(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 201413455 A
(43)公開日： 中華民國 103 (2014) 年 04 月 01 日

(21)申請案號：101135433 (22)申請日： 中華民國 101 (2012) 年 09 月 26 日
(51)Int. Cl.： *G06F12/14 (2006.01)* *G06F21/78 (2013.01)*
(71)申請人：國立交通大學 (中華民國) NATIONAL CHIAO TUNG UNIVERSITY (TW)
新竹市大學路 1001 號
(72)發明人：王繼偉 WANG, CHI WEI (TW) ；謝續平 SHIEH, SHIUHPYNG (TW) ；張佳惠 CHANG, CHIA HUEI (TW)
(74)代理人：蔡清福
申請實體審查：有 申請專利範圍項數：13 項 圖式數：6 共 33 頁

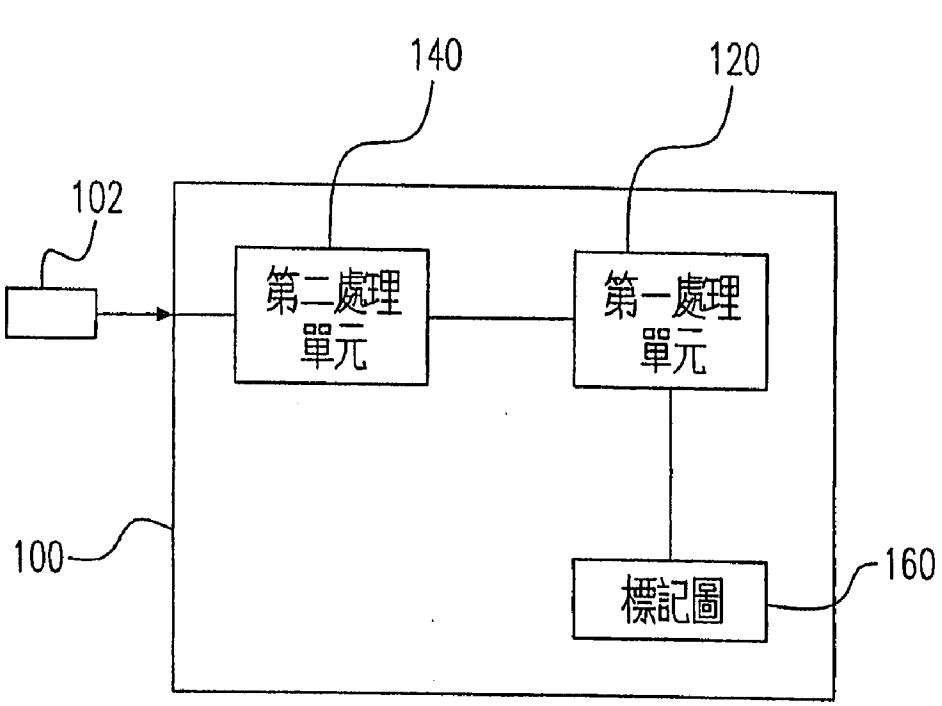
(54)名稱

偵測一隱私資訊有無可能被竊取的裝置及方法

DETECT THE PRIVACY INFORMATION BEEN THEFT POSSIBILITY DEVICE AND METHOD

(57)摘要

一種用於偵測一隱私資訊有無可能被竊取的裝置，包括：一標記圖具有一特定標記和一緩衝區，該特定標記使一具特殊屬性之一資料附有一標記狀態；一輸入/輸出(I/O)裝置，與該緩衝區對應；以及一第一處理單元判斷該緩衝區是否存有該特定標記。



100：裝置
102：指令
120：第一處理單元
140：第二處理單元
160：標記圖

第 1 圖

201413455

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：101135433

※申請日：101. 9. 26 ※IPC 分類：G06F 1/14 (2006.01)
G06F 21/78 (2013.01)

一、發明名稱：（中文/英文）

偵測一隱私資訊有無可能被竊取的裝置及方法

DETECT THE PRIVACY INFORMATION BEEN THEFT POSSIBILITY DEVICE AND METHOD

二、中文發明摘要：

一種用於偵測一隱私資訊有無可能被竊取的裝置，包括：一標記圖具有一特定標記和一緩衝區，該特定標記使一具特殊屬性之一資料附有一標記狀態；一輸入/輸出(I/O)裝置，與該緩衝區對應；以及一第一處理單元判斷該緩衝區是否存有該特定標記。

三、英文發明摘要：

A device for detecting the possibility of privacy information been theft includes a label map, an I/O device and a first processing unit. The label map has a specific label and a buffer region, and the specific label is used for recording the I/O device label status of information having a unique attributes. The I/O device is corresponding to the buffer region, and the first processing unit is used to determine whether there is a specific label therein.

四、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：

100：裝置　　102：指令

120：第一處理單元　　140：第二處理單元

160：標記圖

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】

本發明是有關於一種偵測資訊有無可能被竊取的方法，且特別是有關於偵測隱私資訊有無可能被竊取的方法。

【先前技術】

科技進步，智慧型手機日漸普及，供應商們紛紛發展出許多用於智慧型手機上的應用程式(app)。這些應用程式有些是用於朋友之間聊天的通信軟體，有些用於查交通資訊，更有些用於休閒娛樂，例如：line、台灣公車通、生氣鳥(angry bird)等等。愈來愈多不同種類的應用程式，對智慧型手機的使用者而言，雖然是一大福音，但隨之而來的隱憂是這些應用程式是否會竊取手機裡隱私資訊。

習知的偵測隱私資訊有無可能被竊取的方法，採用檢查手機所送出的封包是否包含隱私資訊的技術方案。但當封包中的資訊被進一步地加密的時候，此方法就不適用。針對這種情況，若想要知道送出的封包中是否有包含隱私資訊就必須追蹤軟體中的資訊流動，藉由資訊流動的情況來判斷該封包是否有包含隱私資訊的可能。

美國專利申請案公開號第2009/0172644號提出了一種使用多執行緒追蹤軟體資訊流動的方法。該方法包含提供一主執行緒與一追蹤執行緒，其中該主執行緒負責執行程式的操作，而該追蹤執行緒用以追蹤該主執行緒執行該程式的操作。

美國專利第 7,958,558 號提出了一種包含追蹤資訊流

動機制的電腦系統，該追蹤資訊流動機制藉由維持並選擇性地傳播與該電腦系統所執行的指令的資訊流動對應的儲存位置的傳播污染狀態(propagating taint status)，來避免該電腦系統承受特定形式的惡意攻擊。在一些實施例中，使用一個衰退取向(decay oriented)的公制單位，一旦退化(aging)的程度到達一預定的衰退臨界值時，中斷污染的傳播。

然而，上述的兩種追蹤資訊流動技術方案皆僅適用於追蹤監測程序內的動態資訊流動或污染狀況，不適用於追蹤整個中央處理單元(CPU)、實體記憶體與硬碟中的資料流動狀況。

此外，習知的偵測資訊流動的技術方案僅適用於處理執行在 Dalvik 虛擬機器(virtual machine)中的位元組碼(byte code)，對於執行於機器階層(machine level)上的程式原生碼(native byte code)並不適用。也就是說，習知的偵測方法只限於在 Dalvik 虛擬機器層中追蹤資訊流動並分析是否有竊取資料的情形發生，而無法偵測到系統的機器階層。

因此，需要提供一種適用於追蹤整個中央處理單元、實體記憶體與硬碟中的資料流動並且能偵測到系統的機器階層是否有竊取資料的情形發生的偵測方法，以解決上述問題。

【發明內容】

本發明之一目的就是在提供一種用於偵測一隱私資訊有無可能被竊取的裝置，該裝置追蹤整個中央處理單元、

實體記憶體與硬碟中的資料流動，以判斷送出之資料是否包含該隱私資訊。

本發明之另一目的就是在提供一種用於偵測一隱私資訊有無可能被竊取的方法，藉以讓使用者能在將應用程式下載至手機上之前，預先檢查此應用程式有無可能竊取手機裡之隱私資訊。

根據本發明之一實施例，提供一種用於偵測一隱私資訊有無可能被竊取的裝置包含：一標記圖具有一特定標記和一緩衝區，該特定標記使一具特殊屬性之一資料附有一標記狀態。一輸入/輸出(I/O)裝置，與該緩衝區對應，以及一第一處理單元判斷該緩衝區是否存有該特定標記。

