



(21)申請案號：107103394

(22)申請日：中華民國 107 (2018) 年 01 月 31 日

(51)Int. Cl.：

G06K19/06 (2006.01)**G06K19/04 (2006.01)****E05B47/00 (2006.01)****H01R31/08 (2006.01)****G06F21/00 (2013.01)**

(71)申請人：一德金屬工業股份有限公司 (中華民國) (TW)

臺南市安南區工業三路 18 號

(72)發明人：沈奕廷 (TW)

(74)代理人：謝依良

申請實體審查：有 申請專利範圍項數：36 項 圖式數：8 共 40 頁

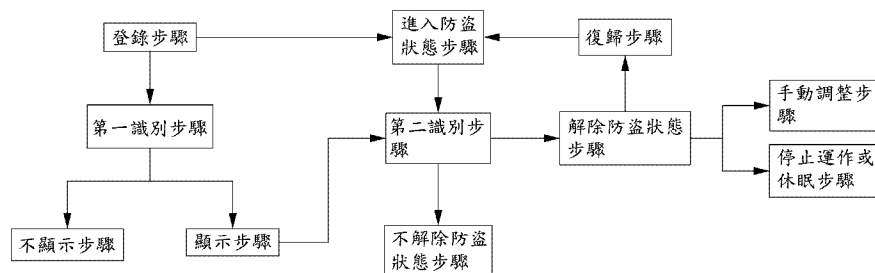
(54)名稱

防盜管制方法及其系統

(57)摘要

一種防盜管制方法及其系統，包括一個電子鑰匙以及一個讀卡設備，其中電子鑰匙包括一個顯示器，所述的讀卡設備包括一個影像讀取器，電子鑰匙執行一個第一識別步驟係決定顯示器是否顯示對應使用者的一個認證識別資料在畫面上，所述防盜設備的影像讀取器讀取電子鑰匙的顯示器畫面上的認證識別資料後判斷是否要設定為解除防盜狀態，如此在電子鑰匙遺失時，拾取者因無法通過第一識別步驟的驗證而無法使用電子鑰匙控制防盜設備。

指定代表圖：



第 4 圖

【發明說明書】

【中文發明名稱】 防盜管制方法及其系統

【技術領域】

【0001】 本發明係關於一種防盜管制方法及其系統，尤指一種透過電子方式識別身分後判斷是否解除防盜狀態的系統以及使用該防盜管制系統的方法。

【先前技術】

【0002】 隨著科技的進步，傳統機械式鎖具也從純機械方式解鎖演變成機械配合電子控制的方式進行解鎖（簡稱電子鎖），已知的電子鎖有一種是使用無線射頻相關技術製成的門禁卡，利用靠卡讀取門禁卡內部的識別資料判斷是否解鎖，這種門禁卡的好處是不需要電池，所以門禁卡具有體積輕薄的優點，另外一種是利用遙控是進行解鎖的技術，透過使用者按壓遙控器的按鈕進行解除防盜（包含解鎖）。

【0003】 所述門禁卡或遙控的解除防盜方式共同的問題在於，當門禁卡或遙控遺失後，拾取之人可以使用所拾得的門禁卡或遙控解除防盜設定，因此傳統的電子鑰匙的安全性仍然不是很充足。

【發明內容】

【0004】 為解決此問題，本發明提供一種防盜管制方法，包括：一個登錄步驟，係將對應一電子鑰匙持有者的至少一比對識別資料與至少一認證識別資

料儲存在電子鑰匙的一記憶體中且設定為一組，將對所述至少一應認證識別資料的至少一防盜解除識別資料儲存在一主記憶體中，一個進入防盜狀態步驟，所述防盜設備的一鎖裝置設定為上鎖狀態，電子鑰匙的一顯示器不顯示所述認證識別資料，一個第一識別步驟，每一次要解除防盜設備的防盜狀態時，輸入暫存的一個即時識別資料與所述比對識別資料比較是否相符，一個不顯示步驟，在即時識別資料與比對識別資料不相符時，電子鑰匙保持防盜狀態，所述顯示器不顯示認證識別資料，一個顯示步驟，在即時識別資料與比對識別資料相符時，電子鑰匙解除防盜狀態，所述顯示器顯示所述認證識別資料於畫面上，一個第二識別步驟，防盜設備的一影像讀取器讀取顯示器畫面上的認證識別資料與防盜解除識別資料比對是否相符，一個不解除防盜狀態步驟，在認證識別資料與防盜解除識別資料不相符時，不解除防盜設備的防盜狀態，所述鎖裝置保持上鎖狀態，一個解除防盜狀態步驟，在認證識別資料與防盜解除識別資料相符時，解除防盜設備的防盜狀態，所述鎖裝置設定為解鎖狀態。

【0005】 本發明另外提供一種一種防盜管制方法，包括：一個登錄步驟，係將對應一電子鑰匙持有者的至少一比對識別資料與至少一認證識別資料儲存在電子鑰匙的一記憶體中且設定為一組，將對應所述至少一認證識別資料的至少一防盜解除識別資料儲存在一主記憶體中，一個電子鑰匙結合步驟，將一電子鑰匙與一防盜設備電連接，使防盜設備供應電子鑰匙運作所需的電力，一個進入防盜狀態步驟，所述防盜設備的一鎖裝置設定為上鎖狀態，電子鑰匙的一顯示器不顯示所述認證識別資料，一個第一識別步驟，在電子鑰匙與防盜設備電連接的狀態下，輸入暫存的一個即時識別資料與所述比對識別資料比較是否相符，一個不顯示步驟，在即時識別資料與比對識別資料不相符時，電子鑰匙

保持防盜狀態，所述顯示器不顯示認證識別資料，一個顯示步驟，在即時識別資料與比對識別資料相符時，電子鑰匙解除防盜狀態，所述顯示器使用防盜設備供應的電力運作而顯示所述認證識別資料於畫面上，一個第二識別步驟，防盜設備的一影像讀取器讀取顯示器畫面上的認證識別資料與防盜解除識別資料比對是否相符，一個不解除防盜狀態步驟，在認證識別資料與防盜解除識別資料不相符時，不解除防盜設備的防盜狀態，所述鎖裝置保持上鎖狀態，一個解除防盜狀態步驟，在認證識別資料與防盜解除識別資料相符時，解除防盜設備的防盜狀態，所述鎖裝置設定為解鎖狀態，一個電子鑰匙脫離步驟，在執行不解除防盜步驟或執行解除防盜步驟之後將電子鑰匙與防盜設備分離，電子鑰匙失去電力，顯示器不顯示認證識別資料。

【0006】 本發明另外提供一種一種防盜管制方法，其包括：將至少一比對識別資料與至少一認證識別資料儲存在一電子鑰匙內，並且將一防盜解除識別資料儲存在防盜設備內，當電子鑰匙比對所輸入的一即時識別資料與比對識別資料相符的狀態下，電子鑰匙的一顯示器顯示所述的至少一認證識別資料，所述防盜設備讀取顯示器顯示的至少一認證識別資料，並比對所物至少一認證識別資料與防盜解除識別資料相符的情況下，防盜設備設定為解除狀態，防盜設備具有的一鎖裝置設定為解鎖狀態，當電子鑰匙比對所輸入的即時識別資料與至少一比對識別資料不相符的狀態下，電子鑰匙的顯示器不顯示所述至少一認證識別資料，防盜設備保持為上鎖狀態。

