(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 201037596 A1
(43)公開日： 中華民國 99 (2010) 年 10 月 16 日

(21)申請案號：098112269 (22)申請日： 中華民國 98 (2009) 年 04 月 14 日
(51)Int. Cl.： *G06F3/06 (2006.01)* *G06F21/00 (2006.01)*
(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：陳建廷 CHEN, JIAN TING (TW) ；陳昱翰 CHEN, YU HAN (TW) ；廖倫德 LIAO, LUN DE (TW) ；趙昌博 CHAO, PAUL C. P. (TW)
(74)代理人：蔡朝安；鄭淑芬
申請實體審查：有 申請專利範圍項數：13 項 圖式數：4 共 14 頁

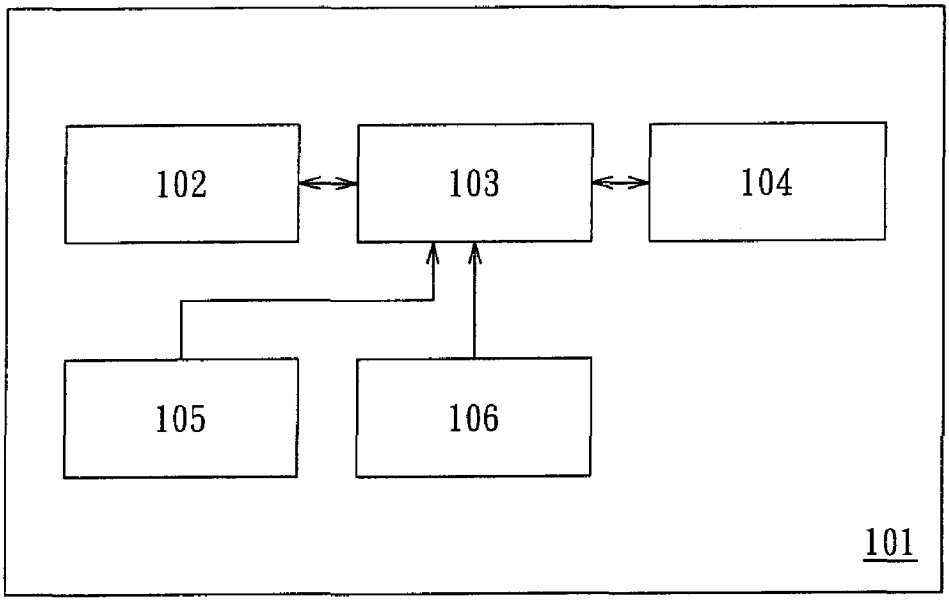
(54)名稱

具安全防護裝置的隨身碟

FLASH DRIVE WITH SECURITY DEVICE

(57)摘要

一種具安全防護裝置的隨身碟，其利用控制器讀取密碼鎖之設定以准許或否准電腦經由連接埠將資料寫入隨身碟的記憶體，並利用連接控制鍵安全地控制隨身碟與電腦之間的斷連。隨身碟的控制器驗證密碼鎖之密碼與電腦使用者之密碼，以避免未經驗證的資料從電腦寫入隨身碟。另外，隨身碟利用控制器接收連結控制鍵的指令而安全地與電腦斷連，以避免不當地拔出隨身碟而毀損儲存於隨身碟的資料，或者輕易地連接。



101：隨身碟
102：USB 介面
103：控制器
104：記憶體
105：連結控制鍵
106：密碼鎖

201037596

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：P8112269

※申請日：98.4.14 ※IPC分類：G06F 3/06 (2006.01)

G06F 21/00 (2006.01)

一、發明名稱：（中文/英文）

具安全防護裝置的隨身碟/FLASH DRIVE WITH SECURITY DEVICE

二、中文發明摘要：

一種具安全防護裝置的隨身碟，其利用控制器讀取密碼鎖之設定以准許或否准電腦經由連接埠將資料寫入隨身碟的記憶體，並利用連接控制鍵安全地控制隨身碟與電腦之間的斷連。隨身碟的控制器驗證密碼鎖之密碼與電腦使用者之密碼，以避免未經驗證的資料從電腦寫入隨身碟。另外，隨身碟利用控制器接收連結控制鍵的指令而安全地與電腦斷連，以避免不當地拔出隨身碟而毀損儲存於隨身碟的資料，或者輕易地連接。

三、英文發明摘要：

A flash drive equipped security devoice is disclosed. The flash drive uses a communication controller to read a setting of a password lock to permit writing data into the flash drive from a computer through a connection port, and uses an automatic communication switch to connect with or cut off from the computer. The communication controller authenticates a password of the password lock and the user's password of the computer for avoid wirting data without authenticating to the disk of the flash drive. Besides, the communication controller receives an instruction of the automatic communication switch to connect with or cut off from the computer to avoid damaging the stored data when improperly pulling the .flash drive out, or builds the connection easily..