根據本發明之另一實施例，提供一種偵測一隱私資訊有無可能被竊取的方法，包含下列步驟：使一具特殊屬性之一資料附有一第一標記狀態，提供一緩衝區，用以輸出一資料；以及判斷所輸出之該資料是否具該第一標記狀態。

根據本發明之又一實施例，提供一種偵測一隱私資訊有無可能被竊取的方法，包含下列步驟：使一具特殊屬性之一資料附有一標記狀態。提供一緩衝區，用以輸出該資料；以及判斷該緩衝區是否存有該具標記狀態之該資料。

由本發明之實施例可知，本發明之偵測一隱私資訊有無可能被竊取的裝置及方法係藉由偵測該緩衝區是否存有該具標記狀態之該資料，來判斷該輸出資料是否包含該隱私資訊。

【實施方式】

以下詳細討論本發明之實施例的製作與使用。然而，應該理解的是，這些實施例提供許多可應用的創新概念，其可在各種特定背景中加以體現。所討論之特定的實施例僅係用以舉例說明，並非用以限制本發明之範圍。

請參照第 1 圖，其繪示本發明之一實施例之用於偵測一隱私資訊有無可能被竊取的裝置 100 之示意圖，裝置 100 包括一第一處理單元 120、一第二處理單元 140、一標記圖 160。該裝置 100 是用以執行一指令 102，並追蹤該指令 102 所造成的隱私資訊流動(privacy information flow)，而該標記圖 160 係用以使具特殊屬性之一資料附有一標記狀態(詳情請參照第 2 圖及下述說明)。該裝置 100 係藉由該標記圖 160 來表示具特殊屬性之該資料的資料流動狀態，以判斷該裝置 100 輸出之一資料中是否包含具特殊屬性之該資料。若該裝置 100 輸出之該資料中包含附有標記狀態的資料，則代表該隱私資訊被竊取。在一實施例中，該裝置 100 係一電腦系統。在另一實施例中，該具特殊屬性之資料代表該資料中包含該隱私資訊。在又一實施例中，該隱私資料為國際移動設備辨識碼(IMEI)、國際行動用戶辨識碼(IMSI)、聯絡人資料、或簡訊。

請參照第 2(a)圖，其繪示本發明之一實施例之偵測一隱私資訊有無可能被竊取的裝置 100 之標記圖 200 之示意圖。該標記圖 200 包含複數個區塊，該些區塊分別與該電腦系統中之複數個儲存位置對應，該些儲存位置的一各自儲存位置可以是一記憶體位置、一暫存器或是一硬碟位置。例如，該標記圖 200 具有一區塊 210 與一區塊 212，

區塊 210 與 212 分別與該電腦系統中記憶體 240 之一記憶體位置 220 與一記憶體位置 222 對應。

當該電腦系統中之一特定儲存位置 224 包含該隱私資訊時，該第一處理單元 120 將該標記圖 160 中與該特定儲存位置 224 對應之一特定區塊 214 標示來具有一特定標記 202，如第 2(a)圖所示。例如，特定儲存位置 224 是一特定記憶體位置、一特定暫存器或是一特定硬碟位置。該特定儲存位置 224 儲存一資料 224a，且特定標記 202 使該資料 224a 附有一標記狀態 Q202。在一實施例中，該特定標記 202 可為一符號。在另一實施例中，該特定標記 202 可用一數值表示。在一實施例中，當該特定儲存位置 224 未包含一隱私資訊時，該第一處理單元 120 將特定區塊 214 標示來具有一特定標記 202W，且特定標記 202W 使該資料 224a 附有一標記狀態 Q202W。

此外，請參照第 1 圖和第 2(a)圖。裝置 100 更包括一輸入/輸出裝置 180，該標記圖 200 包含一緩衝區 2A，該緩衝區 2A 與一輸入/輸出裝置 280 對應，且由一第一組 2B 的區塊 213 所組成。該緩衝區 212 用以表示該裝置 100 所輸出之資料是否包含附有該標記狀態 Q202 之資料。亦即，該緩衝區 212 用以記錄該裝置 100 所輸出之資料是否有包含該隱私資訊。若有，則代表該隱私資訊被竊取。

在一實施例中，標記圖 200 係一位元映射圖，亦即，在標記圖 200 中與裝置 100 的每一個儲存位置對應的一各自區塊都具有一個位元的大小。例如，當標記圖 200 中一第一位元的區塊具有一特定標記 202（比如“1”）時，則表

示與該第一位元對應的一第一特定儲存位置包含該隱私資訊。相反地，當標記圖 200 中一第一位元的區塊具有一特定標記 202W（比如“0”）時，則表示與該第一位元對應的該第一特定儲存位置未包含該隱私資訊。在另一實施例中，該輸入/輸出(I/O)裝置 180 為一網路介面卡，當該緩衝區存有具特定標記 202 之資料時，代表裝置 100 或該輸入/輸出(I/O)裝置 180 欲送出之資料可能包含有隱私資訊。

請同時參照第 1 圖與第 2(a)圖，當該第二處理單元 140 接收該指令 102 時，該第二處理單元 140 轉譯該指令 102 為包含一來源位址區 226 與一目標位址區 228 的資訊流動碼，其中記憶體 240 包含一來源位置區 L226 與一目標位置區 L228，來源位置區 L226 與目標位置區 L228 分別具有來源位址區 226 與目標位址區 228，且該標記圖 200 中的一來源區塊 216 與一目標區塊 218 分別與該來源位址區 226 與該目標位址區 228 對應。來源位置區 L226 與目標位置區 L228 分別儲存來源資料 226a 和目標資料 228a。接著，該第一處理單元 120 接收資訊流動碼，並根據該來源區塊 216 是否具有該特定標記 202，來判斷是否使該目標區塊 218 具有該特定標記 202。亦即，該第一處理單元 120 先檢查在記憶體 240 中該來源位址區 226 所指向之來源資料 226a 是否存有該隱私資訊，來判斷在記憶體 240 中該目標位址區 228 所指向之目標資料 228a 中是否包含該隱私資訊。

請同時參照第 1 圖與第 2(b)圖。在一實施例中，該指令 102 將該來源位址區 226 所指向之該來源資料 226a 複製至具有該目標位址區 228 的目標位置區 L228。該來源位址區

226 包含分別指向一來源位置 L232 與一來源位置 L234 的一來源位址 232 與一來源位址 234，來源位置 L232 與來源位置 L234 分別儲存一來源資料 232a 與一來源資料 234a，其中該來源資料 232a 附有該標記狀態 Q202(亦即，在該標記圖 200 中之一來源區塊 252 具有該特定標記 202，其中該來源區塊 252 與該來源位址 232 對應)，而該來源資料 234a 未附有該標記狀態 Q202（比如附有標記狀態 Q202W)。亦即，該標記圖 200 中之一來源區塊 254 未具有該特定標記 202（比如具有特定標記 202W)，其中該來源區 254 與該來源位址 234 對應。

該目標位址區 228 包含分別指向一目標位置 L236 與一目標位置 L238 的一目標位址 236 與一目標位址 238，目標位置 L236 與目標位置 L238 分別儲存一目標資料 236a 與一目標資料 238a，其中該標記圖 200 中之一目標區塊 256 與一目標區塊 258 分別與該目標位址 236 和該目標位址 238 對應。在此情況下，該第一處理單元 120 根據該來源資料 232a 附有該標記狀態 Q202，來使該目標資料 236a 亦附有該標記狀態 Q202，另由於該來源資料 234a 未附有該標記狀態 Q202（比如附有標記狀態 Q202W)，該第一處理單元 120 判斷該來源資料 234a 未包含任何隱私資訊，因此，該第二目標資料 238a 不需附加該標記狀態 Q202，如第 2(b) 圖所示。

請同時參照第 1 圖與第 2(c)圖。在另一實施例中，該指令 102 將該來源位址區 226 所指向之該來源資料 226a 全部複製至具有該目標位址區的目標位置區 L228。該來源位址區