【0007】 本發明提供運行所述防盜管制方法的一個防盜管制系統，其包括一個電子鑰匙以及一個防盜設備，其中：所述電子鑰匙，包括：一個微處理器，一個記憶體，與微處理器電連接，記憶體內儲存至少一個比對識別資料以

及至少一個認證識別資料，一個顯示器，與微處理器電連接，顯示器可顯示認證識別資料於畫面上，電子鑰匙可輸入可暫存的一個即時識別資料，當輸入的即時識別資料與比對識別資料不相符時，顯示器不顯示認證識別資料於畫面上，當輸入的即時識別資料與比對識別資料相符時，顯示器顯示認證識別資料於畫面上，所述防盜設備包括：一個微處理單元，一個鎖裝置，與微處理單元電連接，微處理單元可設定鎖裝置為上鎖狀態或解鎖狀態，一個主記憶體，與微處理單元電連接，主記憶體中儲存至少一個防盜解除識別資料，一個影像讀取器，與微處理單元電連接，影像讀取器可讀取顯示器顯示於畫面的認證識別資料，且當所讀取的認證識別資料與防盜解除識別資料不相符時，所述鎖裝置設定為上鎖狀態，當所讀取的認證識別資料與防盜解除識別資料相符時，所述鎖裝置設定為解鎖狀態。

【0008】 本發明的防盜管制方法及其系統，即使是電子鑰匙遺失，拾取者無法通過第一識別步驟的驗證，因此拾取者仍然無法使用所拾取的電子鑰匙解除防盜設備的防盜狀態，使用上具有高安全性。

【0009】 在配合圖式說明本發明的說明性實施例的詳細說明之下將可更清楚瞭解本發明。

【圖式簡單說明】

【0010】 第 1 圖為本發明第一實施例的防盜管制系統的示意圖。

【0011】 第 2 圖為本發明第一實施例的防盜管制系統的電子鑰匙外觀圖。

【0012】 第 3 圖為本發明第一實施例的防盜管制系統應用在房間門禁管制時的示意圖。

【0013】 第 4 圖為本發明第一實施例的防盜管制方法的流程圖。

【0014】 第 5 圖為本發明第一實施例的防盜管制系統應用在車輛防盜管制時的示意圖。

【0015】 第 6 圖為本發明第二實施例的防盜管制系統的示意圖。

【0016】 第 7 圖為本發明第二實施例的防盜管制方法的流程圖。

【0017】 第 8 圖為本發明第二實施例的防盜管制方法的流程圖。

【0018】 所有圖式係僅便於解釋基本教導而已，圖式中將對構成說明用實施例之元件的數目、位置、關係、及尺寸之延伸將有所說明或在閱讀及了解以下描述後屬於業界技能。另外，在閱讀及了解以下描述後，配合特定力量、重量、強度、及類似要求之精確尺寸及尺寸比例之改變亦屬業界技能。

【0019】 在不同圖式中係以相同標號來標示相同或類似元件。

【實施方式】

【0020】 參閱第 1 ～ 5 圖所示第一實施例的防盜管制方法及其系統，其中所述的防盜管制系統 1 0 包括一個電子鑰匙 4 0，電子鑰匙 4 0 包括一個微處理器 4 2，電子鑰匙 4 0 進一步包括與微處理器 4 2 電連接的一個第一電極 4 4、一個供電單元 4 6、一個顯示器 4 8、一個記憶體 5 0、一個輸入設備 5 2 以及一個近場通訊模組 5 6，所述記憶體 5 0 係儲存至少一比對識別資料以及至少一認證識別資料，所述輸入設備 5 2 提供電子鑰匙 4 0 持有者輸入暫存的一個即時識別資料，所述的顯示器 4 8 用來顯示所述至少一個認證識別資

料在畫面上，所述顯示器 4 8 可以是一般的液晶螢幕或電子紙，其中所述的顯示器 4 8 以電子紙為最佳，所述供電單元 4 6 係供應電力給電子鑰匙 4 0 運作所需的電力。所述電子鑰匙 4 0 可以為卡片型式或遙控器型式，或者所述電子鑰匙 4 0 也可以是已知的智慧型手機

【0021】 其中所述的至少一比對識別資料、至少一認證識別資料以及所述即時識別資料可以是聲紋、指紋、虹膜、指靜脈、人臉的其中任意至少一種生物特徵或者密碼或圖形，且所述至少一比對識別資料與所述至少一認證識別資料可以是相同的生物特徵或者密碼或圖形或不同的生物特徵或者密碼或圖形。若所述至少一比對識別資料與至少一認證識別資料為生物特徵的其中之一者，則所述的輸入設備 5 2 係採用生物特徵擷取設備，例如指紋擷取裝置、麥克風、虹膜擷取裝置、指靜脈截取裝置或微型攝影機，若所述至少一比對識別資料與至少一認證識別資料為密碼，所述的輸入設備 5 2 採用數字按鍵或觸控螢幕，若所述至少一比對識別資料與至少一認證識別資料為圖形，所述輸入設備 5 2 採用觸控螢幕或觸控板。

【0022】 依據第 1 圖所示，防盜管制系統 1 0 可以包括一個管理設備 5 8，管理設備 5 8 包括一個處理器 6 0 以及與處理器 6 0 電連接的一個第一連線模組 6 2 以及一個管理輸入設備 6 4，所述管理設備 5 8 進一步也可以包括一個電連接器 6 6，所述管理輸入設備 6 4 係配合電子鑰匙 4 0 的所述至少一比對識別資料與至少一認證識別資料是聲紋、指紋、虹膜、指靜脈、人臉或密碼或圖形為其中的哪一種而設定，例如指紋擷取裝置、麥克風、虹膜擷取裝置、指靜脈截取裝置或微型攝影機，若所述至少一比對識別資料與至少一認證識別資料為密碼，所述的管理輸入設備 6 4 採用數字按鍵或觸控螢幕，若所述

至少一比對識別資料與至少一認證識別資料為圖形，所述管理輸入設備 6 4 採用觸控螢幕或觸控板，此外所述管理設備 5 8 可以是管理者的智慧型手機或者電腦，此外若管理設備 5 8 為智慧型手機，則管理設備 5 8 可以不包括所述的電連接器 6 6，如此智慧型手機與電子鑰匙 4 0 透過近場通訊模組 5 6 與第一連線模組 6 2 連線，若管理設備 5 8 是電腦，則管理設備 5 8 可以不包括第一連線模組 6 2，如此電腦可以使用諸如讀卡機當作電連接器 6 6 與電子鑰匙 4 0 的第一電極 4 4 電連接而取得連線。