四、指定代表圖：

(一)本案指定代表圖為：圖 1。

(二)本代表圖之元件符號簡單說明：

101　隨身碟

102　USB 介面

103　控制器

104　記憶體

105　連結控制鍵

106　密碼鎖

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隨身碟，尤其是一種具安全防護裝置的隨身碟。

【先前技術】

目前攜帶電子資料最常用的方式之一是將電子資料儲存於透過通用匯流排介面(universal serial bus, USB)連接電腦的隨身碟，亦稱為行動碟。然而，一般的隨身碟並不具備安全防護的功能，因此資料常常因軟體或硬體的不當操作而遺失、被竊取或損毀，列舉如下：

(1) 軟體上惡意的存取：存取隨身碟的資料已成為不當程式竊取重要資料或散布病毒的重要媒介；以及

(2) 硬體上不當的拔除：未執行卸除隨身碟的指令即拔除已連接電腦的隨身碟，進而造成隨身碟的損毀。

本發明所提出的安全防護方案可有效降低或避免軟體上或硬體上的不當操作，因此可避免隨身碟的資料遺失、被竊取或損毀，並可進一步提升隨身碟的便利性。

【發明內容】

為提升電子資料的安全保護、避免不當的資料存取以及提升隨身碟的便利性，本發明的主要特徵摘要如下：

(1) 密碼鎖(或稱為電子開關)與安全防護韌體：

密碼鎖用以設定及儲存安全密碼；安全防護韌體用以驗證密碼鎖之密碼與電腦使用者之密碼，僅在驗證通過後，始得寫入資料至記憶體，因此可有效防止電腦自動寫入資料至隨身碟。

(2) 連結控制鍵：

觸壓連結控制鍵後，控制器會安全地斷開記憶體與電腦之間的連結，因此可避免使用者不當地拔出隨身碟而毀損儲存於隨身碟的資料。

(3) 提升便利性：

密碼鎖可以是一種電子鎖(或電子開關)，所設定的安全密碼可顯示在硬體上，以避免使用者忘記安全密碼，並可同時避免電腦自動寫入資料至隨身碟；連結控制鍵可透過控制器送出卸除指令，以安全地斷開該隨身碟與該電腦之間的連結，因此使用者無須在電腦上執行卸除隨身碟的指令，進而提升了隨身碟操作的便利性；或者連接於電腦的隨身碟為退出狀態，亦可利用連結控制鍵執行連接指令而與電腦重新建立連接。

【實施方式】

本發明所建議方案利用密碼鎖、安全防護韌體以及連結控制鍵等裝置提昇隨身碟的安全防護措施以避免硬體上或軟體上不當地操作，同時提升隨身碟的便利性，以下利用實施例並配合圖式說明本發明之技術特徵。

本發明一實施例之結構方塊圖，如圖 1。隨身碟 101 以一通用匯流排(universal serial bus, USB)連接埠做為通訊介面，稱為 USB 介面 102。記憶體 104 用以儲存資料，控制器 103 連接於 USB 介面 102 與記憶體 104 以控制電腦與隨身碟 101 間的通訊。密碼鎖 106 與連結控制鍵 105 連接於控制器 103，分別控制寫入的准否以及隨身碟 101 與電腦間通訊的斷連(connection and disconnection)。另外，隨身碟 101 具有一外殼以保護內部電子元件，外殼未示於圖 1。

控制器 103 儲存安全防護韌體以及執行安全防護韌體。密碼鎖 106 為一電子鎖，可採用數位電子鎖或二元電子鎖，是一種利用 IC 電路實作的電子鎖，可避免軟體式的防護鎖易於被入侵的缺點；另外，密碼鎖 106 具有一顯示介面，用以呈現密碼鎖 106 所設定的密碼，以避免

