卡片資訊交換及管理系統之使用性分析

陳姿妏 李文廷
國立高雄師範大學軟體工程與管理學系

Tz-Wen Chen, Wen-Tin Lee*
Department of Software Engineering and Management
National Kaohsiung Normal University

Email: sbt657134@gmail.com, wtlee@nknu.edu.tw

摘　要

在知識管理的時代，如何提昇工作效率，將時間應用在有價值的事物，而將例行瑣碎的雜事，像是卡片管理的工作交給科技產品處理。本論文使用現今普及的智慧型裝置，例如：智慧型手機、平板等，並結合四項技術包含: 1.使用近距離通訊技術(Near Field Communication, NFC）技術，藉由體感的操作讓使用者能更便利的交換卡片資訊。2.交換的資訊則是利用圖形識別中的光學字元識別（Optical Character Recognition, OCR)，使用Online OCR API，將圖片通過圖形辨識後以文字輸出。它影響傳統打字生態，使人們從繁瑣的鍵盤打字工作中解脫，解決了低速資訊輸入與高速資訊處理之間的不平衡，進而提高了效率。3.運用社群網站之互動功能，融入交流的理念，使之不再僅限於個人，例如：使用 Google Contact API 實作來支援 Google 聯絡人同步功能。4.將傳遞的資訊透過資訊安全相關技術加解密 Advanced Encryption Standard 與 RSA 加密演算法做進一步的安全性控制。讓使用者識別及管理日常生活中各式各樣的卡片資訊，可快速取得並使用需要的卡片內容，增加其方便性。

關鍵字：卡片管理、近距離通訊技術(NFC)、光學字元識別技術(OCR)、Google Contact API、RSA 加密演算法

一、緒論

皮夾裡的各式卡片總是無形中就累積成疊，常常在找卡片時遍尋不着。因此，本論文著重於「多卡合一」的構思，但是，本體終究仍是卡片，所以，為了省去這種麻煩，則將構想延伸到現今人手一台的智慧型裝置。當今智慧型裝置的蓬勃發展，行動應用與服務變得更為重要，根據資訊工業策進會的統計，目前全台灣智慧型行動裝置的普及率已經將近七成左右，約有一千四百萬人口在使用行動裝置，並且預計將在 2016 年左右，智慧型手機的市場將達到飽和，而在 2018 年時，平板電腦的普及率將達到四成左右[1]。因此，如何設計出讓使用者方便使用以及客製化的整合性服務是即將面對的重大挑戰。

另外，近年來因應行動網路與智慧型裝置的興起，NFC 技術逐漸成為國際各大廠力拱的行動支付標準之一。NFC 的應用可延伸到各式的領域:如遊戲、汽車、自動化、行動支付、電腦、電子測量(如電錶，可免抄表直接感應)、工業／交通、家電、醫療／教育等等。以家電為例，若家電壞了，可用 NFC 手機感應其機器的錯誤碼，並透過 3G 或 WiFi 發送資料給維修站，即可省略專員檢測並直接安排維修，並大量節省人力資源。而在市場方面，NFC 智慧型手機於 2013 年已成為主流，預估 2015 年將有超過 50%智慧型手機導入[2]，因此，本論文選擇此一技術作為研究方向，期望為智慧型手機帶來更多的應用機會與新價值。

而為了方便使用者儲存卡片至智慧裝置，本論文計劃採取「光學字元識別（Optical Character Recognition, OCR)」的技術，使用 Online OCR Api，將圖片通過圖形辨識後以文字輸出，這跟人工打字的效果是一樣的，但速度卻比人工打字快了幾十倍。它影響傳統打字生態，使人們從繁瑣的鍵盤打字工作中解脫，解決了低速資訊輸入與高速資訊處理之間的不平衡，進而提高了效率。

不同於以往之 App，本論文欲結合社群網站(Social Network)，運用社群網站之互動功能，融入交流的理念，使之不再僅限於個人，例如：支援 Google Contact 同步功能，讓使用者無須經過複雜流程即可輕鬆管理所有人脈資訊。

本論文主要分為五個階段，第一段我們會先由套用了何種開發技術來做描述。第二階段進行系統簡介，介紹我們系統主要的架構。第三階段則為系統各模組介面設計及使用情境描述。第四階段則為系統測試所需具備的環境，及問卷結果的分析。最後第五階段為論文結論與感想。

二、背景知識

本論文實作之系統背景知識分為近距離通訊技術（Near Field Communication, NFC），光學字元識別（Optical Character Recognition, OCR），Google Contact，加解密 Advanced Encryption Standard，及 RSA 加密演算法，分別說明如下:

2.1 NFC(Near Field Communication)[3]

近距離通訊技術，是一種短距離的高頻無線通訊技術，允許電子設備之間進行非接

觸式點對點資料傳輸。且是由非接觸式射頻識別（RFID）與互連技術演變而來。NFC 在單一晶片上結合了感應式讀卡器，感應式卡片和點對點的功能。在數公分（通常是 15 公分以內）距離之間於 13.56MHz 頻率範圍內運作，通過射頻信號自動識別目標對象並獲取相關數據，識別工作無須人工干預，任意兩個設備（如移動電話）接近而不需要線纜接插，就可以實現相互間的通信，滿足任何兩個無線設備間的信息交換、內容訪問、服務交換。

2.2 OCR(Optical Character Recognition) [4][5][6][7]

光學字元識別技術，主要是透過自動化的電腦演算法，將文字的圖片轉換為文字文件。假設文件已經利用相機等硬體設備等輸入系統中，並且該文件來源無特別污損，文字無模糊或是破損的狀況，OCR 的處理流程主要如下列所示：

- 分割單字：OCR 會將所有的文字、數碼和標點符號切割出來。
- 單字細線化：意即將單字的線條變細，讓字體剩下骨架，藉以消除可能造成誤判與不必要的資料量。
- 擷取單字的特徵點：OCR 運用各種方法來擷取單字最特別、最明確的部分，可以用來辨明與其他單字不同的地方，來對這些只剩下個架子的字體做編碼的工作，一般來說，每一個字都 同時採用幾種特徵擷取的技術。
- 比對：OCR 軟體有一套文字的資料庫，當一個字被辨識與編碼之後，會向這個文字資料庫來進行比對的動作，來察看這個編譯過後的訊號，所對應的最接近文字為何，而這個文字即是最後所辨識出來的結果。
- 輸出辨識結果：最後每一個文字都辨識完了之後，即產出這一次的 OCR 的文字檔案。

2.3 Google Contact API: Updating Contacts [8]

要上傳聯絡人資訊，首先要取得該聯絡人資訊，接著修改其資料並發送一個授權 PUT 請求到編輯處且更新。所需技術如下:

- 使用 OAuth2.0 取得授權以使用 Google Contact API。
- 使用 Google Contact API 處理聯絡人資訊，API 內容包含聯絡人元素，查詢、建立、更新及刪除聯絡人資訊等。
- 管理聯絡群組資訊，API 內容包含聯絡群組元素，查詢、建立、更新及刪除聯絡群組資訊等。
- 批次處理聯絡人及聯絡群組。

2.4 AES(Advanced Encryption Standard)

進階加密標準，在密碼學中又稱 Rijndael 加密法，這個標準用來替代原先的 DES，已經被多方分析且廣為全世界所使用。AES 加密過程是在一個 4x4 的位元組矩陣上運作，這個矩陣又稱為「體（state）」，其初值就是一個明文區塊（矩陣中一個元素大小就是明文區塊中的一個 Byte）。（Rijndael 加密法因支援更大的區塊，其矩陣行數可視情況增加）加密時，各輪 AES 加密迴圈（除最後一輪外）均包含 4 個步驟：

- AddRoundKey—矩陣中的每一個位元組都與該次回合金鑰（round key）做 XOR 運算；每個子金鑰由金鑰生成方案產生。
- SubBytes—透過一個非線性的替換函式，用尋找表的方式把每個字節替換成對應的字節。
- ShiftRows—將矩陣中的每個橫列進行循環式移位。
- MixColumns—為了充分混合矩陣中各個直行的操作。這個步驟使用線性轉換來混合每行內的四個位元組。最後一個加密迴圈中省略 MixColumns 步驟，而以另一個 AddRoundKey 取代。

2.5 RSA[9]

RSA 加密演算法，對極大整數做因數分解的難度決定了 RSA 演算法的可靠性。換言之，對一極大整數做因數分解愈困難，RSA 演算法愈可靠。假如有人找到一種快速因數分解的演算法的話，那麼用 RSA 加密的訊息的可靠性就肯定會極度下降。但找到這樣的演算法的可能性是非常小的。今天只有短的 RSA 鑰匙才可能被強力方式破解。到 2013 年為止，世界上還沒有任何可靠的攻擊 RSA 演算法的方式。只要其鑰匙的長度足夠長，用 RSA 加密的訊息實際上是不能被破解的。

