I506468

(19)中華民國智慧財產局

(12)發明說明書公告本 **(11)證書號數：TW I506468 B**

**(45)公告日： 中華民國 104 (2015) 年 11 月 01 日**

(21)申請案號：099117927 (22)申請日： 中華民國 95 (2006) 年 12 月 15 日

(51)Int. Cl.： *G06F21/00 (2013.01)* *G06F11/00 (2006.01)*

(30)優先權：2005/12/30 美國 11/322,677

(71)申請人：英特爾股份有限公司 (美國) INTEL CORPORATION (US)
美國

(72)發明人：布朗 大衛 BROWN, DAVID A. (US)；艾提薩尼 多明尼克 ATTISANI, DOMINICK J. (US)

(74)代理人：林志剛

(56)參考文獻：

TW 535052 US 2004/0150525A1

US 2005/0185552A1

審查人員：許哲睿

申請專利範圍項數：30 項 圖式數：5 共 25 頁

(54)名稱

偵測偽造產品之方法及電子設備

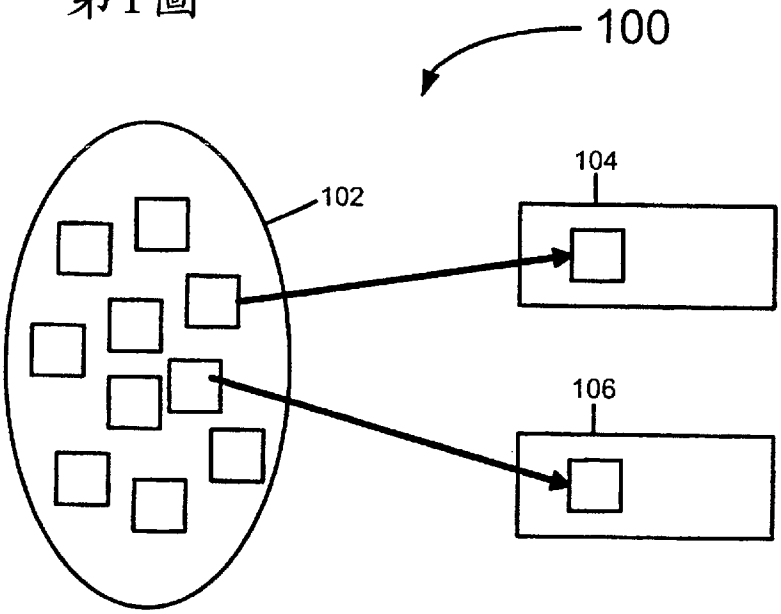
A METHOD OF DETECTING COUNTERFEIT PRODUCTS AND AN ELECTRONIC APPARATUS

(57)摘要

於一些實施例中，邏輯裝置之意圖的用途之指示係儲存於邏輯裝置的暫存器中，以及防止該暫存器之進一步的編程。本文描述其他的實施例並且主張其之專利權。

In some embodiments an indication of an intended use of a logic device is stored in a register of the logic device, and any further programming of the register is prevented. Other embodiments are described and claimed.

第1圖




100・・・方塊圖

102・・・群體

104・・・一群有廠牌的板層級產品

106・・・一群偽造的板層級產品

第 099117927 號　　民國 102 年 9 月 17 日修正頁

公告本

# 發明專利說明書

（本申請書格式、順序，請勿任意更動，※記號部分請勿填寫）

※申請案號：99117927

※申請日期：95 年 12 月 15 日　　※IPC 分類：G06F 21/00 (2006.01)
G06F 11/00 (2006.01)

原申請案號：95147208

一、發明名稱：（中文／英文）

偵測偽造產品之方法及電子設備

A method of detecting counterfeit products and an electronic apparatus

二、中文發明摘要：

於一些實施例中，邏輯裝置之意圖的用途之指示係儲存於邏輯裝置的暫存器中，以及防止該暫存器之進一步的編程。本文描述其他的實施例並且主張其之專利權。

三、英文發明摘要：

In some embodiments an indication of an intended use of a logic device is stored in a register of the logic device, and any further programming of the register is prevented. Other embodiments are described and claimed.

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：方塊圖

102：群體：

104：一群有廠牌的板層級產品

106：一群僞造的板層級產品

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】

本發明主要有關於偵測偽造的產品。

【先前技術】

於一些情況中，諸如英特爾股份有限公司之公司製造個別販售的構件(例如，電腦晶片)以及包含公司個別販售一或更多構件之板層級及/或系統層次產品。在此種情況中，構件有時會從合法的客戶系統設計實施例經由「開放市場」流出至偽造公司之所有與有商標的系統及/或板層級設計的非法偽造操作。因此，產生一種能夠分開與區別由合法 OEM(原始設備製造商)販售與運送的構件以及針對公司有商標或公司所有之板子及/或系統之建構用來在有廠牌的公司系統上使用的構件。

