基於 Wi-Fi 與 Bluetooth 混合式無線識別技術門禁控制系統之設計與實作

徐茂馨[a] 劉嘉惟[a] 高駿嘉[a] 廖子翔[a] 蘇暉凱*[a] 楊明達[b]
國立虎尾科技大學 電機工程系[a]
工業技術研究院[b]
*hksu@nfu.edu.tw

摘要

本文提出一個基於 Wi-Fi (Wireless-Fidelity) 與 Bluetooth 通訊技術之連線特性的裝置識別方法，以減少在使用 Wi-Fi 與 Bluetooth 通訊技術建立資料連線時所需的人為操作，且將此方法整合現階段具普遍性之 RFID (Radio Frequency Identification) 及 NFC (Near Field Communication) 識別技術，完成一套「基於 Wi-Fi 與 Bluetooth 混合式無線識別技術門禁控制系統」。本系統主要架構分為三個子系統：門禁控制器 (Door Controller，DC)、門禁控制閘道器 (Door Control Gateway，DCG) 及門禁控制中心 (Door Control Center，DCC)。門禁控制器依無線通訊技術的支援種類來區別，可分為高階門禁控制器 (High-End Door Controller，H-EDC) 及低階門禁控制器 (Low-End Door Controller，L-EDC) 兩種，其主要藉由多種無線通訊技術來識別使用者所持之識別媒體，並決策其入口的通行開放與否；門禁控制閘道器除了負責監控多個門禁控制器之外，更扮演著門禁控制中心與門禁控制器之間的橋樑。門禁控制器將其產生之識別記錄傳送至門禁控制閘道器，門禁控制閘道器會藉此將識別記錄顯示於 GUI (Graphic User Interface) 並傳送至門禁控制中心進行儲存；門禁控制中心與多個門禁控制閘道器連接來管理各個區域，並透過門禁控制閘道器來管控其底下之門禁控制器。此外，門禁控制中心提供系統管理者與一般使用者兩種角色之操作介面，除了能讓系統管理者進行管理之外，亦可讓一般使用者查詢個人資料與識別紀錄。在系統反應時間之效能測試部分，高階/低階門禁控制器之反應時間皆小於 31ms，故依系統實測及效能評估之結果來觀察，減少了以往在使用 Wi-Fi 與 Bluetooth 通訊技術時多餘的人為操作。

關鍵詞：門禁控制、無線身分識別技術、無線網路、藍芽、近場通訊、無線辨識。

Abstract

This master thesis proposed a device identification method based on the connection property of Wi-Fi and Bluetooth to reduce human operating. The method of device identification integrates with RFID and NFC technology, and implements a door control system with the hybrid wireless identification technology based on Wi-Fi and Bluetooth. This system is divided into three subsystems: Door Controller (DC), Door Control Gateway (DCG) and Door Control Center (DCC). DC is separated to two types according to the ability of the controller: High-End Door Controller (H-EDC) and Low-End Door Controller (L-EDC). Such controllers can identify user device with wireless technologies and control door lockers. In the proposed system, each area has a DCG, and each DCG connects to DC. Thus, DCG also is a bridge between DCC and DC. DCs will send identification records to DCG. The identification record can be shown and stored on the DCG. The DCC is to manage multiple DCGs. Moreover, DCC provides the functions of system management and door-access log for administrators and users. Additionally, the system performance was measured, and the identification time of H-E/L-EDC is less than 31ms. Therefore, according to the result of system performance, the human operating can be reduced when using the door control system with hybrid wireless identification technologies.

Keywords: Door Control, Wireless Identification Technology, Wireless Network, Bluetooth, Near Field Communication, Radio Frequency Identification.

