汽車遙控鑰匙整合指紋辨識之設計與分析

黃皇賓　梁智能　陳柏全
車輛研究測試中心

摘要

本論文主要是探討如何整合指紋辨識於免持鑰匙進入系統，以防止竊賊盜取和安全性攻擊。本論文提出指紋辨識整合於汽車遙控鑰匙的設計。目前為止，免持鑰匙進入系統的安全性探討，主要是針對防止暴力法破解攻擊、統計法攻擊和偽裝攻擊，但卻無法防止竊賊盜取。本論文提出的指紋辨識免持鑰匙進入系統，使用了修改後的車用 AES 加密無線通訊協定，除了提供更安全的保護來防止目前安全性攻擊，更可以防竊賊盜取。此外，利用指紋辨識可以正確分辨不同駕駛者，因此可以更準確的提供駕駛個人化的服務。在系統設計上，我們更考慮了未來可能成為防盜保全產品的因素，如成本，使用壽命和效能。最後更針對本系統的安全性進行分析，以證明本系統的安全性。

關鍵詞：免持鑰匙進入系統、指紋辨識、安全性攻擊。

1. 前言

目前進入汽車和啟動引擎方法主要有傳統機械鎖、汽車遙控器、和免持鑰匙進入系統[1]，但不管是傳統機械鎖、汽車遙控器、和免持鑰匙進入系統都必需使用駕駛者攜帶的汽車鑰匙做為認證的依據。目前針對汽車鑰匙的安全性設計上，都針對其無線通訊的加密，以防止暴力法破解攻擊、統計法攻擊和偽裝攻擊[2]。但實際應用時，駕駛者攜帶的汽車鑰匙有可能被竊賊盜取或遺失之後被其它人撿走，而造成防盜保全上的漏洞。利用駕駛者攜帶的汽車鑰匙做為認證的方法也無法辨識駕駛者的身分，除非每位駕駛者都有個人的汽車鑰匙，因此無法提供駕駛個人化的服務[1]。

生物特徵辨識技術克服了以上的問題。生物特徵辨識技術是利用駕駛者身上的生物特徵做為認證的依據，因此降低了被竊取的風險，也不會因為駕駛者的疏忽而遺失。此外，每位駕駛者的生物特徵是獨一無二的，因此可以做為辨識駕駛者的依據。未來可以提供駕駛個人化的服務。目前的生物特徵辨識技術有指紋、臉型、虹膜、手掌紋、聲音、靜脈、多模式辨識等。根據國際生物辨識組織（International Biometric Group，IBG）的研究指出[3]，2007年的生物特徵辨識市場的市佔率，將以自動指紋辨識（AFIS/Live-Scan）佔33.6%為比例最高，其次依序為指紋（佔25.3%）、臉型（佔12.9%）、中介軟體（佔5.4%）、虹膜（佔5.1%）、手掌紋（佔4.7 %）、聲音(語音)（佔3.2 %）、靜脈（佔3.0%）、多模式辨識（佔2.9 %），以及其他辨識（佔4.0 %）。其中自動指紋辨識和指紋佔了其中的58.9%，由此可知指紋辨識已成為生物辨識中的主流。指紋辨識成為主流的原因為其成本和運算量相較於其它生物特徵辨識比較少，因此較容易被市場接受。

本論文整合指紋辨識技術於免持鑰匙進入系統。整合指紋辨識的免持鑰匙進入系統可以防止暴力法破解攻擊、統計法攻擊、和偽裝攻擊，更可以保證鑰匙被竊賊盜取或遺失之後被其它人撿走後也不能使用。此外，更可利用每位駕駛者的指紋做為辨識駕駛者的依據，以提供駕駛個人化的服務。

2. 背景知識

2.1 指紋辨識技術

指紋辨識技術已經應用在日常生活之中。最常見的不外乎是筆記型電腦上利用指紋辨識技術來取代傳統鍵盤式個人帳號密碼的輸入。另一個應用是出現在行動裝置身上，如 USB 抽取式隨身碟或手機。而宿舍的門禁或自家中的保全門禁系統，也是生活中常見的應用。指紋辨識需經過以下的流程[1]，指紋辨識流程如圖 1：

