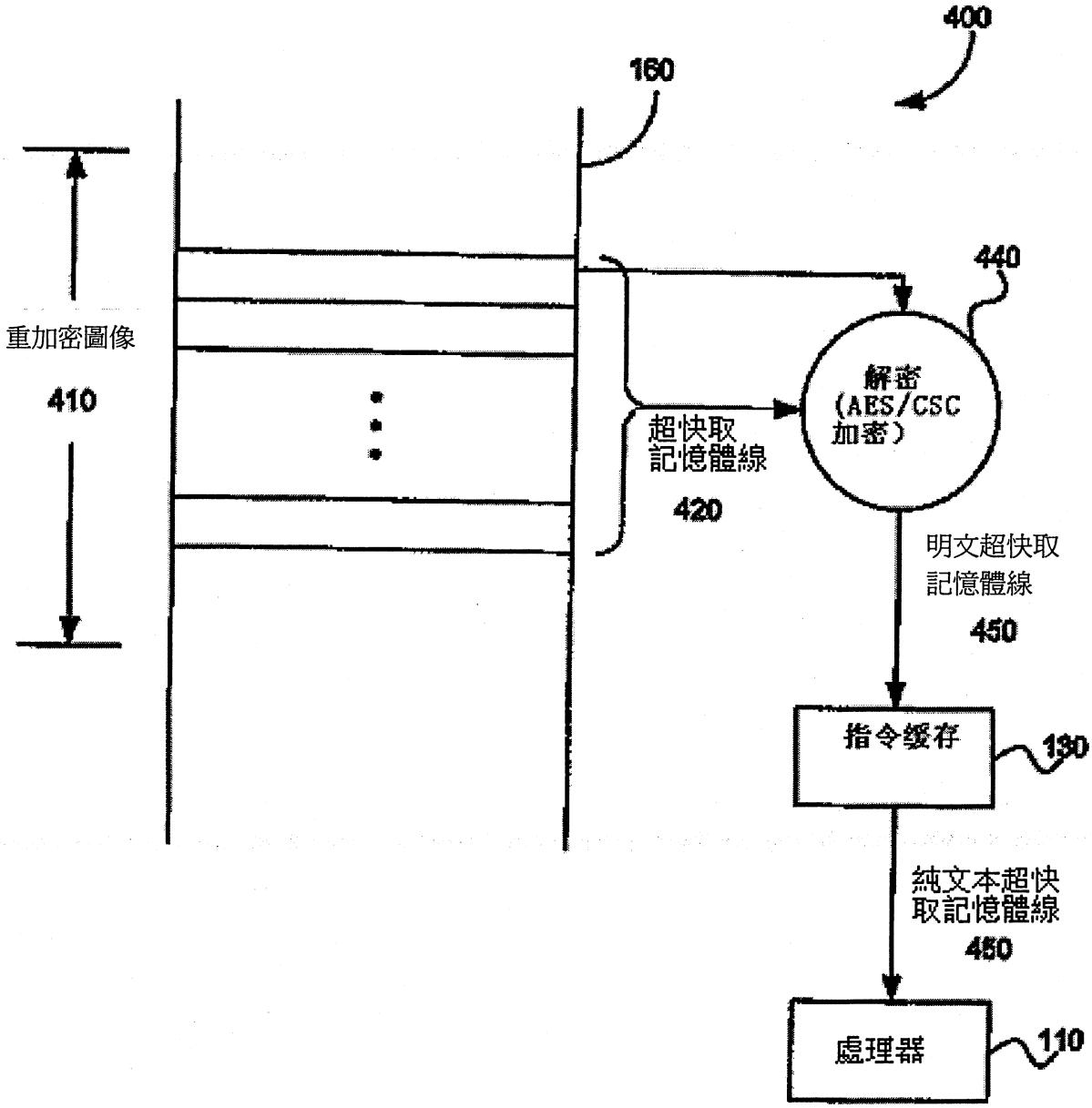
第一圖



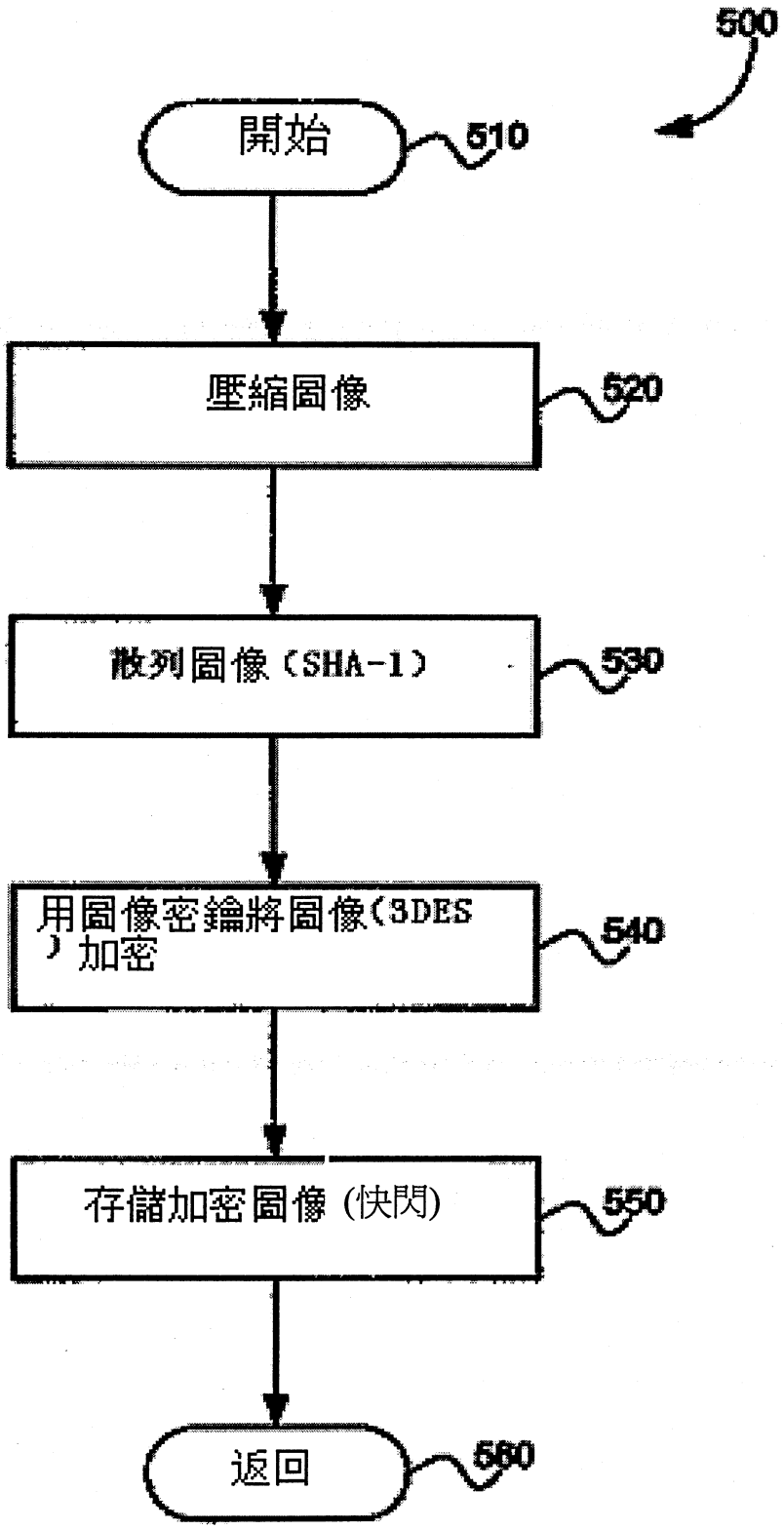