【0023】如第 1 圖所示，防盜管制系統 1 0 包括一個防盜設備 2 0，所述防盜設備 2 0 包括一個微處理單元 2 2，防盜設備 2 0 進一步包括與微處理單元 2 2 電連接的一個鎖裝置 2 4、一個主記憶體 2 6、一個供電模組 2 8、一個第二電極 3 0、一個影像讀取器 3 2 以及一個第二連線模組 3 4，其中主記憶體 2 6 儲存至少一個防盜解除識別資料，所述防盜解除識別資料係配合所述認證識別資料為同一類型，例如認證識別資料為圖形化的聲紋，所述防盜解除識別資料也是圖形化的聲紋，所述的影像讀取器 3 2 可以是一種小型攝影機，用來讀取電子鑰匙 4 0 的顯示器 4 8 顯示在畫面上的認證識別資料，所述供電模組 2 8 可以與市電連接用來供應防盜設備 2 0 運作所需的電力，所述鎖裝置 2 4 可以被微處理單元 2 2 設定為對應防盜設備 2 0 的防盜狀態的上鎖狀態或對應防盜設備的解除防盜狀態的解鎖狀態，且鎖裝置 2 4 依據使用環境可以有不同的變化，例如第 3 圖所示防盜設備 2 0 使用在一房間 7 2 的門禁管制上，所述的鎖裝置 2 4 是安裝於房間 7 2 的一 7 0 門上的一種門鎖，如第 9 圖所示，防盜設備 2 0 用在一車輛 7 5 上，所述鎖裝置 2 4 則是安裝在車輛 7 5

的一車門 7 7 上的鎖具，所述鎖裝置 2 4 設定為上鎖狀態意味著無法操作鎖裝置 2 4 開啟門 7 0 或車門 7 7。

【0024】依據第 1 圖所示，所述防盜管制系統 1 0 進一步可包括與防盜設備 2 0 電連接的一個讀取器 3 8 以及至少一個可控制設備 3 6。所述可控制設備 3 6 依據防盜管制系統 1 0 使用環境可以是不同的設備，例如使用在住家的防盜管制系統 1 0，所述的至少一可控制設備 3 6 可以是一房間 7 2 內的燈光、空調設備、音響設備、電視等（如第 3 圖所示），若所述防盜管制系統 1 0 使用在車輛 7 5 上，則所述至少一可控制設備 3 6 可以是車輛 7 5 的座椅、方向盤、車輛空調、車輛音響．．．等，所述的讀取器 3 8 可以與電子鑰匙 4 0 的近場通訊模組 5 6 連線，進一步透過微處理單元 2 2 輸出一個停止設定值或休眠設定值給所述全部的至少一個可控制設備 3 6。

【0025】本發明提供使用所述第一實施例的防盜管制系統 1 0 的一種防盜管制方法，參閱第 4 圖所示，首先執行一個登錄步驟，係將對應一電子鑰匙 4 0 持有者的至少一比對識別資料與至少一認證識別資料儲存在電子鑰匙 4 0 的一記憶體 5 0 中且設定為一組（一個比對識別資料只對應一個認證識別資料），將對應所述至少一認證識別資料的至少一防盜解除識別資料以及至少一個個人化設定值儲存在防盜設備 2 0 的一主記憶體 2 6 中。

【0026】實質上，透過管理設備 5 8 將所述的至少一比對識別資料與所述的至少一認證識別資料輸入電子鑰匙 4 0 中，所述管理設備 5 8 透過輸入一個管理識別資料而取得管理權限，例如管理設備 5 8 的一個管理系統需要由帳號與密碼共同構成的一組管理識別資料才能登入，登入所述管理系統之後，所述管理設備 5 8 可以透過第一連線模組 6 2 與電子鑰匙 4 0 的近場通訊模組 5

6 連線，或者管理設備 5 8 可以透過電連接器 6 6 與第一電極 4 4 電連接而與電子鑰匙 4 0 連線（並且供應運作所需的電力），進一步允許使用管理設備 5 8 的管理輸入設備 6 4 輸入所述至少一比對識別資料、至少一認證識別資料儲存於記憶體 5 0 中，並且將同時輸入的一個比對識別資料與一個認證識別資料配對成一組（可以有多組），所述每一個配對成一組的一個比對識別資料與一個認證識別資料用來指向特定的單一個使用者（電子鑰匙 4 0 的擁有者）。

【0027】同樣地管理設備 5 8 也能使用第一連線模組 6 2 與第二連線模組 3 4 連線，使用管理輸入設備 6 4 輸入對應所述至少一認證識別資料的至少一防盜解除識別資料儲存於主記憶體 2 6 中，並且將對應所述至少一認證識別資料的一個個人化設定值儲存於主記憶體 2 6 中，如此一個比對識別資料只對應一個認證識別資料，而且一個認證識別資料只對應一個防盜解除識別資料與一個個人化設定值，換句話說，所述的一個比對識別資料、一個認證識別資料、一個防盜解除識別資料以及一個個人化設定值指向單一個使用者，單一的電子鑰匙 4 0 允許輸入多組資料，而且防盜設備 2 0 也允許輸入多組相對應的防盜解除識別資料與個人化設定值，如此單一電子鑰匙 4 0 可以輸入多個不同使用者的識別資料，並且不同使用者使用電子鑰匙 4 0 時，可以被防盜管制系統 1 0 識別何者正在使用。此外，當管理設備 5 8 登出之後，就無法與所述電子鑰匙 4 0 與防盜設備 2 0 連線。此外，所述管理設備 5 8 可以是管理者的智慧型行動電話或者電腦的其中一者。

【0028】在電子鑰匙 4 0 的記憶體 5 0 儲存有所述至少一比對識別資料與至少一認證識別資料，且所述防盜設備 2 0 的主記憶體 2 6 儲存有至少一防盜解除識別資料之後，所述防盜設備 2 0 與電子鑰匙 4 0 會執行進入防盜狀態

步驟，防盜設備 2 0 的微處理單元 2 2 係將鎖裝置 2 4 設定為上鎖狀態，所述電子鑰匙 4 0 進入防盜狀態之後所述顯示器 4 8 就不會將所述至少一認證識別資料顯示在顯示器 4 8 的畫面上。

【0029】 當要使用電子鑰匙 4 0 解除防盜設備 2 0 的防盜狀態時，係執行一個第一識別步驟，使用輸入設備 5 2 將暫存的一個即時識別資料（指要解除防盜設備 2 0 的當時所輸入的識別資料）輸入電子鑰匙 4 0 中，進一步比對所輸入的即時識別資料與比對資料是否相符。

【0030】 若即時識別資料與比對資料不相符，則執行一個不顯示步驟，如此電子鑰匙 4 0 保持防盜狀態，所述顯示器 4 8 不顯示所述的至少一認證識別資料的任一者。若即時識別資料與比對資料相符，則執行一個顯示步驟，電子鑰匙 4 0 解除防盜狀態，所述顯示器 4 8 顯示與該即時識別資料相符的比對識別資料為一組的一個認證識別資料於畫面上。