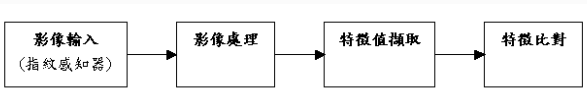

圖 1 指紋辨識流程圖

影像輸入：透過指紋感知器讀取到手指指紋的灰階影像。指紋感知器可分為光學式感知器、電容式感知器、溫差式感知器、和超音波式感知器。 目前市場上最常見的為電容式感知器。電容式感知器是利用微小的電流訊號來刺激皮膚表層，再藉由感測器表面密密麻麻的電容陣列單元，將電訊號的變化儲存起來。原理在於指紋凸脊 (ridge) 處會帶有較大的電荷，相對地在凹溝 (valley) 處的電荷則小得多或甚至不帶電，如此電容陣列即可透過記錄電荷的高低分佈，描繪出紋路形狀及深淺變化的立體圖像。

影像處理：對原始指紋的影像進行強化影像的影像處理，過濾雜訊、影像二值化、邊緣強化和影像旋轉校正。

特徵值擷取：指紋辨識是利用指紋上的特徵，因此需將指紋轉換成特徵值，且需保證不同的指紋不會產生相同的特徵值。演算法從指紋上找 minutiae 節點，如分叉、終止或打圈。最後把這些節點的座標和特徵轉成數值。

特徵比對：最後透過相似度比對的演算法把兩枚指紋的特徵值進行比對，得到兩個指紋的相似度結果後，再進行辨識是否為同一枚指紋。

2.2 免持鑰匙進入系統

免持鑰匙進入系統包含遠端遙控功能、免鑰進入

功能和汽車啟動禁制裝置[4]。駕駛者的手持式汽車遙控鑰匙通訊是透過433MHz（UHF）或125 kHz（LF）頻率。汽車傳送資料到汽車遙控鑰匙是是透過LF，以提供較省電的被動式感應。

當駕駛者拉起汽車車門門把，車上的天線電子控制單元會送出LF訊號到駕駛者的汽車遙控鑰匙。收到訊號後，汽車遙控鑰匙會進行初始化。發射範圍內的汽車遙控鑰匙都會收到訊號，但只有一個汽車遙控鑰匙會被選擇來進行認證。汽車遙控鑰匙認證通過後，天線電子控制單元會送出訊號開啓車門，並送出訊號請車內控制單元啟動駕駛個人化的服務。車上控制單元會根據駕駛者的個人的喜好調整座椅和後視鏡。

遠端遙控功能是指駕駛者在適當的距離可以控制車門開啟或關閉。按下駕駛者的汽車遙控鑰匙上的按鍵後，汽車遙控鑰匙會透過UHF送出單向類比訊號並喚醒車上的UHF接收器。UHF接收器解調UHF類比訊號然後轉換一個數位訊號到天線電子控制單元。天線電子控制單元解析數位訊號後決定執行的動作。免持鑰匙進入系統包含以下單元：

汽車遙控鑰匙：汽車遙控鑰匙包含控制單元可以控制週邊的模組和IO，如天線、電池、UHF傳輸模組和按鈕。

LF天線：在照後鏡或其它無屏蔽效應的位置有安裝天線以發射LF無線訊號到汽車遙控鑰匙。

UHF接收器：UHF接收器當收到汽車遙控鑰匙的UHF訊號會自動喚醒並開始認證。UHF接收器和車上控制單元連接在一起。汽車遙控鑰匙的UHF訊號通過認證後，會送出訊號給車上控制單元，請求開啓車門。

車門手把和按鈕：免持鑰匙進入系統仍然使用現有的車門門把，但在手把旁增加一個額外的按鈕，按下按鈕即執行關門程序。

車門控制模組：車門控制模組透過CAN匯流排和其它模組連接。車門控制模組連接車門手把和車門致動器。

車上控制單元：車上控制單元透過 CAN 匯流排和其它模組連接。車上控制單元可以根據不同鑰匙調整座椅位置和照後鏡位置。此外，也可以透過 CAN 匯流排控制車門控制模組。

