



(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 201912909 A

(43) 公開日：中華民國 108 (2019) 年 04 月 01 日

(21) 申請案號：106130862

(22) 申請日：中華民國 106 (2017) 年 09 月 08 日

(51) Int. Cl.:

*E05B47/00 (2006.01)**G06F21/30 (2013.01)*

(71) 申請人：國立成功大學 (中華民國) NATIONAL CHENG KUNG UNIVERSITY (TW)

臺南市大學路一號

(72) 發明人：李威勳 LEE, WEI-HSUN (TW)；魏健宏 WEI, CHIEN-HUNG (TW)；周建銘 CHOU, CHIEN-MING (TW)

(74) 代理人：吳豐任；李俊陞；戴俊彥

申請實體審查：有 申請專利範圍項數：12 項 圖式數：6 共 25 頁

(54) 名稱

智慧鎖以及智慧鎖控制方法

SMART LOCK AND CONTROL METHOD OF SMART LOCK

(57) 摘要

一種用以設置於一交通載具上的智慧鎖，包含一鎖具；一無線通信模組用以與一用戶終端進行通信；一儲存單元用以預先儲存複數個預定無線裝置之識別資料；以及一驗證單元電連接該鎖具、該無線通信模組以及該儲存單元；其中當該無線通信模組從該用戶終端接收一請求解鎖信號時，該無線通信模組傳送該鎖具之識別資料至該用戶終端，以進一步接收該用戶終端傳來之第一驗證資料，該第一驗證資料是對一第一無線裝置之識別資料與該鎖具之識別資料加密而產生，該驗證單元用以根據該第一驗證資料以對該鎖具進行解鎖。

A smart lock for a vehicle includes a lock unit; a wireless communication module configured to communicate with a user terminal; a storage unit configured to pre-storage identity data of a plurality of wireless devices; and a authenticating unit electrically connected to the lock unit, the wireless communication module and the storage unit; wherein when the wireless communication module receives a unlock request signal from the user terminal, the wireless communication module transfers identity data of the lock unit to the user terminal to further receives first authentication data from the user terminal, the first authentication data is generated by encrypting identity data of a first wireless device and the identity data of the lock unit, the verifying unit is configured to unlock the lock unit according to the first verification data.