【發明內容及實施方式】

本發明之一些實施例有關於偵測偽造產品。

在一些實施例中，於邏輯裝置的暫存器中儲存該邏輯裝置之意圖的用途之指示，以及防止該暫存器之任何進一步的編程。

在一些實施例中，邏輯裝置包含指示該邏輯裝置的意圖的用途之暫存器。

在一些實施例中，從邏輯裝置的暫存器讀取該邏輯裝置之意圖的用途之指示。回應於該讀取而進行該邏輯裝置

是否包含於僞造的產品中之判斷。

在一些實施例中，編程電路於邏輯裝置的暫存器中儲存該邏輯裝置之意圖的用途之指示，以及防止該暫存器的任何進一步的編程。

嘗試偵測僞造板及/或系統層次產品的一種方法爲在用料單(BOM)中包含僅有廠牌及/或有商標之產品的授權製造商可取得的項目。包含在 BOM 中的這個項目可包含開放市場無法輕易取得之所有權安全性技術。特別的設備可用來偵測安全性技術特徵的存在與否。然而，特別偵測設備的散佈很昂貴，而且當錯的人取得特別偵測器時，安全性技術可能會被破解。偵測器亦可能很昂貴或使用上耗時，因此限制了安全性技術的有效性。許多僞造的產品可能會逃過此種解決方案所提供的偵測，因爲太少人可獲得及知道如何使用該偵測設備。

一種替代方式爲公司(例如英特爾股份公司)僅在有該公司之廠牌的板(或系統)上使用一邏輯裝置，並絕不讓開放市場取得那個特定的邏輯裝置。在此模型中，公司的邏輯裝置成爲所有權安全性技術。除了例如在網際網路上提供之以網路爲基礎的小型辨識工具之外無須額外的偵測設備，該工具驗證有公司廠牌或公司所擁有之設計的合法性。只有合法(亦即，內部及/或有公司廠牌的)系統設計能取得此邏輯裝置並允許適當的硬體－軟體「交握(handshake)」。然而，在此情況中，彈性卻不夠，因爲公司無法在沒有整個有廠牌的系統及/或板的情況下提供此邏輯裝置供

販售(例如，在「開放市場」上)。

根據一些實施例，質問板層級產品上的邏輯裝置以判斷是否該板層級產品爲僞造的或由有商標保護的廠牌擁有者或該商標保護的廠牌擁有者之授權的外包商(例如透過軟體)製造的板層級產品。根據一些實施例，多廠牌擁有者可使用共同的邏輯裝置並仍能分別區別出類似或相同功能之商標標示的板層級產品。

根據一些實施例，邏輯裝置包含具有使用例如僅可編程一次的電路實施的一或更多位元的軟體可見之暫存器。

根據一些實施例，製造與散佈協定將獨特的模式編程到針對各商標保護的廠牌擁有者之邏輯裝置的軟體可見之暫存器中，並在各廠牌擁有者的模式寫入確保邏輯裝置的暫存器中之後，確保各廠牌擁有者具有對於邏輯裝置的散佈之控制。

根據一些實施例，製造商提供相同功能性與性能之邏輯裝置給超過一個的客戶。邏輯裝置包含一特徵，其中小的靜態且獨立的軟體程式可原地區別運送至一個客戶的邏輯裝置以及運送至任何其他人的邏輯裝置。可使用軟體序號區別軟體裝置(例如乙太網路裝置的 MAC 位址)，但當使用序號時，該軟體必須存取中央資料庫，因此並非爲獨立亦非靜態，因爲會不斷更新中央資料庫。

根據一些實施例，可追蹤、禁止、及/或限制在包含邏輯裝置的僞造板層級產品上之商標及/或廠牌的未授權的使用。根據一些實施例，可使用防止竄改的軟體稽核工

具來幫助偵測與嚇止在販售再散佈鍊中所有環結之僞造的產品。

第1圖描繪代表將相同邏輯裝置之群體102分類之方塊圖100。將相同邏輯裝置的群體102的一些分類爲邏輯裝置的製造商意圖將邏輯裝置包含在有廠牌的板層級產品中(例如，具有製造商的廠牌及/或任何的外包商之廠牌)之一群有廠牌的板層級產品104。相同邏輯裝置的群體102的其餘者則分類爲一群僞造的板層級產品106(例如，那些意圖由邏輯裝置的製造商在開放市場上個別販售者)。在不增加成本與降低準確性(例如使用法學分析)的情況下，目前可得的軟體無法區分製造商意圖放在有廠牌的板層級產品中之真正的邏輯裝置以及製造商不意圖放在有廠牌的板層級產品中之邏輯裝置(亦即，「僞造的板層級產品」)。

第2圖描繪代表根據本發明之一些實施例之邏輯裝置的分類的方塊圖200。根據一些實施例，藉由邏輯裝置中的暫存器(如廠牌保護暫存器)中的值來分離邏輯裝置群體。在第2圖中，邏輯裝置之群體202包含在諸如廠牌保護暫存器的特別暫存器中具有一值(第2圖中「零」值)的裝置，以及邏輯裝置之群體204在其諸如廠牌保護暫存器的特別暫存器中包含不同的值(第2圖中「一」值)。可由軟體將邏輯裝置的群體202與204區分真正的有廠牌之板層級產品206(例如，僅內部使用及/或受控的散佈產品)以及僞造的板層級產品208(例如，開放市場使用及/或開放散佈產品)。該軟體界由檢視各邏輯單元之特別暫存器(如廠牌保護

