100-7-21

公告本

修正補充 本100年7月27日 P1~P20

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：95139742

※ 申請日期：95、10、27　　※IPC 分類：H04N 7/16 (2011.01)

G06F 3/14 (2006.01)

一、發明名稱：（中文/英文）

用於顯示裝置之防護系統與方法

PROTECTION SYSTEM FOR DISPLAY APPARATUS AND METHOD THEREOF

二、申請人：（共 1 人）

姓名或名稱：（中文/英文）

中強光電股份有限公司/CORETRONIC CORPORATION

代表人：（中文/英文）張威儀/WADE CHANG

住居所或營業所地址：（中文/英文）

新竹科學工業園區新竹市力行路 11 號/NO. 11, LI-HSIN RD, SCIENCE-BASED INDUSTRIAL PARK, HSINCHU, TAIWAN, R.O.C.

國　籍：（中文/英文）中華民國/TW

三、發明人：（共 2 人）

姓　名：（中文/英文）

1. 吳草旺 / Chao-Wang Wu
2. 鄭連福 / Lien-Fu Cheng

國　籍：（中文/英文）1-2. 中國民國/TW

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：

☐ 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。

五、中文發明摘要：

一種用於顯示裝置之防護系統與方法，防護系統包含電子鑰匙及防護模組。防護系統利用多組密碼進行驗證且在每次完成驗證後更新密碼來提高顯示裝置的安全防護。在驗證上，只要電子鑰匙中其中一組密碼符合即允許啟動顯示裝置，而在完成驗證後即逐一進行密碼的更新，利用上述之驗證方式與逐次更新的方式可提高防護系統的方便性與安全性。

六、英文發明摘要：

A protection system for a display apparatus and the method thereof are provided. The protection system comprises an electrical key and a protection module. The protection system performs the security identification with a plurality of group of codes and updates the plurality of group of codes after the security identification finished in every time to improve the security of the display apparatus. In the security identification, the display apparatus is permitted to be turned on while one group of codes is correct, and the plurality of group of codes are updated code by code after the security identification finished. The protection system has higher convenience and security with the methods for the security identification and updating the codes.

七、指定代表圖：

(一)本案指定代表圖為：圖 4

(二)本代表圖之元件符號簡單說明:

C1、C2：第一驗證碼

D1、D2：第一密碼

E1、E2：第二驗證碼

F1、F2：第二密碼

ES：電子鎖電子信號

OS：原始電子信號

403：顯示裝置

205：防護模組

101：電子鑰匙

201：備用電子鑰匙

107：連接器

410：信號切換器

420：處理器

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

九、發明說明：

【發明所屬之技術領域】

本發明是有關於一種電子防護系統，且特別是有關於一種用於顯示裝置之防護系統與方法。

【先前技術】

目前顯示裝置所使用的防盜及資料保密方式，可分為硬體或軟體兩種防護方式。常用的硬體防護方式是採用機械鎖搭配金屬鑰匙，但金屬鑰匙容易遭到複製或盜取，一旦鑰匙被他人拿去複製，便能輕易開鎖而使用顯示裝置。

而常見的軟體防護方式是由加/解密程式來進行資料保密，例如螢幕保護程式，但一般使用者為容易記住密碼與使用方便，所設定的密碼通常都不長，容易遭到破解。此外，尚有利用電子鎖的防護方式，而電子鑰匙中若以固定的電子密碼來防護顯示裝置，則容易被盜拷或破解，若採用微處理器進行密碼的加解密，則其成本太高，且通常電子鑰匙僅有一把，若不甚遺失，即會造成工作的不便。

【發明內容】

本發明的目的其中之一是在提供一種用於顯示裝置之防護系統，利用逐次更新密碼的方式，來防止與提早發現電子鑰匙被盜拷的情況發生。

本發明的目的其中之一是在提供一種用於顯示裝置之防護系統，利用可同時設置兩組密碼獨立的電子鑰匙，以增加使用者的方便性。

本發明的目的其中之一是在提供一種用於顯示裝置之防護方法，藉由比對電子鑰匙的多組密碼與顯示裝置的多組驗證碼的方式，決定是否允許啟動顯示裝置，並在每次辨識密碼成功後，逐一更新密碼及驗證碼，以提高使用上的安全性。

為達到上述與其他目的，本發明提出一種用於顯示裝置之防護系統，此防護系統包含電子鑰匙、連接器、防護模組與信號切換器。其中，電子鑰匙具有第一記憶體，其用以儲存多個第一密碼。連接器設置於顯示裝置之中並適於連接電子鑰匙。防護模組設置於顯示裝置之中並具有第二記憶體及微處理器，第二記憶體用以儲存多個第一驗證碼，該些第一驗證碼對應於該些第一密碼。信號切換器耦接於連接器與防護模組之間，用以切換顯示裝置的電子信號與防護系統的電子信號。當電子鑰匙連接至顯示裝置之連接器時，信號切換器透過連接器接收防護系統的電子信號給微處理器，並使防護模組致能，藉此防護模組之微處理器逐一比對該些第一密碼與該些第一驗證碼，若該些第一密碼其中之一與該些第一驗證碼其中之一相符，則允許啟動顯示裝置且防護模組之微處理器逐一更新各該第一密碼以及與各該第一密碼所對應的第一驗證碼，更新後之該些第一密碼對應於更新後之該些第一驗證碼，若該些第一密碼與該些第一驗證碼都不相符，則禁止啟動顯示裝置。另外，當顯示裝置在該些第一密碼其中之一與該些第一驗證碼其中之一相符的條件下而允許被啟動，且電子鑰匙從

