

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：97141203

※申請日期：2008年10月27日

※IPC分類：

一、發明名稱：(中文/英文)

G06F 9/46
G06F 9/30

仿效經抽象化曝露之功能性

MIMICKING OF FUNCTIONALITY EXPOSED THROUGH AN
ABSTRACTION

二、申請人：(共1人)

姓名或名稱：(中文/英文)

美商·微軟公司

Microsoft Corporation

代表人：(中文/英文)

艾華那諾爾 D 巴特萊

EPPENAUER, D. BARTLEY

住居所或營業所地址：(中文/英文)

美國華盛頓州列德蒙微軟路1號

One Microsoft Way, Building 8, Redmond, WA 98052-6399, U.S.A.

國籍：(中文/英文)

美國/USA

三、發明人：(共2人)

姓名：(中文/英文)

1. 柯恩史丹迪立夫/KORNSTAEDT, LEIF

2. 帕多伊安德魯/PARDOE, ANDREW

國 籍：(中文/英文)

1.德國/GERMANY

2.美國/USA

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：

美國；2007年11月19日；11/941,986

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。

國 籍：(中文/英文)

1.德國/GERMANY

2.美國/USA

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：

美國；2007年11月19日；11/941,986

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】

本發明關於仿效經一抽象化曝露之功能性。

【先前技術】

在運算當中，一應用平台稱為一架構，其可為硬體或軟體，並可允許軟體運作。典型的平台包括一電腦的架構、一作業系統、或程式化語言及其執行時間程式庫。因此，一些應用平台的範例可包括作業系統(例如 MICROSOFT® WINDOWS® 或 Linux) 或執行時間平台(例如 MICROSOFT® .NET Framework 及 Java)。對於一應用平台常見的是具有對於該應用平台為私密的資料或資源。在這種方案中，如果另一個應用想要使用相同資料，該應用先必須與該應用平台通訊以請求該資料，然後必須等待該應用平台來回應於該請求。

對於一應用平台為私密之資料的範例包括執行緒區域儲存器。執行緒區域儲存器為一種技術，其中一作業系統允許每個執行緒來具有其本身私密的資料儲存區域。存取到儲存在該私密儲存區域中的一給定執行緒之資料必須經由該作業系統執行。此對於使用該執行緒區域儲存器之應用的效能有負面的影響。

【發明內容】

本發明揭示仿效一應用平台之功能性的多種科技及技

術。在執行時間當中，對於一應用平台進行分析來識別一所要的功能性如何由該應用平台來實施。當該分析顯示出該應用平台正使用可被仿效的一已知功能，略過與該應用平台之交握，且仿效所想要的功能性。

在一種實施態樣中，為了仿效該功能性，對於使用所想要的功能性之一應用平台開始一已知的功能。其偵測到該已知功能的進入點。機器指令在該已知功能中被解碼。其產生仿效該等機器指令之效果的碼。然後執行仿效該等機器指令之效果的碼。

在一種實施態樣中，仿效機器指令之效果的碼係藉由將該解碼的機器指令之效果表示成一抽象執行狀態來產生。該等解碼的機器指令由該應用平台中的已知功能來產生，其具有另一個應用想要仿效的所想要功能性。該抽象執行狀態被轉換到一抽象表述。然後碼由該抽象表述所產生。

此發明內容說明係用來介紹在一簡化型式中選出的觀念，其在以下的詳細說明中會進一步說明。此內容說明並非要提出所主張之標的的關鍵特徵或基本特徵，也並非要做為輔助決定所主張之標的的範疇。

【實施方式】

此處所述之科技及技術可在一般性內文中描述為一種應用來仿效一應用平台的功能性，但該等科技及技術除此之外亦可用於其它目的。在一種實施態樣中，此處所述的

一或多種技術可實施成在想要存取對於一應用平台為私密的資料或資源的任何種類的程式或服務內的特徵。

第 1 圖為存取對於一應用平台為私密的資料或資源的一典型交握程序 10 之示意圖。如前所述，當一應用 12 想要使用對於一應用平台 16 為私密的資料或資源 18，請求資料的應用 12 首先必須與應用平台 16 通訊來請求資料或資源 18，然後必須等待該應用平台來回應該請求。在該請求可被處理之前，請求資料的應用 12 首先必須與應用平台 16 建立一交握 14。此處所使用的術語「交握(handshake)」代表包括一種機制，其中一應用可請求一應用平台代表該應用來執行一服務。該交握為開啟請求資料的應用 12 與應用平台 16 之間的通訊通道。一旦建立交握 14 之後，該請求可被遞交到應用平台 16，該應用平台可存取資料或資源 18 來得到所請求的資訊，並傳回該資料到請求資料的應用 12。

在一種實施態樣中，如第 2 圖所示，一仿效系統 20 被提供來允許應用平台功能性被仿效，如此資料或資源可由一應用來存取，其另對於一應用平台為私密。如第 2 圖所示，請求資料的應用 22 使用一仿效技術來直接存取資料或資源 24，其另已經對於應用平台 26 為私密。如此處所使用的術語「仿效(mimick)」代表包括執行應用碼，其具有與實施該服務的應用平台碼為相同的語義效果。正被仿效的該應用平台碼之功能性及該應用碼之功能性無法為一觀察者所分辨，除了所想要的行為改變，例如較佳的效能