第二圖



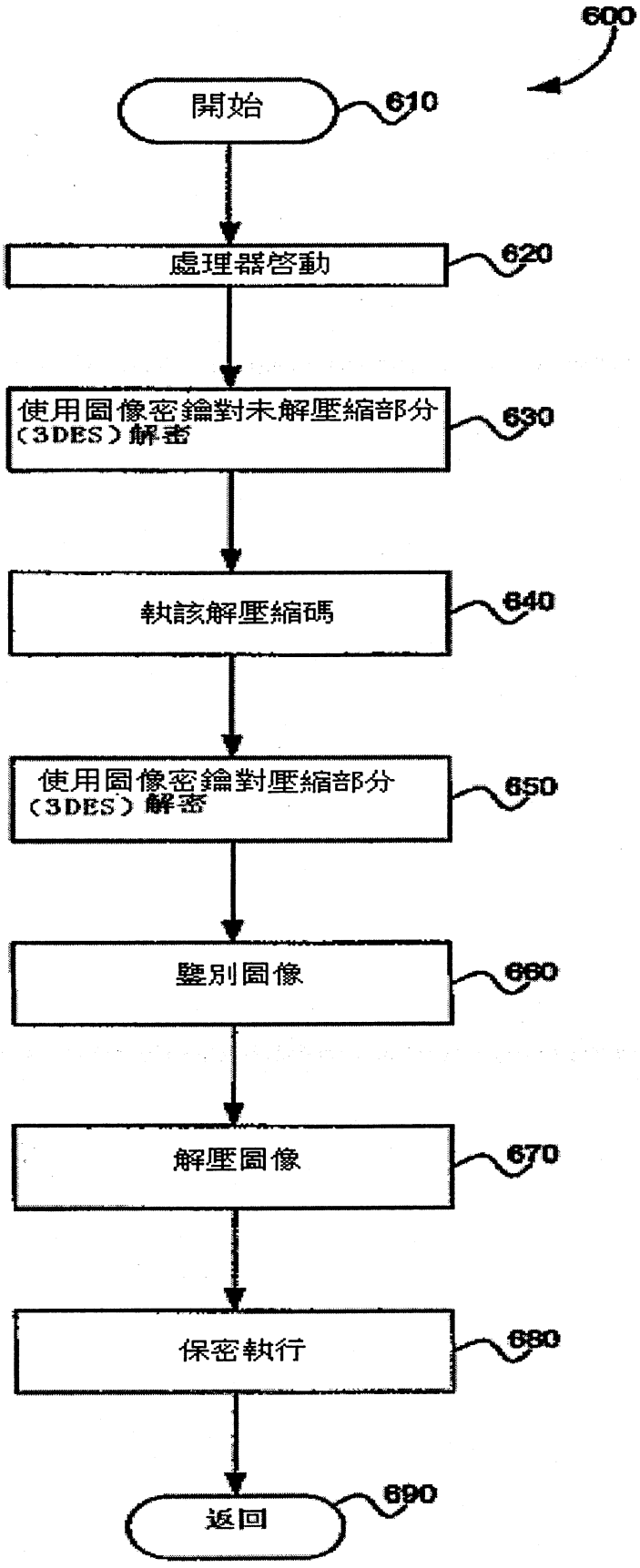
第三圖


400
160
重加密圖像
410
440
解密
(AES/CSC
加密)
超快取
記憶體線
420
明文超快取
記憶體線
450
指令緩存
130
純文本超快
取記憶體線
460
處理器
110