顯示裝置之連接器被移除時，信號切換器致使防護模組失能，藉此信號切換器透過連接器接收顯示裝置的電子信號給微處理器。

在本發明另一實施例中，上述防護系統包括一備用電子鑰匙，用以儲存多個第二密碼，而防護模組則包括多個第二驗證碼，第二驗證碼對應於第二密碼。其中，當備用電子鑰匙連接至顯示裝置時，防護模組逐一比對第二密碼與第二驗證碼，若第二密碼其中之一與第二驗證碼其中之一相符時，則允許啟動該顯示裝置並逐一更新各該第二密碼以及與各該第二密碼所對應的第二驗證碼。上述備用電子鑰匙中第二密碼與第二驗證碼的比對與更新方式上述電子鑰匙相似，在此不加累述。

在本發明又一實施例中，微處理器對所接收之顯示裝置的電子信號進行處理，藉以致使顯示裝置顯示影像。

本發明另提出一種防護方法，其中顯示裝置耦接防護系統，防護方法包含下列步驟：判斷一電子鑰匙是否連接於一顯示裝置之一連接器；當該電子鑰匙連接於該顯示裝置之該連接器時，透過該顯示裝置之該連接器接收該防護系統的電子信號給設置在該顯示裝置中的一微處理器，並使該防護系統致能，藉以透過該微處理器逐一比對該電子鑰匙中之多個第一密碼與該顯示裝置之多個第一驗證碼，若該些第一密碼其中之一與該些第一驗證碼其中之一相符，則允許啟動該顯示裝置並透過該微處理器逐一更新各該第一密碼以及與各該第一密碼所對應的第一驗證碼，更

新後之該些第一密碼對應於更新後之該些第一驗證碼，若判斷該些第一密碼與該些第一驗證碼皆不相符，則禁止啟動該顯示裝置；以及當該電子鑰匙從該顯示裝置之該連接器被移除，且該顯示裝置在該些第一密碼其中之一與該些第一驗證碼其中之一相符的條件下而允許被啟動時，透過該顯示裝置之該連接器接收該顯示裝置的電子信號給該微處理器，並使該防護系統失能。

在本發明另一實施例中，上述之防護方法，其中更包括判斷備份電子鑰匙是否連接於顯示裝置之連接器；以及當備份電子鑰匙連接於顯示裝置之連接器時，透過顯示裝置之連接器接收防護系統的電子信號給微處理器，並使防護系統致能，藉以透過微處理器逐一比對備份電子鑰匙中之多個第二密碼與顯示裝置之多個第二驗證碼，若該些第二密碼中其中之一與該些第二驗證碼其中之一相符，則允許啟動顯示裝置。上述之防護方法之其餘細節均以詳述於上述防護系統之說明中，在本技術領域具有通常知識者，經由本發明之揭露，應可輕易推知，在此不加累述。

在本發明另一實施例中，上述之防護方法，其中更包括微處理器對所接收之顯示裝置的電子信號進行處理，以致使顯示裝置顯示影像

綜上所述，由於本發明利用逐次更新密碼的方式，因此可有效防止電子鑰匙被盜拷的情況發生。在每次使用後，上一筆密碼隨即失效，所以盜拷的電子鑰匙會在原電子鑰匙使用後失效。而使用者亦可經由原電子鑰匙的失效

與否，判斷是否有被盜拷的情況發生。而電子鑰匙中的密碼採取逐一更新以及逐一比對的方式來進行密碼驗證與比對，可避免因部分密碼資料毀損而無法繼續使用的缺點。另外，本發明更利用備用鑰匙的觀念，同時設置兩組密碼獨立的電子鑰匙，以增加使用者的方便性，避免工作延誤。

為讓本發明之上述和其他目的、特徵和優點能更明顯易懂，下文特舉較佳實施例，並配合所附圖式，作詳細說明如下。

【實施方式】

圖 1 為根據本發明一實施例之用於顯示裝置之防護系統之方塊圖。防護系統 100 包含電子鑰匙 101、防護模組 105 及連接器 107。防護模組 105 及連接器 107 設置於顯示裝置 103 之中，連接器 107 可用以連接電子鑰匙 101。電子鑰匙 101 可藉由連接器 107 與防護模組 105 進行溝通，其中，連接器 107 的傳輸介面可為影像圖形陣列(Video Graphics Array, VGA)介面、RS232 介面、數位視覺介面(Digital Visual Interface , DVI)、通用串列匯流排(universal series bus, USB) 介面或者高品質多媒體影音介面(High-Definition Multimedia Interface, HDMI)等。而防護模組 105 與電子鑰匙 101 亦可經由無線傳輸介面來進行資料的傳遞，在本發明中並不限定電子鑰匙 101 與防護模組 105 之間的資料傳遞方式。

電子鑰匙 101 具有一記憶體用以儲存多個第一密碼 D1、D2。防護模組 105 具有一記憶體及一微處理器，防護模組 105 之記憶體用以儲存多個第一驗證碼 C1、C2，第一