226 包含分別指向一來源位置 L232 與一來源位置 L234 的一來源位址 232 與一來源位址 234，來源位置 L232 與來源位置 L234 分別儲存一來源資料 232a 與一來源資料 234a，其中該來源資料 232a 附有該標記狀態 Q202，而該來源資料未附有該標記狀態 Q202。

該目標位址區 228 包含指向一目標位置 L236 的一目標位址 236，目標位址 236 儲存一目標資料 236a，其中該標記圖 200 中之一目標區 256 與該目標位址 236 對應。在此情況下，由於該來源資料 232a 附有該標記狀態 Q202，該第一處理單元 120 判斷該來源資料 232a 包含該隱私資訊，因此，該目標資料 236a 需附加該標記狀態 Q202，如第 2(c)圖所示。

請參照回第 2(a)圖，在一實施例中，該第一組 2B 的區塊 213 未包含該來源區塊 216 與該目標區塊 218；亦即，該來源區塊 216 與該目標區塊 218 皆未位於該緩衝區 212 中。亦即，該指令 102 未傳送出任何資料。在另一實施例中，該第一組 2B 區塊 213 包含該目標區塊 218；亦即，該目標區塊 218 位於該緩衝區 212 中；此情況表示該指令 102 欲傳送一資料出去。此時，該第一處理單元 120 檢查該目標區塊 218 是否具有該標記狀態以做出一判定。當該判定是肯定，則該第一處理單元 120 認定該指令 102 欲傳送包含該隱私資訊之該資訊出去，也就是說，該隱私資訊被竊取。

在根據第 1 圖與第 2(a)~2(c)圖的一實施例中，一種用於偵測一隱私資訊有無可能被竊取的裝置 100 包括一標記圖（160 或 200）、一輸入/輸出(I/O)裝置 180 和一第一處理

單元 120。標記圖 200 具有一特定標記 202 和一緩衝區 2A，特定標記 202 使一具特殊屬性之一資料（比如 226a）附有一標記狀態 Q202。輸入/輸出(I/O)裝置 180 與緩衝區 2A 對應。第一處理單元 120 判斷緩衝區 2A 是否存有特定標記 202。在一實施例中，該特殊屬性是一隱私屬性。

請參照第 3 圖，其繪示本發明之一實施例說明追蹤資訊流動的示意圖。記憶體 300 包含分別儲存一第一資料 302a 與一第二資料 304a 的一第一部分 302 與一第二部分 304。當記憶體 300 之該第一部分 302 包含該隱私資訊時，儲存於該第一部分 302 之該第一資料 302a 會被標記為附有該標記狀態 Q202，來表示該第一資料 302a 包含該隱私資訊。也就是說，標記圖 310 中與該第一部分 302 對應之一第三區塊 312 被標記為具有該特定標記 202。接著，當裝置 100 執行了一些指令，使得該第一部分 302 的該第一資料 302a 被複製到該第二部分 304 時，則儲存於該第二部分 304 的該第二資料 304a 亦會被標記為附有該標記狀態 202，以致該第二資料 304a 可能也包含該隱私資訊 306。標記圖 310 中與該第二部分 304 對應之一第四區塊 314 被標記為具有該特定標記 202。

在一實施例中，裝置 100 也可能計算儲存於該第一部份 302 中之該第一資料 302a，並將計算結果儲存在該第二部份 304，此時該第二部份 304 亦會被標記為附有該標記狀態 202。亦即，本發明並不限制使該第二部份 304 附有該標記狀態 202 的方式。本發明中將上述儲存於該第一部份 302 之該第一資料 302a 影響到儲存於該第二部分 304 中

之該第二資料302b的過程稱為所執行指令所造成的隱私資訊流動。

經由上述說明，習知技藝者應可理解本發明藉由觀察該緩衝區212是否存有包含該特定標記202的資料，來判斷該裝置是否被指示送出包含該隱私資訊的資料。本發明之一目的是希望能提供一裝置讓使用者能在將未知的應用程式下載至手機上執行之前，預先在此裝置上執行此未知的應用程式，以檢查此應用程式是否會竊取裝置裡預設之假的隱私資訊。因此，本發明所提出之裝置100希望該裝置100被指示送出的資訊(封包)均能順利地被送出。

一般而言，當應用程式想要偷取隱私資訊時，它需要連到一個外部伺服器，以將偷取到的隱私資訊送出去。可是，這個外部伺服器可能是一個眾所周知的惡意網站，所以在網域名稱系統(DNS)查詢的階段就被DNS伺服器擋掉了，造成該應用程式無法送出偷取到的隱私資訊，也使得我們無法偵測到該應用程式會偷取隱私資訊。

為了避免這個情況發生，請參照第4圖，其繪示本發明之另一實施例之用於偵測一隱私資訊有無可能被竊取的裝置400之示意圖。該裝置400包含一追蹤裝置402、一攔截器404與一伺服器406，其中該追蹤裝置402更包含一網路介面卡408，該追蹤裝置402為裝置100之一實施配置。一待測程式410執行於該追蹤裝置402上。該攔截器404檢查該追蹤裝置402所送出的一第一封包412，當該第一封包包含一DNS查詢時，該攔截器404攔截該第一封包412並響應該第一封包412而提供一第二封包414給該追蹤裝

置 402，以將該追蹤裝置 402 所欲送出的資料(封包)416 導向該伺服器 406，藉此使得該待測程式 410 順利傳出該資料(封包)416，其中該第二封包 414 包含該伺服器 406 之 IP 位址。

值得注意的是，在手機中有一些正當程式也會需要透過該緩衝區 212 將隱私資訊傳送出去。例如，當手機要連 3G 網路時，手機需要跟手機基地台連線，以傳送隱私資訊(手機的國際移動設備辨識碼(IMEI)與國際行動用戶辨識碼(IMSI))給基地台，藉此使得手機可以上網。在一實施例中，為了避免因為上述正當程式送隱私資訊出去的行為而誤判該待測程式 410 為竊取隱私資訊的應用程式，因此需要一個方法來判別送出隱私資訊的程式是正當程式或是待測程式 410。

在一實施例中，一種判別該送出之封包之目標 IP 位址是否為該待測程式所填的方法被利用來判斷送出隱私資訊之程式為手機常駐程式或該待測程式。一般而言，該目標 IP 位址寫在待測程式 410 裡面。但在一些特殊的情況中，應用程式不是直接填寫目標 IP 位址而是給一個網域名稱(domain name)，藉由 DNS 查詢去取得對應的目標 IP 位址。針對上述 2 種情況，在一實施例中，將待測程式 410 視為另一標記源的解決方法，並說明如下。

請參照第 5 圖，其繪示本發明之另一實施例之偵測一隱私資訊有無可能被竊取的裝置 400 之標記圖 500 之示意圖。裝置 400 包含追蹤裝置 402，且追蹤裝置 402 包含標記圖 500 和記憶體 510。如第 5 圖所示，該標記圖 500 中之一待測程式區塊 502 與該待測程式 410 所在之記憶體位

置 512 對應。該第一處理單元 120 將在該標記圖 500 中與一記憶體位置區 514 對應之一組 5B 區塊 504 標記為具有一特定標記 506 來使記憶體位置區 514 附有一標記狀態 Q506。該記憶體位置區 514 存有包含該隱私資訊的資訊，且將該標記圖 500 中之該待測程式區塊 502 標記為具有一特定標記 508 來使記憶體位置 512 附有一標記狀態 Q508。如此一來，當裝置 400 所欲輸出之資料附有該標記狀態 506 時，則裝置 400 確定該所欲輸出之資料包含該隱私資訊。欲當裝置 400 所輸出之資料附有該標記狀態 508，則裝置 400 確定該所欲輸出之資料的目標 IP 位址為該待測程式 410 所填。當裝置 400 所欲輸出之資料附有該標記狀態 506 與該標記狀態 508，則裝置 400 確定該所欲輸出之資料包含該隱私資訊，且其目標 IP 位址為該待測程式 410 所填。亦即，該待測程式 410 竊取隱私資訊。