假設 Alice 想要通過一個不可靠的媒體接收 Bob 的一條私人訊息。她可以用以下的方式來產生一個公鑰和一個私鑰：

- 隨意選擇兩個大的質數 p 和 q，p 不等於 q，計算 N=pq。
- 根據歐拉函式，求得 r=\varphi (N) = \varphi (p)\varphi (q)=(p-1)(q-1)
- 選擇一個小於 r 的整數 e，使 e 與 r 互質。並求得 e 關於 r 的模反元素，命名為 d（求 d 令 ed \equiv 1 \pmod{r}）。（模反元素存在，若且

唯若 e 與 r 互質）

- 將 p 和 q 的記錄銷毀。
- (N,e)是公鑰，(N,d)是私鑰。Alice 將她的公鑰(N,e)傳給 Bob，而將她的私鑰(N,d)藏起來。

三、系統簡介及主要架構

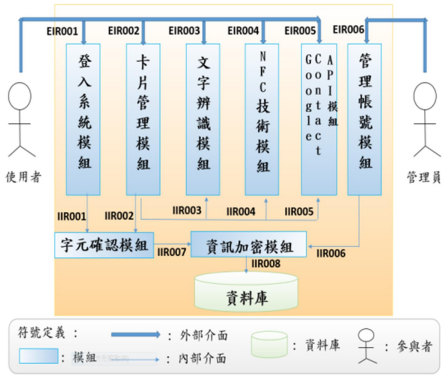


圖 1 系統架構圖

本系統主要於 Android 平台進行開發，使用者使用了登入系統、卡片管理、文字辨識、NFC 技術及 Google Contact 模組，來對系統進行操作，登入系統及卡片管理因為涉及到個人資料問題所以會使用到字元確認及資訊加密模組來加強安全性，而管理員使用管理帳號模組來管理資料，如同上述，使用到字元確認及資訊加密模組來加強安全性，而經由加密過後的資料皆儲存於資料庫。其中各模組功能如下

模組	功能
登入系統模組	使用者在此進行帳號登入與註冊等動作，使用者在進行後續的動作如掃描卡片...等之前，都需要先行登入方可進行。
卡片管理模組	使用者輸入的卡片資料皆在此進行管理，一般可使用手機 NFC 掃描卡片上的晶片資料，然後上傳到雲端資料庫，若是像名片等無晶片的卡片類型，使用者則可以選擇手動輸入資料上傳。
文字辨識模組	此模組的是用來辨識相片中的文字，並將辨識出來的資料，轉換成手機中聯絡人的格式，供使用者作修改。
NFC 技術模組	此模組的主要功能是在要與他人進行交換名片的動作時，可以利用 NFC 的技術進行交換的動作。
Google Contact API 模組	此模組的主要功能是在文字辨識模組辨識完後，可以利用此模組同步到 Google Contact，或是手機聯絡人，或是 FB 連絡人，供使用者做連絡人管理。
管理帳號模組	管理使用者帳戶模組提供系統管理員管理眾多使用者帳戶的相關功能，譬如雲端資料、會員帳號、卡片資料的新增，刪除、修改、查詢都包含於此。
字元確認模組	此模組的主要功能是在確認欄位輸入的時候，避免使用者輸入不合規格的字串，藉此保護系統的安全。
資訊加密模組	此模組的主要功能是利用 AES 和 RSA 來去加密傳輸的資料，藉此保護使用者個資的安全。

根據系統架構圖定義外部介面需求與內部介面需求如下:

外部介面需求(External Interface Requirements)

編號	需求描述
EIR001	使用者透過輸入帳號密碼來登入並使用系統
EIR002	使用者可以對卡片進行上傳或刪除等管理動作
EIR003	卡片經由文字辨識技術轉換
EIR004	卡卡片經由 NFC 技術進行交換
EIR005	卡片辨識完成後，可以同步至 Google Contact
EIR006	管理者可以管理系統使用者

內部介面需求(Internal Interface Requirements)

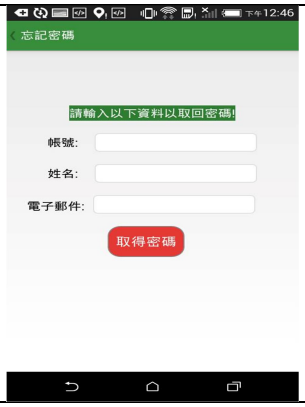
編號	需求描述
IIR001	登入系統輸入資料，必須透過字元確認模組檢查
IIR002	卡片詳細資料修改或新增必須經過字元確認模組處理
IIR003	卡片管理模組透過文字辨識模組進行文字辨識
IIR004	卡片管理模組使用 NFC 模組進行卡片的交換
IIR005	卡片管理模使用 Google Contact 進行同步
IIR006	將所有使用者的資訊提供給資訊加密模組做處理
IIR007	將確認格式正確之字串利用加密模組處理
IIR008	所有資料經過資料加密後存入資料庫