或附加的功能性。

此處所述可使用的部份或所有仿效技術之一種範例係利用執行緒區域儲存器。如前所述，執行緒區域儲存器為一種技術，其中一作業系統允許每個執行緒來具有其本身私密的資料儲存區域。對於儲存在該私密儲存區域中的一給定執行緒之資料的存取基本上必須經由該作業系統執行。使用在此處進一步詳細說明的部份或所有仿效技術，請求資料的應用 22 可直接存取儲存在執行緒區域儲存器中的資料，而不需要經由與該應用平台（其在此例中為該作業系統）的交握及請求程序。

現在參照第 3 圖至第 6 圖以及第 2 圖，用於實施仿效系統 20 之一些技術在此進一步說明。在一些實施態樣中，第 3 圖至第 6 圖之程序係至少部份實施在（第 7 圖）運算裝置 500 之作業邏輯中。

第 3 圖為牽涉到在執行時間當中發現及仿效應用平台功能性之高階平台的一種實施態樣之作業流程圖 100。在執行時間中，一應用平台被詢問或另被分析來察看如何實施一特定功能性（階段 102）。該特定功能性可為由一應用平台所提供的任何功能性，其存取另一個應用現在想要存取的私密資料或資源。如果該分析顯示出正在使用的一已知功能可被仿效（決策點 104），然後該等技術可用於仿效該應用平台功能性及略過該交握（階段 106）。如此處所使用的術語「已知功能」代表包括一功能、程序、例式或其它邏輯，其可獨立於該應用平台而做為一個整體來執行。

該仿效程序在第 4 圖中進一步詳細說明。

如果該分析並未顯示該應用平台正在使用可被仿效的已知功能(決策點 104)，則該交握由該應用平台啟始，並經由該應用平台使用該已知功能(如第 1 圖所示)來存取該等資料或資源(正常化)(階段 108)。

現在參照第 4 圖，所示為一種實施態樣的作業流程圖 120，其例示出牽涉到仿效該應用平台之發現的功能性之更為細部的階段。在執行時間中，開始一已知功能，其使用了所想要的功能性，例如在執行緒區域儲存器中的一存取器功能(階段 122)。該系統決定該功能的進入點，其基本上為該第一機器指令的位址(階段 124)。該等機器指令被解碼(階段 126)。如果尚未產生另一功能來仿效所想要功能性之效果(決策點 128)，則產生仿效該等機器指令的效果之碼，然後執行新產生的碼(階段 132)。此碼產生程序於第 5 圖中更為詳細的說明。如果已經產生另一功能(決策點 128)，則已經產生的既有碼被執行來仿效該應用平台的效果(階段 132)。

第 5 圖為牽涉到產生仿效該等機器指令之效果的碼之該等階段的一種實施態樣之作業流程圖 150。該系統代表做為一抽象執行狀態之解碼的機器指令之效果(階段 152)。如此處所使用的術語「抽象執行狀態(abstract execution state)」代表包括關於該程式的事實，其在其執行的一給定時間點獨立地反應該程式的狀態。正確地代表程式狀態所需要的事實包括要被執行之指令的語義效果及

程式資料的數值。現在將討論一非限制性範例來進一步例示一抽象執行狀態之觀念。假設該應用平台的介面規格曝露一資料存取器，其做為根據一應用二元化介面 (ABI, “Application Binary Interface”) 呼叫的功能。假設該 ABI 需要例如欄位移位之參數被寫入到記憶體 (該機器堆疊) 及一些暫存器，其在要該呼叫 (到該機器堆疊) 之前儲存，並在該呼叫之後恢復。該執行狀態可包括該等機器暫存器與堆疊插槽的數值。該應用仿真在該應用平台中的指令，但並不以實際數值及暫存器/堆疊插槽上來執行它們。而是，變數係做為位置保存器而非實際數值，且該抽象執行狀態映射暫存器/堆疊插槽到包含那些變數之表述 (其相對於由於使用該等變數之實際數值來評估該等抽象表述所得到的實際數值)。

該抽象執行狀態依需要可對於要被存取之特定資料欄位來特殊化 (階段 154)。例如，所存在的資訊可由執行時間中一應用程式使用，而當其被編譯時該應用平台即不可使用。該碼藉由利用此執行時間資訊來建立更有效率的碼來特殊化。然後該抽象執行狀態被轉換成一抽象表述 (階段 156)，然後碼由該抽象表示來產生 (階段 158)。如此處所使用的術語「抽象表述 (abstract expression)」代表包括一程式的表示，其中包括其指令及該程式資料的語義效果。一碼產生器可採用一抽象表述做為輸入，並產生碼，其在當執行時可利用該程式的特定資料值來評估該表述，以產生一種狀態，其為由該抽象表述所描述的一實例。

一旦碼由該抽象表述產生之後(階段 158)，該碼可視需要被嵌入到其它碼當中(階段 160)。嵌入(inline)為一編譯器最佳化方式，其可被執行來直接包括在一程式中的一些碼，所以其被包括做為一編譯的可執行程式之一部份，因此比自一獨立程式庫或可執行程式來存取該碼要快。例如，想要仿效該應用平台之功能性的應用可嵌入所撰寫的碼來直接與其中其它的碼執行該仿效，藉以改善當執行該仿效的功能性時之效能。第 6 圖為牽涉在包含暫存器及暫存器移位之方案中使用仿效的該等階段之作業流程圖 180。該系統決定該應用平台正在使用的暫存器及其移位(階段 182)，並選擇一種方法來使用，其將可仿效該功能性(階段 184)。然後該選擇的方法使用該基礎位址與先前被決定由該應用平台使用的暫存器來執行(階段 186)。