在一實施例中，應用程式不是直接填寫目標 IP 位址而是給一個網域名稱(domain name)，藉由 DNS 查詢去取得對應的目標 IP 位址。如上所述，在第 4 圖中追蹤裝置 402 使一攔截器 404 攔截 DNS 查詢，並通過該 DNS 查詢而提供一伺服器 406 的 IP 位址給伺服器 406。因此，在這個情況下，該第一處理單元 120 不是將標記圖 500 的該待測程式區塊 502 標記為具有該特定標記 508，而是將在標記圖 500 中與儲存該伺服器 IP 位址之記憶體位置對應之一區塊 532 標記為具有特定標記 508。當裝置 400 所欲輸出之資料附有標記狀態 506 與 508，則裝置 400 確定該待測程式 410 竊取隱私資訊。

在一實施例中，該標記圖 500 中之每一區塊包含複數

位元，例如，一第一區塊包含一第一位元與一第二位元，分別用以記錄是否包含該隱私資訊與目標 IP 位址來源。

請參照第 6(a)圖與第 6(b)圖，其繪示本發明之一實施例之偵測一隱私資訊有無可能被竊取的方法 600 的流程圖。該方法 600 包含：步驟 602，使一具特殊屬性之一資料附有一第一標記狀態。接著，步驟 604，提供一緩衝區，用以輸出一資料。然後，步驟 606，判斷所輸出之該資料是否具該第一標記狀態。

在一實施例中，該方法 600 更包含下列步驟：步驟 608，接收一指令，該指令包含一來源位址與一目標位址。接著，步驟 610，根據存於該來源位址之一第一資料是否包含該具第一標記狀態之該資料，來判斷是否使該目標位址之一第二資料附有該第一標記狀態。

在另一實施例中，該方法更包含下列步驟，如第 6(b)圖所示。步驟 612，提供一待測程式。步驟 614，使該待測程式之一資料附有一第二標記狀態。步驟 616，判斷所輸出之該資料是否具該第一標記狀態與該第二標記狀態。當所輸出之該資料具有該第一標記狀態而未具有該第二標記狀態時，代表所輸出之該資料雖然包含隱私資訊，但並非是該待測程式所竊取。相反地，當所輸出之該資料具有該第一標記狀態與該第二標記狀態時，代表該待測程式竊取隱私資訊。

實施例

1. 一種用於偵測一隱私資訊有無可能被竊取的裝置，包括：

一標記圖具有一特定標記和一緩衝區，該特定標記使一具

特殊屬性之一資料附有一標記狀態；

一輸入/輸出(I/O)裝置，與該緩衝區對應；以及

一第一處理單元判斷該緩衝區是否存有該特定標記。

2. 根據實施例 1 所述的裝置，其中具標記狀態之資料係一含一隱私資料之資料。

3. 根據上述實施例中任意一個實施例所述的裝置，其中隱私資料為國際移動設備辨識碼(IMEI)、國際行動用戶辨識碼(IMSI)、聯絡人資料、或簡訊。

4. 根據上述實施例中任意一個實施例所述的裝置，其中該裝置更包括一記憶體，該記憶體具一來源位址區及一目標位址區分別儲存一第一及一第二資料，該第一處理單元根據該第一資料是否包含該具標記狀態之資料，來判斷是否使該第二資料附有該標記狀態。

5. 根據上述實施例中任意一個實施例所述的裝置，其中該裝置更包括一第二處理單元，該第二處理單元接收一指令，並將該指令轉譯為一資訊流動碼，其中該資訊流動碼包含該指令之該來源位址區與該目標位址區。

6. 根據上述實施例中任意一個實施例所述的裝置，其中該輸入輸出(I/O)裝置為一網路介面卡。

7. 根據上述實施例中任意一個實施例所述的裝置，更包括一攔截器，用以攔截從該裝置中送出的網域名稱系統(DNS)查詢，並回應一 IP 位址給該裝置。

8. 根據上述實施例中任意一個實施例所述的裝置，其中該處理單元判斷該緩衝區所存在之該具標記狀態之該資料是否具有該 IP 位址。

9. 一種偵測一隱私資訊有無可能被竊取的方法，包括：

使一具特殊屬性之一資料附有一第一標記狀態；

提供一緩衝區，用以輸出一資料；以及

判斷所輸出之該資料是否具該第一標記狀態。

10. 根據實施例 9 所述的方法，其中該方法更包括下列步驟：

提供一待測程式；

使該待測程式之一資料附有一第二標記狀態；以及

判斷所輸出之該資料是否具該第二標記狀態。

11. 根據上述實施例 9-10 中任意一個實施例所述的方法，當所輸出之該資料具有該第一標記狀態與該第二標記狀態，代表所輸出之該資料包含一隱私資訊，且該資料具有該待測程式所填之一 IP 位址。

12. 一種偵測一隱私資訊有無可能被竊取的方法，包括：

使一具特殊屬性之一資料附有一標記狀態；

提供一緩衝區，用以輸出該資料；以及

判斷該緩衝區是否存有該具標記狀態之該資料。

13. 根據上述實施例 12 所述的方法，其中該方法更包括下列步驟：

接收一指令，該指令包含一來源位址與一目標位址；

根據存於該來源位址之一第一資料是否包含該具標記狀態之該資料，來判斷是否使存於該目標位址之一第二資料附有該標記狀態。

一般習知的偵測應用程式是否竊取隱私資料的方法，只能檢查到 Dalvik 虛擬機器層，因此，需要提供一種適用於追蹤整個中央處理單元、實體記憶體與硬碟中的資料流動並且能偵測到系統的機器階層是否有竊取資料的情形發生的偵測方法，讓使用者可以在將未知的應用程式下載至手機上執行之前，預先檢查該應用程式會不會竊取手機裡的隱私資料。

雖然本發明已以實施方式揭露如上，然其並非用以限定本發明，任何熟習此技藝者，在不脫離本發明之精神和範圍內，當可作各種之更動與潤飾，因此本發明之保護範圍當視後附之申請專利範圍所界定者為準。

【圖式簡單說明】

讓本發明之上述和其他目的、特徵、優點與實施例能更明顯易懂，所附圖式之說明如下。其中附圖中之各種特徵並未依比例繪示，可任意地放大或縮小各種特徵之尺寸。

第 1 圖係繪示本發明之一實施例之用於偵測一隱私資訊有無可能被竊取的裝置 1 之示意圖。

第 2(a)圖係繪示本發明之一實施例之偵測一隱私資訊有無可能被竊取的裝置之標記圖之示意圖。

第 2(b)圖係本發明之一實施例之偵測一隱私資訊有無可能被竊取的裝置之標記圖之示意圖。。

第 2(c)圖係繪示本發明之一實施例之偵測一隱私資訊有無可能被竊取的裝置之標記圖之示意圖。

第 3 圖係繪示本發明之一實施例說明追蹤資訊流動的示

意圖。

第4圖係繪示本發明之另一實施例之用於偵測一隱私資訊有無可能被竊取的裝置之示意圖

第5圖係繪示本發明之另一實施例之偵測一隱私資訊有無可能被竊取的裝置之標記圖之示意圖。

第6(a)圖係繪示本發明之一實施例之偵測一隱私資訊有無可能被竊取的方法的流程圖。

第6(b)圖係繪示本發明之另一實施例之偵測一隱私資訊有無可能被竊取的方法的流程圖。

【主要元件符號說明】

100：裝置
102：指令
120：第一處理單元
140：第二處理單元
160：標記圖
200：標記圖
202：特定標記
202W：特定標記
210：區塊
212：區塊
213：區塊
214：特定區塊
216：來源區塊
218：目標區塊
220：記憶體位置
222：記憶體位置
224：特定儲存位置
224a：資料
226：來源位址區
226a：來源資料
228：目標位址區
228a：目標資料
232：來源位址
232a：來源資料
234：來源位址
234a：來源資料
236：目標位址
236a：目標資料
238：目標位址
238a：目標資料
240：記憶體
252：來源區塊
254：來源區塊
256：目標區塊
258：目標區塊
280：輸入/輸出裝置
300：記憶體
302：第一部分
302a：第一資料
304：第二部分

304a：第一資料
310：標記圖
312：第三區塊
314：第四區塊
400：裝置
402：追蹤裝置
404：攔截器
406：伺服器
408：網路介面卡
410：待測程式
412：第一封包
414：第二封包
416：資料
500：標記圖
502：待測程式區塊
504：區塊
506：特定標記
508：特定標記
510：記憶體
512：記憶體位置
514：記憶體位置區
600：方法
602：步驟
604：步驟
606：步驟
608：步驟
610：步驟
612：步驟
614：步驟
616：步驟
2A：緩衝區
2B：第一組
5B：一組
L226：來源位置區
L228：目標位置區
L232：來源位置
L234：來源位置
L236：目標位置
L238：目標位置
Q202：標記狀態
Q202W：標記狀態
Q506：標記狀態