2.3 車用 AES 加密無線通訊協定

免持鑰匙進入系統主要的通訊裝置包含駕駛者的汽車遙控鑰匙和車上的訊號接收傳送裝置。操作命令是利用RF無線通訊技術由汽車遙控鑰匙傳送到車上的訊號接收裝置。RF無線通訊是直接在開放空間傳送，因此訊號很容易被汽車竊賊攔截後解析出認證資料，而造成保全上的漏洞。車用AES加密無線通訊協定結合了AES加密的演算法和虛擬亂數，由汽車遙控鑰匙產生的虛擬亂數可以做為變動式金鑰，因此車用AES加密無線通訊協定可以成功防止安全性攻擊，如暴力法破解攻擊、統計法攻擊和偽裝攻擊。

車用AES加密無線通訊協定的通訊流程，如圖2。一開始汽車遙控鑰匙傳送訊號交換的要求給汽車。公式c1 = E(KEY, Car_ID)表示Car_ID利用金鑰KEY加密後產生密文c1。公式m1 = D(KEY, c1)表示c1利用金鑰KEY解碼出明文m1。解碼出來的m1即為Car_ID。Car_ID通過認證後，車上訊號傳送器傳送一個應答封包給汽車遙控鑰匙。所有的應答封包都用明文表示。公式c2 = E(KEY, PRN)表示汽車遙控鑰匙產生128bit的虛擬亂數並用金鑰KEY加密成c2密文。如果汽車成功解密了c2後，會回傳一個應答封包。公式m2 = D(KEY, c2)表示c2利用金鑰KEY解碼出明文m2。解碼出來的m2即為PRN。當汽車遙控鑰匙收到應答封包，一開始用的金鑰KEY會換成金鑰PRN，之後汽車遙控鑰匙會利用金鑰PRN對之後傳送給汽車的操作指令進行加密。公式c3 = E(PRN, OPERATION)表示利用金鑰PRN對操作指令OPERATION加密成密文c3。公式m3 = D(PRN, c3)表示c3利用金鑰PRN解碼出明文m3。解碼出來的m3即為OPERATION。如果通訊一直無法成功，且超過通訊時間，汽車遙控鑰匙會自動傳送一個中止通訊的訊號，並結束通訊。