四、系統介面設計

4.1 登入系統模組

A	介面	介面敘述
帳號登入		登入系統後便可以進行卡片管理，針對各式卡片類別進行分類。

B	介面	介面敘述
註冊帳號		帳號欄位包含帳號名稱、密碼、信箱地址、使用者姓名及生日，輸入完成後點選確定，系統進行資料驗證 後將資料更新至資料庫。

C	介面	介面敘述
密碼查詢		輸入欄位包含帳號、姓名及信箱，輸入完畢後點選取得密碼，若核對資料完成系統會自動將密碼寄至輸入之信箱地址。

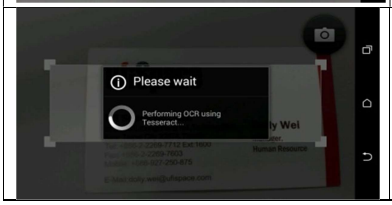
4.2 卡片管理模組

A	介面	介面敘述
卡片分類		登入系統後便可以進行卡片管理，針對各式卡片類別進行分類。

B	介面	介面敘述
手動輸入卡片		選擇左上角的手動新增按鈕，接著選擇新增名片或卡片。
手動輸入卡片		開始填寫卡片資料後點選右上角勾勾即可完成。

C	介面	介面敘述
卡片刪除		選擇右上角的功能按鈕，接著選擇欲執行的動作：刪除卡片。

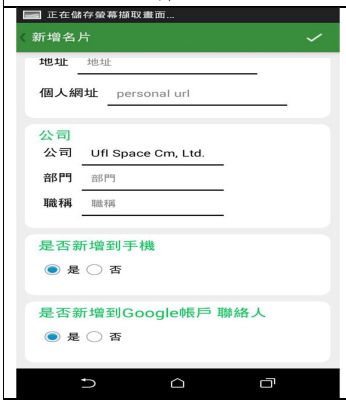
4.3 文字辨識模組

介面	介面敘述
	將相片進行文字辨識：首先，先對要進行辨識的名片進行拍照。
	開始進行辨識。

4.4 NFC 技術模組

介面	介面敘述
	利用 NFC 的技術進行交換名片：選擇右上角的交換名片按鈕，進行名片傳輸。

4.5 Google Contact API 模組

介面	介面敘述
	將聯絡人同步到 Google Contact：選擇新增到 Google Contact，即可透過登入帳號並給予權限同步資料。

五、系統測試與分析

在執行系統測試前，需先符合測試環境以及軟硬體的需求，再開始實際操作測試，其中各需求如下：

5.1 操作環境(Operational Environment)

本環境操作於 Android 手機平台，Android 手機版本需大於 4.4.2 以上，並且裝置在 5 吋以上之規格為最佳體驗。操作環境設定如下:

(1)需支援 NFC(Near-Fieled Communication)近場通訊之功能

(2)需可以利用 3G or 4G or WiFi 連上網

5.2 硬體需求(Hardware Specification and Configuration)

項次	名稱	數量	規格	備註
1	與 Android 相容之智慧型裝置	2	支援 NFC 技術且 Android 版本 4.2 以上、具備相機功能	
2	Network	1	Ethernet Network	

5.3 軟體需求(Software Specification and Configuration)

項次	名稱	數量	規格	備註
1	Android	1	Server with 10 Users	
2	SQLite	1	With 10 Users	
3	Java	1	版本 1.8 以上	