指定代表圖：

符號簡單說明：

10 . . . 智慧鎖

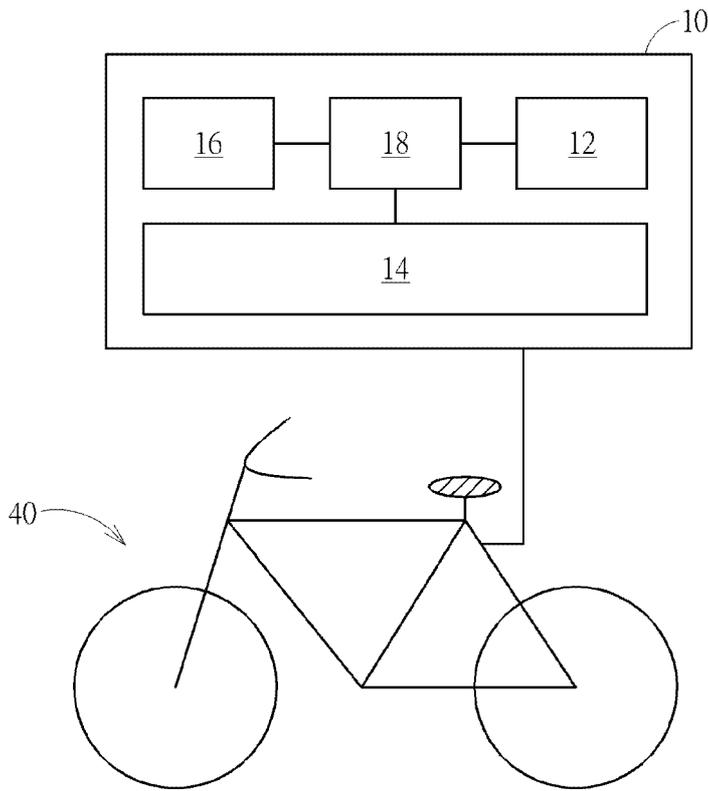
12 . . . 鎖具

14 . . . 無線通信模
組

16 . . . 儲存單元

18 . . . 驗證單元

40 . . . 自行車



第1圖

【發明說明書】

【中文發明名稱】 智慧鎖以及智慧鎖控制方法

【英文發明名稱】 SMART LOCK AND CONTROL METHOD OF SMART LOCK

【技術領域】

【0001】 本發明是相關於一種用於交通載具之智慧鎖，尤指一種可根據周圍無線裝置之識別資料以對交通載具進行上鎖或解鎖之智慧鎖。

【先前技術】

【0002】 習知公共自行車的租借與歸還需要藉由特定的自行車架來管理，當使用者欲租用自行車或歸還自行車時，必須在設置於定點的特定自行車架進行租用或歸還。然而，設置於定點的自行車架不僅體積龐大佔空間，並且架設成本高。目前市面上亦有搭載全球定位系統(Global Positioning System, GPS)之公共自行車可以租用，搭載GPS之公共自行車之租用及歸還並不需要藉由特定自行車架，可以於任意地點或指定地點進行租用及歸還。然而，GPS之定位功能於陰天或雨天時效能較差，天氣不好時可能導致搭載GPS之公共自行車定位錯誤，甚至於接收不到衛星訊號而無法定位，進而使得使用者無法得知公共自行車的位置。

【發明內容】

【0003】 本發明之目的在於提供一種可根據周圍無線裝置之識別資料以對交通載具進行上鎖或解鎖之智慧鎖，以解決先前技術的問題。

【0004】 本發明智慧鎖用以設置於一交通載具上，該智慧鎖包含一鎖具、一

無線通信模組、一儲存單元以及一驗證單元。該鎖具用以上鎖或解鎖該交通載具，該無線通信模組用以與一用戶終端進行通信，該儲存單元用以預先儲存複數個預定無線裝置之識別資料，該驗證單元電連接該鎖具、該無線通信模組以及該儲存單元，其中當該無線通信模組從該用戶終端接收一請求解鎖信號時，該無線通信模組傳送該鎖具之識別資料至該用戶終端，以進一步接收該用戶終端傳來之第一驗證資料，該第一驗證資料是對一第一無線裝置之識別資料與該鎖具之識別資料加密而產生，該驗證單元用以根據該鎖具之識別資料解密該第一驗證資料以得到該第一無線裝置之識別資料，以及用以當該第一無線裝置之識別資料符合該複數個預定無線裝置其中之一之識別資料時對該鎖具進行解鎖。

【0005】 在本發明智慧鎖的一實施例中，該無線通信模組另用以接收該第一無線裝置之識別資料，當該驗證單元判斷接收之該第一無線裝置之識別資料不符合該複數個預定無線裝置其中之一之識別資料時，該驗證單元不傳送該鎖具之識別資料至該用戶終端。

【0006】 在本發明智慧鎖的一實施例中，該第一驗證資料是由該用戶終端或一雲端伺服器對該用戶終端所傳送之該第一無線裝置之識別資料與該鎖具之識別資料加密而產生。

【0007】 在本發明智慧鎖的一實施例中，當該無線通信模組從該用戶終端接收一請求上鎖信號時，該無線通信模組進一步接收該用戶終端傳來之一第二驗證資料，該第二驗證資料是根據一第二無線裝置之識別資料與該鎖具之識別資料加密而產生，該驗證單元用以根據該鎖具之識別資料解密該第二驗證資料以

得到該第二無線裝置之識別資料，以及用以當該第二無線裝置之識別資料符合該複數個預定無線裝置其中之一之識別資料時對該鎖具進行上鎖。

【0008】 在本發明智慧鎖的一實施例中，該無線通信模組另用以接收該第二無線裝置之識別資料，當該驗證單元判斷接收之該第二無線裝置之識別資料不符合該複數個預定無線裝置其中之一之識別資料時，該驗證單元不傳送該鎖具之識別資料至該用戶終端。

【0009】 在本發明智慧鎖的一實施例中，其中該第二驗證資料是由該用戶終端或一雲端伺服器對該用戶終端所傳送之該第二無線裝置之識別資料與該鎖具之識別資料加密而產生。