1. 前言

在過去有關於身分識別方法的相關研究中，曾出現透過 Wi-Fi 與 Bluetooth 通訊技術來進行身分識別之研究[3-5]。在這兩種無線通訊技術的環境底下，使用者所持之識別媒體須事先建立與門禁控制器之間的連線後，該裝置才能與門禁控制器交換識別資料或控制指令來進行身分辨識。例如，在 Wi-Fi 通訊技術下，識別媒體須事先加入門禁控制器所在的無線區域網路內，並成功建立 TCP Socket 或者 UDP Socket 之連線後，才能與門禁控制器進行識別資料或控制指令的交換；而在 Bluetooth 通訊技術下，識別媒體與門禁控制器於連線前須進行掃描以及裝置配對，等待配對完成並建立連線後，才能進行識別資料或控制指令的交換。

由上述可得知在進行 Wi-Fi 及 Bluetooth 連線的前置作業下，將會花費較多作業時間以及繁瑣的前置設定。故若以反應時間及實用性層面來考量，皆會發現以下問題：1. 識別媒體須事先安裝該識別系統之應用程式；2. 識別媒體皆須針對門禁控

制器進行繫鎖的前置設定；3. 識別媒體與門禁控制器建立資料傳輸通道後，以交換資料方式來進行身分識別之行為，因此考慮其人為操作時間以及使用便利性的改進空間仍然很大。

本文為改善原先使用 Wi-Fi 與 Bluetooth 通訊技術進行身分識別時，會耗費太多時間在前置設定作業之人為操作上，故提出一個不同於過去使用 Wi-Fi 與 Bluetooth 通訊技術相關系統之識別方法，並以減少識別媒體之人為操作、不影響識別媒體之連線狀態及確保識別媒體之唯一性為目標，且整合現階段具普遍性之 RFID 及 NFC 技術，完成一套「基於 Wi-Fi 與 Bluetooth 混合式無線識別技術門禁控制系統」。

2. 相關知識背景

本文利用 Wi-Fi 與 Bluetooth 之連線特性提出混合式無線識別技術。在 Wi-Fi 識別部分，Wi-Fi 訊框之擷取方式是利用運行於 Monitor 模式之無線網路裝置來進行。由表 1 所示，參考 To DS 及 From DS 可得知當 STA 在傳收無線網路訊框時，路徑 1 以及路徑 2 之訊框以發送者 MAC Address 作為識別依據；路徑 3 之訊框則是以接收者 MAC Address 為識別依據；路徑 4 為 AP 之間交換的訊框，故不加以參考。綜合上述方法來作為混合式無線識別技術之 Wi-Fi 部分。如圖 1 所示，在混合式無線識別技術之 Bluetooth 部分，則是藉由 Master 裝置對 Slave 裝置發送 Inquiry 訊息後，Slave 裝置傳回具唯一性之 BD_ADDR，藉此來做為 Bluetooth 裝置識別之依據。本文除了提出上述之 Wi-Fi 裝置識別方法與 Bluetooth 裝置識別方法外，亦整合入了現階段最具普遍性之 RFID 識別方法及 NFC 識別方法，完成一套門禁控制系統。

表 1 Wi-Fi 訊框資料流向路徑表

Frame Type	Path	To DS	From DS	Addr1	Addr2	Addr3	Addr4
IBSS	1	0	0	DA	SA	BSSID	x
To AP	2	1	0	BSSID	SA	DA	x
From AP	3	0	1	DA	BSSID	SA	x
WDS	4	1	1	RA	TA	DA	SA

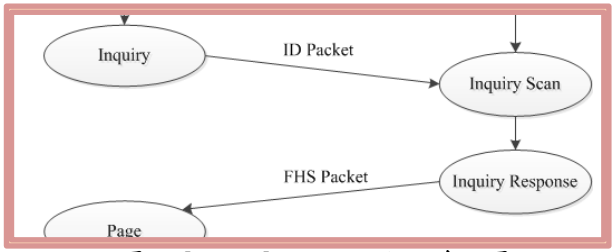

圖 1 Bluetooth 之 Inquiry 流程圖

3. 系統架構

本文利用 Wi-Fi 之訊框特性及 Bluetooth 建立連線前之 Inquiry 作業所出現的連線特性，提出一個基於 Wi-Fi 與 Bluetooth 通訊技術之裝置識別方法，並將該方法整合目前具普遍性之 RFID 與 NFC 身分識別方式，完成一套「基於 Wi-Fi 與 Bluetooth 混合式無線識別技術門禁控制系統」。而該系統主要可分為四個部分來討論：