七、申請專利範圍：

1. 一種用於偵測一隱私資訊有無可能被竊取的裝置，包括：

一標記圖，具有一特定標記和一緩衝區，該特定標記使一具特殊屬性之一資料附有一標記狀態；

一輸入/輸出(I/O)裝置，與該緩衝區對應；以及

一第一處理單元判斷該緩衝區是否存有該特定標記。

2. 如申請專利範圍第 1 項所述之裝置，其中該具標記狀態之資料係一含一隱私資料之資料。

3. 如申請專利範圍第 2 項所述之裝置，其中該隱私資料為國際移動設備辨識碼(IMEI)、國際行動用戶辨識碼(IMSI)、聯絡人資料、或簡訊。

4. 如申請專利範圍第 1 項所述之裝置，其中該裝置更包括一記憶體，該記憶體具一來源位址區及一目標位址區分別儲存一第一及一第二資料，該第一處理單元根據該第一資料是否包含該具標記狀態之資料，來判斷是否使該第二資料附有該標記狀態。

5. 如申請專利範圍第 4 項所述之裝置，其中該裝置更包括一第二處理單元，該第二處理單元接收一指令，並將該指令轉譯為一資訊流動碼，其中該資訊流動碼包含該指令之該來源位址區與該目標位址區。

6. 如申請專利範圍第 1 項所述之裝置，其中該輸入輸出(I/O)裝置為一網路介面卡。

7. 如申請專利範圍第 1 項所述之裝置，更包括一攔截器，用以攔截從該裝置中送出的網域名稱系統(DNS)查詢，並回應一 IP 位址給該裝置。

8. 如申請專利範圍第 7 項所述之裝置，其中該處理單元判斷該緩衝區所存在之該具標記狀態之該資料是否具有該 IP 位址。

9. 一種偵測一隱私資訊有無可能被竊取的方法，包括：

使一具特殊屬性之一資料附有一第一標記狀態；

提供一緩衝區，用以輸出一資料；以及

判斷所輸出之該資料是否具該第一標記狀態。

10. 如申請專利範圍第 9 項所述之方法，其中該方法更包括下列步驟：

提供一待測程式；

使該待測程式之一資料附有一第二標記狀態；以及

判斷所輸出之該資料是否具該第二標記狀態。

11. 如申請專利範圍第 10 項所述之方法，當所輸出之該資料具有該第一標記狀態與該第二標記狀態，代表所輸出之該資料包含一隱私資訊，且該資料具有該待測程式所填之一 IP 位址。