【0031】 當電子鑰匙 4 0 的顯示器 4 8 畫面顯現所述至少一認證識別資料之後，進一步執行一個第二識別步驟，使用防盜設備 2 0 的一影像讀取器 3 2 讀取顯示器 4 8 畫面上的認證識別資料，所述微處理單元 2 2 將所取得的認證識別資料與所述至少一防盜解除識別資料的比對是否與其中任意一者相符。

【0032】 影像讀取器 3 2 取得的認證識別資料與所述至少一防盜解除識別資料全部都不相符時執行一個不解除防盜狀態步驟，如此防盜設備 2 0 保持在防盜狀態，所述鎖裝置 2 4 保持為上鎖狀態。影像讀取器 3 2 取得的認證識別資料與所述至少一防盜解除識別資料的其中一者相符時執行一個解除防盜狀態步驟，解除防盜設備 2 0 的防盜狀態，所述鎖裝置 2 4 設定為解鎖狀態，此外，在防盜設備 2 0 設定為解除防盜狀態的同時，所述微處理單元 2 2 同時使

用與該相符的認證識別資料對應的一個個人化設定時設定所述至少一個可控制設備 3 6。

【0033】 在使用個人化設定值設定所述至少一可控制設備 3 6 之後，仍然可以執行一個手動調整步驟，使用者可以自行手動調整所述可控制設備 3 6 的設定值。再者也可以執行一個停止運作或休眠步驟，使用電子鑰匙 4 0 與一讀取器 3 8 連線，驅動防盜設備 2 0 輸出一個停止設定值或休眠設定值給所述可控制設備 3 6，可控制設備 3 6 執行停止運作或休眠。

【0034】 在鎖裝置 2 4 設定為解鎖狀態且被操作之後及／或者手動設定防盜設備 2 0 進入防盜狀態時可以執行一個復歸步驟，使得防盜設備 2 0 重新執行進入防盜狀態步驟。

【0035】 本發明的防盜管制系統 1 0 可以應用在許多不同的場合或情況，參閱第 2 ～ 3 圖所示，為了方便說明，係假設所述防盜管制系統 1 0 使用在一般的住家門禁管制，所述鎖裝置 2 4 為一個門 7 0 上的一個門鎖，所述影像讀取器 3 2 安裝在門 7 0 的外側（室外），，所述至少一可控制設備 3 6 為家中的燈光、空調設備、音響設備以及電視，所述至少一比對識別資料與至少一認證識別資料是持有者的聲紋圖形，如此電子鑰匙 4 0 上的輸入設備 5 2 就是微型麥克風，此外，進一步假設所述電子鑰匙 4 0 具備供電單元 4 6 供應電力，因此所述防盜設備 2 0 不包括所述第二電極 3 0。

【0036】 假設單一電子鑰匙 4 0 設定有一位第一使用者與一位第二使用者，在這樣的狀態下，所述管理設備 5 8 使用管理識別資料取得管理權限後，透過電連接器 6 6（例如讀卡器）與電子鑰匙 4 0 連線，進一步電子鑰匙 4 0 的第一個持有者可以對著管理輸入設備 6 4 說出特定的聲音（例如：請開

門)，使得管理設備 5 8 將電子鑰匙 4 0 持有者所發出的聲音轉換成可視的聲紋圖形後傳送至電子鑰匙 4 0 的記憶體 5 0 儲存，並且可以設定所述聲紋圖形成為比對識別資料及／或認證識別資料，假設所述比對識別資料為第一個聲紋圖形（例如：請開門），認證識別資料為第二個聲紋圖形（例如：是我），將第一個使用者的比對識別資料（第一個聲紋圖形）與認證識別資料（第二個聲紋圖形）配對成第一使用者資料，同樣地，在第一個使用者完成後，第二個使用者同樣使用管理設備 5 8 的管理輸入設備 6 4 說出特定的聲音（可以與第一個使用者相同或不相同），進一步將對應第二個使用者的比對識別資料（第三個聲紋圖形）與認證識別資料（第四個聲紋圖形）配對成第二使用者資料。

【0037】完成第一與第二使用者資料登錄之後，管理設備 5 8 的第一連線模組 6 2 與防盜設備 2 0 的第二連線模組 3 4 連線，進一步第一使用者利用管理設備 5 8 的管理輸入設備 6 4 說出『是我』的聲音，並且管理設備 5 8 將第一使用者說出的話語轉換成可視的聲紋圖形儲存在防盜設備 2 0 的主記憶體 2 6 中當成一個防盜解除識別資料，在這樣的狀態下該第一使用者的防盜解除識別資料呈現的聲紋圖形與第一使用者的認證識別資料的聲紋圖形會相同，此外在登錄防盜解除識別資料的同時也能透過管理設備 5 8 設定所述房間 7 2 內的燈光、空調設備、音響設備、電視（可控制設備）的個人化設定值，例如設定燈光的亮度、顏色，空調設備是否運作、溫度、風量大小，音響設備的大小聲、是否開啟，電視是否開啟、開啟時的頻道．．．等，使得一個防盜解除識別資料能夠對應一個個人化設定值，同樣地，第二使用者也透過相同方式，將對應第二使用者的防盜解除識別資料（與第二使用者的認證識別資料相符）以

及個人化設定值（可與第一個使用者相同或不相同）儲存在防盜設備 2 0 的主記憶體 2 6 內。

【0038】 在管理設備 5 8 與電子鑰匙 4 0 離線之後，所述的電子鑰匙 4 0 就進入防盜狀態，而且管理設備 5 8 與防盜設備 2 0 離線之後，防盜設備 2 0 就進入防盜狀態（進入防盜狀態步驟），如此電子鑰匙 4 0 的顯示器 4 8 不會顯示所述第一或第二使用者的認證識別資料，所述的鎖裝置 2 4 設定為上鎖狀態時，門 7 0 無法被開啟，而且假設門 7 0 內的一房間 7 2 內的燈光、空調設備、音響設備與電視假設為關閉或休眠狀態（進入防盜狀態步驟）。

【0039】 假設第一使用者欲使用電子鑰匙 4 0 開門 7 0，第一使用者使用輸入設備 5 2（微型麥克風）說出『請開門』，所述輸入設備 5 2 擷取使用者的聲音後轉換成聲紋圖形構成所述即時識別資料，並且微處理器 4 2 比對所述即時識別資料與已登錄的第一使用者的比對識別資料相符（與第二使用者的比對識別資料不相符），如此顯示器 4 8 係顯示對應第一使用者的認證識別資料在畫面上（不顯示第二使用者的認證識別資料）。

【0040】 進一步，將電子鑰匙 4 0 靠近防盜設備 2 0 的影像讀取器 3 2，所述影像讀取器 3 2 讀取顯示器 4 8 畫面上顯示的第一使用者的認證識別資料，並且使用所讀取的認證識別資料與主記憶體 2 6 中的兩個防盜解除識別資料比較（第二識別步驟），而可到與第一使用者的防盜解除識別資料相符的結果，如此微處理單元 2 2 設定鎖裝置 2 4 為解鎖狀態，如此防盜設備 2 0 就被設定為解除防盜狀態，第一使用者可以操作門 7 0 上的門鎖（鎖裝置 2 4）將門 7 0 開啟進入房間 7 2 中，並且在防盜設備 2 0 設定為解除防盜狀態的同時，微處理單元 2 2 使用對應第一使用者的認證識別資料（或防盜解除識別資