- 第一部分：介紹基於 Wi-Fi 與 Bluetooth 混合式無線識別技術門禁控制系統之系統架構及運作流程。
- 第二部分：介紹子系統-高階/低階門禁控制器之系統架構及運作流程。
- 第三部分：介紹子系統-門禁控制閘道器之系統架構及運作流程。
- 第四部分：介紹子系統-門禁控制中心之系統架構及運作流程。

本文所提出的「基於 Wi-Fi 與 Bluetooth 混合式無線識別技術門禁控制系統」之系統架構如圖 2 所示，主要可分為三個子系統：門禁控制中心、門禁控制閘道器以及門禁控制器。

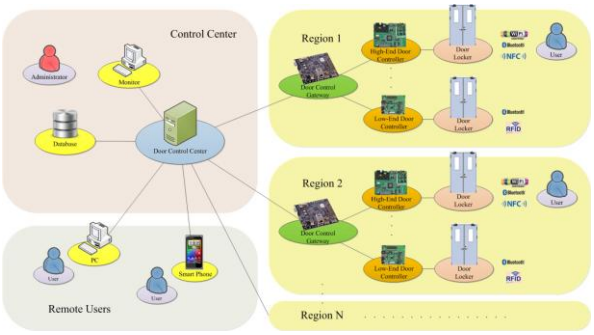

圖 2 門禁控制系統之系統架構

門禁控制中心擁有一個中央資料庫，負責儲存識別媒體之相關資料、門禁控制閘道器與門禁控制器相關設定以及使用者之識別記錄...等功能，並提供操作介面給予系統管理者進行識別媒體與系統裝置的資料編輯。另外，門禁控制中心亦提供一般使用者之操作介面，讓使用者可查詢個人相關資訊。而門禁控制中心為了達到多重區域控管之目的，將與多個門禁控制閘道器連接，使其可藉由門禁控制閘道器來進行多重區域控管；門禁控制閘道器除了扮演著區域管理者的角色以及監控多個門禁控制器之外，更扮演著門禁控制中心與門禁控制器之間的橋樑，使門禁控制器識別後所產生之識別記錄，能透過門禁控制閘道器傳送至門禁控制中心進行識別記錄之儲存；而高階/低階門禁控制器扮演著出入口的把關者，透過多種無線通訊技術來識別使用者所持識別媒體，負責開放通行與否的決策。

4. 系統設計與實作

本文所提出之基於 Wi-Fi 與 Bluetooth 混合式無線識別技術門禁控制系統可分為門禁控制器、門禁控制閘道器及門禁控制中心等三個子系統，各子系統皆負責不同之工作，在本章將討論各子系統軟硬體之相關設計。

4.1 高階門禁控制器設計

如圖 3 所示為高階門禁控制器硬體元件圖，高階門禁控制器採用 ADI Engineering Sidewinder 為系統開發平台，其核心為 IXP465。由於 Sidewinder 已提供 USB 2.0 通訊介面，因此 USB to GPIO 模組可直接透過 USB 連接至 Sidewinder；NFC 模組須將其 TTL 電位轉換為 RS232 電位後，再透過 USB to Serial 轉接線連接至 Sidewinder；Bluetooth Module 直接透過 USB to Serial 轉接線連接至 Sidewinder。而 Wi-Fi Module 則是透過 mini-PCI 連接至 Sidewinder。