現在將描述一非限制性範例來進一步例示暫存器及暫存器移位之觀念。一給定作業系統(其為一應用平台)可保留一些機器暫存器，其代表應用碼並不允許為了它們本身的儲存目的而使用它們。這些機器暫存器將由該作業系統使用做為簿記目的，並由作業系統功能所存取。在執行緒區域儲存器之範例中，一給定機器暫存器可在執行緒建立時被初始化，以指向到「執行緒環境區塊」。該執行緒環境區塊為一種結構，其在由該作業系統所決定的一移位處包含指向到執行緒區域儲存器之一插槽陣列的一欄位。為了仿效及存取到執行緒區域儲存器，其將必須做成決定，其係關於那個保留的機器暫存器指向到該執行緒環境區塊，

及該執行緒區域儲存插槽存在於那一個移位。例如，在 x86 平台上的 MICROSOFT® WINDOWS® NT 將使用 FS 暫存器來指向到該執行緒環境區塊，且該移位對於前 64 個執行緒區域儲存插槽將為 $3600+4*(\text{執行緒區域儲存插槽索引})$ 。在第 6 圖所述的程序中，此基礎位址及該 FS 暫存器將可用於執行該選擇的方法(階段 186)。

現在請參照第 7 圖，所示為用於實施該系統一或多個部份之示例性電腦系統包括一運算裝置，例如運算裝置 500。在其最基本的組態中，運算裝置 500 基本上包括至少一處理單元 502 及記憶體 504。根據運算裝置的實際組態及種類，記憶體 504 可為揮發性(如 RAM)、非揮發性(如 ROM、快閃記憶體等)或兩者的某種組合。此最基本組態在第 7 圖中由虛線 506 所示。

此外，裝置 500 亦可具有額外的特徵/功能。例如，裝置 500 亦可包括額外的儲存器(可移除及/或不可移除式)，其包括但不限於磁碟或光碟或磁帶。這些額外的儲存器在第 7 圖中例示有可移除儲存器 508 及不可移除儲存器 510。電腦儲存媒體包括以任何方法或技術來儲存資訊的揮發性及非揮發性、可移除及不可移除媒體，像是電腦可讀取指令、資料結構、程式模組或其它資料。記憶體 504、可移除儲存器 508 及不可移除儲存器 510 皆為電腦儲存媒體的範例。電腦儲存媒體包括(但不限於)RAM、ROM、EEPROM、快閃記憶體或其它記憶體技術、CD-ROM、數位多功能碟片(DVD)或其它光學儲存、磁性卡匣、磁帶、

磁碟儲存或其它磁性儲存裝置，或任何其它媒體可用於儲存所要的資訊，並可由裝置 500 存取。任何這些電腦儲存媒體可為裝置 500 的一部份。

運算裝置 500 包括一或多個通訊連接 514，其允許運算裝置 500 與其它電腦/應用 515 通訊。裝置 500 亦可具有輸入裝置 512，例如鍵盤、滑鼠、筆、語音輸入裝置、觸控輸入裝置等。輸出裝置 511，例如一顯示器、喇叭、印表機等，亦可包含在其中。這些裝置皆為本技藝中所熟知，不需要在此贅述。

雖然該標的已經以特定於結構化特徵及/或方法性動作的語言來描述，其應瞭解到在附屬申請專利範圍中所定義的標的並不必要地限制於上述之特定特徵或動作。而是上述的特定特徵與動作係以實施該等申請專利範圍之範例型式來揭露。在如此處所述的實施態樣之精神之下及/或藉由以下的申請專利範圍之所有等效物、改變、及修正皆要受到保護。

例如，在該電腦軟體技藝中的專業人士將可瞭解到此處所述的範例可在一或多部電腦上不同的組織化，以包括比該等範例中所述之較少或額外的選項或特徵。

【圖式簡單說明】

第 1 圖為存取對於一應用平台為私密的資料或資源的一典型交握之示意圖。

第 2 圖為仿效應用平台功能性來取得另對於一應用平

台為私密的資料或資源之示意圖。

第 3 圖為牽涉到在執行時間當中發現及仿效應用平台功能性之高階階段的一種實施態樣之作業流程圖。

第 4 圖為牽涉到仿效該應用平台之發現的功能性之該等階段的一種實施態樣之作業流程圖。

第 5 圖為牽涉到仿效該等機器指令之效果的碼之該等階段的一種實施態樣之作業流程圖。

第 6 圖為牽涉在包含暫存器及暫存器移位之方案中使用仿效的該等階段之作業流程圖。

第 7 圖為一種實施態樣之一電腦系統的示意圖。

【主要元件符號說明】

10 交握程序	506 運算裝置
12 請求資料的應用	508 可移除式儲存器
14 交握	510 不可移除式儲存器
16 應用平台	511 輸出裝置
18 資料或資源	512 輸入裝置
20 仿效系統	514 通訊連接
22 請求資料的應用	515 電腦/應用
24 資料或資源	
26 應用平台	
500 運算裝置	
502 處理單元	
504 記憶體	