【0010】 本發明智慧鎖控制方法包含提供一智慧鎖設置於一交通載具上，該智慧鎖預先儲存複數個預定無線裝置之識別資料；當該智慧鎖接收一用戶終端所傳送之一請求解鎖信號時，該智慧鎖傳送該智慧鎖之識別資料至該用戶終端；該智慧鎖接收該用戶終端傳來之一第一驗證資料，該第一驗證資料是對一第一無線裝置之識別資料與該智慧鎖之識別資料加密而產生；該智慧鎖根據該智慧鎖之識別資料解密該第一驗證資料以得到該第一無線裝置之識別資料；以及當該智慧鎖判斷該第一無線裝置之識別資料符合該複數個預定無線裝置其中之一之識別資料時；該智慧鎖解鎖該交通載具。

【0011】 在本發明智慧鎖控制方法的一實施例中，該智慧鎖控制方法另包含提供一智慧鎖設置於一交通載具上，該智慧鎖預先儲存複數個預定無線裝置之識別資料；當該智慧鎖接收一用戶終端所傳送之一請求解鎖信號時，該智慧鎖

傳送該智慧鎖之識別資料至該用戶終端；該智慧鎖接收該用戶終端傳來之一第一驗證資料，該第一驗證資料是對一第一無線裝置之識別資料與該智慧鎖之識別資料加密而產生；該智慧鎖根據該智慧鎖之識別資料解密該第一驗證資料以得到該第一無線裝置之識別資料；以及當該智慧鎖判斷該第一無線裝置之識別資料符合該複數個預定無線裝置其中之一之識別資料時；該智慧鎖解鎖該交通載具。

【0012】 相較於先前技術，本發明智慧鎖於設置特定無線裝置的地點即可進行解鎖以租用自行車或進行上鎖以歸還自行車，可改善習知公共自行車需要架設龐大自行車架的缺點。另外，本發明智慧鎖於解鎖或上鎖程序之間所使用的無線通信技術可不包含GPS，因此本發明可以改善搭載GPS之公共自行車之定位會受天氣影響的缺點。

【圖式簡單說明】

【0013】

第1圖是本發明智慧鎖的功能方塊示意圖。

第2圖是本發明智慧鎖根據用戶終端之請求對交通載具進行解鎖之第一實施例的示意圖。

第3圖是本發明智慧鎖根據用戶終端之請求對交通載具進行上鎖之第一實施例的示意圖。

第4圖是本發明智慧鎖根據用戶終端之請求對交通載具進行解鎖之第二實施例的示意圖。

第5圖是本發明智慧鎖根據用戶終端之請求對交通載具進行上鎖之第二實施例的示意圖。

第6圖是本發明智慧鎖控制方法的流程圖。

【實施方式】

【0014】 請參考第1圖，第1圖是本發明智慧鎖的功能方塊示意圖。如第1圖所示，本發明智慧鎖10包含一鎖具12、一無線通信模組14、一儲存單元16以及一驗證單元18。智慧鎖10用以設置於一交通載具上，於本實施例中，智慧鎖10是用以設置於一自行車上，且可藉由鎖具12對自行車進行上鎖或解鎖。無線通信模組14用以與一用戶終端進行通信，於本實施例中，用戶終端可以是一手機並且藉由藍牙(Bluetooth)或近場通信(Near-field communication, NFC)通信技術與智慧鎖10的無線通信模組14進行通信，但本發明並不以此為限，用戶終端50也可以是不同裝置(例如平板電腦)經由不同的通信技術與無線通信模組14進行通信。儲存單元16用以預先儲存資料，驗證單元18電連接鎖具12、無線通信模組14以及儲存單元16。驗證單元18用以和用戶終端進行驗證程序以對鎖具12進行解鎖或上鎖。