料)的個人化設定值設定房間7 2內的燈光、空調設備、音響設備以及電視(解除防盜狀態步驟)。

【0041】將防盜設備2 0設定為解除防盜狀態之後，所述電子鑰匙4 0再次進入防盜狀態使得顯示器4 8不顯示所述任一認證識別資料(全部都不顯示)，所述第一使用者開啟門7 0並且進入房間7 2內之後，門7 0再次關上時，防盜設備2 0回復為防盜狀態(復歸步驟)，如此門7 0無法從外側開啟但可以從內側開啟。

【0042】假設為第二使用者使用電子鑰匙4 0開門7 0，執行第一識別步驟時，能夠從第二使用者所輸入的即時識別資料使得顯示器4 8顯示第二使用者的認證識別資料，進一步防盜設備2 0讀取第二使用者認證識別資料與第二使用者的防盜解除資料相符，將防盜設備2 0設定為解除防盜狀態，設定鎖裝置2 4為解鎖狀態，同時使用第二使用者的個人化設定值設定房間7 2內的燈光、空調設備、音響設備、電視。

【0043】此外，所述房間7 2內的燈光、空調設備、音響設備、電視等都可以另外以手動的方式進行調整(手動調整步驟)，以及若要離開房間7 2將燈光、空調設備、音響設備、電視全部關閉或休眠，則可持電子鑰匙4 0靠近所述房間7 2內的讀取器3 8，使得電子鑰匙4 0的近場通訊模組5 6與讀取器3 8連線，如此防盜設備2 0就會輸出一個停止設定值或休眠設定值設定所述燈光、空調設備、音響設備、電視全部停止及／或休眠。

【0044】假設電子鑰匙4 0遺失，拾取者使用電子鑰匙4 0的輸入設備5 2輸入即時識別資料(第一識別步驟)，拾取者的即時識別資料轉換成的聲紋圖形與第一及第二使用者的聲紋圖形並不相符，因此顯示器4 8不會顯示第

一或第二使用者的認證識別資料在畫面上，即便拾取者所講出的話語剛好與第一或第二使用者相同，也無法使顯示器 4 8 顯示第一或第二使用者的認證識別資料在畫面上，例如拾取者講出與第一使用者相同的『請開門』，其轉換成聲紋圖形時，因為拾取者與第一使用者的聲調不同，而產生不同的聲紋圖形，執行第一識別步驟時，仍無法辨別該聲紋圖形與第一使用者的比對識別資料的聲紋圖形相符，進一步，所述電子鑰匙 4 0 無法被拾取者用來將防盜設備 2 0 設定為解除防盜狀態。

【0045】本發明的防盜管制方法及其系統除了用在所述房間 7 2 的門禁管制之外，也能用在諸如車輛的門禁管制，參閱第 5 圖所示，所述的鎖裝置 2 4 是一車輛 7 5 的一車門 7 7 的鎖裝置，相較於用在房間 7 2 的門禁管制，所述用在車輛 7 5 的門禁管制的差異只在於所述可控制設備 3 6 並不相同而已，詳細的說，本發明的防盜管制方法及其系統用在車輛上時，所述的可控制設備 3 6 可以是車輛座椅、方向盤、音響、空調的調整，如此可以在解除防盜狀態步驟執行的同時，將車輛的座椅、方向盤、音響、空調利用個人化設定值調整至符合個人習慣的狀態，不同的使用者持相同或不同的電子鑰匙 4 0，對於單一車輛有不同駕駛的情況下具有很高的便利性。

【0046】本發明的防盜管制方法及其系統除了第 1 ～ 5 圖所示的第一實施例之外也能有其他的變化，參閱第 6 ～ 7 圖所示第二實施例的防盜管制方法及其系統，重複的部份將不再次贅述，以下只針對兩個實施例差異之處作說明，其中電子鑰匙 4 0 可以不包括供電單元 4 6，所述防盜設備 2 0 可以包括一個主輸入設備 3 5，並且將所述影像讀取器 3 2 與第二電極 3 0 整合為一個讀卡設備 2 9（參閱第 8 圖所示）。

【0047】 所述第二實施例的防盜管制方法及其系統的登錄步驟與第一實施例相同，但由於電子鑰匙 4 0 不包括供電單元 4 6，因此執行所述第一識別步驟之前需先執行一個電子鑰匙結合步驟，實際上是將電子鑰匙 4 0 插入所述讀卡設備 2 9 中，使電子鑰匙 4 0 的第一電極 4 4 與防盜設備 2 0 的第二電極 3 0 電連接，如此防盜設備 2 0 的供電模組 2 8 供應電子鑰匙 4 0 運作所需的電力，如此所述顯示器 4 8 與影像讀取器 3 2 對齊，在這個狀態下，所述電子鑰匙 4 0 的顯示器 4 8 位於所述讀卡設備 2 9 內部無法被肉眼看見（如第 8 圖所示），進一步在電子鑰匙 4 0 有電力的狀態下，使用防盜設備 2 0 的主輸入設備 3 5 輸入即時識別資料（例如口述請開門）與電子鑰匙 4 0 的比對識別資料進行比對（第一識別步驟）。

【0048】 當比對輸入的即時識別資料與任一比對識別資料均不相符的情況下，所述顯示器 4 8 不顯示認證識別資料在畫面上（不顯示步驟），如此防盜設備 2 0 無法讀取認證識別資料而保持在防盜狀態，所述鎖裝置 2 4 也保持上鎖狀態，在執行不顯示步驟之後可進一步執行電子鑰匙脫離步驟，將電子鑰匙 4 0 與讀卡設備 2 9 分離。

【0049】 當比對輸入的即時識別資料與其中一比對識別資料均相符的情況下，所述顯示器 4 8 顯示對應該比對識別資料的一認證識別資料（與該比對識別資料為一組的認證識別資料）在畫面上（顯示步驟），進一步防盜設備 2 0 讀取對應顯示器 4 8 畫面上的認證識別資料與所述的防盜解除識別資料比對是否相符（第二識別步驟）。

【0050】 若所讀取的認證識別資料與全部的防盜解除識別資料均不相符，則防盜設備 2 0 保持防盜狀態，所述鎖裝置 2 4 保持在上鎖狀態（不解除

防盜狀態步驟），進一步可以執行電子鑰匙脫離步驟，將電子鑰匙 4 0 與讀卡設備 2 9 分離。

【0051】 若所讀取的認證識別資料與其中一個防盜解除識別資料相符，則防盜設備 2 0 設定為解除防盜狀態，所述鎖裝置 2 4 設定為解鎖狀態（解除防盜狀態步驟），同時防盜設備 2 0 使用對應該認證識別資料的個人化設定值設定所述的各可控制設備（解除防盜狀態步驟）。完成解除防盜狀態步驟之後進一步可以執行電子鑰匙脫離步驟，將電子鑰匙 4 0 與讀卡設備 2 9 分離，而且也可執行所述手動調整步驟，手動調整各可控制設備 3 6，此外，執行所述電子鑰匙脫離步驟之後，電子鑰匙 4 0 的第一電極 4 4 與防盜設備 2 0 的第二電極 3 0 分離，電子鑰匙 4 0 沒有電力所述顯示器 4 8 不顯示任何的認證識別資料，而且所述防盜設備 2 0 重新進入防盜狀態，所述的鎖裝置 2 4 設定為上鎖狀態（復歸步驟）。