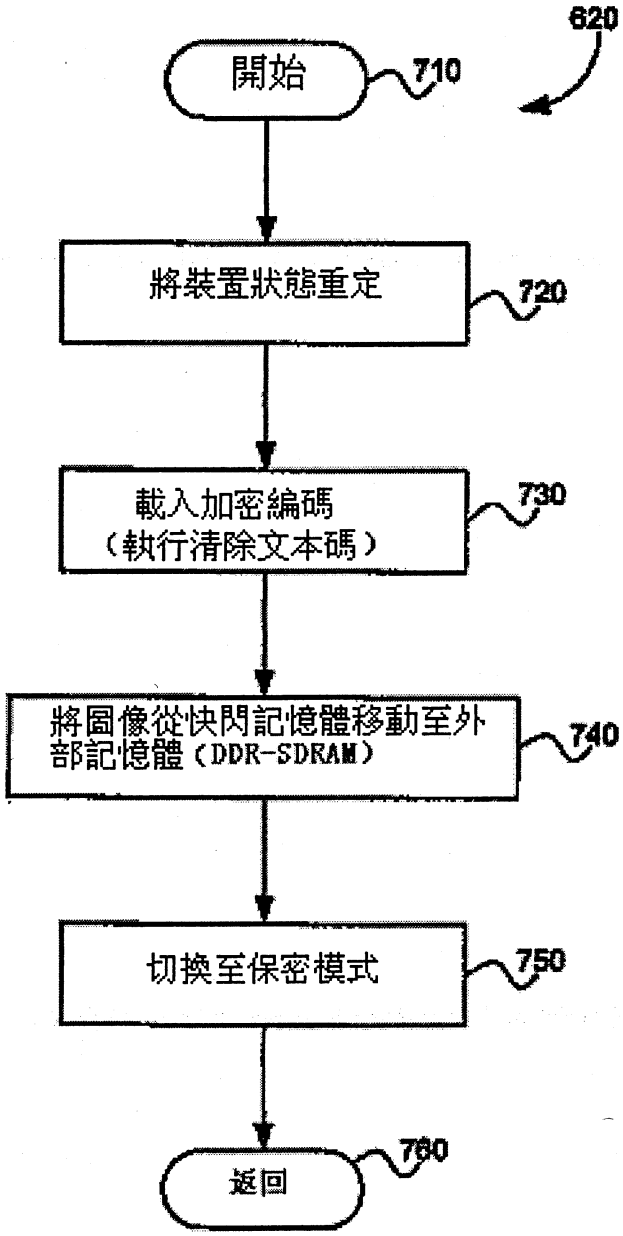
第四圖


500
開始
510
壓縮圖像
520
散列圖像（SHA-1）
530
用圖像密鑰將圖像（3DES）加密
540
存儲加密圖像（快閃）
550
返回
560