驗證碼 C1、C2 對應於第一密碼 D1、D2。而電子鑰匙 101 與防護模組 105 採用的記憶體例如是可抹除可程式記憶體 (erasable programmable read only memory，EPROM)。而防護模組 105 之記憶體亦可利用顯示裝置 105 中所設置的記憶體來達成。而防護模組 105 之微處理器的運算功能可利用顯示裝置 103 中負責處理影像顯示的微處理器來加以實現，並不需要另外設置獨立的微處理器，以降低設計成本。而本實施例中所提及之顯示裝置亦可為投影機等類似之顯示裝置，其中，防護模組則可利用投影機中之微處理器，例如 DDP2000，來進行密碼驗證的工作。

在防護系統 100 致能時，防護模組 105 會判斷電子鑰匙 101 是否連接至顯示裝置 103；當電子鑰匙 101 經由連接器 107 連接至顯示裝置 103 時，防護模組 105 利用微處理器逐一比對第一密碼 D1、D2 與第一驗證碼 C1、C2，若第一密碼 D1、D2 其中之一與第一驗證碼 C1、C2 其中之一相符，則允許啟動顯示裝置 103；若第一密碼 D1、D2 與第一驗證碼 C1、C2 皆不相符，則禁止啟動顯示裝置 103。

此外，當第一密碼 D1、D2 與第一驗證碼 C1、C2 比對完成，並允許啟動顯示裝置 103 時。防護模組 105 之微處理器會自動地逐一更新第一密碼 D1、D2 與第一驗證碼 C1、C2，更新後之第一密碼 D1、D2 對應於更新後之第一驗證碼 C1、C2。而在完成驗證碼的比對及更新之後，便可以移除所使用的電子鑰匙 101，以防止顯示裝置 203 與所使用的電子鑰匙同時被偷。

在每次使用後，藉由第一密碼 D1、D2 與第一驗證碼 C1、C2 的自動更新，可提高安全性，避免密碼遭到破解與複製。而新密碼的產生，會因時間因素、密碼原則與不同產品而有所變異，因此不同裝置每次會產生不同的新密碼，以供下次驗證所使用。由於電子鑰匙的密碼會因使用而改變，因此當電子鑰匙被拷貝時，等到原電子鑰匙產生新密碼後，拷貝的電子鑰匙即失去功用。反之，若拷貝的電子鑰匙先使用，則原電子鑰匙會失去功用，進而提醒保管者電子鑰匙可能有被盜用的情況發生而加以防範。

而逐一更新密碼與驗證碼的做法，其主要作用是在讀取或更新密碼過程中，若不小心移除電子鑰匙或是發生斷電等意外，也只會造成電子鑰匙之多個密碼的其中之一被毀損，其餘密碼並未受到波及。因此，電子鑰匙仍然可以保有應有的功能，也就是以密碼作為辨識保護之用。當然，上述方式亦適用於多個密碼與多個驗證碼之比對，在本技術領域具有通常知識者，經由本發明之揭露，應可輕易推知實施方式，在此不加累述。

另外，請參照圖 2，防護模組 205 可更包含一備用電子鑰匙。電子鑰匙 101 與備用電子鑰匙 201 中所儲存的密碼互為獨立，並不互相影響。使用者可藉由電子鑰匙 101 或備用電子鑰匙 201 啟動顯示裝置 203。由於電子鑰匙有兩套（包括備用電子鑰匙），一旦不慎遺失其中一套電子鑰匙，尚有備分電子鑰匙可使用，不會造成工作的延誤。

備用電子鑰匙 201 具有一記憶體，記憶體用以儲存多

個第二密碼，在本實施例中則以兩個第二密碼 F1、F2 為例。防護模組 205 之記憶體中則儲存有對應於電子鑰匙 101 與備用電子鑰匙 201 的第一驗證碼 C1、C2 與第二驗證碼 E1、E2。當電子鑰匙 101 或備用電子鑰匙 201 連接至顯示裝置 205 時，防護模組 205 會根據相對應的驗證碼，決定是否允許啟動顯示裝置 203。而在完成驗證碼的比對之後，便可以移除所使用的電子鑰匙 101 或備用電子鑰匙 201，以防止顯示裝置 203 與所使用的電子鑰匙同時被偷。

關於防護模組 205 對於顯示裝置 203 的啟動防護功能，則可依照使用需求，設定為重新插拔電源（如外部的交流（AC）電源）時才需要重新驗證電子鑰匙（電子鑰匙 101 或備用電子鑰匙 201）。或者設定為每次當顯示裝置開機（例如啟動顯示裝置上的電源開關（POWER ON），此方式可適用於使用電池的顯示裝置）時，即需要重新驗證電子鑰匙。亦可設定為在一預定時間中未使用顯示裝置即需要重新驗證電子鑰匙，如同螢幕保護程式。

接下來，以流程圖進一步說明本發明之防護方法，請參閱第 3 圖。首先，在步驟 S310 中，判斷電子鑰匙 101 是否連接於顯示裝置 203。若電子鑰匙 101 連接於顯示裝置，則進行步驟 S350，讀取電子鑰匙 101 中之多個第一密碼 D1、D2，並辨識這些第一密碼 D1、D2 中其中之一與顯示裝置 203 中第一驗證碼 C1、C2 之其中之一是否相符，若其中之一相符，則進入步驟 S360，逐一更新第一密碼 D1、D2 與第一驗證碼 C1、C2，並允許啟動顯示裝置 203。若