暫存器)的內容而區分真正與僞造的板層級單元，使敏銳的使用者能發現此詐欺。

根據一些實施例，第2圖額外描繪邏輯裝置群體210，其包含在諸如廠牌保護暫存器的特別暫存器中沒有值或(某些不明確值)(第2圖中「?」值)的邏輯裝置。根據一些實施例，軟體進一步區分這種邏輯裝置爲僞造產品208(例如100%僞造的構件，例如沒有製造公司工廠的來源之邏輯裝置)。在此種情況中，僞造構件在暫存器中不具有偵測軟體可偵測到之例如「0」或「1」，並且例如會被讀成「?」(失敗)。根據一些實施例，將此種失敗的裝置可連同第2圖中所示之僞造的板層級產品208宣告爲禁運品。根據一些實施例，將此種失敗的裝置宣告爲禁運品並且放置在與僞造的板層級產品208不同的僞造類別中。透過與僞造的板層級產品208之通知相同及/或與僞造的板層級產品208稍微不同之適當的建議通知可因此進一步保護廠牌與消費者。

第3圖描繪代表根據本發明之一些實施例的邏輯裝置的編程之方塊圖300。方塊圖300包含被編程之邏輯裝置302與編程電路304。邏輯裝置302包含可編程暫存器306(如廠牌保護暫存器)。根據一些實施例，暫存器306可爲一位元。根據一些實施例，暫存器306可爲任何位元數量。根據一些實施例，暫存器306可含有可調整之位元數量。

根據一些實施例，可編程暫存器306爲加至邏輯裝置302的僅可編程一次之暫存器，其辨別邏輯裝置的意圖之

用途(例如，辨別意圖將該邏輯裝置包含在邏輯裝置的製造商及/或外包商、客戶、被授權者等等的板層級及/或系統層次設計中或辨別意圖將該邏輯裝置個別販售)。根據一些實施例，

根據一些實施例，可編程電路304可編程邏輯裝置及/或暫存器之任何電路。可編程電路304可例如在硬體、軟體、及/或韌體中實施。

根據一些實施例，可編程暫存器306爲僅可編程一次之暫存器。根據一些實施例，可(例如使用軟體)分離及/或區分否則爲相同的邏輯裝置的群體。根據一些實施例，藉由將有區別的模式編程到諸如暫存器306的暫存器中，可由軟體辨別運送到特許(licensed)製造具有製造邏輯裝置之公司的廠牌之板子之工廠的矽(例如可由任何有興趣者自由與廣泛散佈的軟體)。不被特許製造具有製造邏輯裝置之公司的廠牌之板子之工廠將無法取得由具有該公司的廠牌之板子所需之編程有區別模式之邏輯裝置。雖然不被特許之工廠仍能獲得邏輯裝置(例如一般的構件)並製造出複製的板層級及/或系統層次產品(假冒爲板子及/或系統的僞造品)，僞造板子(或系統)將無法通過軟體辨識測試(因而辨別該板子及/或系統爲禁運品)。根據一些實施例，用於具有公司廠牌的板子及/或系統之相同的邏輯裝置可販售到開放市場上，其具有編程至暫存器(廠牌保護暫存器)中的不同模式。依照此方式，可證實真正的有廠牌的板子而無需額外的外加式安全裝置。

根據一些實施例，可編程暫存器(例如暫存器306及/或廠牌保護暫存器)的長度超過一位元。當暫存器的長度超過一位元，根據一些實施例，可將每一個獨特的二元模式分配給例如用來保護不同的廠牌及/或不同的商標。製造邏輯裝置的公司(例如英特爾公司)可擁有一些或所有該些不同的廠牌及/或不同的商標，以及另外的(諸)公司可擁有一些或所有該些不同的廠牌及/或不同的商標(例如製造邏輯裝置的公司之一或更多客戶)。暫存器中(例如暫存器306)之額外的位元以及額外的暫存器可例如允許製造商提供廠牌及/或商標保護特徵給一些或全部的客戶。此外，製造商可使用此種廠牌及/或商標保護來追蹤流入開放市場中的材料，以及可能流入板子及/或系統僞造操作者的手中。藉由辨別此種流出，製造商及/或其客戶、OEM、獲許可者等等可判斷出最後落入僞造操作者的手中之產品的洩漏處。

根據一些實施例，編程電路(例如電路304)在製造邏輯裝置(例如邏輯裝置302)的期間編程暫存器(例如暫存器306)的每一個位元。可在對於製造商方便的製造流程的任何地方進行暫存器編程的步驟。然而，根據一些實施例，一旦完成編程，分離邏輯裝置群體，使得每一群邏輯裝置內不會有混合的廠牌保護模式。根據一些實施例，可使用任何技術來編程暫存器，只要編程不被抹除或修改。根據一些實施例，編程鎖定特徵防止在邏輯裝置離開製造工廠後進一步的編程任何位元。