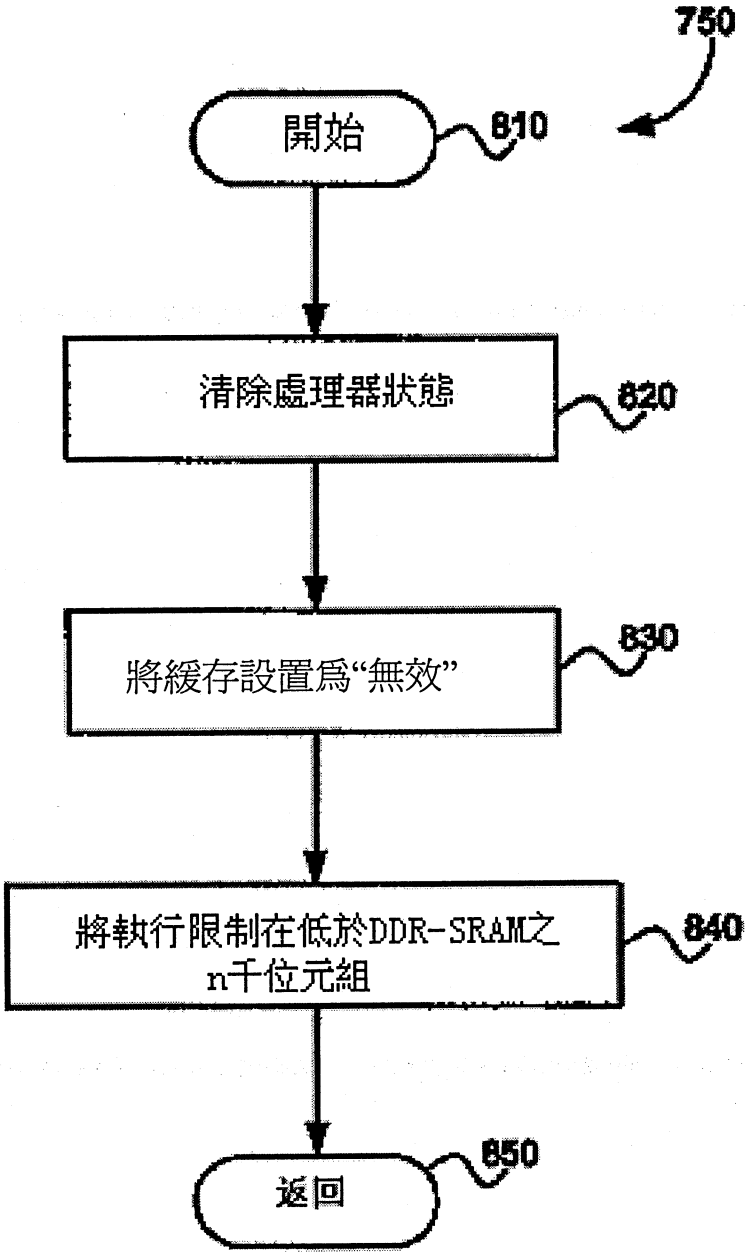
第五圖


600
開始
610
處理器啓動
620
使用圖像密鑰對未解壓縮部分（3DES）解密
630
執該解壓縮碼
640
使用圖像密鑰對壓縮部分（3DES）解密
650
鑒別圖像
660
解壓圖像
670
保密執行
680
返回
690