皆不符合，則進入步驟 S370，禁止啟動顯示裝置 203。

在步驟 S310 中，若電子鑰匙 101 未連接於顯示裝置 203 時，則進行步驟 S320，也就是判斷備份電子鑰匙 201 是否連接於顯示裝置 203，若備份電子鑰匙未連接於顯示裝置，則執行步驟 S370，禁止啟動顯示裝置；若備份電子鑰匙 201 連接於顯示裝置 205，則執行步驟 S330，讀取並比對備份電子鑰匙之多個第二密碼 F1、F2，判斷第二密碼 F1、F2 中與顯示裝置 203 中之第二驗證碼 E1、E2 是否相符，若其中之一相符，則逐一更新第二密碼 F1、F2 與第二驗證碼 E1、E2，並允許啟動顯示裝置 203(步驟 S340)。若皆不符合，則禁止啟動顯示裝置 203(步驟 S370)。關於本實施例中防護方法之其餘操作細節皆以詳述於上述圖 1、圖 2 之說明中，在此不加累述。

而防護系統 100 之連接器 107 可使用顯示裝置原有的連接器或增設一組新的連接器以作為防護系統之連接器 107，透過連接器 107 提供電子鑰匙（或備用電子鑰匙）與顯示裝置進行資料的傳遞。請參照圖 4，當連接器 107 採用顯示裝置原有的連接器時，防護系統 100 更包括一信號切換器 410，信號切換器 410 經由連接器 107 接收顯示裝置的電子信號(簡稱為原始電子信號 OS)或防護系統的電子信號(簡稱為電子鎖電子信號 ES)，顯示裝置 403 則可利用信號切換器 410 來切換原始電子信號 OS 與電子鎖電子信號 ES，而防護模組 205 則利用顯示裝置 403 中之處理器 420 的運算功能加以實現。請參閱圖 5，當顯示裝置 403 處於正

常操作的情況下時，信號切換器 410 則切換至原始電子信號 OS，並使防護模組 205 失能；當顯示裝置 403 需要重新驗證時，例如移除電源後的第一次電源開啟，信號切換器 410 則切換至電子鎖電子信號 ES，並致能防護模組 205，以驗證電子鑰匙，其驗證方式請參照上述圖 2 之說明，在此不加累述，在驗證完成後，信號切換器 410 則切換至原始電子信號 OS，以便進行影像的顯示。當然，亦可經由防護模組 205 來控制信號切換器 410 的資料傳輸類型。換言之，信號切換器 410 可在進行驗證時，使顯示裝置 403 的傳輸介面具有與電子鑰匙溝通的功能，而在移除電子鑰匙後，恢復顯示裝置 403 傳輸介面原有的功能。

在本發明另一實施例中，電子鑰匙與顯示裝置之間可藉由不同的連接器來進行資料的傳遞。如圖 6 所示，顯示裝置 603 具有不同介面之連接器 107、117、127，而電子鑰匙 101、111、121 則分別支援連接器 107、117、127 之傳輸介面。當顯示裝置 603 需要重新進行電子鑰匙的驗證時，使用者可使用電子鑰匙 101、111、121 其中之一來進行驗證，本實施例中則以電子鑰匙 101 為例。防護模組 205 可經由控制信號切換器來取得電子鑰匙 101 中之第一密碼以進行驗證，其驗證方式請參照圖 1～圖 5 之說明，在此不加累述。防護模組 205 亦可擴充為利用指紋、聲紋、光訊號等任何可用來分辨使用者的電子裝置，以增加防護模組 205 的防護功能與便利性。

本實施例中，電子鑰匙中的資料(即所謂密碼)可比傳

統密碼更為冗長(例如可達數十位元)，而使用者也不需記憶密碼內容，因此安全性與便利性大為提高。此外，在驗證為正確密碼後，也可自動加密及自動變更電子鑰匙中之密碼組。若接收到的資料錯誤則會重新要求執行驗證程序，直到驗證為正確之密碼資料為止，否則將無法開機或正常使用顯示裝置。因此，即使顯示裝置被盜取，亦無法正常啟動顯示裝置，不僅增加顯示裝置的安全性，亦降低顯示裝置被竊的風險。

由於顯示裝置在做完密碼確認工作後，會隨即更新電子鑰匙中既有的密碼，因此電子鑰匙中的密碼是會隨著每次使用而改變的，所以竊賊就算複製遺失的電子鑰匙，也會因其中的密碼與驗證碼不合而無法使用。若竊賊先使用複製的電子鑰匙，則會使被複製的電子鑰匙無法使用，使用者即可藉由原先電子鑰匙的失效與否推知是否有被盜用的情況發生，提高顯示裝置的安全控管。

雖然本發明已以較佳實施例揭露如上，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，當可作些許之更動與潤飾，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】