五、中文發明摘要：

本發明揭示仿效一應用平台之功能性的多種科技及技術。在執行時間當中，對於一應用平台進行分析來識別一所要的功能性如何由該應用平台來實施。當該分析顯示出該應用平台正使用可被仿效的一已知功能，略過與該應用平台之交握，且仿效所想要的功能性。為了仿效該功能性，對於使用所想要的功能性之該應用平台開始該已知的功能。其偵測到該已知功能的進入點。機器指令在該已知功能中被解碼。其產生仿效該等機器指令之效果的碼。然後執行仿效該等機器指令之效果的碼。

六、英文發明摘要：

Various technologies and techniques are disclosed for mimicking functionality of an application platform. At runtime, an analysis is performed of an application platform to identify how a desired functionality is implemented by the application platform. When the analysis reveals that the application platform is using a known function that can be mimicked, a handshake with the application platform is bypassed and the desired functionality is mimicked. To mimic the functionality, the known function is started for the application platform that uses the desired functionality. An entry point of the known function is detected. Machine instructions are decoded in the known function. Code that mimicks an effect of the machine instructions is generated. The code that mimicks the effect of the machine instructions is then executed.

十、申請專利範圍：

1. 一種具有電腦可執行指令之電腦可讀取媒體，該等電腦可執行指令使得一電腦執行以下步驟：

在執行時間當中，執行一應用平台的分析來識別一所要的功能性如何由該應用平台來實施；及

當該分析顯示出該應用平台正使用可被仿效的一已知功能時，則略過與該應用平台之交握，且仿效所想要的功能性。

2. 如申請專利範圍第 1 項所述之電腦可讀取媒體，另具有電腦可執行指令來使得一電腦執行以下步驟：

當該分析顯示出該應用平台並未在使用可被仿效的一已知功能時，則啟始與該應用平台之交握，且經由該應用平台使用所想要的功能性。

3. 如申請專利範圍第 1 項所述之電腦可讀取媒體，其中該仿效所想要的功能性之步驟包括以下步驟：

開始該應用平台的已知功能；

決定該已知功能的一進入點；

解碼在該已知功能中的機器指令；

產生仿效該等機器指令之效果的碼；及

執行仿效該等機器指令之效果的碼。

4. 如申請專利範圍第 1 項所述之電腦可讀取媒體，其中

解碼該等機器指令之步驟包括以下步驟：

將所解碼的機器指令之效果表示成一抽象執行狀態；及

轉換該抽象執行狀態成為一抽象表述。

5. 如申請專利範圍第 4 項所述之電腦可讀取媒體，其中該產生碼步驟可用於自該抽象表述產生該碼。
6. 如申請專利範圍第 1 項所述之電腦可讀取媒體，其中該仿效所想要的功能性之步驟包括以下步驟：

識別該應用平台正在使用來實施所想要的功能性之一暫存器及一暫存器移位；及

藉由使用一基礎位址及被識別的該暫存器來執行設計成仿效所想要功能性之方法。
7. 如申請專利範圍第 6 項所述之電腦可讀取媒體，另具有電腦可執行指令來使得一電腦執行以下步驟：

自複數可使用方法中選擇設計成仿效所想要功能性之方法。
8. 如申請專利範圍第 1 項所述之電腦可讀取媒體，其中該所想要的功能性為執行緒區域儲存器。
9. 如申請專利範圍第 8 項所述之電腦可讀取媒體，其中