使用者忘記安全密碼。當電腦傳輸資料至隨身碟 101 時，控制器 103 讀取密碼鎖 106 的密碼以及電腦使用者的密碼，並透過安全防護韌體驗證密碼鎖 106 的密碼與電腦使用者的密碼。若驗證成功，則控制器 103 准許資料寫入記憶體 104；反之，若驗證失敗，則控制器 103 不准資料寫入記憶體 104。

控制器 103 可接收連結控制鍵 105 的指令，而安全地斷開或建立記憶體 104 與電腦之間的連結。 當連接於電腦的隨身碟未執行卸除指令時，使用按下連接控制鍵以發出卸除指令，因此隨身碟可自由的卸除；或者連結於電腦的隨身碟實際上已卸除，使用者可藉由連結控制鍵 105 建立隨身碟與電腦之通訊。

本發明之一實施例是利用密碼驗證的方法來防止電腦自動寫入資料至隨身碟 101。密碼驗證的方法是在電腦傳輸資料至隨身碟 101 時，驗證密碼鎖 106 所設定密碼與電腦使用者密碼，若驗證成功，始准許資料寫入至隨身碟 101 的記憶體 104，反之則拒絕資料寫入隨身碟。驗證密碼的方法以安全防護韌體方式紀錄於控制器 103。以下圖 2a 與圖 2b 所示實施例，說明本發明資料寫入的安全防護方法之精神。

如圖 2a 所示實施例之資料寫入的安全防護方法，包括下列步驟。當電腦傳輸資料至隨身碟時，讀取使用者輸入至電腦的驗證密碼(S100)，並讀取密碼鎖所設定之安全密碼(S200)。然後，驗證電腦使用者的密碼以及密碼鎖的密碼(S300)。若驗證成功，則准許資料寫入至隨身碟(S400)；若驗證失敗，則不准資料寫入至隨身碟(S500)。

如圖 2b 所示實施例之資料寫入的安全防護方法，與上述的驗證方法的差異在於計算驗證失敗次數，詳細說明如下：

當電腦傳輸資料至隨身碟時，讀取電腦使用者的密碼(S100)，讀取密碼鎖所設定的密碼(S200)。然後，驗證電腦使用者的密碼以及密碼鎖之密碼(S300)。若驗證成功，則准許資料寫入至隨身碟(S400)；若驗證失敗，則計數驗證失敗的次數(S600)，並比較驗證失敗次數與一

臨界值(S610)。若驗證失敗的次數高於臨界值，則判斷資料為惡意寫入操作，不准資料寫入至隨身碟(S500)；若驗證失敗的次數未達臨界值，則要求使用者重新輸入驗證密碼，並持續驗證二密碼 (S300)。

驗証電腦用者的密碼與密碼鎖的密碼(S300)可以直接比對二者是否一致，一致時表示成功，不一致表示失敗；或是驗證一演算法，即電腦使用者的密碼及/或密碼鎖的密碼經由演算法後所得到真假值，分別表示驗證成功及失敗。

另外，判斷驗證密碼與安全密碼不一致或判斷為惡意寫入後，控制器 103 可發出警告信息，其可以於電腦的一顯示器顯示對話框的方式通知使用者，或者是使設置於隨身碟上的一顯示燈顯示一信息燈號的方式通知使用者。

圖 3a 與圖 3b 所示分別為數位式電子鎖與二元式電子鎖的實施例。圖 3a 所示隨身碟之外殼具有控制鍵 105 與數位式電子鎖 106。電子鎖 106 的位元數目可依需求調整，此實施例是三個位元的電子鎖。電子鎖 106 的每一個位元的值可以是數字、字元或是其組合，每一個位元的值可藉由設定鈕 107 設定位元的值，此三個位元所設定的位元值構成密碼。

圖 3b 所示隨身碟之外殼具有控制鍵 105 與二元式電子鎖 106。電子鎖 106 的位元數目可依需求調整，此實施例是四個位元的電子鎖，電子鎖 106 每一個位元的值可為真或假，利用此四個位元值構成密碼。