圖 1 為根據本發明之一實施例之用於顯示裝置之防護系統之方塊圖。

圖 2 為根據本發明另一實施例之用於顯示裝置之防護系統之方塊圖。

圖 3 為根據本發明另一實施例之用於顯示裝置之防護

方法之流程圖。

圖 4 為根據本發明另一實施例之用於顯示裝置之防護系統之方塊圖。

圖 5 為根據圖 4 之信號切換器之信號傳遞方式之示意圖。

圖 6 為根據本發明另一實施例之電子鑰匙與顯示裝置之連結關係示意圖。

【主要元件符號說明】

C1、C2：第一驗證碼

D1、D2：第一密碼

E1、E2：第二驗證碼

F1、F2：第二密碼

CS：控制信號

ES：電子鎖電子信號

OS：原始電子信號

S310～S370：流程圖步驟

100：防護系統

103、203、403、603：顯示裝置

105、205：防護模組

101、111、121：電子鑰匙

201：備用電子鑰匙

107、117、127：連接器

410：信號切換器

420：處理器

十、申請專利範圍：

1.一種用於顯示裝置之防護系統，包含：

一電子鑰匙，具有一第一記憶體用以儲存多個第一密碼；

一連接器，設置於該顯示裝置之中並適於連接該電子鑰匙；

一防護模組，設置於該顯示裝置中並具有一第二記憶體及一微處理器，該第二記憶體用以儲存多個第一驗證碼，該些第一驗證碼對應於該些第一密碼；以及

一信號切換器，耦接於該連接器與該防護模組之間，用以切換該顯示裝置的電子信號與該防護系統的電子信號；

其中，當該電子鑰匙連接至該顯示裝置之該連接器時，該信號切換器透過該連接器接收該防護系統的電子信號給該微處理器，並使該防護模組致能，藉此該防護模組之該微處理器逐一比對該些第一密碼與該些第一驗證碼，若該些第一密碼其中之一與該些第一驗證碼其中之一相符，則允許啟動該顯示裝置且該防護模組之該微處理器逐一更新各該第一密碼以及與各該第一密碼所對應的第一驗證碼，更新後之該些第一密碼對應於更新後之該些第一驗證碼，若該些第一密碼與該些第一驗證碼都不相符，則禁止啟動該顯示裝置，

其中，當該顯示裝置在該些第一密碼其中之一與該些第一驗證碼其中之一相符的條件下而允許被啟動，且該電

子鑰匙從該顯示裝置之該連接器被移除時，該信號切換器致使該防護模組失能，藉此該信號切換器透過該連接器接收該顯示裝置的電子信號給該微處理器。

2.如申請專利範圍第 1 項所述之用於顯示裝置之防護系統，其中該微處理器對所接收之該顯示裝置的電子信號進行處理，藉以致使該顯示裝置顯示影像。

3.如申請專利範圍第 1 項所述之用於顯示裝置之防護系統，更包括一備用電子鑰匙具有一第三記憶體，該第三記憶體用以儲存多個第二密碼，而該防護模組之該第二記憶體更包括多個第二驗證碼，該些第二驗證碼對應於該些第二密碼，其中當該備用電子鑰匙連接至該顯示裝置之該連接器時，該防護模組之該微處理器逐一比對該些第二密碼與該些第二驗證碼，若該些第二密碼其中之一與該些第二驗證碼其中之一相符時，則允許啟動該顯示裝置且該防護模組之該微處理器逐一更新各該第二密碼以及與各該第二密碼所對應的第二驗證碼，更新後之該些第二密碼對應於更新後之該些第二驗證碼。

4.如申請專利範圍第 1 項所述之用於顯示裝置之防護系統，其中該連接器可為一 VGA 介面、一 RS232 介面、一 DVI 介面、一 USB 介面或一 HDMI 介面。

5.如申請專利範圍第 1 項所述之用於顯示裝置之防護系統，更包括一無線通信介面，用以連接至該電子鑰匙。

6.一種用於顯示裝置之防護方法，其中該顯示裝置耦接一防護系統，該防護方法包括下列步驟：

判斷一電子鑰匙是否連接於一顯示裝置之一連接器；

當該電子鑰匙連接於該顯示裝置之該連接器時，透過該顯示裝置之該連接器接收該防護系統的電子信號給設置在該顯示裝置中的一微處理器，並使該防護系統致能，藉以透過該微處理器逐一比對該電子鑰匙中之多個第一密碼與該顯示裝置之多個第一驗證碼，若該些第一密碼其中之一與該些第一驗證碼其中之一相符，則允許啟動該顯示裝置並透過該微處理器逐一更新各該第一密碼以及與各該第一密碼所對應的第一驗證碼，更新後之該些第一密碼對應於更新後之該些第一驗證碼，若判斷該些第一密碼與該些第一驗證碼皆不相符，則禁止啟動該顯示裝置；以及

當該電子鑰匙從該顯示裝置之該連接器被移除，且該顯示裝置在該些第一密碼其中之一與該些第一驗證碼其中之一相符的條件下而允許被啟動時，透過該顯示裝置之該連接器接收該顯示裝置的電子信號給該微處理器，並使該防護系統失能。

7.如申請專利範圍第6項所述之用於顯示裝置之防護方法，更包括：

該微處理器對所接收之該顯示裝置的電子信號進行處理，以致使該顯示裝置顯示影像。

8.如申請專利範圍第6項所述之用於顯示裝置之防護方法，更包括：

判斷一備份電子鑰匙是否連接於該顯示裝置之該連接器；以及

當該備份電子鑰匙連接於該顯示裝置之該連接器時，透過該顯示裝置之該連接器接收該防護系統的電子信號給該微處理器，並使該防護系統致能，藉以透過該微處理器逐一比對該備份電子鑰匙中之多個第二密碼與該顯示裝置之多個第二驗證碼，若該些第二密碼中其中之一與該些第二驗證碼其中之一相符，則允許啟動該顯示裝置。

9.如申請專利範圍第8項所述之用於顯示裝置之防護方法，其中於比對該些第二密碼之步驟中，若該些第二密碼其中之一與該些第二驗證碼其中之一相符，則逐一更新各該第二密碼以及與各該第二密碼所對應的第二驗證碼，更新後之該些第二密碼對應於更新後之該些第二驗證碼。