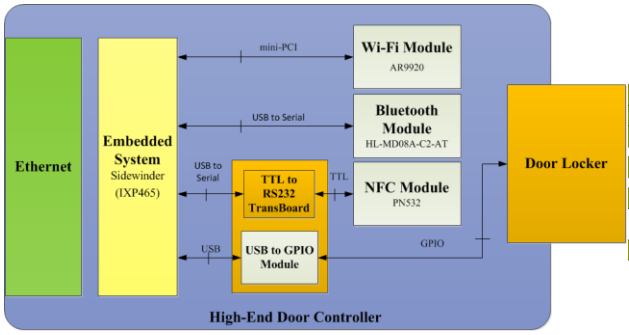

圖 3 高階門禁控制器硬體元件圖

4.2 低階門禁控制器設計

低階門禁控制器硬體元件如圖 4 所示，其採用 Microchip APP1632 為開發平台，並搭配 PIC32MX795F512L 之 MCU 為系統核心，另加裝 Ethernet 網路模組。無線通訊模組方面，Bluetooth 模組及 RFID 模組經由 RS232 電位轉換為 TTL 電位後連接至 PIC32MX795F512L 之 UART 接腳。另外，門鎖控制訊號由 PIC32MX795F512L 之 GPIO 直接輸出。

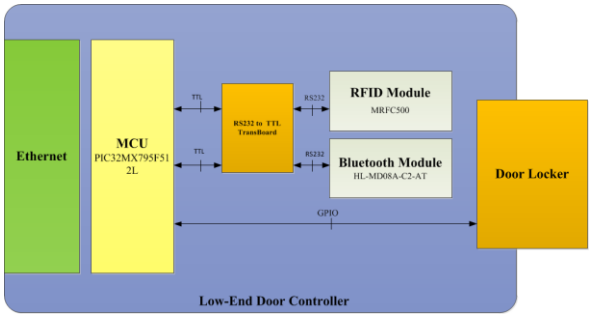

圖 4 低階門禁控制器硬體元件圖

4.3 門禁控制閘道器設計

門禁控制閘道器主要之功能在於蒐集其負責區域下所有高階/低階門禁控制器所傳來之識別記錄，以及提供使用者白名單給其所屬之門禁控制器，並利用圖形化介面使區域管理者進行監控。

當門禁控制閘道器啟動後會進入系統狀態頁面，而畫面上方共有四個分頁按鈕，分別為 Home、Log Message、Direct Control 以及 About 頁面。門禁控制閘道器啟動後會向門禁控制中心下載其所管理區域之相對地圖及使用者白名單…等相關資料。如圖 5 所示為門禁控制閘道器之系統狀態頁面，管理者可透過此畫面右半部了解該區域之結構以及其底下門禁控制器之裝設地點。而畫面之左半邊可分為上下兩欄，上欄在描述目前下拉式選單內所選擇之門口的相關訊息，如連線狀態、所屬規格及前次識別記錄等等；下欄為門禁控制閘道器之系統運作狀態，其可記錄各門禁控制器之連線與斷線以及識別記錄等。

圖 5 門禁控制閘道器之系統狀態頁面

4.4 門禁控制中心設計

為了讓使用者在存取門禁控制中心相關服務時，不會受到平台及作業系統的限制，因而採用 HTTP Server 來實現門禁控制中心。HTTP Server 選擇 Apache 作為伺服器以及 MySQL 作為資料庫。而門禁控制中心之使用者介面則是採用 HTML、PHP、CSS 及 JavaScript 等組合來呈現。

門禁控制中心主要在於儲存其底下之門禁控制閘道器與高階/低階門禁控制器相關資料，以及一般使用者與系統管理者的相關資訊。因此可將實體分為 4 類：門禁控制閘道器、門禁控制器、一般使用者以及系統管理者。

門禁控制中心主要在於儲存其底下之門禁控制閘道器與高階/低階門禁控制器相關資料，以及一般使用者與系統管理者的相關資訊。因此可將實體分為 4 類：門禁控制閘道器、門禁控制器、一般使用者以及系統管理者。

系統需儲存哪些使用者可以出入哪些門口，命名其為 Pass 實體型態；另外，系統需儲存使用者

在出入門口時所產生之識別記錄，命名其為 Log 實體型態，因此整理出上述幾個實體型態後，可以得到如圖 6 所示之門禁控制中心實體關聯圖 (Entity-Relationship Diagram，ERD)。