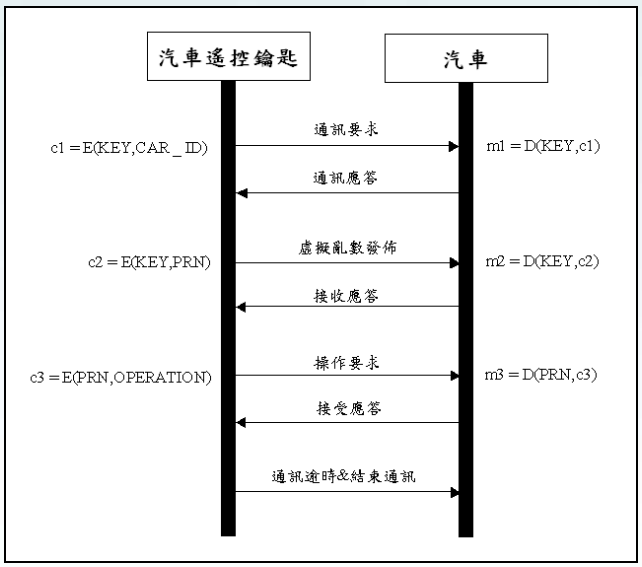

圖 2 車用 AES 加密無線通訊流程圖

3. 系統架構

3.1 指紋辨識免持鑰匙進入系統架構

本論文所設計的指紋辨識免持鑰匙進入系統的架構圖，如圖3所示。指紋辨識免持鑰匙進入系統包含汽車遙控鑰匙、天線接收傳輸模組、車門手把和按鈕、車門控制模組，和車用電腦。任何人在未通過指紋認證的情況下無法使用汽車遙控鑰匙。通過指紋認證後，即啓動汽車遙控鑰匙的被動式鑰匙功能，當駕駛者拉起汽車車門門把，車上的天線接收傳輸模組會送出RF (125 kHz)訊號到駕駛者的汽車遙控鑰匙。收到訊號後，汽車遙控鑰匙會啟動並和汽車進行安全認證。汽車遙控鑰匙認證通過後，車門控制模組會送出訊號開啓車門，並送出訊號請車用電腦啟動駕駛個人化的服務。汽車遙控鑰匙可以根據指紋來辨識目前的駕駛者，並透過無線通訊模組送出駕駛者的ID，以提供車用電腦參考，以設定目前的駕駛者的喜好參數值，如座椅位置、後視鏡位置、和MP3曲目等。

整個安全認證的流程是採用車用AES加密無線通訊協定。車用AES加密無線通訊協定結合了AES加密的演算法和虛擬亂數，汽車遙控鑰匙和汽車之間利用無線訊號傳輸的資料，都經過AES加密，且利用虛擬亂數做為變動式金鑰。本系統的安全認證的流程不怕汽

車竊賊攔截汽車遙控鑰匙和汽車之間的認證資料，因為認證資料採用了AES的加密技術加密，所以無法取得真正的認證資料，除非能破解AES加密技術，但目前為止還找不到可行的方法。此外，汽車竊賊想利用攔截到的RF訊號直接開啟車門也是不可行，因為每次認證的RF訊號都加入了虛擬亂數，因此每次認證都會改變。

指紋辨識免持鑰匙進入系統包含以下單元：

汽車遙控鑰匙：汽車遙控鑰匙包含SoC控制晶片可以控制無線傳輸模組、電容式指紋感知器和週邊的模組和IO，如天線、電池、UHF傳輸模組和按鈕。

天線接收傳輸模組：天線接收傳輸模組包含UHF訊號接收器、LF訊號發射器、和天線，並透過CAN匯流排和其它模組連接。天線裝設於照後鏡位置。

車門手把和按鈕：本系統跟其它免持鑰匙進入系統一樣，仍然使用現有的車門門把，但在手把旁增加一個額外的按鈕，按下按鈕即執行關門程序。拉起門把時則進行認證程序，通過後即自動開門。