【0015】 舉例來說，請參考第2圖，第2圖是本發明智慧鎖根據用戶終端之請求對交通載具進行解鎖之第一實施例的示意圖。如第2圖所示，當使用者藉由用戶終端50對智慧鎖10傳送請求解鎖信號時，智慧鎖10的無線通信模組14在接收到該請求解鎖信號後會將鎖具12的識別資料(例如識別碼)傳送至用戶終端50。使用者在收到鎖具12的識別資料並且確認想要租用(或解鎖)的目標後，使用者可藉由用戶終端50尋找並接收一第一無線裝置60之識別資料。於本實施例中，第一無線裝置60為一Wi-Fi無線路由器，其識別資料為該Wi-Fi無線路由器的媒體存取控制(Media Access Control, MAC)位址，但本發明並不以此限。其中，用戶終端50並不需要與第一無線裝置60有Wi-Fi的網路連線，用戶終端50既使在未和第

一無線裝置60連線的情況下，用戶終端50也可以經由Wi-Fi的聆聽模式(Listening Mode, Sniffing Mode or Monitoring Mode)接收第一無線裝置60的媒體存取控制位址。第一無線裝置60可以設置於特定地點(例如超商、賣場或其他公共場所)以利使用者租借或歸還自行車40。用戶終端50接收了第一無線裝置60之MAC位址後，用戶終端50可將該MAC位址以及鎖具12的識別資料傳送至一雲端伺服器70，雲端伺服器70用以根據一預定演算法(例如雜湊(hash))對用戶終端50所傳送之第一無線裝置60之MAC位址以及鎖具12之識別資料加密而產生一第一驗證資料並且將該第一驗證資料傳送至用戶終端50。用戶終端50接收了雲端伺服器70加密產生的第一驗證資料後可將第一驗證資料傳送至智慧鎖10的無線通信模組14。智慧鎖10在接收第一驗證資料後驗證單元18可根據該預定演算法及鎖具12之識別資料對第一驗證資料解密以得到第一無線裝置60之MAC位址。儲存單元16預先儲存了複數個無線裝置之MAC位址，驗證單元18在解密第一驗證資料後可將所得到的第一無線裝置60之MAC位址與預先儲存於儲存單元16的MAC位址比對，若第一無線裝置60之MAC位址符合預先儲存於儲存單元16的MAC位址其中之一時(代表租借地點是在清單中)，驗證單元18可進一步對鎖具12進行解鎖。若第一無線裝置60之MAC位址不符合預先儲存於儲存單元16的MAC位址其中之一時(代表租借地點不在清單中)，驗證單元18並不對鎖具12進行解鎖。

【0016】 換句話說，當使用者欲解鎖自行車40時，使用者的位置必須位於特定的無線裝置周圍，使用戶終端50可以接收到特定無線裝置的識別資料並傳送該特定無線裝置的識別資料至雲端伺服器70加密產生第一驗證資料。特定無線裝置的識別資料所加密產生的第一驗證資料就像是一把用以解鎖的鑰匙，由用戶終端50傳送該第一驗證資料至智慧鎖10以進行解鎖。於本實施例中，特定無線裝置為特定Wi-Fi無線路由器，例如可以與特定電信商、超商或賣場合作，將

歸屬於該特定電信商、超商或賣場的Wi-Fi無線路由器作為本發明智慧鎖的特定無線裝置，使得本發明智慧鎖必須位於該特定電信商、超商或賣場的Wi-Fi無線路由器周圍才能解鎖，但本發明並不以此為限。另外，於本實施例中，第一驗證資料是由雲端伺服器70加密產生，但本發明並不以此為限，第一驗證資料亦可以由用戶終端50自行加密產生。