該已知功能為一存取器功能。

10. 一種用於在執行時間中仿效一應用平台的功能性之方法，至少包含以下步驟：

在執行時間中，開始使用一所需要功能性之一應用平台的一已知功能；

決定該已知功能的一進入點；

解碼在該已知功能中的機器指令；

產生仿效該等機器指令之效果的碼；及

執行仿效該等機器指令之效果的碼。

11. 如申請專利範圍第 10 項所述之方法，其中該產生步驟於當該碼先前尚未被產生來仿效該等機器指令之效果時執行。

12. 如申請專利範圍第 10 項所述之方法，其中該所想要的功能性為執行緒區域儲存器。

13. 如申請專利範圍第 12 項所述之方法，其中該已知功能為一存取器功能。

14. 如申請專利範圍第 10 項所述之方法，其中該已知功能的進入點被決定為在該已知功能中該等機器指令的第一機器指令。

15. 如申請專利範圍第 10 項所述之方法，另包含以下步驟：

於執行該碼之前使得仿效該效果之碼嵌入 (inline) 於其它碼來達到一更快的執行效能。

16. 一種用於產生仿效機器指令之效果的碼之方法，至少包含以下步驟：

將解碼的機器指令之效果表示成一抽象執行狀態，該等解碼的機器指令已經由在一應用平台中的一功能所產生，其具有其它應用所想要仿效的一所想要的功能性；

轉換該抽象執行狀態成為一抽象表述；及
由該抽象表述產生碼。

17. 如申請專利範圍第 16 項所述之方法，另包含以下步驟：

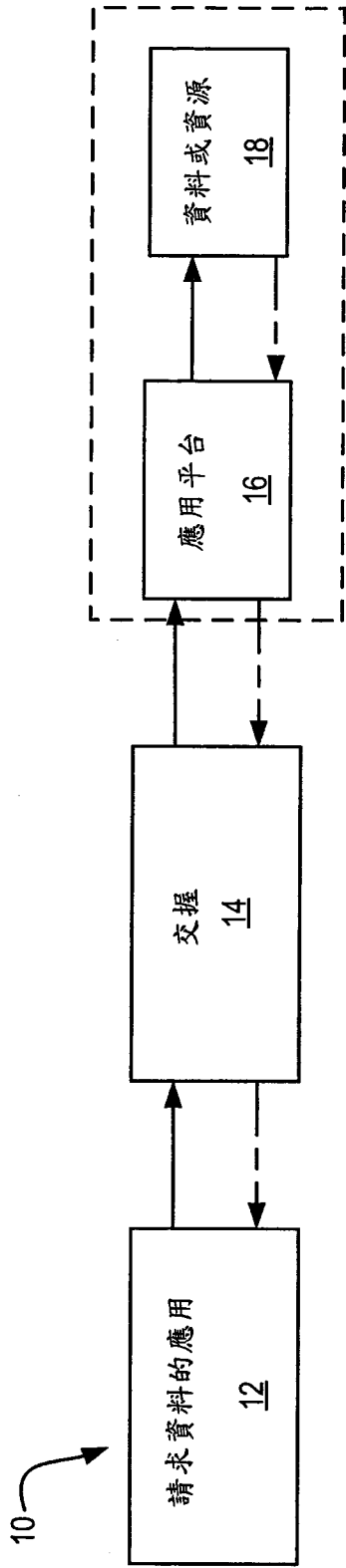
於轉換該抽象執行狀態之前特殊化該抽象執行狀態到要被存取的一特定資料欄位。

18. 如申請專利範圍第 16 項所述之方法，另包含：

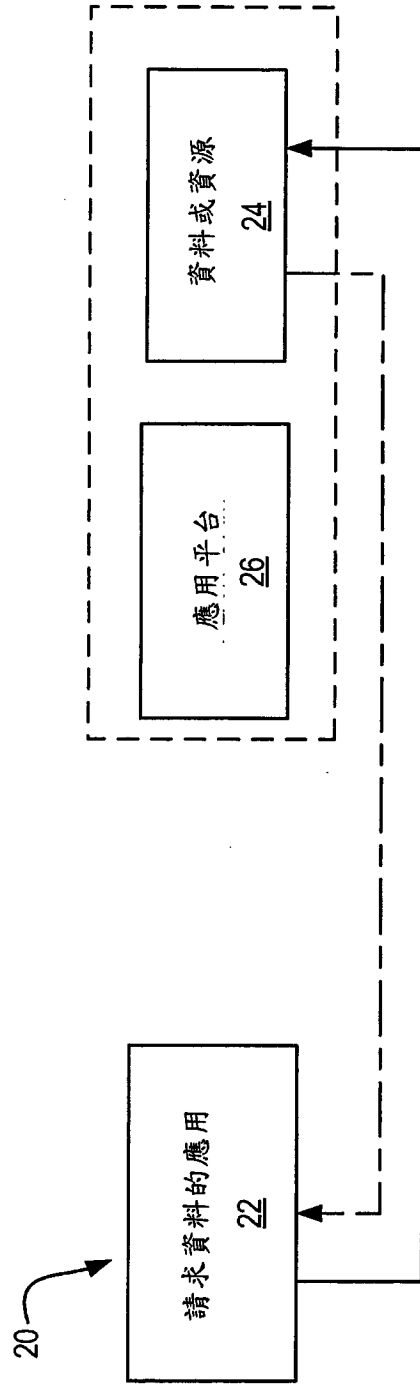
將該產生的碼嵌入到其它碼當中。

19. 如申請專利範圍第 18 項所述之方法，其中該其它碼被直接嵌入到仿效所想要功能性之其它應用當中。

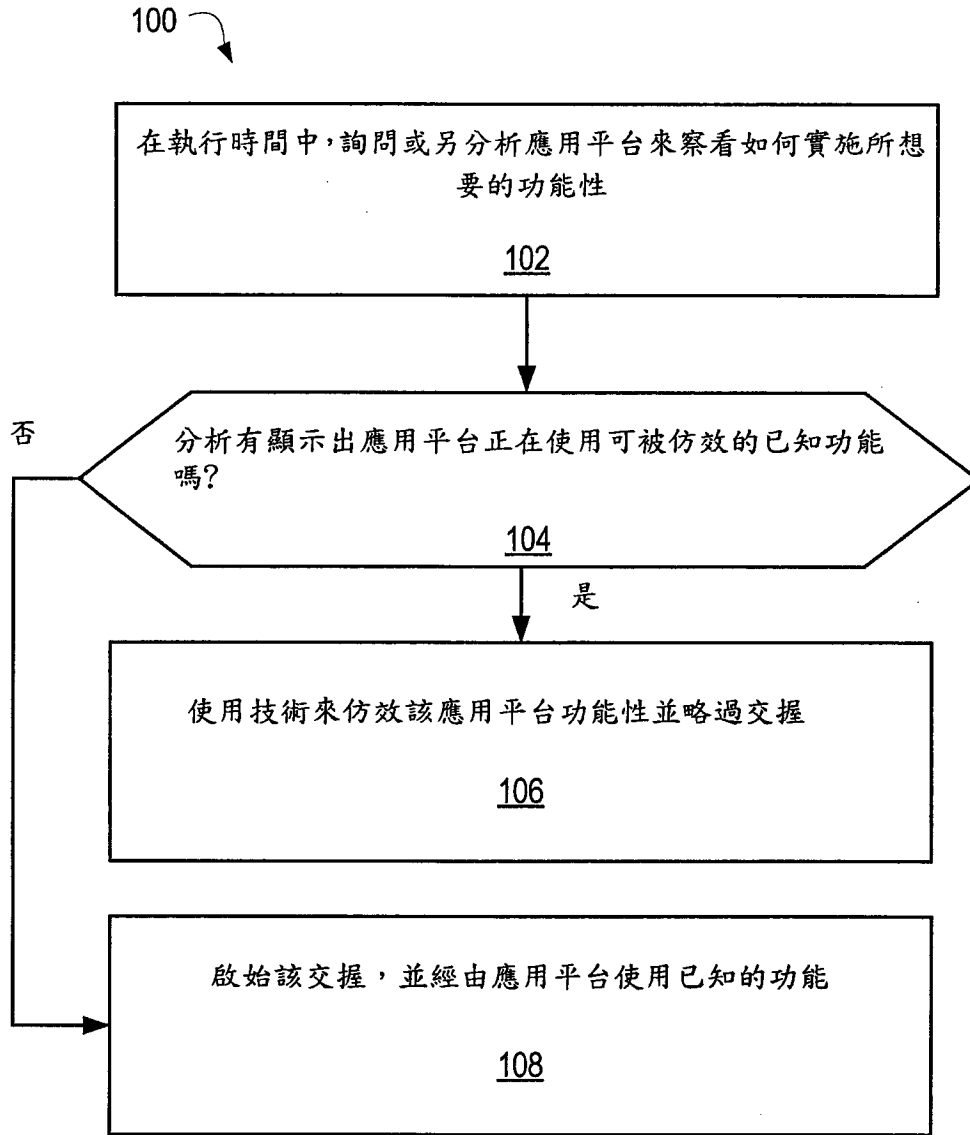
20. 如申請專利範圍第 19 項所述之方法，其中該其它碼被直接嵌入到其它應用當中來在當仿效該所想要的功能性時改善該其它應用的效能。