根據一些實施例，編程至廠牌保護暫存器中的模式必須爲使用該邏輯裝置的操作系統(OS)軟體可見的。該暫存器係其中安裝有該邏輯裝置之該系統的使用周邊輸入/輸出通道結構而可定址爲一唯讀位置。

根據一些實施例，廠牌保護暫存器不會影響或控制邏輯裝置的任何其他功能性特徵。在此種實施例中，此暫存器的唯一功能係呈現已編程的模式(例如給 OS 軟體)。

根據一些實施例，作爲僞造偵測技術的廠牌保護暫存器的穩健性隨著包含該暫存器之邏輯裝置的複雜度增加而改善。難以僞造高複雜度的邏輯裝置，並且僞造的邏輯裝置可用來在開放市場中提供未編程的廠牌保護暫存器之一替代來源。例如，針對具有等於或高於乙太網路控制器(或其他嵌入式控制器)之複雜度的邏輯裝置，廠牌保護暫存器係非常的穩健。

根據一些實施例，具有暴露在直接複製下之電路的較不複雜的裝置必須增進廠牌保護暫存器。例如，根據一些實施例，實施使用先進加密技術的辨識協定來防止100%構件僞造品將系統及/或板層級複製品虛假地辨別爲正品。對於諸如先進 CPU 及乙太網路及無線致能構件設計，目前通常無須此種額外的措施，因通常認爲此電路不會暴露在直接複製下。

根據一些實施例，用來顯示廠牌保護模式給用戶之操作系統(OS)使用的軟體必須從安全的來源提供給用戶。因此，根據一些實施例，希望證實包含具有廠牌保護暫存器

的邏輯裝置之板層級及/或系統層次產品的真實性之任何人可從安全的來源獲得新的一份證實軟體。這確保軟體不會被企圖偽造板層級及/或系統層次產品的其他人所竄改。

第4圖描繪根據本發明之一些實施例之流程圖400。在方塊402，將識別資訊載入一暫存器中。例如，在方塊402，將識別其中有該暫存器之邏輯裝置的預期用途之資訊(例如，意圖該邏輯裝置用於有廠牌的板層級產品中或在開放市場上個別販售)載入一暫存器中。在方塊404，防止進一步編程該暫存器(例如，使得該邏輯裝置用於有廠牌的板層級產品中或該邏輯裝置在開放市場上個別販售的意圖無法被更改)。根據一些實施例，例如，藉由第3圖中所示的編程電路304來實施流程圖400。

第5圖描繪根據本發明之一些實施例之流程圖500。在方塊502，從安全來源獲得證實軟體(如將被測試之邏輯裝置的製造商的網站)。接著在方塊504，執行一測試，以確保該證實軟體未被竄改。若在504該證實軟體未被竄改，則在506進行證實，其證實出例如邏輯裝置的暫存器辨別邏輯裝置意圖用於板層級及/或系統層次裝置中。

雖已參照特定實行描述一些實施例，亦可能有根據一些實施例的其他實行。此外，描述於圖中及/或本文中的電路元件或其他特徵的配置及/或順序無須以所示與所述的特定方式加以配置。亦可能有根據一些實施例的許多其他配置。

圖中的每一個系統中，在一些情況中，元件可各具有相同的參考符號或不同的參考符號，以暗示所呈現的這些元件可能爲不同及/或類似者。然而，元件可有足夠的彈性，以具有不同的實施例並與本文中所示或所述的一些或所有系統一同運作。圖中所示的各種元件可爲相同或不同。何者稱爲第一元件以及稱爲第二元件爲隨意的。

在實施方式與申請專利範圍中，可使用「耦接」及「連接」的詞彙與其衍生詞。應注意到這些用詞並非意圖做爲同義詞。更確切地，於特定實施例中，「連接」可用來表示互相直接實體或電性接觸之兩個或更多元件。「耦接」意指直接實體或電性接觸之兩個或更多元件。然而，「耦接」亦可指不直接實體或電性接觸之兩個或更多元件，但仍相互共同操作或互動。

於本文中，以及一般而言，演算法係視爲導致希望之結果的自我一致的動作或操作序列。這些包含物理量之物理操縱。通常，但非絕對，這些量具有能被儲存、傳送、結合、比較、或以其他方式操縱之電性或磁性信號的形式。已證實有時候，主要爲了慣用的原因，方便以位元、值、元件、符號、字元、術語、數字、或類似者參照這些信號。然而，應了解到所有這些與類似的用語應該與適當的物理量關聯，並僅爲這些量的方便標示。

可在硬體、韌體、及軟體之一者或結合中實行一些實施例。亦可以儲存在機器可讀取媒體上的指令來實行一些實施例，可由運算平台讀取與執行指令以履行本文中描述

的操作。機器可讀取媒體可包含任何以機器(如電腦)可讀取的形式來儲存或傳送資訊的機制。例如，機器可讀取媒體可包含唯讀記憶體(ROM)、隨機存取記憶體(RAM)、磁碟儲存媒體、光碟儲存媒體、快閃記憶體裝置、電性、光性、聽覺性或以其他形式傳播的信號(如載波、紅外線信號、數位信號、傳輸及/或接收信號的介面等等)以及其他者。