【0052】 此外，在執行電子鑰匙脫離步驟之後，也能透過讀取器 3 8 執行所述停止運作或休眠步驟，使防盜設備 2 0 使用停止設定值或休眠設定值將全部的可控制設備 3 6 設定為停止運作或休眠。

【0053】 本發明各實施例的防盜管制系統 1 0，即使是電子鑰匙 4 0 遺失，拾取者無法通過第一識別步驟的驗證，因此拾取者仍然無法使用所拾取的電子鑰匙 4 0 解除防盜設備 2 0 的防盜狀態，使用上具有高安全性。

【0054】 本發明的各實施例的防盜管制系統 1 0，透過個人化設定值與防盜解除識別資料配對成一組之後，使得防盜設備 2 0 可以依據使用電子鑰匙 4 0（單一或不同電子鑰匙 4 0 都適用）的使用者對應的個人化設定值設定所述至少一個可控制設備 3 6，使得所述可控制設備 3 6 可以在解除防盜設備 2

0 的防盜狀態的同時預設成符合該使用者習慣的狀態，使用上具有極高的便利性。

【0055】 所述各實施例的停止運作或休眠步驟，可以在短時間同時停止或休眠複數個可控制裝置，使用在家庭中，具有極高的便利性，並且具有節約電能的優點。

【0056】 第二實施例所述的防盜管制系統 1 0，因為電子鑰匙 4 0 與讀卡設備 2 9 結合時，所述顯示器 4 8 被包覆在讀卡設備 2 9 內部（如第 圖所示），進一步顯示器 4 8 顯示認證識別資料在畫面上時，無法被影像讀取器 3 2 以外的人或裝置看見或識別，可以有效地防止認證識別資料外洩，提高電子鑰匙 4 0 使用時的安全性。

【0057】 第二實施例的電子鑰匙 4 0 沒有設置供電單元 4 6，進一步若所述顯示器 4 8 採用電子紙，所述電子鑰匙 4 0 可以薄型化成卡片狀，具有攜帶方便兼具高安全性的優點。

【0058】 本發明的基本教導已加以說明，對具有本領域通常技能的人而言，許多延伸和變化將是顯而易知者。舉例言之，各實施例的防盜管制方法的登錄步驟可以不包括輸入個人化設定值，在缺少個人化設定值的狀態下，本發明的防盜管制方法仍然可以提供很好的防盜管制效果。或者，第一實施例的防盜管制防法及其系統的電子鑰匙 4 0 可以不包括供電單元 4 6，如此電子鑰匙 4 0 可以透過第一與第二電極 4 4、3 0（第一與第二識別步驟）電連接或者第一電極 4 4 與電連接器 6 6 電連接（登錄步驟）取得電力，使得電子鑰匙 4 0 可以如常運作。或者，第二實施例的防盜設備 2 0 可以不包括主輸入設備 3 5，如此，在電子鑰匙 4 0 與讀卡設備 2 9 結合時，電子鑰匙 4 0 的輸入設備

5 2 外露在讀卡設備 2 9 外側，因而執行第一與第二識別步驟時，可以使用電子鑰匙 4 0 的輸入設備 5 2 輸入即時識別資料。或者，比對識別資料與認證識別資料並非一定需要相同的資料，例如比對識別資料為使用者的指紋，認證識別資料與防盜解除識別資料都是使用者的聲紋圖形。或者，所述防盜設備 2 0 所述的主記憶體 2 6 並非只能設置在防盜設備 2 0 之中，例如使用管理設備 5 8 的記憶體（例如電腦的硬碟）也能當成儲存防盜解除識別資料的儲存裝置，而在這樣的狀態下，執行第二識別步驟時，防盜設備 2 0 與管理設備 5 8 連線並讀取所述至少一防盜解除識別資料進行與所讀取的認證識別資料進行比較。

【0059】再者，本發明圖式與說明書所列舉的房間或車輛使用環境只是幫助能夠更多地理解本發明的技術特徵與所能達成的功效而已，本發明的防盜管制方法及其系統並非限制在只能是用於所述兩種場合。

【0060】由於說明書揭示的本發明可在未脫離本發明精神或大體特徵的其它特定形式來實施，且這些特定形式的一些形式已經被指出，所以，說明書揭示的實施例應視為舉例說明而非限制。本發明的範圍是由所附的申請專利範圍界定，而不是由上述說明所界定，對於落入申請專利範圍的均等意義與範圍的所有改變仍將包含在其範圍之內。

【符號說明】

【0061】

1 0 防盜管制系統	2 0 防盜設備	2 2 微處理單元
2 4 鎖裝置	2 6 主記憶體	2 8 供電模組
3 0 第二電極	3 2 影像讀取器	3 4 第二連線模組

3 5 主輸入設備	3 6 可控制設備	3 8 讀取器
4 0 電子鑰匙	4 2 微處理器	4 4 第一電極
4 6 供電單元	4 8 顯示器	5 0 記憶體
5 2 輸入設備	5 6 近場通訊模組	5 8 管理設備
6 0 處理器	6 2 第一連線模組	6 4 管理輸入設備
6 6 電連接器	7 0 門	7 2 房間
7 5 車輛	7 7 車門	



201935322

【發明摘要】

【中文發明名稱】 防盜管制方法及其系統

【中文】

一種防盜管制方法及其系統，包括一個電子鑰匙以及一個讀卡設備，其中電子鑰匙包括一個顯示器，所述的讀卡設備包括一個影像讀取器，電子鑰匙執行一個第一識別步驟係決定顯示器是否顯示對應使用者的一個認證識別資料在畫面上，所述防盜設備的影像讀取器讀取電子鑰匙的顯示器畫面上的認證識別資料後判斷是否要設定為解除防盜狀態，如此在電子鑰匙遺失時，拾取者因無法通過第一識別步驟的驗證而無法使用電子鑰匙控制防盜設備。

【指定代表圖】 第 4 圖

【代表圖之符號簡單說明】

【發明申請專利範圍】

【第1項】 一種防盜管制方法，包括：

一個登錄步驟，係將對應一電子鑰匙持有者的至少一比對識別資料與至少一認證識別資料儲存在電子鑰匙的一記憶體中且設定為一組，將對所述至少一應認證識別資料的至少一防盜解除識別資料儲存在一主記憶體中；