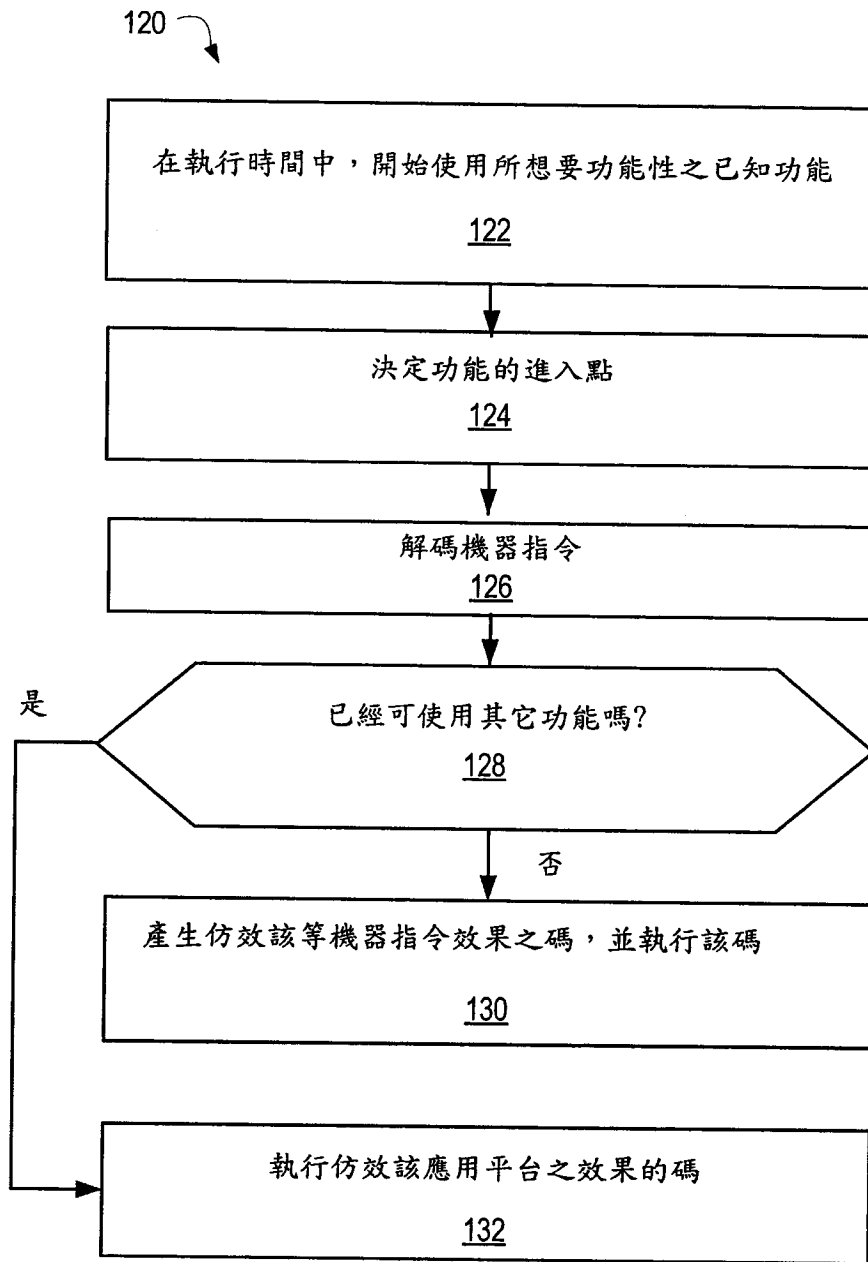
第 1 圖



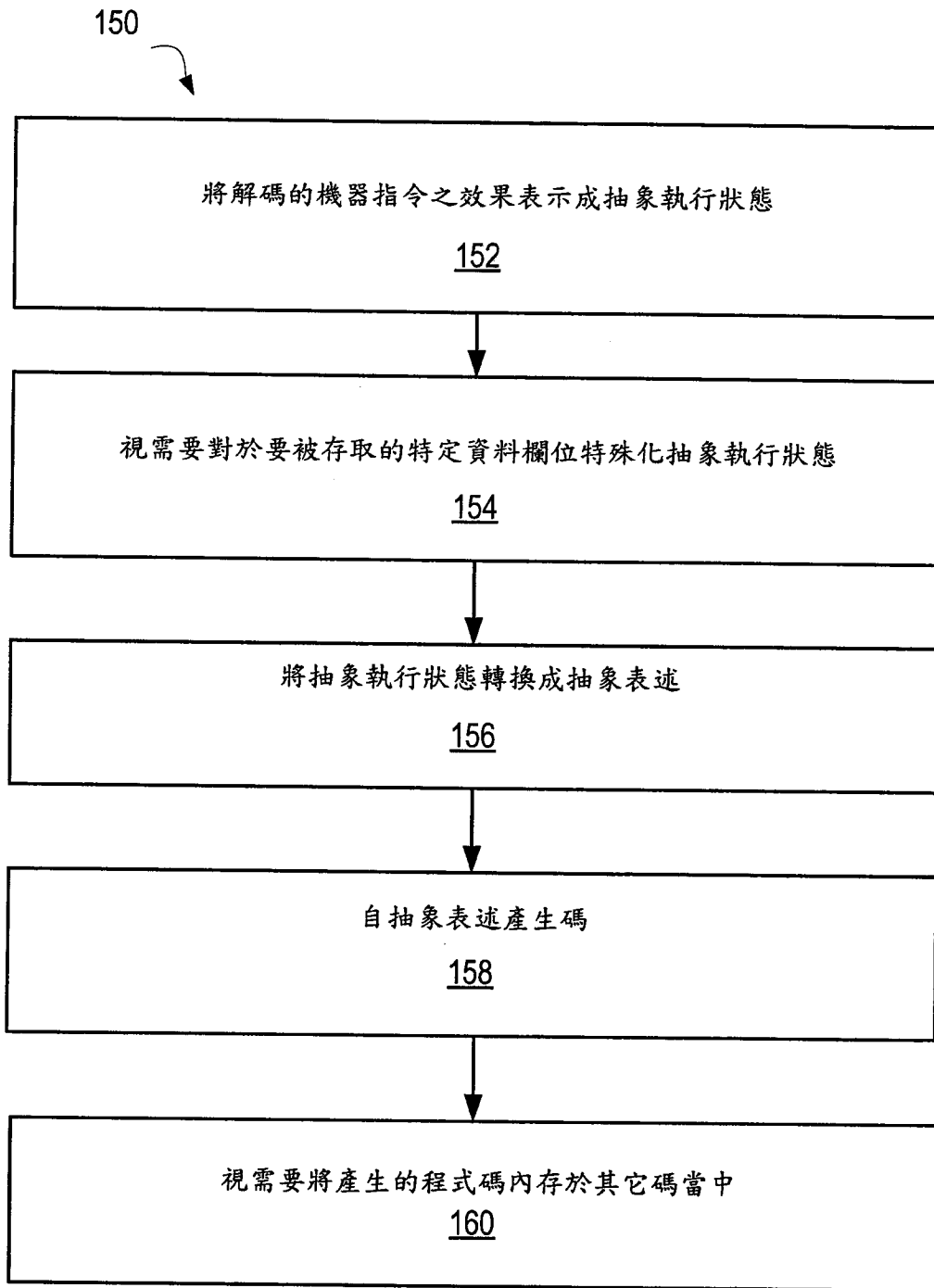
第 2 圖



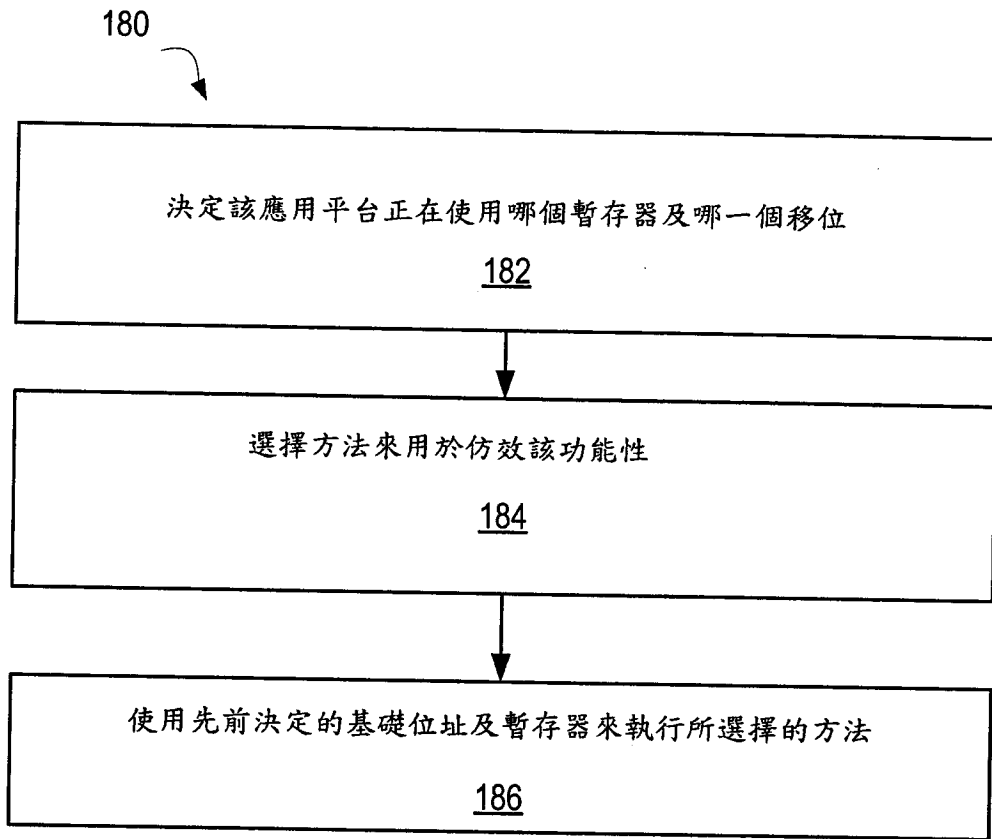
第 3 圖