【0017】 請參考第3圖，第3圖是本發明智慧鎖根據用戶終端之請求對交通戴具進行上鎖之示意圖。如第3圖所示，當使用者租用了自行車40使用完畢且欲歸還自行車40時，使用者可藉由用戶終端50對智慧鎖10傳送一請求上鎖信號。與解鎖過程相似地，智慧鎖10的無線通信模組14接收該請求上鎖信號後會將鎖具12的識別資料傳送至用戶終端50。使用者在收到鎖具12的識別資料後，藉由用戶終端50尋找並接收一第二無線裝置62之識別資料。於本實施例中，第二無線裝置62為不同於第一無線裝置60的一Wi-Fi無線路由器，其識別資料為該Wi-Fi無線路由器的媒體存取控制位址，但本發明並不以此為限，使用者解鎖與上鎖智慧鎖10亦可以藉由同一個Wi-Fi無線路由器的MAC位址，也就是智慧鎖10可以於同一地點解鎖與上鎖。相似地，用戶終端50接收了第二無線裝置62之MAC位址後，用戶終端50可將該MAC位址以及鎖具12的識別資料傳送至一雲端伺服器70，雲端伺服器70可根據該預定演算法對用戶終端50所傳送之第二無線裝置62之MAC位址以及鎖具12之識別資料加密而產生一第二驗證資料並且將該第二驗證資料傳送至用戶終端50。用戶終端50接收了雲端伺服器70加密產生的第二驗證資料後可將第二驗證資料傳送至智慧鎖10的無線通信模組14。智慧鎖10在接收第二驗證資料後驗證單元18可根據該預定演算法及鎖具12之識別資料對第二驗證資料解密以得到第二無線裝置62之MAC位址。驗證單元18可再將所得到的第二無線裝置62之MAC位址與預先儲存於儲存單元16的MAC位址比對，若第二

無線裝置62之MAC位址符合預先儲存於儲存單元16的MAC位址其中之一時(代表歸還地點是在清單中)，驗證單元18可進一步對鎖具12進行上鎖。若第二無線裝置62之MAC位址不符合預先儲存於儲存單元16的MAC位址其中之一時(代表歸還地點不在清單中)，驗證單元18並不對鎖具12進行上鎖。相似地，於本實施例中，第二驗證資料是由雲端伺服器70加密產生，但本發明並不以此為限，第二驗證資料亦可以由用戶終端50自行加密產生。

【0018】 另外，本發明智慧鎖10可以處於一暫時上鎖模式。使用者藉由第一驗證資料解鎖智慧鎖10並進一步租用自行車40後，當該使用者必須暫時離開自行車40需要對自行車40上鎖，但是不想要歸還自行車40時，使用者可藉由用戶終端50使智慧鎖10切換至暫時上鎖模式。當智慧鎖10被切換至暫時上鎖模式時，驗證單元18不需要接收及驗證第二驗證資料即可對鎖具12直接進行上鎖。使用者可藉由用戶終端50再次傳送第一驗證資料至智慧鎖10的無線通信模組14以解除智慧鎖10的暫時上鎖模式。另一方面，使用者在租用或歸還自行車40時亦可以傳送一全球定位系統(Global Positioning System, GPS)資料至雲端伺服器70，使雲端伺服器70紀錄自行車租還的地點，或是雲端伺服器70可預先儲存所有特定無線裝置之識別資料的地點資料，當使用者傳送無線裝置之識別資料至雲端伺服器70時以產生驗證資料時，雲端伺服器70可藉由無線裝置之識別資料所對應的預先儲存之地點資料以得知自行車租用與歸還的地點，並且進一步將可租用之公共自行車之地點提供給其他使用者。

【0019】 依據上述配置，當使用者欲租用自行車40時，可藉由用戶終端50接收第一無線裝置60之識別資料並傳送第一驗證資料至智慧鎖10的無線通信模組14，驗證單元18在驗證第一無線裝置60為特定無線裝置之一後解鎖自行車40。

另外，再藉由用戶終端50接收第二無線裝置62之識別資料並傳送第二驗證資料至智慧鎖10的無線通信模組14，驗證單元18在驗證第二無線裝置62為特定無線裝置之一後上鎖自行車40。本發明智慧鎖可利用特定無線裝置的發送的識別資料產生解鎖上鎖的驗證資料，使用者需要在可接收特定無線裝置信號的地點才能租用或歸還自行車，因此不設置自行車架也能限制使用者歸還自行車之地點。再者，本發明實施例中用戶終端用於解鎖及上鎖程序所使用的無線通信技術可以為藍芽(或NFC)以及Wi-Fi，並且雲端伺服器可預先儲存所有特定無線裝置之識別資料的地點資料，因此自行車40租用或歸還時的定位地點不會受到天氣影響。