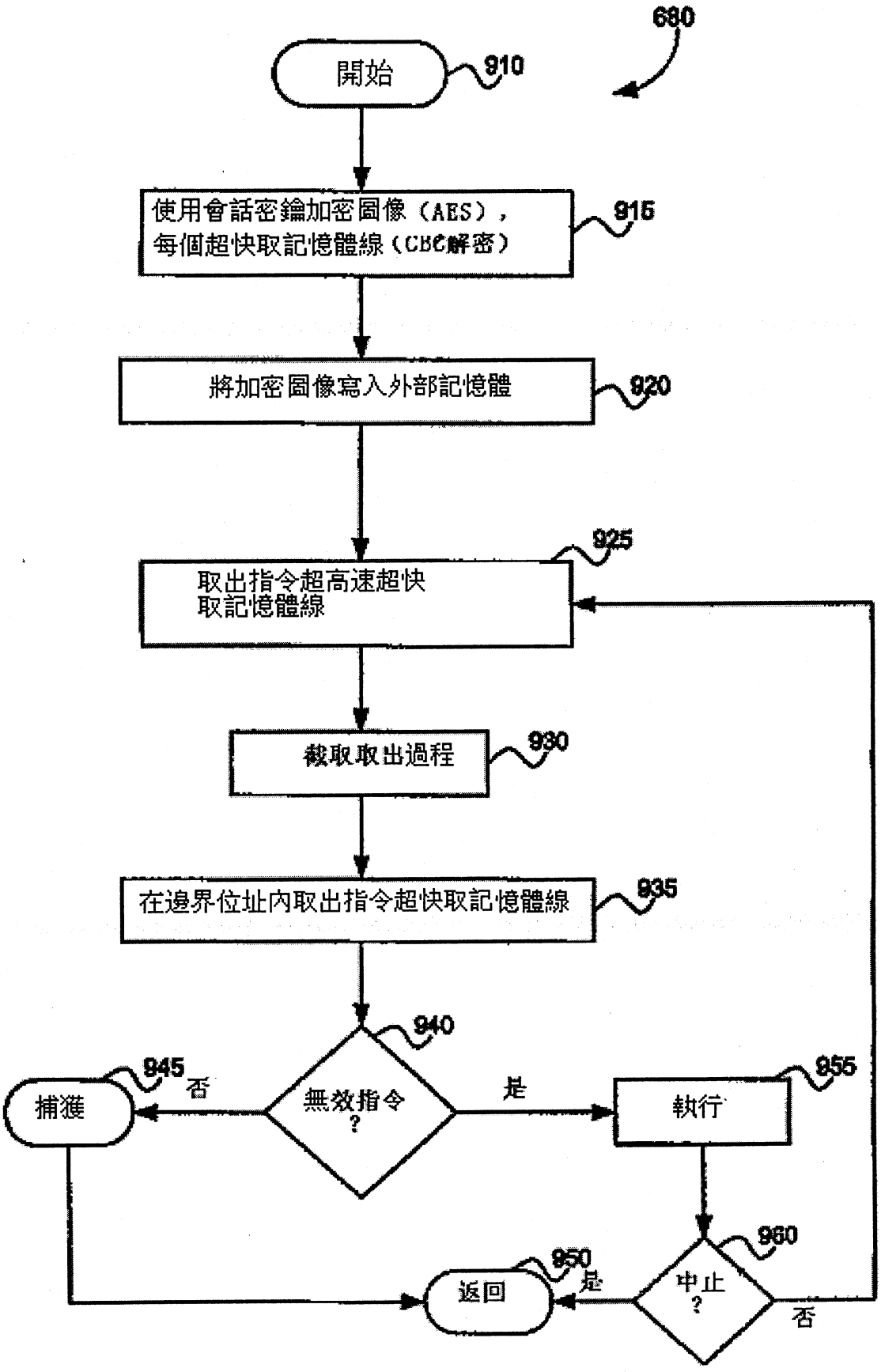
第六圖


620
開始
710
將裝置狀態重定
720
載入加密編碼
（執行清除文本碼）
730
將圖像從快閃記憶體移動至外部記憶體（DDR-SDRAM）
740
切換至保密模式
750
返回
760