12. 一種偵測一隱私資訊有無可能被竊取的方法，包括：

使一具特殊屬性之一資料附有一標記狀態；

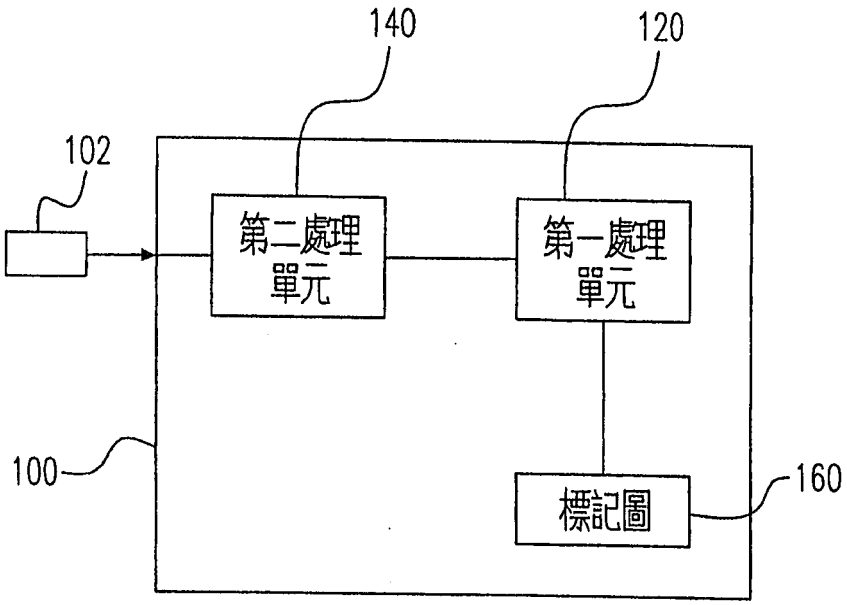
提供一緩衝區，用以輸出該資料；以及

判斷該緩衝區是否存有該具標記狀態之該資料。

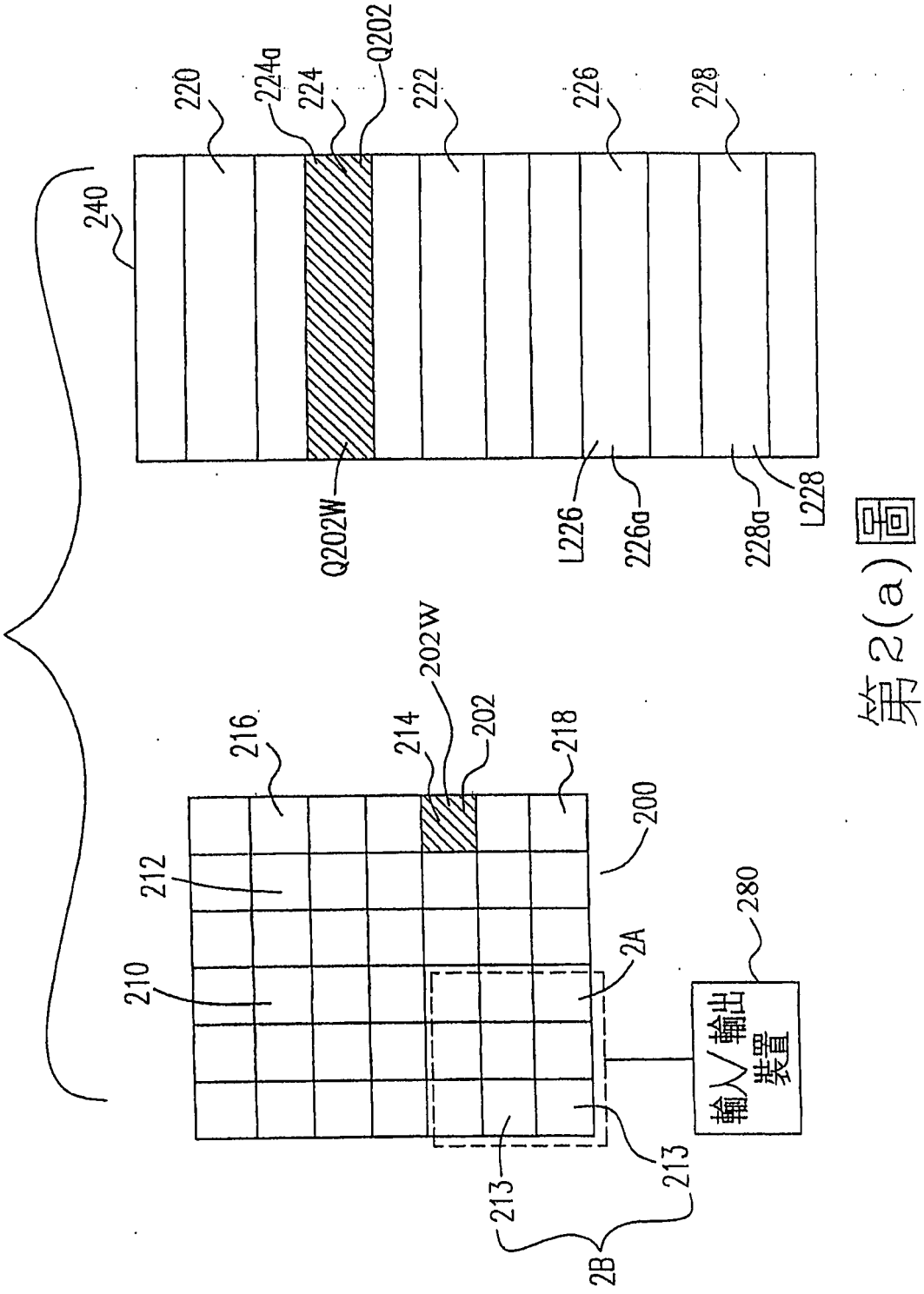
13. 如申請專利範圍第 12 項所述之方法，其中該方法更包括下列步驟：

接收一指令，該指令包含一來源位址與一目標位址；

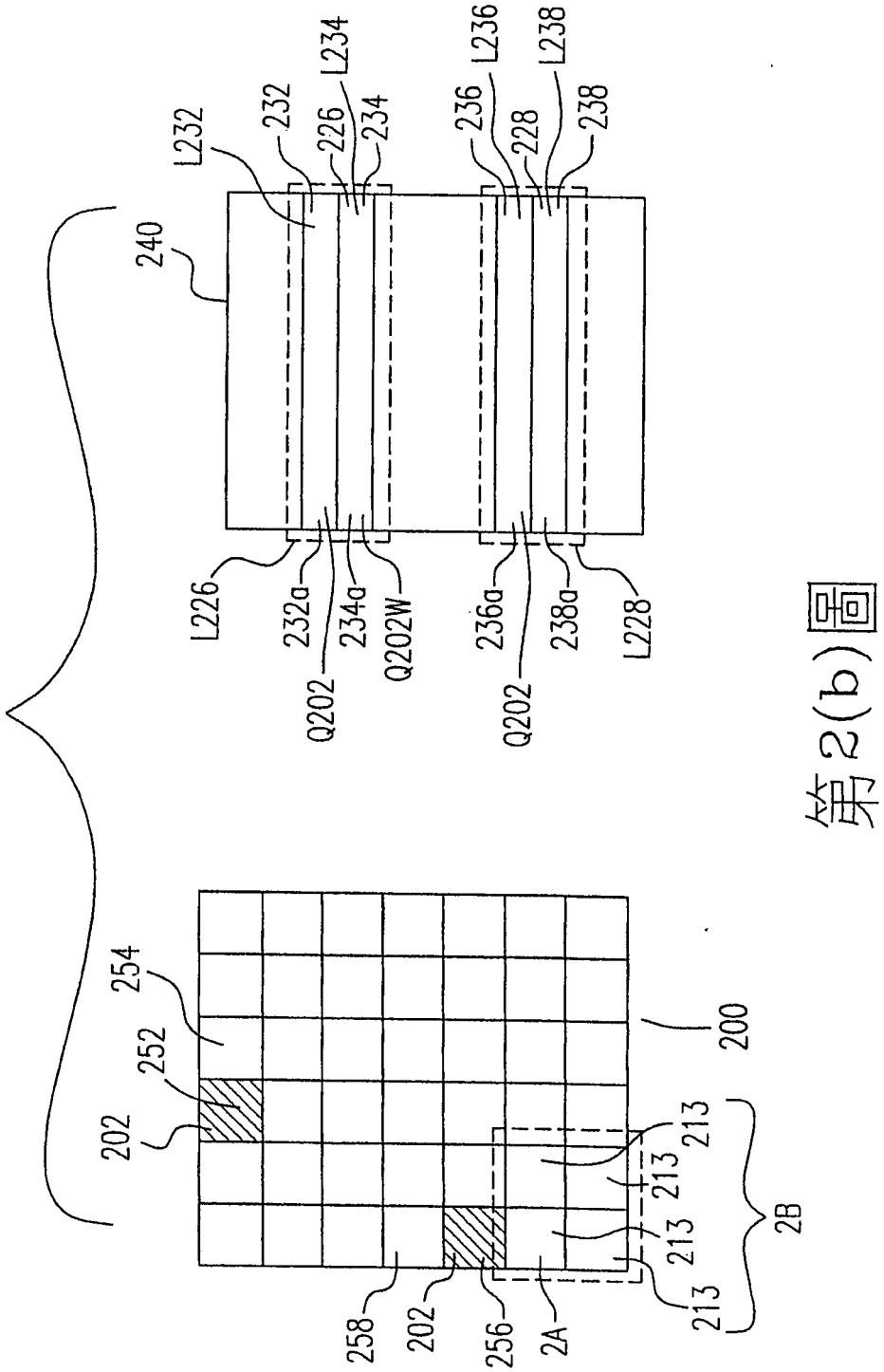
根據存於該來源位址之一第一資料是否包含該具標記狀態之該資料，來判斷是否使該目標位址之一第二資料附有該標記狀態。



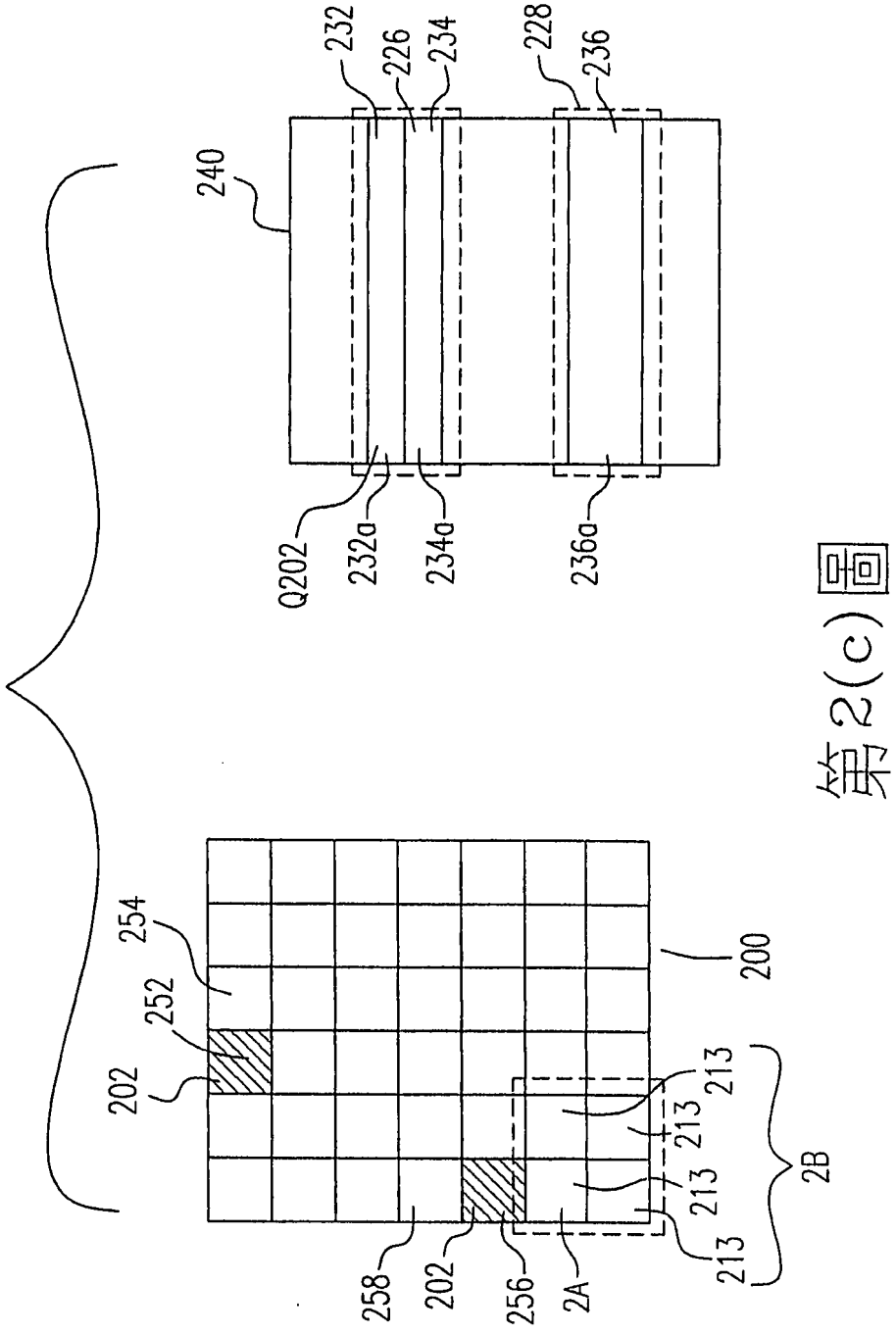
第1圖


240
220
224a
224
Q202
222
226
228
Q202W
L226
226a
228a
L228
202W
214
202
216
218
200
212
210
2A
280
輸入/輸出裝置
213
213
2B