一實施例爲本發明之一實行例或範例。此說明書中對於「實施例」、「一實施例」、「一些實施例」、「其他實施例」之參照意指連同該實施例描述之特定特徵、結構、或特性係包含在至少一些實施例中，但非絕對在本發明的所有實施例中。「實施例」、「一實施例」、「一些實施例」的各種出現並非絕對參照至相同的實施例。

本文中描述與圖解的所有構件、特徵、結構、特性等等並非必需包含在(諸)特定實施例中。若說明書指出，例如，「可(may、might)」、「能(can、could)」包含一特定構件、特徵、結構、或特性，則並非必需包含那個特定的構件、特徵、結構、或特性。若說明書或申請專利範圍參照「一」元件，不代表該元件只有一個。若說明書或申請專利範圍參照「額外的」元件，不排除該額外的元件超過一個。

雖本文中可能使用流程圖及/或狀態圖來描述實施例，本發明不限於那些圖或本文中對應之說明。例如，流程無須以本文中圖解及描述的完全一樣的順序進行每一個所

述的方塊或狀態。

本發明不限於本文中所列之特定細節。確實，熟悉該項技藝者在得到此揭露的好處後將可理解到能夠做出在本發明的範疇內之上述說明與圖示之許多其他的變異。因此，由包含任何修正之下列申請專利範圍界定本發明的範疇。