測試環境符合後，再來即需要測試資料，其中測試資料來源可分成下面的資料來源：

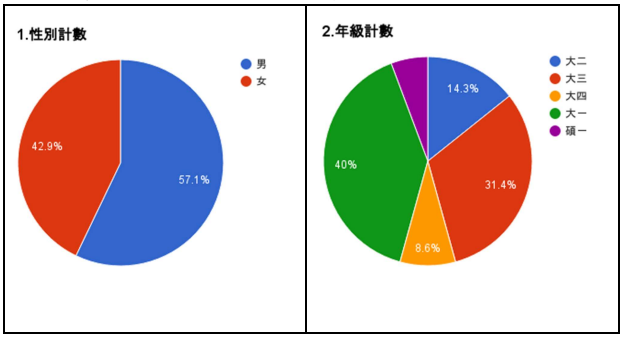
(1) 中英文卡片實體

(2) 會員基本資料

(3) 手動輸入或自動辨識後之名片資訊

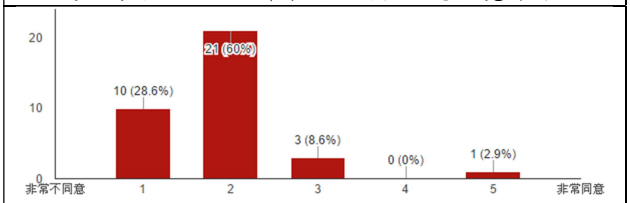
根據上述前置準備完成後，即找尋測試者實際操作此系統，並以問卷填寫的方式，收集測試者給予此系統的回饋，將這些結果做成圖表分析並說明，統整後的結果如下：

- 統計樣本的男女與年級比率



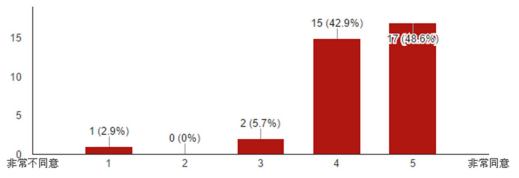
- 問卷呈現及分析結果（Questionnaire Analysis）

1. 我認為介面上的設計讓使用者無法憑直覺操作。



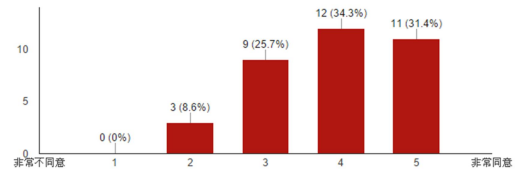
分析：此題是反面敘述之題目，多數人不同意。

2. 我認為介面上的文字字體設計可以清楚閱讀。



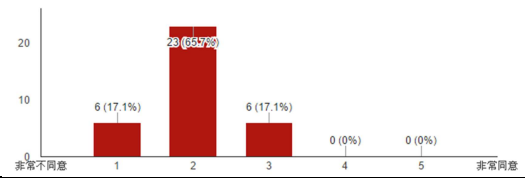
分析：多數人非常同意介面上的文字字體設計可以清楚閱讀。

3. 我認為介面上的頁面設計色彩呈現清楚美觀。



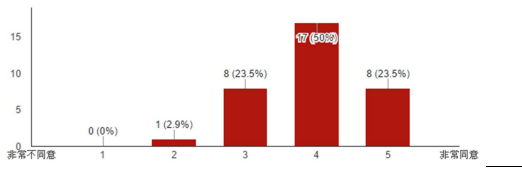
分析：由圖表可知分佈人數呈現平均的趨勢，因此對於介面上的頁面設計色彩呈現或許可以再多作加強。

4. 我認為介面上的按鈕設計無法清楚了解該按鈕功能並使用。



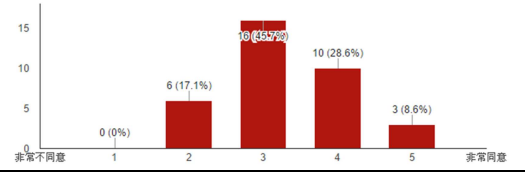
分析：此題是反面敘述之題目，多數人不同意。

5. 我認為介面上的設計在發生操作錯誤時，提供即時說明訊息是有利於使用者了解錯誤訊息並修正的。



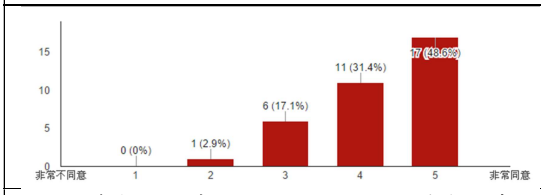
分析：多數人非常同意介面上的設計在發生操作錯誤時，提供即時說明訊息是有利於使用者了解錯誤訊息並修正的。

6. 我認為拍照辨識的準確度是高的，顯示成果與原始資料是差異不大的。



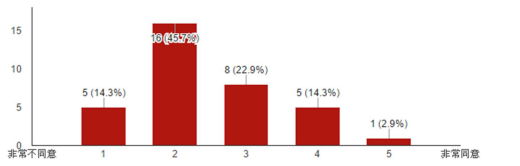
分析：同意分數大約落在同意的區間，對於非常同意的選項只有少量，因此或許可以再加強拍照辨識度。