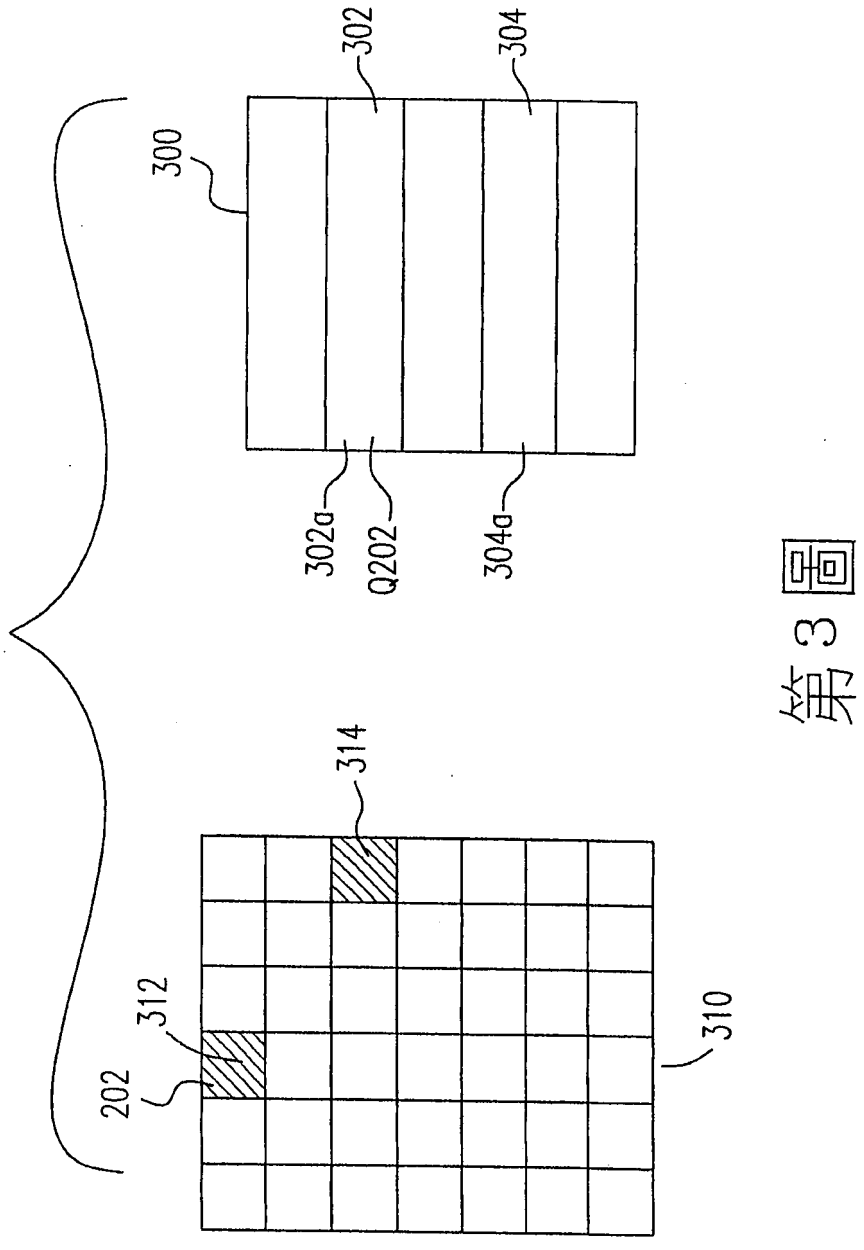
第2(a)圖


L232
232
L234
226
234
L236
236
228
L238
238
240
L226
232a
234a
Q202W
236a
238a
L228
Q202
Q202
254
252
202
200
213
213
213
213
213
2B
258
202
256
2A

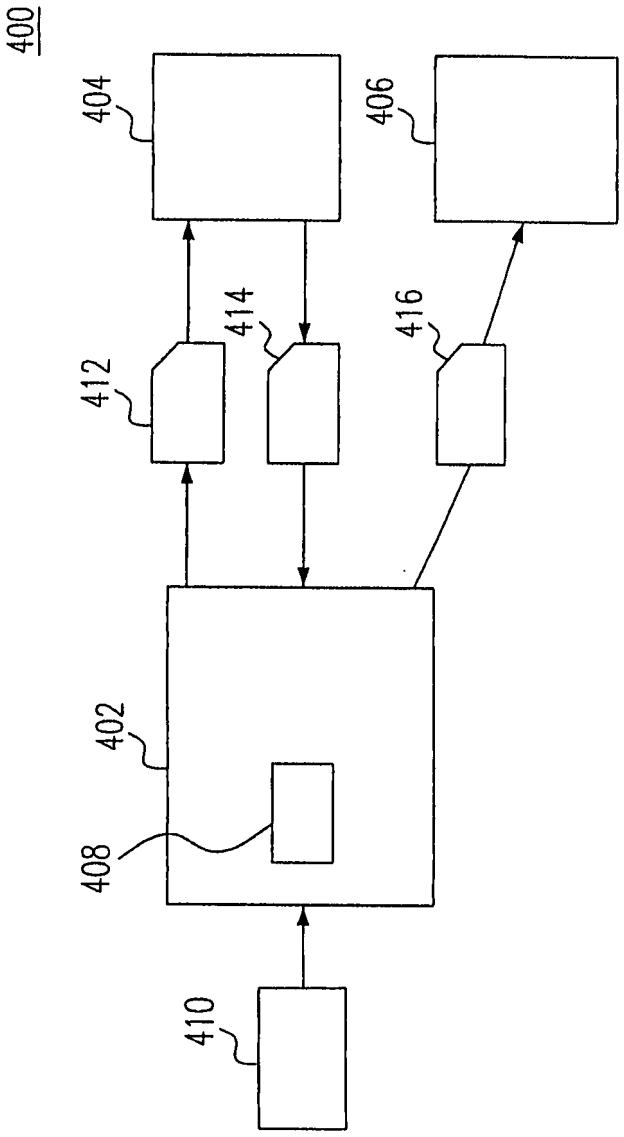
第2(b)圖


232
226
234
228
236
240
Q202
232a
234a
236a
254
252
202
200
213
213
213
213
213
258
202
256
2A
2B