【圖式簡單說明】

從上述實施方式以及本發明之一些實施例之附圖可更完整地了解本發明，實施方式與附圖不應視爲將本發明限制於所述之特定實施例，而僅做爲解釋與了解之意圖。

第1圖描繪根據本發明之一些實施例之邏輯裝置的分類。

第2圖描繪根據本發明之一些實施例之邏輯裝置的分類。

第3圖描繪根據本發明之一些實施例的方塊圖。

第4圖描繪根據本發明之一些實施例之流程圖。

第5圖描繪根據本發明之一些實施例之流程圖。

【主要元件符號說明】

100、200、300：方塊圖

102：群體：

104：一群有廠牌的板層級產品

106：一群僞造的板層級產品

202、204、210：群體

206：真正有廠牌的板層級產品

208：僞造的板層級產品

302：邏輯裝置

304：編程電路

306：可編程暫存器

400、500：流程圖

**七、申請專利範圍：**

1.一種偵測偽造產品之方法，包含：

於一裝置中儲存該裝置是否爲真正的裝置之加密的指示，該指示係經由靜態且獨立的程式以提供有關該裝置之合法性的資訊，其中該裝置包含邏輯裝置。

2.如申請專利範圍第 1 項之方法，其中該儲存的指示應用於判斷該裝置是否爲偽造的裝置。

3.如申請專利範圍第 1 項之方法，進一步包含回應於該儲存的指示以判斷該裝置是否爲偽造的裝置。

4.如申請專利範圍第 1 項之方法，其中該真正的裝置爲真正的有廠牌的裝置。

5.如申請專利範圍第 1 項之方法，其中該裝置包含一用以儲存該加密的指示之積體電路。

6.如申請專利範圍第 1 項之方法，其中該裝置包含一積體電路。

7.如申請專利範圍第 1 項之方法，其中該指示爲該裝置之意圖的用途之指示。

8.如申請專利範圍第 7 項之方法，其中該意圖的用途包含該裝置應個別販售的指示以及該裝置應包含於有廠牌的產品中的指示之一者以上。

9.如申請專利範圍第 7 項之方法，其中該意圖的用途包含該裝置應包含於板層級產品中的指示以及該裝置應個別販售的指示之一者以上。

10.如申請專利範圍第 1 項之方法，其中該指示可定

址為一唯讀位置。

11.如申請專利範圍第 1 項之方法，其中該指示不影響或控制該裝置的任何其他功能特徵。

12.如申請專利範圍第 1 項之方法，進一步包含：

解密該指示；及

回應於該解密的指示而判斷該裝置是否為偽造的裝置。

13.如申請專利範圍第 1 項之方法，其中該裝置包含一用以儲存該加密的指示之記憶體裝置。

14.如申請專利範圍第 1 項之方法，其中該裝置為記憶體裝置。

15.如申請專利範圍第 14 項之方法，其中該記憶體裝置為暫存器。

16.一種電子設備，包含：

一裝置，用以儲存該裝置是否為真正的裝置之加密的指示，該指示係經由靜態且獨立的程式以提供有關該裝置之合法性的資訊，其中該裝置包含邏輯裝置。

17.如申請專利範圍第 16 項之設備，其中該儲存的指示應用於判斷該裝置是否為偽造的裝置。

18.如申請專利範圍第 16 項之設備，該裝置進一步協助回應於該儲存的指示以判斷該裝置是否為偽造的裝置。

19.如申請專利範圍第 16 項之設備，其中該真正的裝置為真正的有廠牌的裝置。

20.如申請專利範圍第 16 項之設備，進一步包含一用

以儲存該加密的指示之積體電路。

21.如申請專利範圍第 16 項之設備，其中該裝置包含一積體電路。

22.如申請專利範圍第 16 項之設備，其中該指示爲該裝置之意圖的用途之指示。

23.如申請專利範圍第 22 項之設備，其中該意圖的用途包含該裝置應個別販售的指示以及該裝置應包含於有廠牌的產品中的指示之一者以上。

24.如申請專利範圍第 22 項之設備，其中該意圖的用途包含該裝置應包含於板層級產品中的指示以及該裝置應個別販售的指示之一者以上。

25.如申請專利範圍第 16 項之設備，其中該指示可定址爲一唯讀位置。

26.如申請專利範圍第 16 項之設備，其中該指示不影響或控制該裝置的任何其他功能特徵。

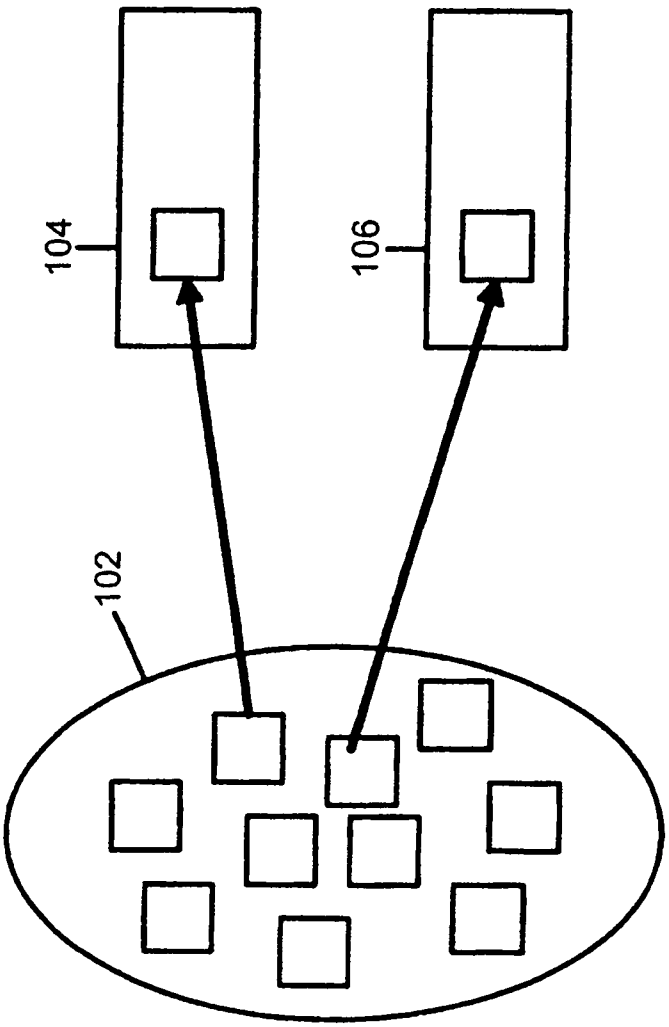
27.如申請專利範圍第 16 項之設備，其中該指示可被解密以協助判斷該裝置是否爲僞造的裝置。