一個進入防盜狀態步驟，所述防盜設備的一鎖裝置設定為上鎖狀態，電子鑰匙的一顯示器不顯示所述認證識別資料；

一個第一識別步驟，每一次要解除防盜設備的防盜狀態時，輸入暫存的一個即時識別資料與所述比對識別資料比較是否相符；

一個不顯示步驟，在即時識別資料與比對識別資料不相符時，電子鑰匙保持防盜狀態，所述顯示器不顯示認證識別資料；

一個顯示步驟，在即時識別資料與比對識別資料相符時，電子鑰匙解除防盜狀態，所述顯示器顯示所述認證識別資料於畫面上；

一個第二識別步驟，防盜設備的一影像讀取器讀取顯示器畫面上的認證識別資料與防盜解除識別資料比對是否相符；

一個不解除防盜狀態步驟，在認證識別資料與防盜解除識別資料不相符時，不解除防盜設備的防盜狀態，所述鎖裝置保持上鎖狀態；

一個解除防盜狀態步驟，在認證識別資料與防盜解除識別資料相符時，解除防盜設備的防盜狀態，所述鎖裝置設定為解鎖狀態。

【第2項】 如申請專利範圍第 1 項的防盜管制方法，其中登錄步驟進一步包括將對應一可控制設備與所述至少一認證識別資料的至少一個人化設定值儲存

在主記憶體中，在執行解除防盜狀態步驟時依據防盜設備所讀取的所述至少一認證識別資料選擇對應的所述至少一個人化設定值設定可控制設備。

【第3項】如申請專利範圍第2項的防盜管制方法，進一步包括：

一個手動調整步驟，在所述至少一個人化設定值設定可控制設備之後，允許手動調整所述可控制設備的設定值。

【第4項】如申請專利範圍第2項的防盜管制方法，進一步包括：

一個停止運作或休眠步驟，在所述至少一個人化設定值設定可控制設備之後，使用電子鑰匙與一讀取器連線，防盜設備輸出一個停止設定值或休眠設定值給所述可控制設備，可控制設備執行停止運作或休眠。

【第5項】如申請專利範圍第1項的防盜管制方法，其中所述至少一比對識別資料與所述至少一認證識別資料可以是聲紋、指紋、虹膜、指靜脈、人臉的其中任意至少一種生物特徵或者密碼或圖形。

【第6項】如申請專利範圍第5項的防盜管制方法，其中所述至少一比對識別資料與所述至少一認證識別資料可以是同一生物特徵或不同一生物特徵。

【第7項】如申請專利範圍第1項的防盜管制方法，進一步包括：

一個復歸步驟，在鎖裝置設定為解鎖狀態且被操作之後及／或者手動設定防盜設備進入防盜狀態時，防盜設備重新執行進入防盜狀態步驟。

【第8項】如申請專利範圍第1項的防盜管制方法，其中所述第一識別步驟係利用電子鑰匙的一輸入設備輸入即時識別資料並且由電子鑰匙的一微處理器比較與比對識別資料是否相符。

【第9項】如申請專利範圍第1項的防盜管制方法，其中所述登錄步驟進一步包括：

一管理設備，輸入預設的一管理授權資料取得管理權限後與一電子鑰匙或未設定的防盜設備的其中一者連線；

在管理設備與電子鑰匙連線後，使用管理設備的一管理輸入設備輸入所述至少一比對識別資料以及所述至少一認證識別資料並儲存於電子鑰匙的一記憶體中；

在管理設備與防盜設備連線後，使用管理輸入設備輸入防盜解除識別資料儲存於防盜設備的主記憶體內。

【第10項】一種防盜管制方法，包括：

一個登錄步驟，係將對應一電子鑰匙持有者的至少一比對識別資料與至少一認證識別資料儲存在電子鑰匙的一記憶體中且設定為一組，將對應所述至少一認證識別資料的至少一防盜解除識別資料儲存在一主記憶體中；

一個電子鑰匙結合步驟，將一電子鑰匙與一防盜設備電連接，使防盜設備供應電子鑰匙運作所需的電力；

一個進入防盜狀態步驟，所述防盜設備的一鎖裝置設定為上鎖狀態，電子鑰匙的一顯示器不顯示所述認證識別資料；

一個第一識別步驟，在電子鑰匙與防盜設備電連接的狀態下，輸入暫存的一個即時識別資料與所述比對識別資料比較是否相符；

一個不顯示步驟，在即時識別資料與比對識別資料不相符時，電子鑰匙保持防盜狀態，所述顯示器不顯示認證識別資料；

一個顯示步驟，在即時識別資料與比對識別資料相符時，電子鑰匙解除防盜狀態，所述顯示器使用防盜設備供應的電力運作而顯示所述認證識別資料於畫面上；

一個第二識別步驟，防盜設備的一影像讀取器讀取顯示器畫面上的認證識別資料與防盜解除識別資料比對是否相符；

一個不解除防盜狀態步驟，在認證識別資料與防盜解除識別資料不相符時，不解除防盜設備的防盜狀態，所述鎖裝置保持上鎖狀態；

一個解除防盜狀態步驟，在認證識別資料與防盜解除識別資料相符時，解除防盜設備的防盜狀態，所述鎖裝置設定為解鎖狀態；

一個電子鑰匙脫離步驟，在執行不解除防盜步驟或執行解除防盜步驟之後將電子鑰匙與防盜設備分離，電子鑰匙失去電力，顯示器不顯示認證識別資料。

【第11項】如申請專利範圍第10項的防盜管制方法，其中所述第一識別步驟係電子鑰匙的一輸入設備使用防盜設備供應的電力運作而被操作輸入所述即時識別資料。

【第12項】如申請專利範圍第10項的防盜管制方法，其中所述第一識別步驟係使用防盜設備的一主輸入設備輸入所述即時識別資料。

【第13項】如申請專利範圍第10項的防盜管制方法，其中所述登錄步驟係在電子鑰匙與防盜設備電連接時，使用防盜設備的一主輸入設備輸入所述至少一比對識別資料與所述至少一認證識別資料。

【第14項】如申請專利範圍第10項的防盜管制方法，其中登錄步驟進一步包括將對應一可控制設備與所述至少一認證識別資料的至少一個人化設定值儲存在防盜設備的主記憶體中，在執行解除防盜狀態步驟時依據防盜設備所讀取的所述至少一認證識別資料選擇對應的所述至少一個人化設定值設定可控制設備。

【第15項】 如申請專利範圍第 1 4 項的防盜管制方法，進一步包括：

一個手動調整步驟，在所述至少一個人化設定值設定可控制設備之後，允許手動調整所述可控制設備的設定值。

【第16項】 如申請專利範圍第 1 4 項的防盜管制方法，進一步包括：

一個停止運作或休眠步驟，在所述至少一個人化設定值設定可控制設備且執行電子鑰匙脫離步驟之後，使用電子鑰匙與一讀取器連線，電子鑰匙使用讀取器發出的訊號而供電出一個停止設定值或休眠設定值給所述可控制設備，可控制設備執行停止運作或休眠。

【第17項】 如申請專利範圍第 1 0 項的防盜管制方法，其中所述至少一比對識別資料與所述至少一認證識別資料可以是聲紋、指紋、虹膜、指靜脈、人臉的其中任意至少一種生物特徵或者密碼或圖形。