【0020】 請參考第4圖，第4圖是本發明智慧鎖根據用戶終端之請求對交通戴具進行解鎖之第二實施例的示意圖。如第4圖所示，當智慧鎖10的無線通信模組14接收到使用者藉由用戶終端50所傳送請求解鎖信號時，智慧鎖10可利用無線通信模組14經由Wi-Fi通信技術(例如經由Wi-Fi的聆聽模式)檢查周圍是否有特定無線裝置，例如智慧鎖10可以從服務無線裝置名單中檢查各個無線裝置之MAC位址是否符合預先儲存於儲存單元16的MAC位址其中之一，而當智慧鎖10利用無線通信模組14檢查出周圍並不具有特定無線裝置時(代表租借地點不在清單中)，智慧鎖10的驗證單元18拒絕用戶終端50的解鎖請求(例如不傳送鎖具12之識別資料至用戶終端50以進行後續解鎖程序)，當智慧鎖10的無線通信模組14檢查出第一無線裝置60之識別資料符合預先儲存於儲存單元16的MAC位址其中之一時(代表租借地點是在清單中)，智慧鎖10的驗證單元18接受用戶終端50的解鎖請求並使無線通信模組14將鎖具12的識別資料傳送至用戶終端50，以進一步接收用戶終端50傳來之第一驗證資料，驗證單元18再對第一驗證資料進行驗證程序以進一步對鎖具12進行解鎖。產生第一驗證資料之程序以及驗證第一驗證資料

之程序相似於解鎖之第一實施例，在此不再加以說明。

【0021】 請參考第5圖，第5圖是本發明智慧鎖根據用戶終端之請求對交通戴具進行上鎖之第二實施例的示意圖。如第5圖所示，本發明當智慧鎖10無線通信模組14接收到使用者藉由用戶終端50所傳送請求上鎖信號時，智慧鎖10可利用無線通信模組14經由Wi-Fi通信技術檢查周圍是否有特定無線裝置。相似地，當智慧鎖10利用無線通信模組14經由Wi-Fi通信技術檢查出周圍並不具有特定無線裝置時(代表歸還地點不在清單中)，則智慧鎖10的驗證單元18拒絕用戶終端50的上鎖請求(例如不傳送鎖具12之識別資料至用戶終端50以進行後續上鎖程序)，當智慧鎖10的無線通信模組14檢查出第二無線裝置62之識別資料符合預先儲存於儲存單元16的MAC位址其中之一時(代表歸還地點是在清單中)，智慧鎖10的驗證單元18接受用戶終端50的上鎖請求並使無線通信模組14將鎖具12的識別資料傳送至用戶終端50，以進一步接收用戶終端50傳來之第二驗證資料，驗證單元18再對第二驗證資料進行驗證程序以進一步對鎖具12進行上鎖。產生第二驗證資料之程序以及驗證第二驗證資料之程序相似於上鎖之第一實施例，在此不再加以說明。本發明智慧鎖對交通戴具進行上鎖或解鎖之第二實施例可以於收到解鎖請求信號或上鎖請求信號時檢查周圍是否有特定無線裝置，並且於周圍不具有特定無線裝置時拒絕用戶終端的解鎖請求或上鎖請求，以避免使用者在無法租用或歸還的地點持續嘗試上鎖或解鎖而造成時間的浪費。

【0022】 另一方面，當智慧鎖10對交通戴具進行上鎖或解鎖時，用戶終端50或智慧鎖10可以將上鎖時間及解鎖時間(或租借時間長度)傳送至雲端伺服器70，以進一步對用戶終端50上的使用者帳號進行計費。