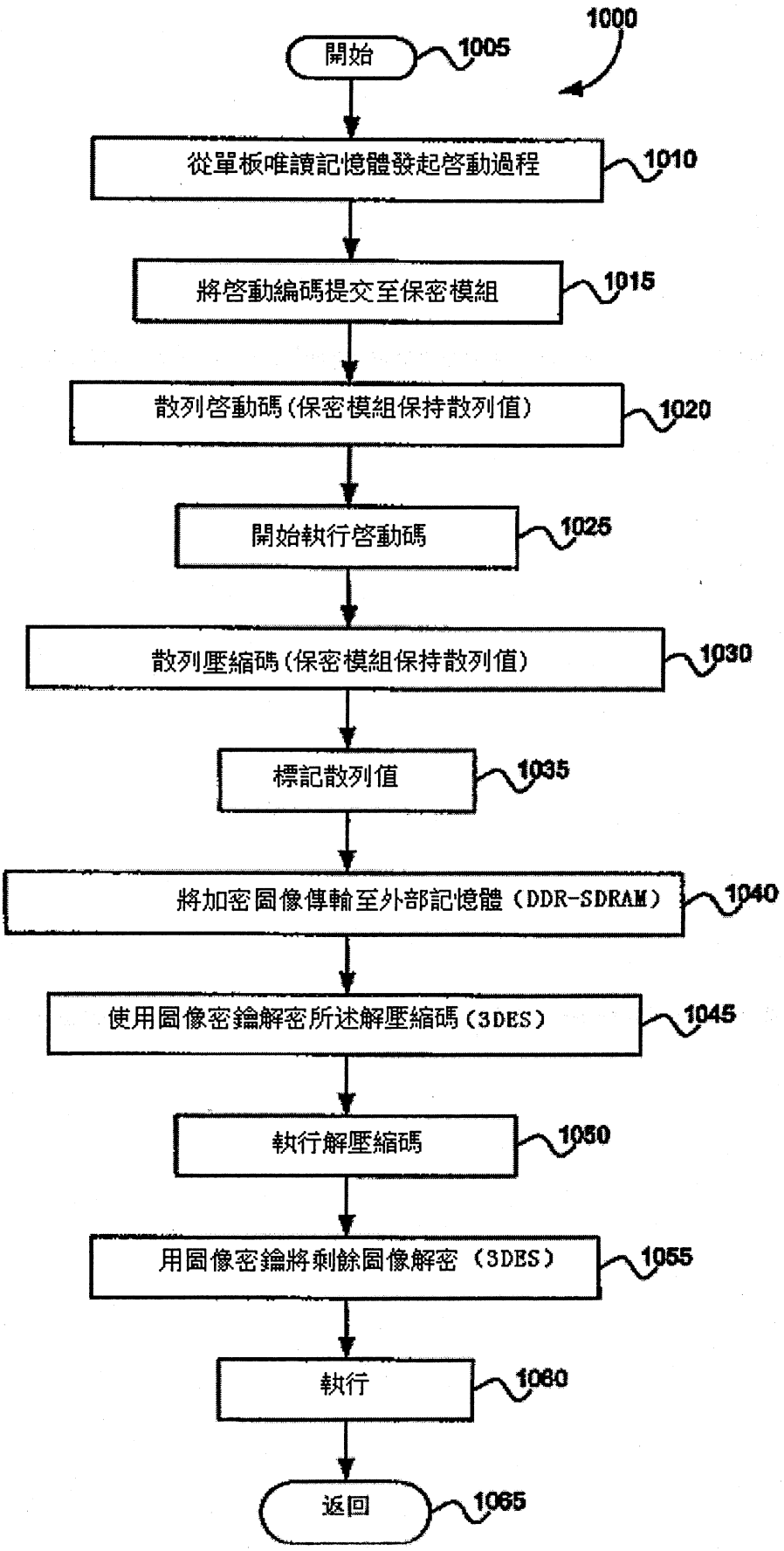
第七圖


750
開始
810
清除處理器狀態
820
將緩存設置爲“無效”
830
將執行限制在低於DDR-SRAM之
n千位元組
840
返回
850

第八圖


680
開始
910
使用會話密鑰加密圖像（AES），
每個超快取記憶體線（CBC解密）
915
將加密圖像寫入外部記憶體
920
925
取出指令超高速超快
取記憶體線
截取取出過程
930
在邊界位址內取出指令超快取記憶體線
935
940
無效指令
？
否
是
945
捕獲
955
執行
960
中止
？
是
否
950
返回

第九圖


1000
開始
1005
從單板唯讀記憶體發起啓動過程
1010
將啓動編碼提交至保密模組
1015
散列啓動碼(保密模組保持散列值)
1020
開始執行啓動碼
1025
散列壓縮碼(保密模組保持散列值)
1030
標記散列值
1035
將加密圖像傳輸至外部記憶體(DDR-SDRAM)
1040
使用圖像密鑰解密所述解壓縮碼(3DES)
1045
執行解壓縮碼
1050
用圖像密鑰將剩餘圖像解密(3DES)
1055
執行
1060
返回
1065

第十圖

七、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:

保密嵌入式處理器系統 105

處理器 110

指令超快取記憶體 130

保密控制器 140

基礎結構 145

記憶體控制器 150

外部記憶體 160

密鑰管理模組 170

快閃記憶體模組 175

外部介面 180

周邊零件連接（PCI）介面 185

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

十、申請專利範圍：

1．一種用於處理器指令的保密執行之系統，包括：

一第一記憶體，其包含啟動代碼及用第一密鑰所加密之圖像，所述圖像包含第一部分和第二部分，所述第一部分用於解密所述第二部分；

一保密嵌入式處理器系統，其包括：

一處理器；

一與所述處理器相通訊之指令超快取記憶體；

一與所述指令超快取記憶體通訊之記憶體控制器；

一與所述指令超快取記憶體通訊之保密控制器；及

一第二記憶體，其位於所述保密嵌入式處理器系統之外部，並與所述第一記憶體、記憶體控制器及保密控制器通訊，

其中，所述用第一密鑰加密之圖像被傳輸至所述第二記憶體，存儲在所述第二記憶體中的連續存儲空間內，所述連續存儲空間的起點在第一位址並且終點在終端位址，所述指令超快取記憶體被設置為無效狀態，用所述第一密鑰加密之圖像被所述保密控制器解密，並由所述保密控制器使用第二密鑰再加密，位於由所述第一位址和終端位址限定的所述連續存儲空間內、用所述第二密鑰加密之圖像以超快取記憶體線為單位從所述第二記憶體被讀取，再用所述第二密鑰進行解密，然後存儲於所述指令超快取記憶體中，以被所述處理器所執行。

2．如申請專利範圍第 1 項所述之系統，其中所述保密控制器包括使用三重資料加密標準（3DES）演算法及所述第一密鑰對所述被加密圖像進行解密之邏輯電路。

3．如申請專利範圍第 1 項所述之系統，其進一步包括一密鑰管理模組，該密鑰管理模組包括：

以加密形式接收所述第一密鑰之邏輯電路；

使用會話密鑰對所述被加密之第一密鑰進行解密之邏輯電路；

將所述第一密鑰轉發到所述保密控制器之邏輯電路。

4．如申請專利範圍第 1 項所述之系統，其中所述保密控制器中包括：使用高級加密標準（AES）演算法重加密所述圖像的邏輯電路；及使用所述 AES 演算法解密所述超快取記憶體線的邏輯電路。

5．一種提供處理器指令的保密執行的方法，其包括以下步驟：

a. 啓動處理器，以將加密編碼載入到外部記憶體中，所述加密編碼包含第一部分和第二部分，所述第一部分用於解密所述第二部分；將與所述處理器相關聯之一指令超快取記憶體設置爲無效狀態；

b. 使用圖像密鑰對所述加密編碼中解壓縮之部分進行解密，以產生解密解壓縮碼之第一部分；

c. 執行所述解密解壓縮碼之第一部分；

d. 使用所述圖像密鑰對所述加密編碼中之壓縮部分進行解

97 1 18

密，以產生一圖像；

e. 鑒別所述圖像；

f. 解壓縮該圖像從而使其佔據外部記憶體中之連續的一部分，起點在第一地址並且終點在終端地址；及

g. 執行所述圖像之保密執行，其進一步包括：

i. 以超快取記憶體線爲單位加密圖像；

ii. 從由所述第一地址和終端地址限定的所述外部記憶體中之所述連續的一部分中取出一加密超快取記憶體線；

iii. 截取所述取出過程；

iv. 解密所取出之加密超快取記憶體線；

v. 確定解密超快取記憶體線是否有效；

vi. 若解密超快取記憶體線無效，捕獲該解密超快取記憶體線；及

vii. 若解密超快取記憶體線有效，執行所述解密超快取記憶體線。

6·如申請專利範圍第5項所述之方法，其中使用三重資料加密標準（3DES）演算法執行所述解密步驟b及d。

7·如申請專利範圍第5項所述之方法，在執行步驟a之前，所述方法進一步包括以下步驟：

h·確定所述圖像密鑰是否失效，僅於所述圖像密鑰還沒有失效之條件下，才執行所述步驟a—g。

8．如申請專利範圍第5項所述之方法，執行步驟a之前，所述方法進一步包括以下步驟：

h．產生加密編碼。

9．如申請專利範圍第8項所述之方法，其中所述步驟h包括：

i．壓縮所述圖像；

ii．對所述圖像進行散列處理以產生一散列值；

iii．加密所述圖像；及

iv．存儲所述加密編碼。

10．如申請專利範圍第9項所述之方法，其中在所述步驟h.ii.中，使用保密散列演算法1（SHA-1）對所述圖像進行散列處理。