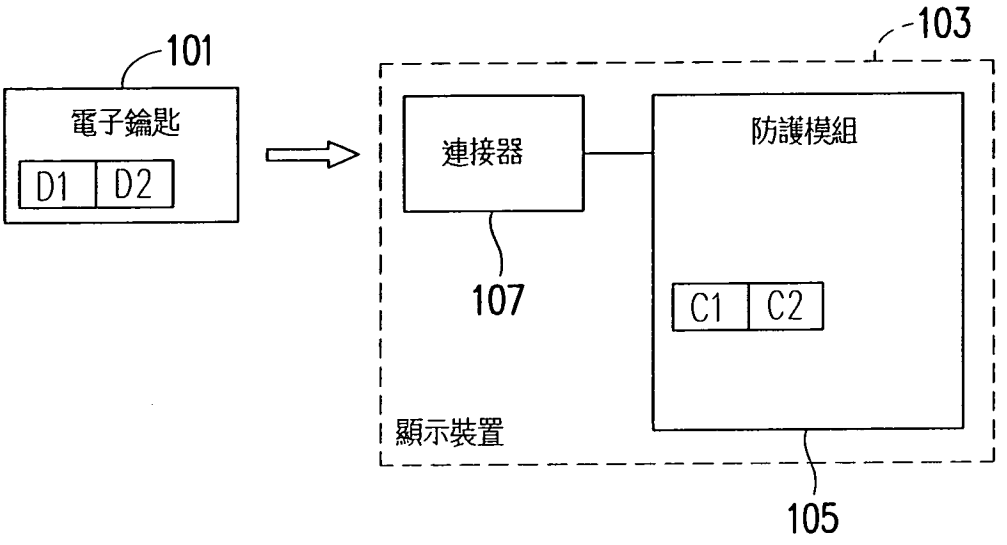
101
電子鑰匙
D1
D2
103
連接器
107
防護模組
C1
C2
顯示裝置
105

圖 1

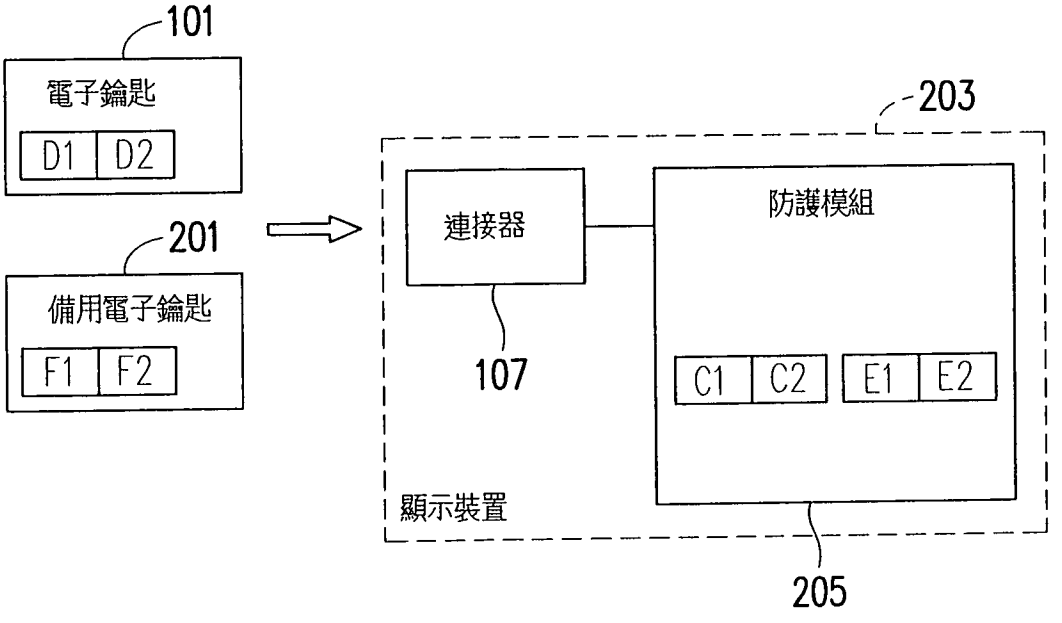
101
電子鑰匙
D1
D2
201
備用電子鑰匙
F1
F2
203
連接器
107
防護模組
C1
C2
E1
E2
顯示裝置
205