圖 4 所示隨身碟之實施例，除具有控制鍵 105 與數位式電子鎖 106 外，更包含一顯示燈 108，用以顯示驗證密碼與安全密碼不一致的信息燈號。

以上所述之實施例僅係為說明本發明之技術思想及特點，其目的在使熟習此項技藝之人士能夠瞭解本發明之內容並據以實施，當無法以之限定本發明之專利範圍，即大凡依

本發明所揭示之精神所作之均等變化或修飾，仍應涵蓋在本發明之專利範圍內。

【圖式簡單說明】

圖 1 所示為本發明具安全防護的隨身碟實施例之架構圖。

圖 2a 與圖 2b 所示為本發明密碼驗證方法實施例之流程圖。

圖 3a 與圖 3b 所示為本發明具安全防護的隨身碟實施例之外觀示意圖，用以說明數位式電子鎖與二元式電子鎖。

圖 4 所示為本發明具安全防護的隨身碟實施例之外觀示意圖，用以說明顯示驗證燈號之信息燈。

【主要元件符號說明】

101　隨身碟

102　USB 介面

103　控制器

104　記憶體

105　連結控制鍵

106　密碼鎖

107　設定鈕

108　顯示燈

S100、S200、S300、S400、S500、S600、S610　步驟

七、申請專利範圍：

1. 一種具安全防護功能的隨身碟，包含：

一連接埠，用以連接一電腦；

一記憶體；

一控制器，設置於該連接埠與該記憶體間，用以儲存及執行一安全防護韌體；以及

一密碼鎖，連接該控制器，其中該安全防護韌體驗證該密碼鎖之密碼與該電腦密碼，以判斷該外部電腦是否可寫入一資料至該記憶體。

2. 如請求項 1 所述之具安全防護功能的隨身碟，其中該密碼鎖為一電子鎖。

3. 如請求項 1 所述之具安全防護功能的隨身碟，其中該密碼鎖具有一顯示介面，用以呈現該密碼鎖所設定之一安全密碼。

4. 如請求項 1 所述之具安全防護功能的隨身碟，其中該電腦傳輸該資料至該記憶體時，該控制器執行該安全防護韌體之方法，其驗證該密碼鎖之密碼與該電腦之使用者密碼，以准許或拒絕寫入該資料至該記憶體。

5. 如請求項 4 所述之具安全防護功能的隨身碟，更包含一顯示燈，連接該控制器，其中當驗證失敗時，該顯示燈顯示一信息燈號。

6. 如請求項 1 所述之具安全防護功能的隨身碟，更包含一連結控制鍵，連接該控制器，用以接收一觸壓動作而使該控制器安全地卸除/建立該記憶體與該電腦間的連結。

7. 一種資料寫入的安全防護方法，用以驗證一電腦將一資料寫入一隨身碟之操作，該資料寫入的安全防護方法包含：

當該電腦傳輸該資料至該隨身碟時，讀取該隨身碟的一密碼鎖所設定之一安全密碼，並讀取該電腦之一使用者密碼；以及

驗證該安全密碼與該使用者密碼，若驗證成功，則准許該資料寫入

該隨身碟；若驗證失敗，則否准該資料寫入該隨身碟。

8. 如請求項 7 所述之資料寫入的安全防護方法，於驗證密碼之步驟是比對該安全密碼與該使用者密碼是否一致，若一致表示驗證成功，若不一致表示驗證失敗。

9. 如請求項 7 所述之資料寫入的安全防護方法，於驗證密碼之步驟是驗證一演算法，其利用該安全密碼與該使用者密碼經由一演算法以得到一真假值，用以表示驗證成功或驗證成功失敗。