【第18項】 如申請專利範圍第 1 7 項的防盜管制方法，其中所述至少一比對識別資料與所述至少一認證識別資料可以是同一生物特徵或不同一生物特徵。

【第19項】 如申請專利範圍第 1 0 項的防盜管制方法，進一步包括：

一個復歸步驟，在鎖裝置設定為解鎖狀態且被操作之後及／或者手動設定防盜設備進入防盜狀態時，防盜設備重新執行進入防盜狀態步驟。

【第20項】 一種防盜管制方法，其包括：將至少一比對識別資料與至少一認證識別資料儲存在一電子鑰匙內，並且將一防盜解除識別資料儲存在防盜設備內，當電子鑰匙比對所輸入的一即時識別資料與比對識別資料相符的狀態下，電子鑰匙的一顯示器顯示所述的至少一認證識別資料，所述防盜設備讀取顯示器顯示的至少一認證識別資料，並比對所物至少一認證識別資料與防盜解

除識別資料相符的情況下，防盜設備設定為解除狀態，防盜設備具有的一鎖裝置設定為解鎖狀態，當電子鑰匙比對所輸入的即時識別資料與至少一比對識別資料不相符的狀態下，電子鑰匙的顯示器不顯示所述至少一認證識別資料，防盜設備保持為上鎖狀態。

【第21項】如申請專利範圍第20項的防盜管制方法，其中進一步包括將對應一可控制設備與所述至少一認證識別資料的至少一個人化設定值儲存在防盜設備中，在執行解除防盜狀態步驟時依據防盜設備所讀取的所述至少一認證識別資料選擇對應的所述至少一個人化設定值設定可控制設備。

【第22項】如申請專利範圍第21項的防盜管制方法，進一步包括：

一個手動調整步驟，在所述至少一個人化設定值設定可控制設備之後，允許手動調整所述可控制設備的設定值。

【第23項】如申請專利範圍第21項的防盜管制方法，進一步包括：

一個停止運作或休眠步驟，在所述至少一個人化設定值設定可控制設備之後，使用電子鑰匙與一讀取器連線，防盜設備輸出一個停止設定值或休眠設定值給所述可控制設備，可控制設備執行停止運作或休眠。

【第24項】如申請專利範圍第20項的防盜管制方法，其中所述至少一比對識別資料與所述至少一認證識別資料可以是聲紋、指紋、虹膜、指靜脈、人臉的其中任意至少一種生物特徵或者密碼或圖形。

【第25項】如申請專利範圍第24項的防盜管制方法，其中所述至少一比對識別資料與所述至少一認證識別資料可以是同一生物特徵或不同一生物特徵。

【第26項】 一種防盜管制系統，包括一個電子鑰匙以及一個防盜設備，其中：

所述電子鑰匙，包括：

一個微處理器；

一個記憶體，與微處理器電連接，記憶體內儲存至少一個比對識別資料以及至少一個認證識別資料；

一個顯示器，與微處理器電連接，顯示器可顯示認證識別資料於畫面上，電子鑰匙可輸入可暫存的一個即時識別資料，當輸入的即時識別資料與比對識別資料不相符時，顯示器不顯示認證識別資料於畫面上，當輸入的即時識別資料與比對識別資料相符時，顯示器顯示認證識別資料於畫面上；

所述防盜設備包括：

一個微處理單元；

一個鎖裝置，與微處理單元電連接，微處理單元可設定鎖裝置為上鎖狀態或解鎖狀態；

一個主記憶體，與微處理單元電連接，主記憶體中儲存至少一個防盜解除識別資料；

一個影像讀取器，與微處理單元電連接，影像讀取器可讀取顯示器顯示於畫面的認證識別資料，且當所讀取的認證識別資料與防盜解除識別資料不相符時，所述鎖裝置設定為上鎖狀態，當所讀取的認證識別資料與防盜解除識別資料相符時，所述鎖裝置設定為解鎖狀態。

【第27項】 如申請專利範圍第 2 6 項所述的防盜管制系統，進一步包括：

一個可控制設備，與微處理單元電連接，所述主記憶體進一步儲存對應所

述可控制設備的一個人化設定值，當鎖裝置被設定為解鎖狀態時，所述微處理單元使用所述個人化設定值設定所述可控制設備。

【第28項】 如申請專利範圍第27項所述的防盜管制系統，進一步包括：

一個讀取器，與防盜設備的微處理單元電連接，當讀取器讀取所述電子鑰匙時，所述微處理單元使用一個停止設定值或休眠設定值設定所述可控制設備為停止或休眠狀態。

【第29項】 如申請專利範圍第26項所述的防盜管制系統，電子鑰匙進一步包括：

一個第一電極，與微處理器電連接；

所述防盜設備進一步包括：

一個供電模組，與微處理單元電連接；

一個第二電極，與微處理單元電連接，當電子鑰匙的第一電極與防盜設備的第二電極沒有電連接時，所述顯示器無法運作，當電子鑰匙的第一電極與防盜設備的第二電極電連接時，顯示器可顯示認證識別資料於畫面上。

【第30項】 如申請專利範圍第29項所述的防盜管制系統，其中所述防盜設備進一步包括：

一個主輸入設備，與微處理單元電連接，所述可暫存的即時識別資料係在電子鑰匙的第一電極與防盜設備的第二電極電連接的狀態下，使用主輸入設備輸入。

【第31項】 如申請專利範圍第29項所述的防盜管制系統，其中所述影像讀取器與第二電極共同構成為一個讀卡設備，所述電子鑰匙可選擇地與讀卡設

備可拆卸地結合後，所述第二電極與第一電極電連接，所述顯示器位於讀卡設備內側且與影像讀取器對齊。

【第32項】 如申請專利範圍第26項所述的防盜管制系統，電子鑰匙進一步包括：

一個供電單元，與微處理器電連接，供電單元供應電子鑰匙運作所需的電力。

【第33項】 如申請專利範圍第32項所述的防盜管制系統，其中電子鑰匙進一步包括：

一個輸入設備，與微處理器電連接，所述可暫存的即時識別資料係由輸入設備輸入。

【第34項】 如申請專利範圍第32項所述的防盜管制系統，進一步包括：

一個管理設備，包括一個處理器以及與處理器電連接的一個第一連線模組以及一個管理輸入設備，所述電子鑰匙進一步包括與微處理器電連接的一個近場通訊模組，當近場通訊模組與第一連線模組連線時，可使用管理輸入設備將所述至少一比對識別資料與至少一認證識別資料輸入電子鑰匙的記憶體中儲存。

【第35項】 如申請專利範圍第29項所述的防盜管制系統，進一步包括：

一個管理設備，包括一個處理器以及與處理器電連接的一個電連接器以及一個管理輸入設備，當第一電極與電連接器電連接時，可使用管理輸入設備將所述至少一比對識別資料與至少一認證識別資料輸入電子鑰匙的記憶體中儲存。

【第36項】 如申請專利範圍第 2 6 項所述的防盜管制系統，其中所述電子鑰匙的顯示器是由電子紙所構成。