28.如申請專利範圍第 16 項之設備，其中該邏輯裝置包含一用以儲存該加密的指示之記憶體裝置。

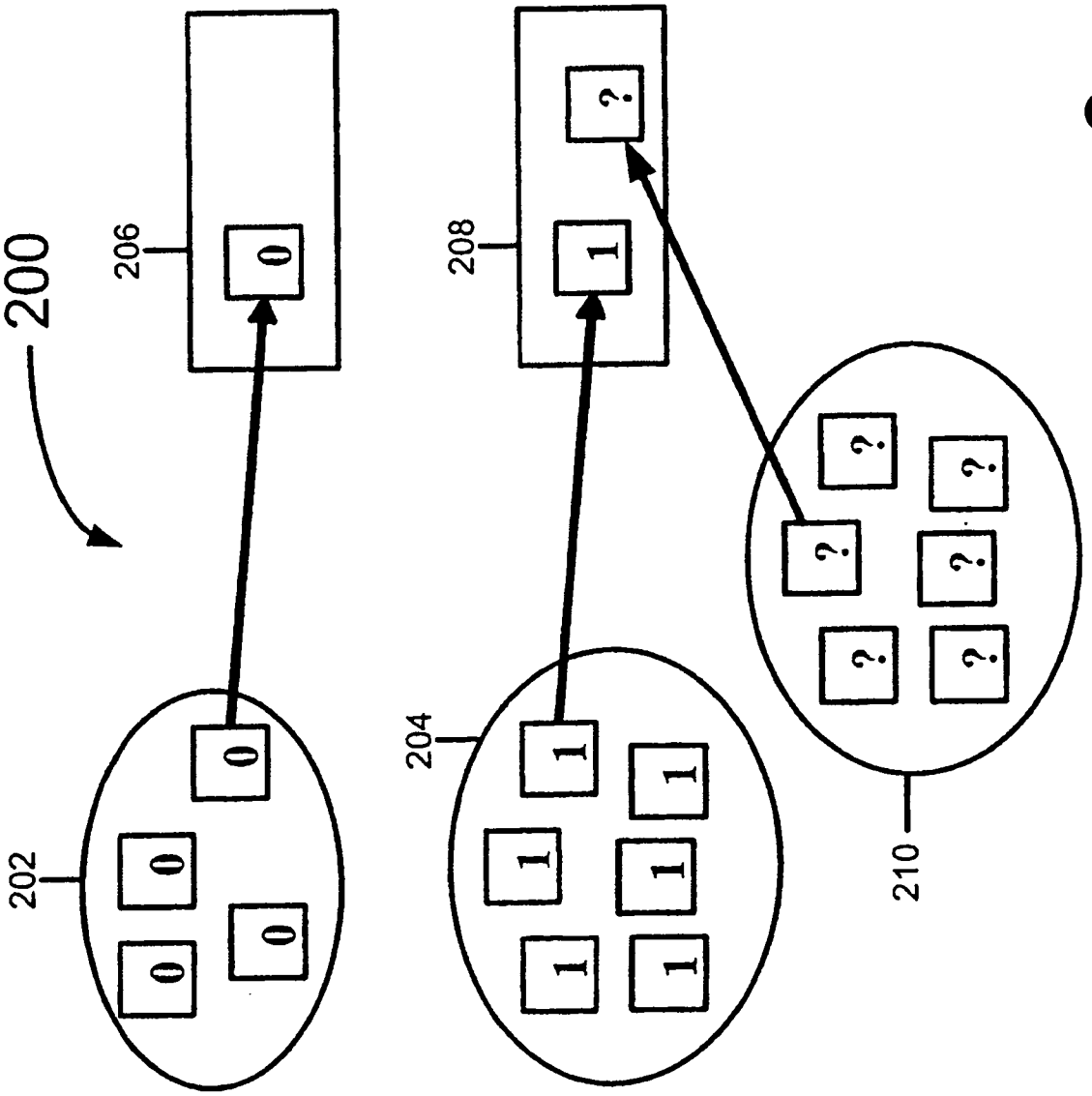
29.如申請專利範圍第 16 項之設備，其中該邏輯裝置爲記憶體裝置。

30.如申請專利範圍第 29 項之設備，其中該記憶體裝置爲暫存器。