10. 如請求項 7 所述之資料寫入的安全防護方法，更包含計算驗證失敗的次數，其中若驗證失敗的次數達到一臨界值，則判斷該次寫入為惡意寫入。

11. 如請求項 10 所述之資料寫入的安全防護方法，於判斷為惡意寫入時，更包含發出一警告信息之步驟。

12. 如請求項 11 所述之資料寫入的安全防護方法，其中發出該警告信息係於該電腦的一顯示器顯示一信息對話框。

13. 如請求項 11 所述之資料寫入的安全防護方法，其中發出該警告信息係於該隨身碟顯示一信息燈號。

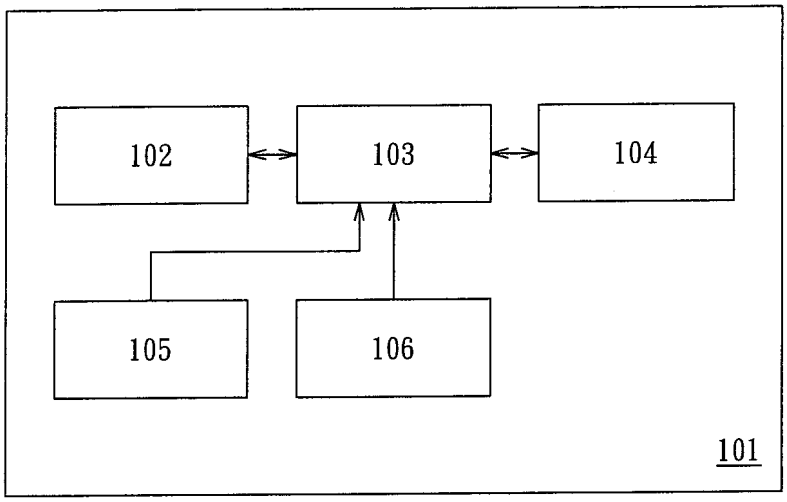

102
103
104
105
106
101

圖1

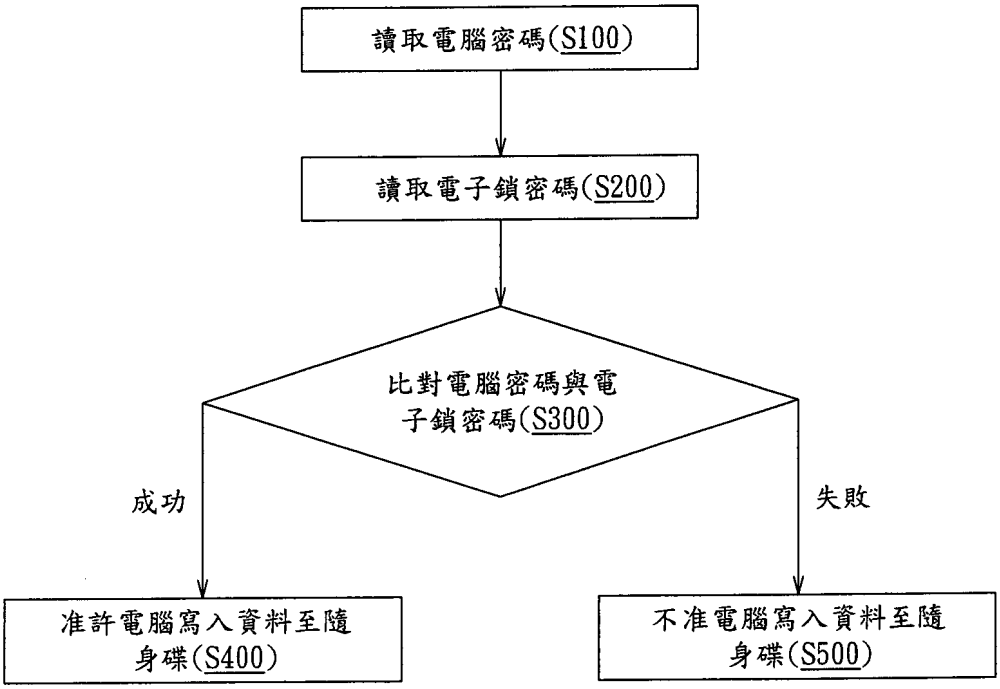

讀取電腦密碼(S100)
讀取電子鎖密碼(S200)
比對電腦密碼與電子鎖密碼(S300)
成功
失敗
准許電腦寫入資料至隨身碟(S400)
不准電腦寫入資料至隨身碟(S500)