圖 2

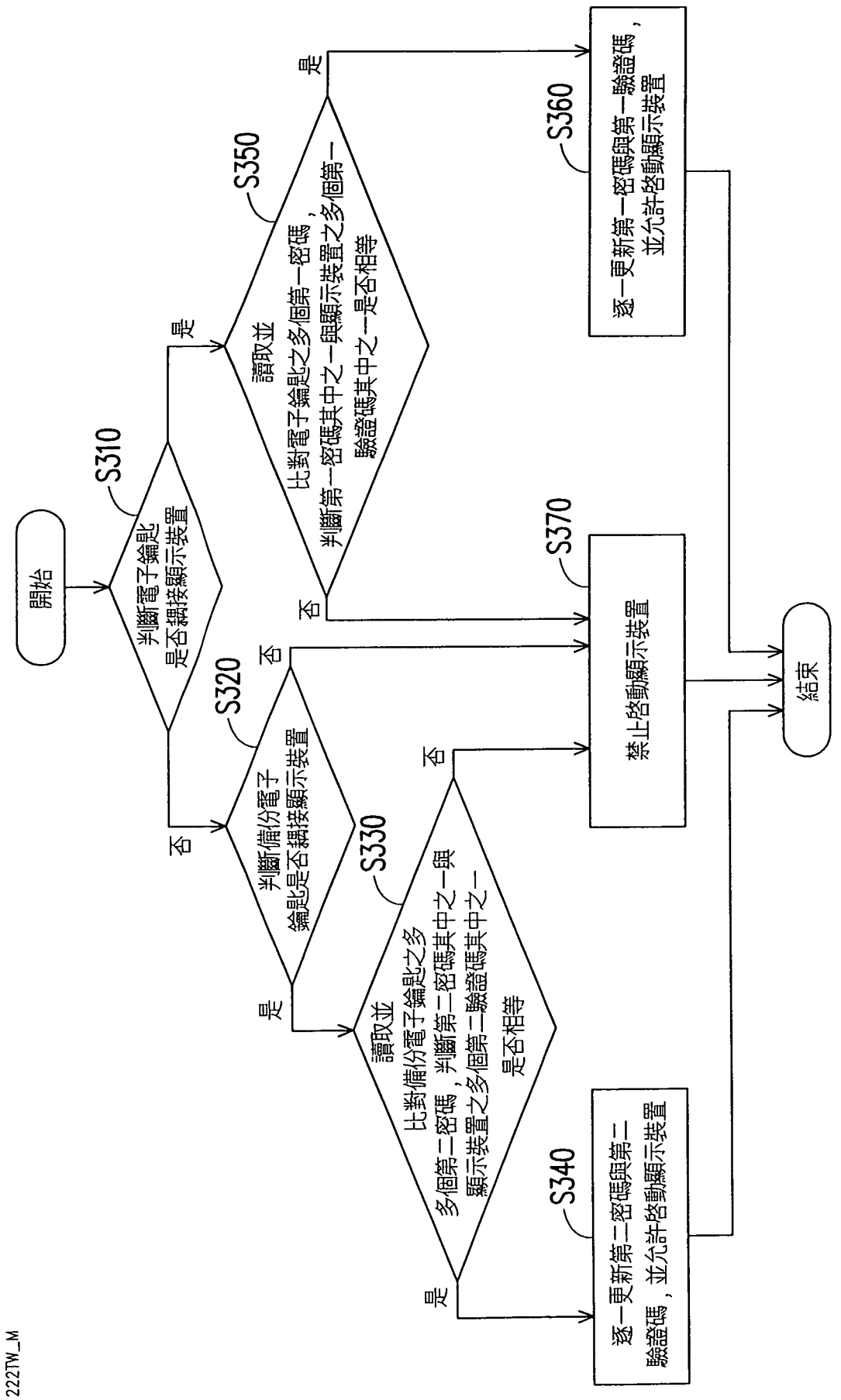
開始
S310
判斷電子鑰匙
是否耦接顯示裝置
是
否
S320
判斷備份電子
鑰匙是否耦接顯示裝置
是
否
S330
讀取並
比對備份電子鑰匙之多
多個第二密碼，判斷第二密碼其中之一與
顯示裝置之多個第二驗證碼其中之一
是否相等
是
否
S340
逐一更新第二密碼與第二
驗證碼，並允許啓動顯示裝置
S350
讀取並
比對電子鑰匙之多個第一密碼，
判斷第一密碼其中之一與顯示裝置之多個第一
驗證碼其中之一是否相等
是
否
S360
逐一更新第一密碼與第一驗證碼，
並允許啓動顯示裝置
S370
禁止啓動顯示裝置
結束

圖 3

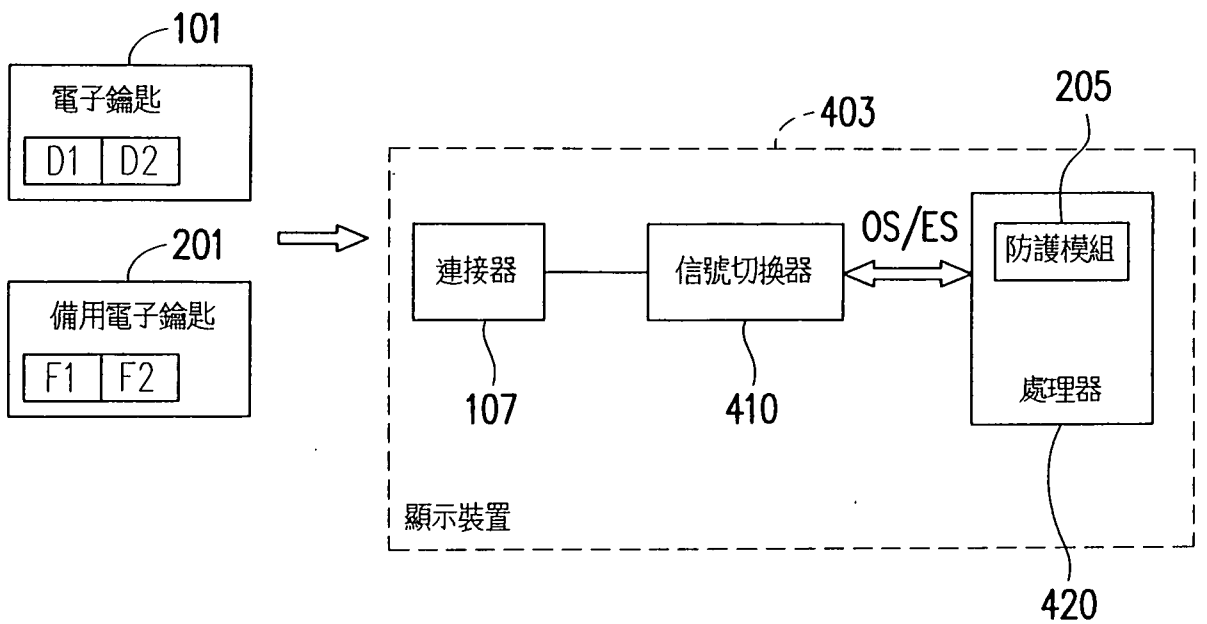
101
電子鑰匙
D1
D2
201
備用電子鑰匙
F1
F2
403
205
連接器
信號切換器
OS/ES
防護模組
處理器
107
410
420
顯示裝置