【0023】 請參考第6圖，第6圖是本發明智慧鎖控制方法的流程圖100。本發明智慧鎖控制方法的流程如下列步驟：

【0024】 步驟110：提供一智慧鎖設置於一交通載具上，該智慧鎖預先儲存複數個預定無線裝置之識別資料；

【0025】 步驟120：當該智慧鎖接收一用戶終端所傳送之一請求解鎖信號時，該智慧鎖傳送該智慧鎖之識別資料至該用戶終端；

【0026】 步驟130：該智慧鎖接收該用戶終端傳來之一第一驗證資料，該第一驗證資料是對一第一無線裝置之識別資料與該智慧鎖之識別資料加密而產生；

【0027】 步驟140：該智慧鎖根據該智慧鎖之識別資料解密該第一驗證資料以得到該第一無線裝置之識別資料；及

【0028】 步驟150：當該智慧鎖判斷該第一無線裝置之識別資料符合該複數個預定無線裝置其中之一之識別資料時；該智慧鎖解鎖該交通載具。

【0029】 相較於先前技術，本發明智慧鎖於設置特定無線裝置的地點即可進行解鎖以租用自行車或進行上鎖以歸還自行車，可改善習知公共自行車需要架設龐大自行車架的缺點。另外，本發明智慧鎖於解鎖或上鎖程序之間所使用的無線通信技術可不包含GPS，因此本發明可以改善搭載GPS之公共自行車之定位會受天氣影響的缺點。

以上所述僅為本發明之較佳實施例，凡依本發明申請專利範圍所做之均等變化與修飾，皆應屬本發明之涵蓋範圍。

【符號說明】

【0030】

10	智慧鎖
12	鎖具
14	無線通信模組
16	儲存單元
18	驗證單元
40	自行車
50	用戶終端
60	第一無線裝置
62	第二無線裝置
70	雲端伺服器
100	流程圖
110至150	步驟



201912909

申請日: 106/09/08

IPC分類:

E05B 47/00 (2006.01)**G06F 21/30** (2013.01)**【發明摘要】****【中文發明名稱】** 智慧鎖以及智慧鎖控制方法**【英文發明名稱】** SMART LOCK AND CONTROL METHOD OF SMART

LOCK

【中文】

一種用以設置於一交通載具上的智慧鎖，包含一鎖具；一無線通信模組用以與一用戶終端進行通信；一儲存單元用以預先儲存複數個預定無線裝置之識別資料；以及一驗證單元電連接該鎖具、該無線通信模組以及該儲存單元；其中當該無線通信模組從該用戶終端接收一請求解鎖信號時，該無線通信模組傳送該鎖具之識別資料至該用戶終端，以進一步接收該用戶終端傳來之第一驗證資料，該第一驗證資料是對一第一無線裝置之識別資料與該鎖具之識別資料加密而產生，該驗證單元用以根據該第一驗證資料以對該鎖具進行解鎖。

【英文】

A smart lock for a vehicle includes a lock unit; a wireless communication module configured to communicate with a user terminal; a storage unit configured to pre-storage identity data of a plurality of wireless devices; and a authenticating unit electrically connected to the lock unit, the wireless communication module and the storage unit; wherein when the wireless communication module receives a unlock request signal from the user terminal, the wireless communication module transfers identity data of the lock unit to the user terminal to further receives first authentication data from the user terminal, the first authentication data is generated by encrypting identity data of a first wireless device and the identity data of the lock

unit, the verifying unit is configured to unlock the lock unit according to the first verification data.

【指定代表圖】第（ 1 ）圖。

【代表圖之符號簡單說明】

10	智慧鎖
12	鎖具
14	無線通信模組
16	儲存單元
18	驗證單元
40	自行車

【特徵化學式】

無

【發明申請專利範圍】

【第1項】 一種智慧鎖，用以設置於一交通載具上，該智慧鎖包含：

一鎖具，用以上鎖或解鎖該交通載具；

一無線通信模組，用以與一用戶終端進行通信；

一儲存單元，用以預先儲存複數個預定無線裝置之識別資料；以及

一驗證單元，電連接該鎖具、該無線通信模組以及該儲存單元；

其中當該無線通信模組從該用戶終端接收一請求解鎖信號時，該無線通信模組傳送該鎖具之識別資料至該用戶終端，以進一步接收該用戶終端傳來之第一驗證資料，該第一驗證資料是對一第一無線裝置之識別資料與該鎖具之識別資料加密而產生，該驗證單元用以根據該鎖具之識別資料解密該第一驗證資料以得到該第一無線裝置之識別資料，以及用以當該第一無線裝置之識別資料符合該複數個預定無線裝置其中之一之識別資料時對該鎖具進行解鎖。

【第2項】 如請求項1所述的智慧鎖，其中該無線通信模組另用以接收該第一無線裝置之識別資料，當該驗證單元判斷接收之該第一無線裝置之識別資料不符合該複數個預定無線裝置其中之一之識別資料時，該驗證單元不傳送該鎖具之識別資料至該用戶終端。