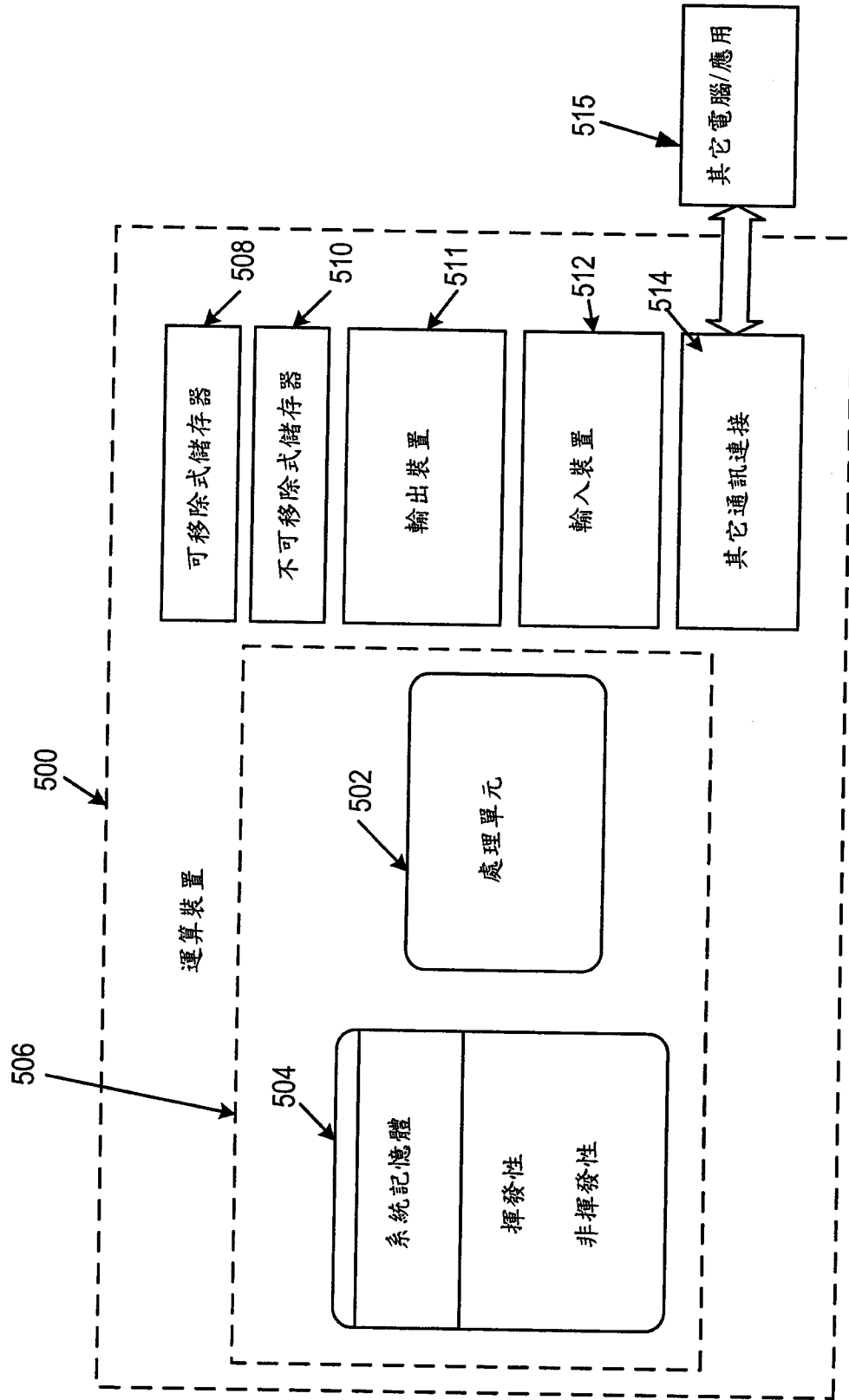
第 4 圖



第 5 圖



第 6 圖



第 7 圖

七、指定代表圖：

(一)、本案指定代表圖為：第(3)圖。

(二)、本代表圖之元件代表符號簡單說明：

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