門禁控制中心之網站依使用角色可分為系統管理者及一般使用者，兩者皆為獨立個體，故門禁控制中心網頁管理介面之路徑也就跟著不同。系統管理者之角色可針對系統裝置或者是使用者裝置進行配置。在系統裝置方面，其主要針對目前資料庫內之門禁控制器及門禁控制閘道器等進行增刪與編輯；而在使用者裝置方面，主要針對使用者相關資料與識別媒體資料之修改，亦可對使用者進行增加或者刪減之動作。一般使用者之角色除了可瀏覽自身識別記錄及通行權限等相關資料，方便使用者取得所需資訊之外，亦可針對使用裝置之資料進行修改。

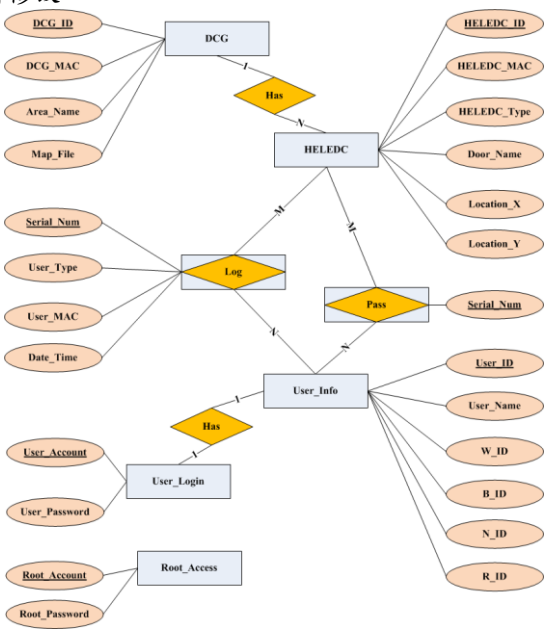

圖1 門禁控制中心之實體關聯圖

門禁控制中心除了提供網站給管理者及使用者使用外，在背景下提供了許多與門禁控制閘道器相關的功能模組，例如資料更新模組及資料上傳模組等。如圖 7 所示為系統管理者之網站架構圖。與一般使用者之使用的網站不同，門禁控制中心之系統管理者擁有一獨立存取之網站。

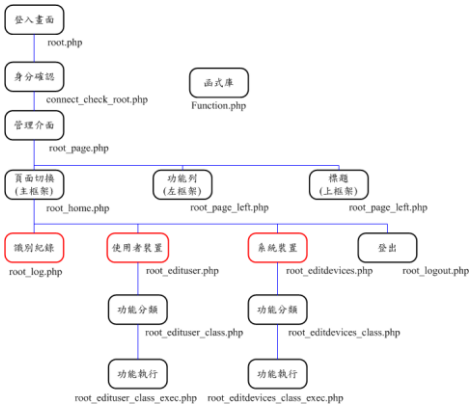

圖 7 系統管理者角色之網站架構圖

5 系統實測與效能評估

5.1 系統實測

在本節中，將套用情境來說明本文所提出之門禁控制系統整體之運作流程，其測試情境設定如下：新區域 Research and Development Department 將受本文所提出之制系統控管，其地圖檔為 research.png，且底下設有兩個出入口：West Door 及 East Door，分別安裝低階門禁控制器與高階門禁控制器；另外新增兩名使用者：EmnaLab 及 MaoSinSyu。

使用者即可利用其控制器所支援之識別技術來進行識別。如圖 8(a)所示，為使用者 MaoSinSyu 於低階門禁控制器前，利用智慧型手機之 Bluetooth 裝置來進行身分識別；如圖 8(b)所示，為使用者 MaoSinSyu 於高階門禁控制器前，利用智慧型手機之 Wi-Fi 裝置來進行身分識別。各控制器比對自身之使用者白名單後來決定是否解除門鎖，圖中各控制器皆已識別出使用者所持之識別媒體為可通行之裝置，並輸出門鎖控制訊號。

(a) 低階門禁控制器使用 Bluetooth 識別　(b) 高階門禁控制器使用 Wi-Fi 識別

圖 8 使用者於門禁控制器進行識別

5.2 效能評估

本文將系統安裝在一無 Wi-Fi 及 Bluetooth 等通訊干擾下之空間作為測試環境，並針對高階門禁控制器與低階門禁控制器進行系統反應時間與使用者白名單下載速度等效能測試。測試媒體採用智慧型手機與 RFID 卡。而資料平均次數為 20 次。