【第3項】 如請求項1所述的智慧鎖，其中該第一驗證資料是由該用戶終端或一雲端伺服器對該用戶終端所傳送之該第一無線裝置之識別資料與該鎖具之識別資料加密而產生。

【第4項】 如請求項1所述的智慧鎖，其中當該無線通信模組從該用戶終端接收

一請求上鎖信號時，該無線通信模組進一步接收該用戶終端傳來之一第二驗證資料，該第二驗證資料是根據一第二無線裝置之識別資料與該鎖具之識別資料加密而產生，該驗證單元用以根據該鎖具之識別資料解密該第二驗證資料以得到該第二無線裝置之識別資料，以及用以當該第二無線裝置之識別資料符合該複數個預定無線裝置其中之一之識別資料時對該鎖具進行上鎖。

【第5項】 如請求項4所述的智慧鎖，其中該無線通信模組另用以接收該第二無線裝置之識別資料，當該驗證單元判斷接收之該第二無線裝置之識別資料不符合該複數個預定無線裝置其中之一之識別資料時，該驗證單元不傳送該鎖具之識別資料至該用戶終端。

【第6項】 如請求項4所述的智慧鎖，其中該第二驗證資料是由該用戶終端或一雲端伺服器對該用戶終端所傳送之該第二無線裝置之識別資料與該鎖具之識別資料加密而產生。

【第7項】 一種智慧鎖控制方法，包含：

提供一智慧鎖設置於一交通載具上，該智慧鎖預先儲存複數個預定無線裝置之識別資料；

當該智慧鎖接收一用戶終端所傳送之一請求解鎖信號時，該智慧鎖傳送該智慧鎖之識別資料至該用戶終端；

該智慧鎖接收該用戶終端傳來之一第一驗證資料，該第一驗證資料是對一第一無線裝置之識別資料與該智慧鎖之識別資料加密而產生；

該智慧鎖根據該智慧鎖之識別資料解密該第一驗證資料以得到該第一無線裝置之識別資料；以及

當該智慧鎖判斷該第一無線裝置之識別資料符合該複數個預定無線裝置其中之一之識別資料時；該智慧鎖解鎖該交通載具。

【第8項】 如請求項7所述的智慧鎖控制方法，另包含：

該智慧鎖接收該第一無線裝置之識別資料；以及

當該智慧鎖判斷接收之該第一無線裝置之識別資料不符合該複數個預定無線裝置其中之一之識別資料時，該智慧鎖不傳送該智慧鎖之識別資料至該用戶終端。

【第9項】 如請求項7所述的智慧鎖控制方法，其中該第一驗證資料是由該用戶終端或一雲端伺服器對該用戶終端所傳送之該第一無線裝置之識別資料與該智慧鎖之識別資料加密而產生。

【第10項】 如請求項7所述的智慧鎖控制方法，另包含：

當該智慧鎖接收該用戶終端所傳送之一請求上鎖信號時，該智慧鎖傳送該智慧鎖之識別資料至該用戶終端；

該智慧鎖接收該用戶終端傳來之一第二驗證資料，該第二驗證資料是對一第二無線裝置之識別資料與該智慧鎖之識別資料加密而產生；

該智慧鎖根據該智慧鎖之識別資料解密該第二驗證資料以得到該第二無線裝置之識別資料；以及

當該智慧鎖判斷該第二無線裝置之識別資料符合該複數個預定無線裝置其中之一之識別資料時，該智慧鎖上鎖該交通載具。

【第11項】 如請求項10所述的智慧鎖控制方法，另包含：

該智慧鎖接收該第二無線裝置之識別資料；以及
當該智慧鎖判斷接收之該第二無線裝置之識別資料不符合該複數個預定無線裝置其中之一之識別資料時，該智慧鎖不傳送該智慧鎖之識別資料至該用戶終端。

【第12項】 如請求項10所述的智慧鎖控制方法，其中該第二驗證資料是由該用戶終端或一雲端伺服器對該用戶終端所傳送之該第二無線裝置之識別資料與該智慧鎖之識別資料加密而產生。