車門控制模組：車門控制模組連接車門手把和車門致動器，並透過CAN匯流排和其它模組連接。

車用電腦：車用電腦提供駕駛個人化的服務，並透過CAN匯流排控制其它模組，如座椅、後視鏡、音響系統控制和空調系統控制等。

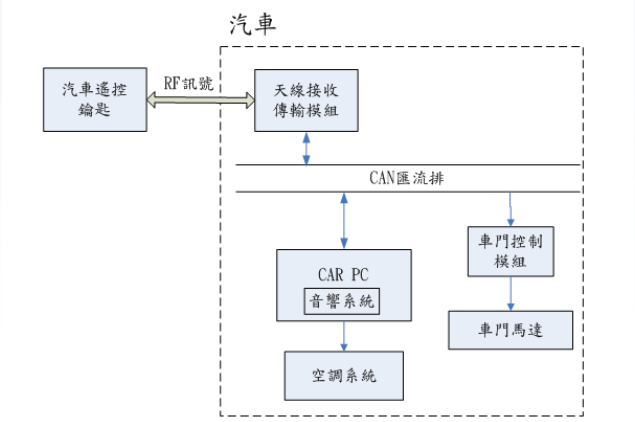

圖3 指紋辨識免持鑰匙進入系統架構圖

3.2 汽車遙控鑰匙的設計

免持鑰匙進入系統中，汽車遙控鑰匙是最重要的認證單元，可以做為打開車門和啟動引擎的依據。本論文整合指紋辨識系統於汽車遙控鑰匙，以防止汽車遙控鑰匙有可能被盜取或遺失之後被其它人撿走後，用來打開車門和啟動引擎。本論文設計的汽車遙控鑰匙的架構圖，如圖4所示。SoC控制晶片從電容式指紋感知器讀取到駕駛者指紋的灰階的影像，並利用演算法找出指紋影像上的特徵點。特徵點的座標和特徵會轉換成代表駕駛者指紋的特徵值。SoC控制晶片負責指紋的特徵值比對和管理。SoC控制晶片會把駕駛者指紋的指紋特徵和記憶體中的所有指紋特徵進行相似度比對，以決定駕駛者是否通過認證。駕駛者通過指紋認證後，汽車遙控鑰匙會點亮認證通過的狀態燈，駕駛者可以使用汽車遙控鑰匙的鑰匙功能或透過按鈕進行指紋新增或刪除的管理動作。汽車遙控鑰匙的鑰匙功能啟動後，汽車遙控鑰匙透過RF訊號接收器來接收汽車傳送的資料，RF訊號接收器接受到資料後會送給SoC控制晶片。SoC控制晶片根據汽車傳送過來的資料，透過RF訊號傳送器回應資料給汽車。SoC控制晶片執行整個無線通訊流程，並對傳送的資料利用AES演算法加密。AES加密演算法需要大量的運算，因此本系統採用的SoC控制晶片提供了硬體的AES加解密，以加速運算和節省電力。

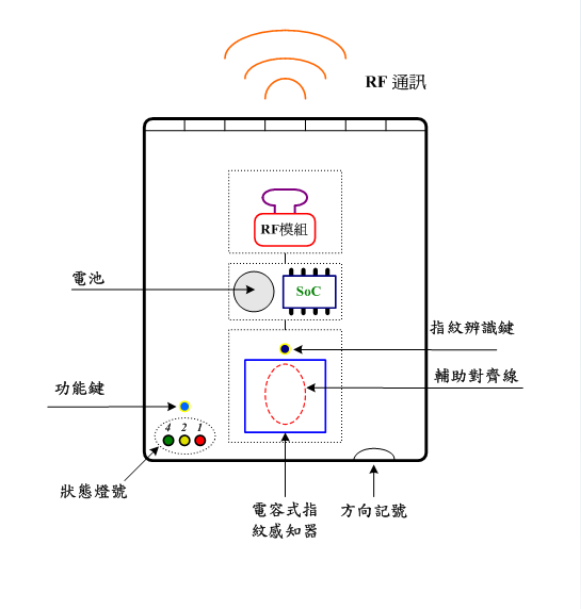

圖4 汽車遙控鑰匙架構圖

汽車遙控鑰匙在控制單元的設計上是採用晶片系統（System-on-Chip）的設計。將原本需提供大量運算資源的指紋辨識系統和汽車遙控鑰匙的控制系統整合於同一顆晶片中。將原來需透過外部傳輸訊號轉變成晶片的內部傳輸的訊號，不但縮短傳輸距離，亦可大幅增加訊號傳輸頻寬及速度，進而使效能大幅提升。系統原本所須之元件數也大幅減少，面積及體積亦隨之縮小。如此一來更適用於體積小的汽車遙控鑰匙。原本消耗於各IC元件間之外部訊傳遞之電能也將大幅減少，以延長汽車遙控鑰匙的電池壽命。汽車遙控鑰匙在指紋感知器的選用上是採用電容式指紋感知器。電容式指紋感知器的好處有成本低，體積小，並能抵抗環境的化學反應，所以很適合整合於體積小成本低的汽車遙控鑰匙[5]。

4. 系統分析

4.1 安全度分析

4.1.1 竊賊盜取

竊賊盜取是指竊賊假裝成泊車小弟、修車師、或其它手法竊取汽車遙控鑰匙，以達到竊車的目的。本論文中的免持鑰匙進入系統的汽車遙控鑰匙需要通過駕駛者指紋認證才能使用，因此就算竊賊用任何手法取得汽車遙控鑰匙也無法使用。竊賊盜取針對本論文中的免持鑰匙進入系統是無效，除非竊賊能取得駕駛者的指紋，但可能性是微乎其微。