評估一套系統的好壞，其對於使用者行為之反應速度為重要考量之一。本文在測試環境中安排了高階門禁控制器與低階門禁控制器，針對使用者所進行之識別行為來進行系統反應速度測試。當使用者持識別媒體進入門禁控制器探測範圍 (本文設定其 RSSI 小於 -20dbm，約 1 公尺) 後，門禁控制器一接收到使用者識別媒體之訊框的瞬間為系統反應時間之起點，控制器經訊框分析、資料查詢比對到送出門鎖控制指令後，電控門鎖因控制指令而動作之瞬間為系統反應時間之終點。

如圖 9 所示，將系統反應時間測試數據轉換為直條圖後，可觀察出各門禁控制器之反應時間平均皆小於 31ms。另外，可發現使用 SQLite 之高階門禁控制器，系統反應時間比低階門禁控制器較為長，其原因在於高階門禁控制器進行識別時，需將讀取存放於 Flash Memory 之使用者白名單。而低階門禁控制器則是讀取存放於 RAM 之使用者白名單，故兩者速度才有如此的差異。本文將高階門禁控制器之 SQLite 取代為 RAM 後，重新進行系統反應速度測試，可發現高階門禁控制器從 RAM 讀取使用者白名單之速度明顯加快一倍以上。

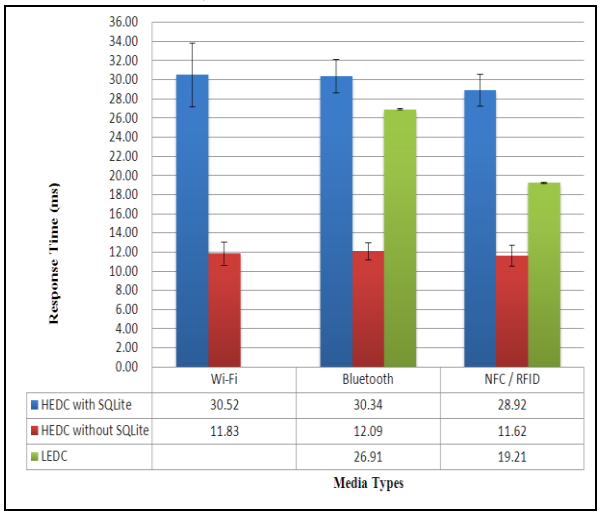

圖 9 系統反應時間比較圖

在門禁控制系統之效能測試上，本小節另外評估了高階/低階門禁控制器之使用者白名單下載速度，其對於各控制器之程式運作排程上為另一重要參考。門禁控制器另外須避免因使用者白名單尚在進行更新，卻發生控制器在擷取到裝置碼後而沒有資料可以進行比對的情況發生。因此本文在此小節將針對門禁控制器在進行使用者白名單下載時，其所花費之時間進行評估與測試。當高階/低階門禁控制器因定時更新或是門禁控制閘道器進行強制更新時，會以該時間點作為使用者白名單更新之時間起點。而在高階/低階門禁控制器更新使用者白名單並且儲存完成時，會以該時間點作為更新使用者白名單之時間終點。

如圖 10 所示，為高階/低階門禁控制器之使用者白名單下載速度測試圖，其測試下載的資料量分別為 10、20、50、80、100、200 及 500 筆使用者白名單，依控制器所支援的識別方式各進行 20 次清單下載測試，將其所測得之 20 個時間取平均值，並計算 95%信賴區間。可觀察到依照下載資料量的不同，各控制器所花費之時間亦會跟著有明顯差異。另外，依該圖可明顯發現高階門禁控制器之白名單下載時間皆比低階門禁控制器較為多，其原因一樣是在於高階門禁控制器是將使用者白名單存入其位於 Flash Memory 之資料庫內，以保持資料永久性。而低階門禁控制器則是將白名單暫存於 RAM，故兩者速度才有如此的差異。