圖 4

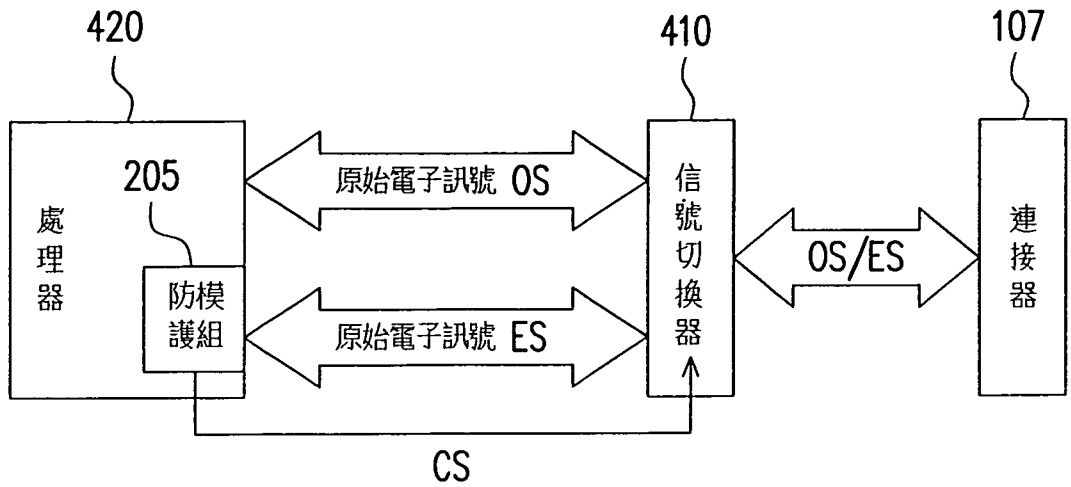
420
410
107
205
處理器
防模護組
原始電子訊號 OS
原始電子訊號 ES
信號切換器
OS/ES
連接器
CS

圖 5

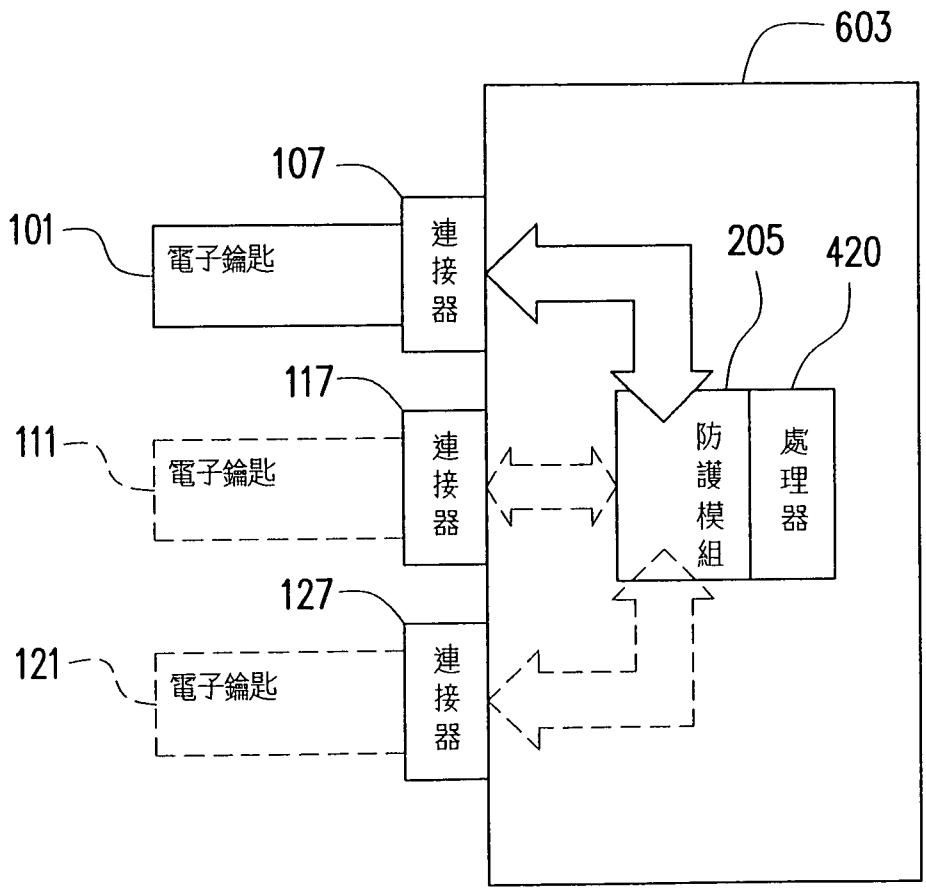
603
107
101
電子鑰匙
連接器
205
420
117
111
電子鑰匙
連接器
防護模組
處理器
127
121
電子鑰匙
連接器

圖 6