4.1.2 暴力法破解攻擊

本論文中的免持鑰匙進入系統使用車用 AES 加密無線通訊協定。車用 AES 加密無線通訊協定使用金鑰長度為 128bit 的 AES 加密演算法。128bit 的金鑰提供了 2^{128} 可能的金鑰組合，這麼多的組合，就算利用每

秒可以檢查10^{18}可能金鑰組合的電腦也需要大約10^{13}才能破解，因此要使用暴力法破解攻擊在有效時間破解是不可能的。

4.1.3 統計法攻擊

統計法攻擊是從已知的內文和部份密碼中猜出可能的金鑰。車用 AES 加密無線通訊協定是使用固定金鑰對汽車認證碼加密。本論文中的免持鑰匙進入系統的汽車認證碼和固定金鑰是出廠時由汽車廠商提供,且不公開，因此無法使用統計法攻擊。

4.1.4 偽裝攻擊

偽裝攻擊是指竊賊攔截汽車和汽車遙控鑰匙之間通訊的無線訊號。竊賊使用同樣的訊號和汽車認證，就能通過認證。車用 AES 加密無線通訊協定使用的是可變動的金鑰，因此每次和汽車認證的金鑰都不同。如此一來，竊賊就無法使用同樣的訊號來通過認證。

4.2 安全性和便利性的分析

本論文設計的指紋辨識於免持鑰匙進入系統將指紋辨識系統整合於汽車遙控鑰匙，可以成功防止竊賊盜取。但在使用上必需事先通過指紋認證才能使用汽車遙控鑰匙。如果每次使用都需要指紋認證將會造成駕駛者使用上的不方便。雖然在汽車遙控鑰匙的設計已針對省電問題加以考量，但相較於其它免持鑰匙進入系統的汽車遙控鑰匙，多出指紋認證的功能，執行此功能會消耗相對多的電力。在未來的使用設計上需要針對使用者的習慣來設定通過認證後汽車遙控鑰匙的使用時間，如認證後可使用一小時，這樣如果只是暫時離開汽車，就不用重新認證。認證次數減少後電力消耗也會跟著減少。但較長的使用時間會增加竊賊盜取的風險，因此未來在使用設計應針對駕駛者使用習慣和竊賊的竊盜習性進行分析，以提供駕駛者方便又安全的系統。

5. 結論

本論文成功整合指紋辨識於免持鑰匙進入系統可以防止暴力法破解攻擊、統計法攻擊和偽裝攻擊，和竊賊盜取。論文中提出了完整的指紋辨識免持鑰匙進入系統的設計和完整的無線通訊認證流程，因此在實作上提供很高的參考價值。論文最後，針對系統的安全性做了深入的探討，證明本系統的高度安全性。本論文提供了更安全的免持鑰匙進入系統以保護汽車，更可以根據每位駕駛者的指紋做為辨識駕駛者的依據，以提供駕駛個人化的服務，創造舒適的開車環境。在指紋辨識免持鑰匙進入系統的設計上，更考量未來實作成產品的必備因素，如成本，使用壽命和效能，因此未來更有機會被車廠或廠商接受，以成為真正的汽車防盜保全產品，來有效降低失竊率。

6. 參考文獻

[1] Lichtermann, J., Pettit, R. “Automotive Application of Biometric Systems and Fingerprint,” *SAE World Congress*, 2000.

[2] Xiao Ni, Weiren Shi, V. F. S. Fook, “AES Security Protocol Implementation for Automobile Remote Keyless System,” *IEEE 65th Vehicular Technology Conference*, 2007.

[3] International Biometric Group, available at http://www.biometricgroup.com/

[4] S. Schmitz, C. Roser, “A New State-Of-The-Art Keyless Entry System,” *SAE International Congress and Exposition*, 1998.

[5] Mohamed K. Shahin, A. M. Badawi, M. S. kamel, ”On-Line, Low-Cost and Pc-Based Fingerprint Verification System Based on Solid-State Capacitance Sensor,” *In Proceedings of IEEE, International Conference on Industrial Electronics, Technology and Automation IETA*, 2001.