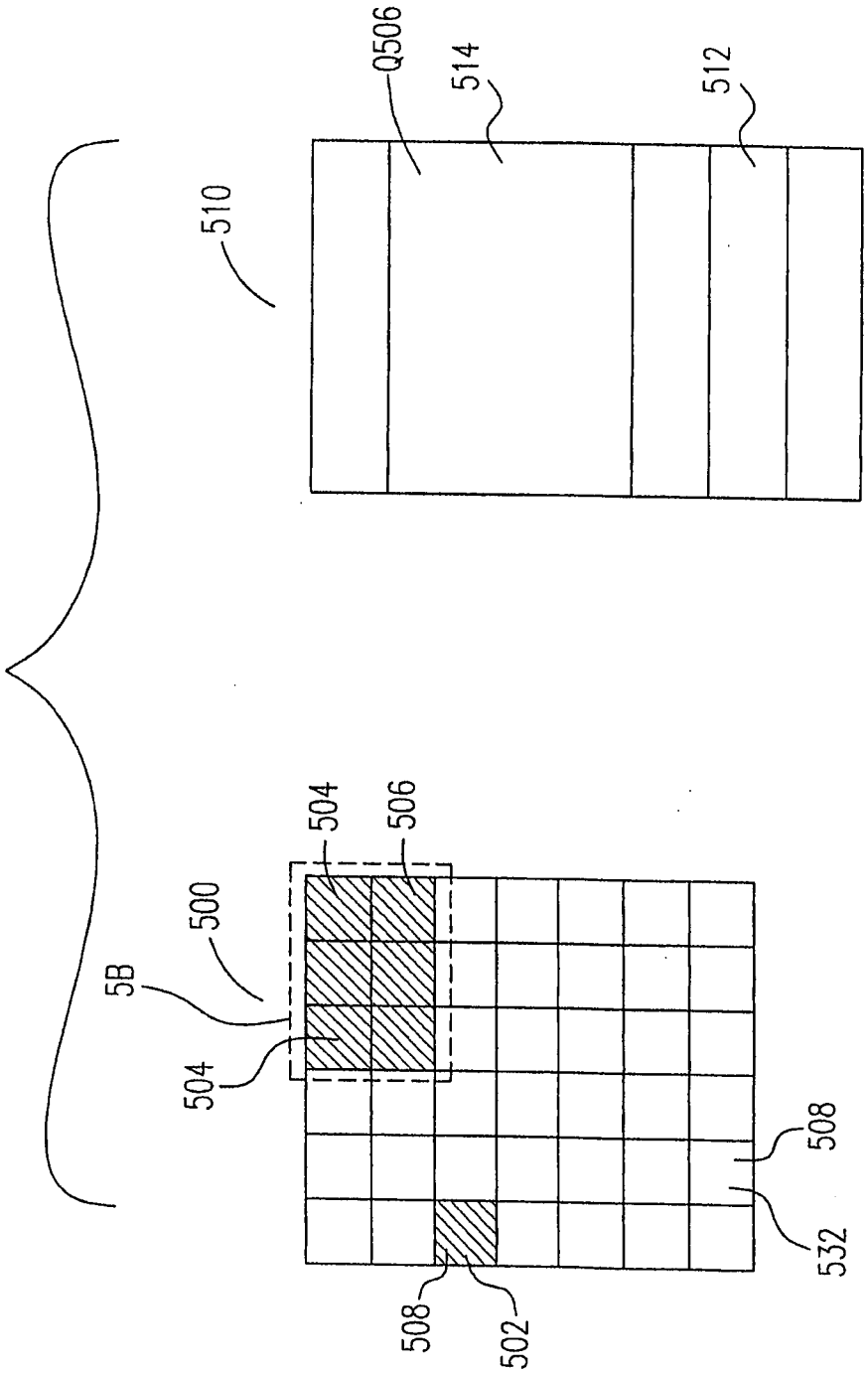
第2(c)圖



第3圖

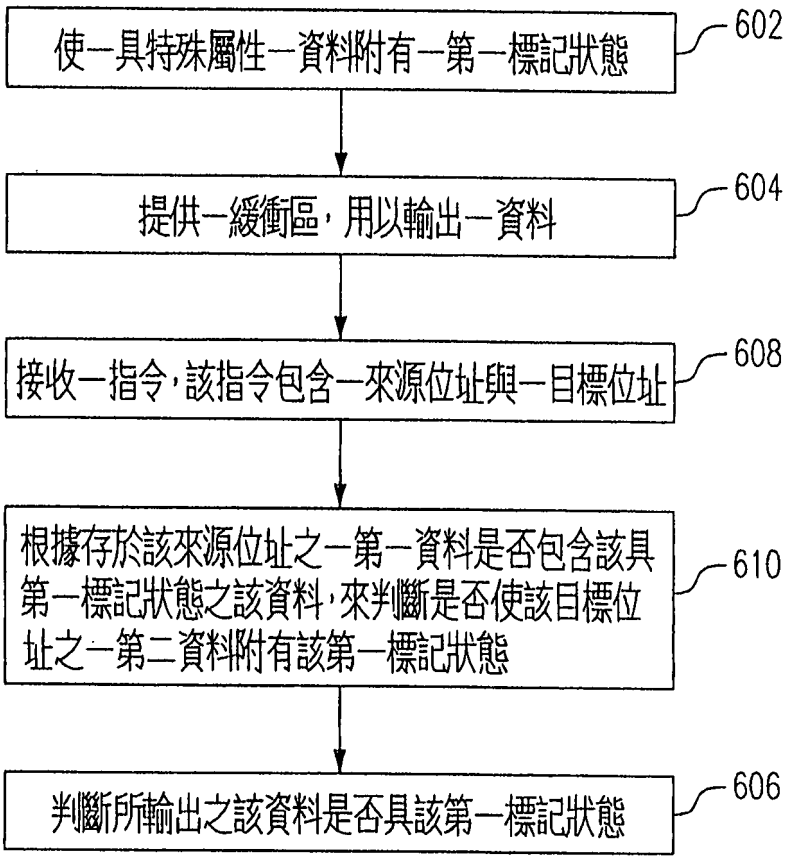


第4圖

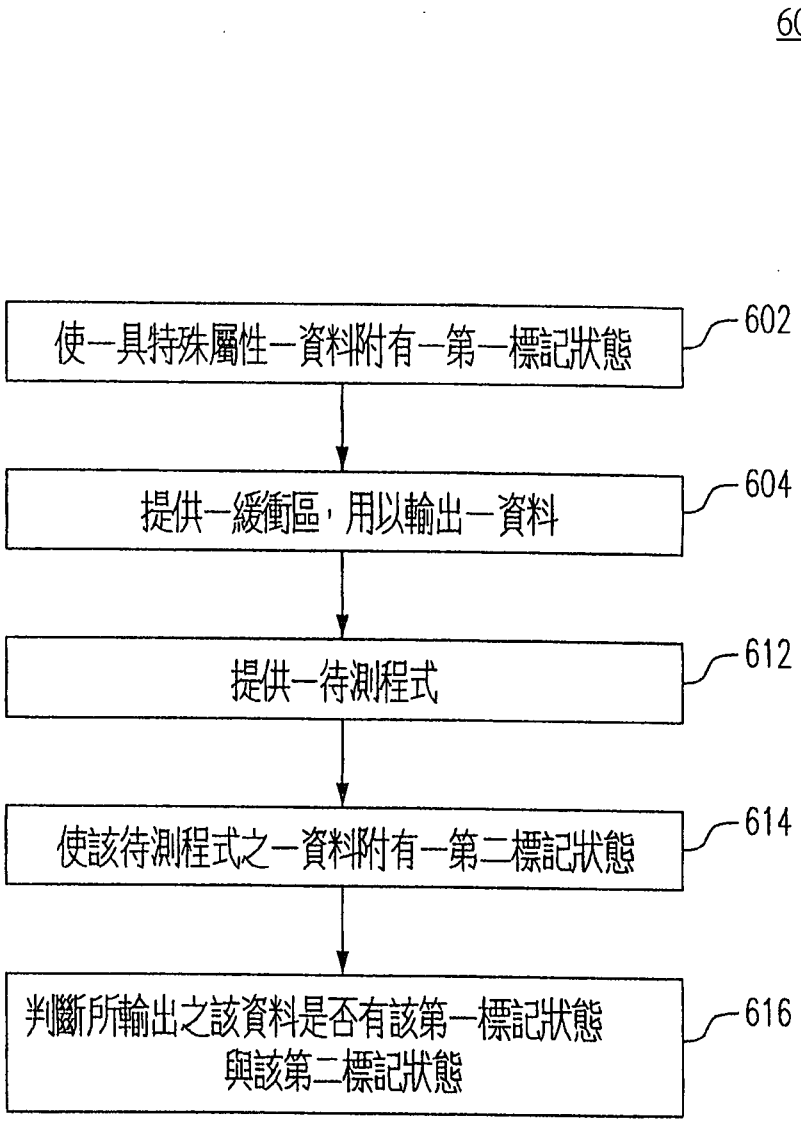


第5圖

600


使一具特殊屬性一資料附有一第一標記狀態
602
提供一緩衝區，用以輸出一資料
604
接收一指令，該指令包含一來源位址與一目標位址
608
根據存於該來源位址之一第一資料是否包含該具第一標記狀態之該資料，來判斷是否使該目標位址之一第二資料附有該第一標記狀態
610
判斷所輸出之該資料是否具該第一標記狀態
606

第6(a)圖


600
使一具特殊屬性一資料附有一第一標記狀態
602
提供一緩衝區，用以輸出一資料
604
提供一待測程式
612
使該待測程式之一資料附有一第二標記狀態
614
判斷所輸出之該資料是否有該第一標記狀態與該第二標記狀態
616

第6(b)圖