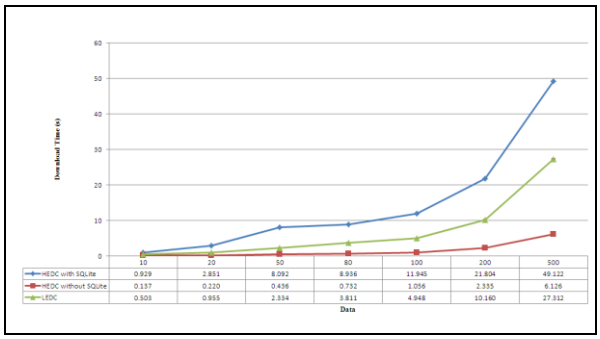

圖 10 門禁控制器白名單更新速度折線圖

6 結論與未來展望

本文利用 Wi-Fi 與 Bluetooth 通訊技術連線特性之裝置識別方法，並整合現階段具普遍性之 RFID 及 NFC 識別技術，完成一套「基於 Wi-Fi 與 Bluetooth 混合式無線識別技術門禁控制系統」。該系統之架構規劃了三個子系統：門禁控制器、門禁控制閘道器以及門禁控制中心，且各子系統皆負責不同之工作。門禁控制器依照無線通訊技術的支援種類來區別，可分為高階門禁控制器 (High-End Door Controller，H-EDC) 以及低階門禁控制器 (Low-End Door Controller，L-EDC) 兩種，其主要工作負責透過多種無線通訊技術來識別使用者所持之識別媒體，並負責開放通行與否的決策；門禁控制閘道器主要負責監控多個門禁控制器之外，亦扮演著門禁控制中心與門禁控制器之間的橋樑，使門禁控制器經識別動作後所產生之識別記錄，能透過門禁控制閘道器傳送至門禁控制中心進行識別記錄之儲存；門禁控制中心提供使用者之操作介面，讓使用者可查詢自身之相關資訊，且門禁控制中心為了達到多重區域控管之目的，其會與多個門禁控制閘道器連接，使其可利用門禁控制器來進行多區域之控管，讓各區域皆擁有門禁控制閘道器來進行區域管理。

本系統進行使用者白名單下載速度之效能評估後，可明顯發現高階門禁控制器白名單下載時間皆比低階門禁控制器較為多，而其原因在於高階門禁控制器是將白名單存入其資料庫之內，以保持資料永久性。而低階門禁控制器則是將白名單暫存於 RAM，因此兩者速度才有如此的差異。另外，系統反應時間之效能測試，屏除人為因素不考慮，可觀察到高階與低階門禁控制器之反應時間皆小於 31ms，屬於可接受範圍之內。因此，依照系統實測以及效能評估下來觀察，確實明顯地改善原先識別媒體在使用 Wi-Fi 與 Bluetooth 通訊技術與門禁控制器進行身分識別時的速度，去除了因網路相關前置設定所耗費的時間。本系統利用多種無線通訊技術作為身分之識別依據，未來可應用於人員進出管控或者服務業之暫時性身分識別依據，如人員進出管制、簽到退、電影票、遊樂園門票或其他暫時性服務之身分識別…等應用。

本系統藉由 Wi-Fi 與 Bluetooth 通訊技術的連線特性來使用智慧型手機進行身分識別，雖已達到不需識別媒體人工操作、不需安裝應用程式及確保裝置唯一性之目的，但由於所有識別媒體皆採無線技術，必然存在著遭到竊聽的可能性，故未來須加強安全性之部分。另外，在某裝置因斷電或其他外力因素而失去連線，為顧及系統之維護性，在未來將會加入 Error Code 機制，以利於維修人員進行系統修復。

參考文獻

[1] X. Li, G. Xu and L. Li, “RFID Based Smart Home Architecture for improving lives,” in Proc. 2008 2nd International Conference on Anti-counterfeiting, Security and Identification, 20-23 Aug. 2008, pp. 440-443.

[2] T. Mantoro and A. Milisic, "Smart card authentication for Internet applications using NFC enabled phone," in Proc. 2010 International Conference on Information and Communication Technology for the Muslim World (ICT4M), 13-14 Dec. 2010, pp. D13-D18.