圖2a

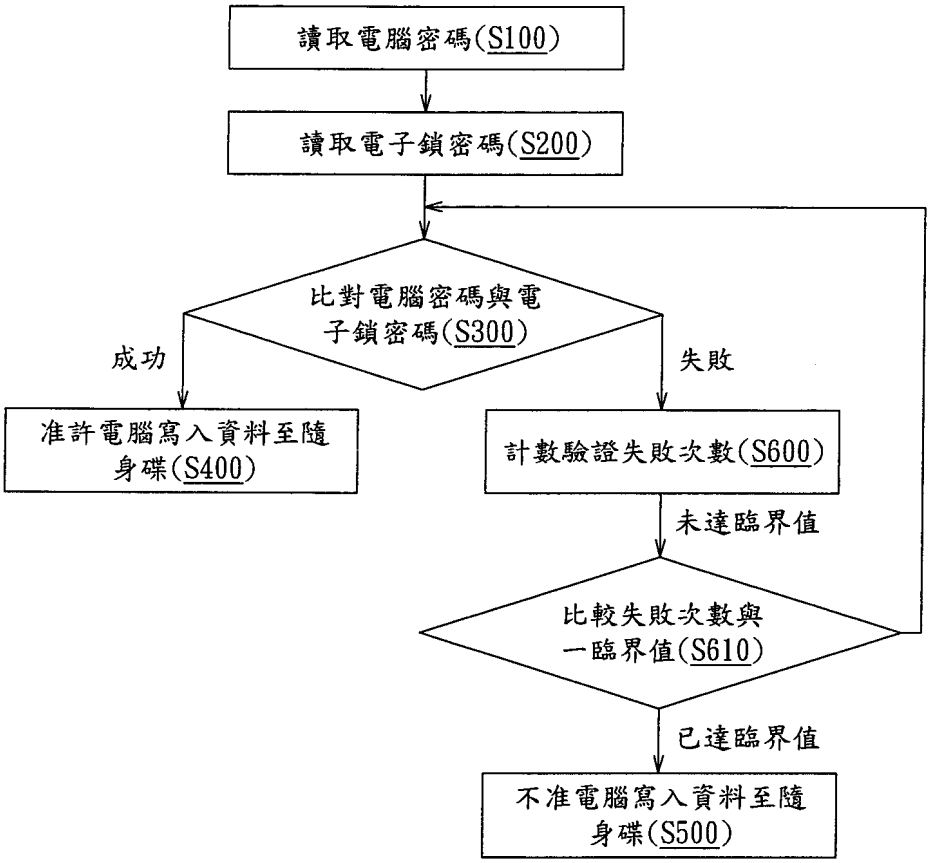

讀取電腦密碼(S100)
讀取電子鎖密碼(S200)
比對電腦密碼與電子鎖密碼(S300)
成功
失敗
准許電腦寫入資料至隨身碟(S400)
計數驗證失敗次數(S600)
未達臨界值
比較失敗次數與一臨界值(S610)
已達臨界值
不准電腦寫入資料至隨身碟(S500)

圖2b

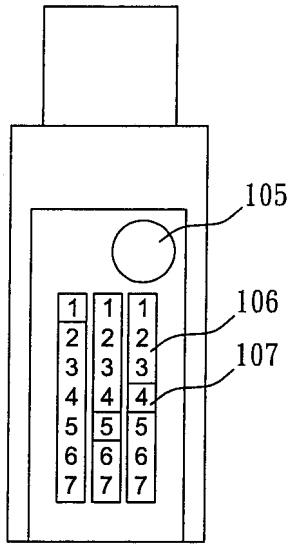

105
106
107
1 2 3 4 5 6 7
1 2 3 4 5 6 7
1 2 3 4 5 6 7

圖3a

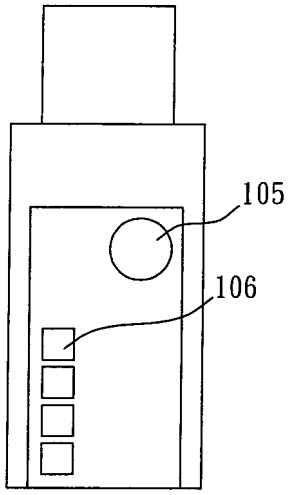


圖3b

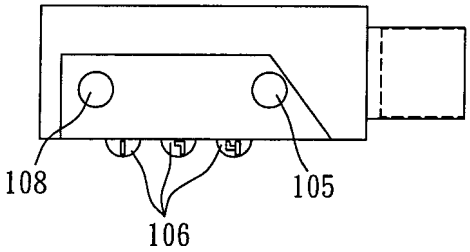


圖4