851526-1

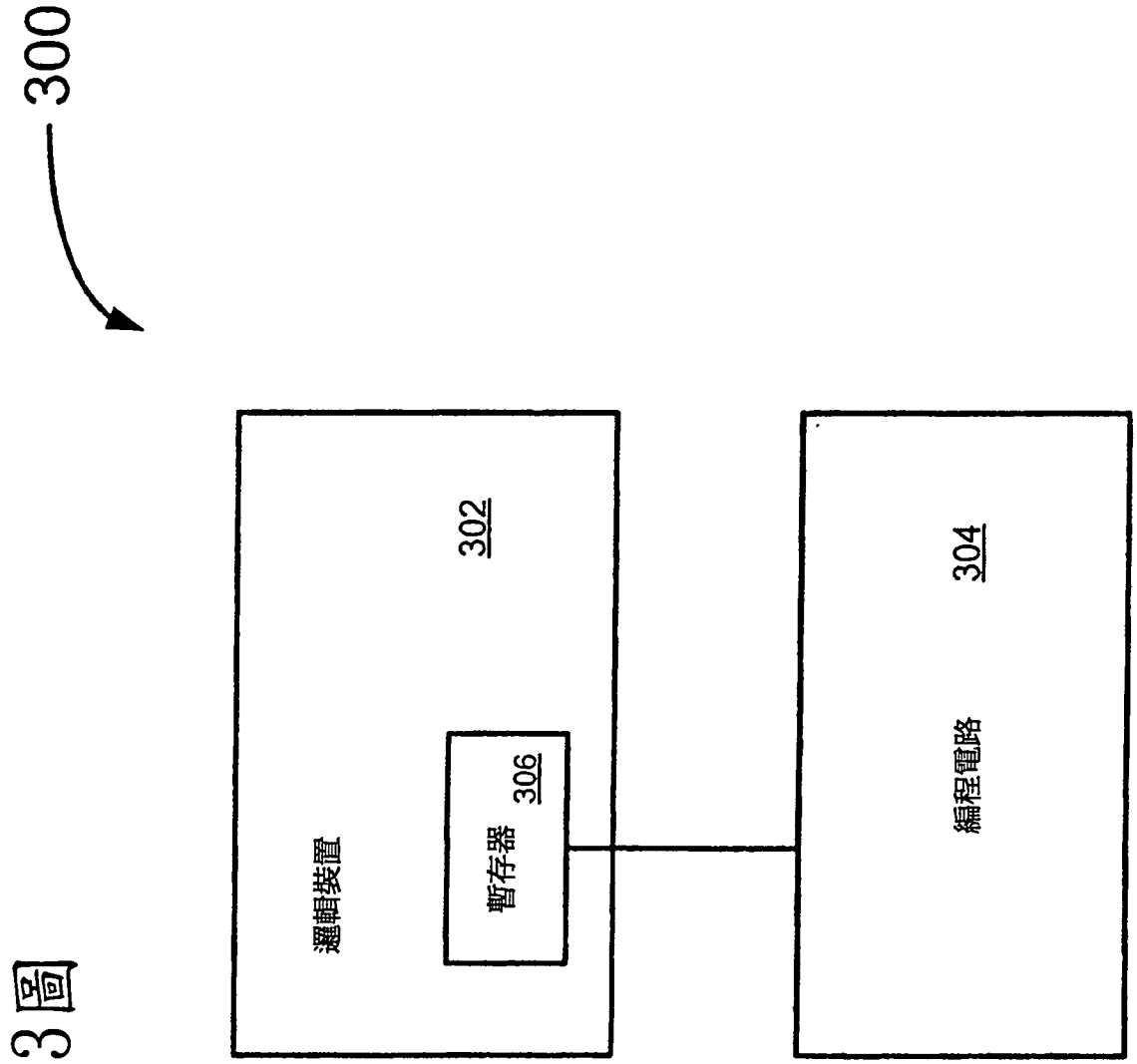


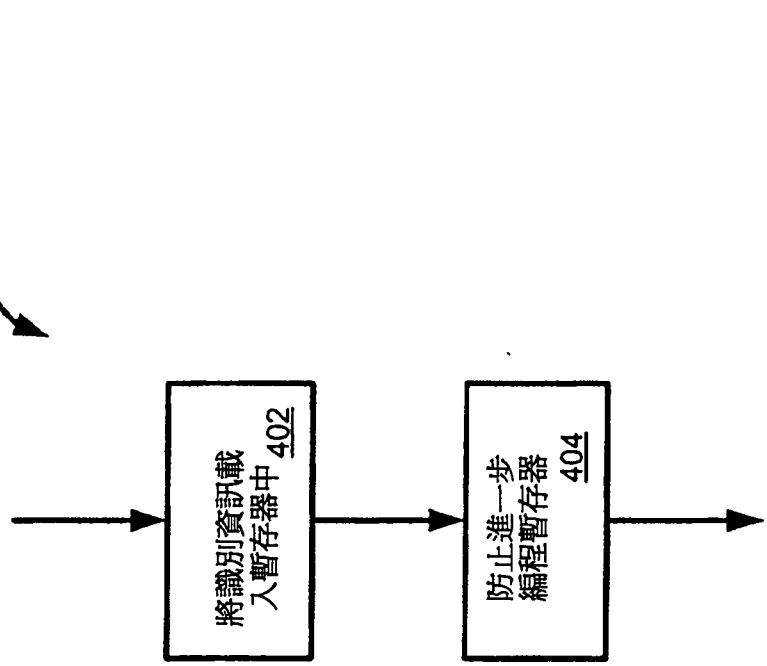

第1圖



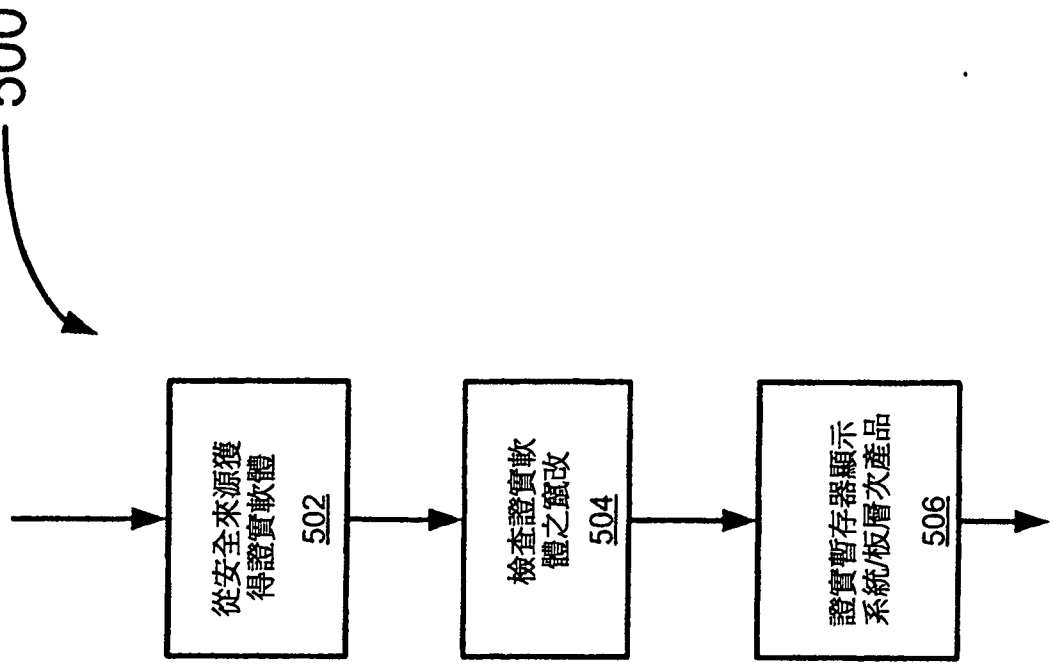

第2圖

第3圖






第4圖




第5圖