[3] K. Y. Lian, S. J. Hsiao and W. T. Sung, “Home safety handwriting pattern recognition system,” in Proc. 2012 IEEE 11th International Conference on Cognitive Informatics & Cognitive Computing (ICCI*CC), 22-24 Aug. 2012, pp. 477-483.

[4] 籃嘉華，「無線網路技術應用於門禁系統之研究與實作」，國立中央大學資訊工程研究所，碩士論文，2004。

[5] J. Potts and S. Sukittanon, “Exploiting Bluetooth on Android mobile devices for home security application,” in Proc. 2012 Proceedings of IEEE Southeastcon, 15-18 March 2012, pp. 1-4.

[6] G. Dhivya C. Sethukkarasi and R. Pitchiah, “Wireless access control system based on IEEE 802.15.4,” in Proc. 2013 IEEE International Conference on Consumer Electronics (ICCE), Jan 2013, pp. 659-660.

[7] P. Wu, G. C. Wu, W. B. Xie, J. G. Lu and P. Li, “Remote Monitoring Intelligent System Based on Fingerprint Door Lock,” in Proc. 2010 International Conference on Intelligent Computation Technology and Automation (ICICTA), 11-12 May 2010, pp. 1012-1014.

[8] C. Z. Li and J. S. Lin, “Face recognition based on auto-switching magnetic door lock system using microcontroller,” in Proc. 2012 International Conference on System Engineering and Technology (ICSET), 11-12 Sept. 2012, pp. 1-6.

[9] “ Wireless Operating Modes”, http://wireless.kernel.org/en/users/Documentation/modes.

[10] W. S. Conner, J. Kruys, K. Kim and J. C. Zuniga, “IEEE 802.11s Tutorial Overview of the Amendment for Wireless Local Area Mesh Networking”, 13 Nov 2006.

[11] T. Thamrin, S. Sahib, “The Inquiry and Page Procedure in Bluetooth Connection,” Soft Computing and Pattern Recognition, 2009. SOCPAR '09. International Conference of, Dec. 2009, pp.218-222, 4-7.

[12] IEEE 802.11-2012, “IEEE Standard for Information Technology Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks Specific Requirements: - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications”, 29 March 2012.

[13] “Wi-Fi (Wireless Fidelity)”, http://www.wi-fi.org, 10 June 2013.

[14] IEEE 802.15.1-2005, “IEEE Standard for Information Technology Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements - Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs)”, 14 June 2005.

[15] 繆嘉新，「NFC 技術演進與標準化」，中華電信研究所，2008。

[16] EPCglobal Inc., “EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz – 960 MHz”, 10 June 2013.

[17] 劉穎昌，「RFID and NFC」，正隆 RFID 應用驗測中心，2008。

[18] ADI Engineering, Inc., “Sidewinder Board User’s Manual IXP465 Development Platform”, 17 July 2006.

[19] Wistron Neweb Corporation, “Approval Sheet for Model DNMA-92: An IEEE 802.11n a/b/g Mini-PCI module”, 13 Oct 2009.

[20] HotLife Electronic Technology Co.，「Bluetooth Serial Module HL-MD08A-C2 使用手冊」，2012。

[21] “ PN532 Board”, http://www.xfpga.com/html_products/PN532-breakout-board-24.html, 10 June 2013.

[22] USBIO Tech., “USB2ISP-2.0C Datasheet”, http://www.usb-i2c-spi.com, 10 June 2013.

[23] “ Airodump-ng”, http://www.aircrack-ng.org/doku.php?id=airodump-ng.

[24] Microchip Technology，「Microchip APP1632 使用說明書 (TW-UG-APP1632-E)」，http://www.microchip.com.tw，2010。

[25] Microchip Technology，「MCU4101T v2.0 Introduction PIC32 & MPLAB C32」，http://www.microchip.com.tw，2008。

[26] 鵬驥實業有限公司，http://pongee.diytrade.com.，2013。

[27] pandaboard.org, “OMAP4460 Pandaboard ES System Reference Manual”, http://pandaboard.org, 10 June 2013.