7. 我認為拍照辨識來新增名片或聯絡人的功能是符合需求且方便使用的。



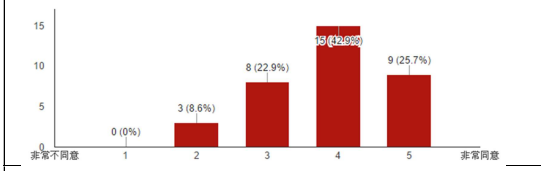
分析：多數人同意拍照辨識的功能是符合需求且方便使用的。

8. 我認為透過手動新增來新增名片或聯絡人的功能不符合我的需求且麻煩。



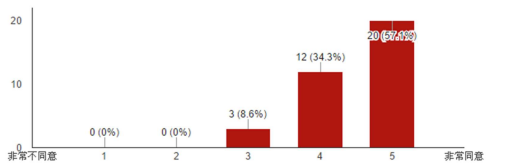
分析：此題是反面敘述之題目，多數人非常不同意，有少數無意見或中立。

9. 我認為透過手機相互碰觸來交換名片此項功能，的確比現實生活中直接交換名片的動作來得更便利且簡單操作。



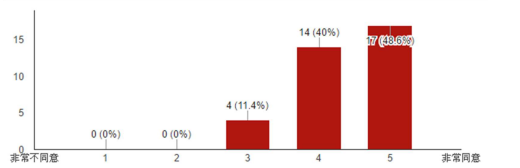
分析：多數人同意透過手機相互碰觸來交換名片此項功能，的確比現實生活中直接交換名片的動作來得更便利且簡單操作。

10. 我認為能在取得名片資料後進行新增至手機聯絡人是快速且方便的。



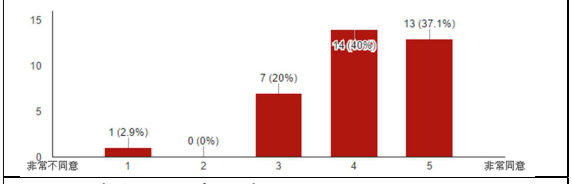
分析：多數人同意能在取得名片資料後進行新增至手機聯絡人是快速且方便的。

11. 我認為能在取得名片資料後進行新增至 Google 聯絡人是快速且方便的。



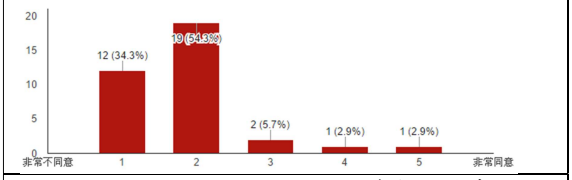
分析：多數人同意在取得名片資料後進行新增至 Google 聯絡人是快速且方便的。

12. 我認為能自行選擇新增聯絡人的目的位置（ex：手機 or Google Contact）是必要且符合我的需求的。



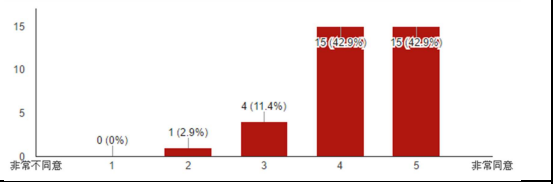
分析：多數人非常同意能自行選擇新增聯絡人的目的位置（ex：手機 or Google Contact）是必要且符合需求的，只有少數表示不同意。

13. 我認為名片夾的分類是不必要的。



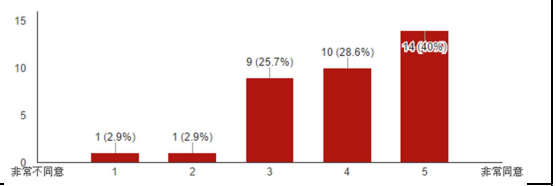
分析：此題是反面敘述之題目，多數人非常不同意；但也有少數表示同意，認為分類可能不是那麼必要。

14. 我認為使用前註冊的動作是必要且有利於個人隱私保護。



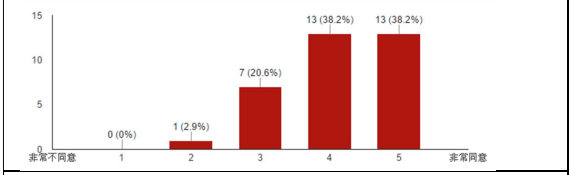
分析：多數人同意使用前註冊的動作是必要且有利於個人隱私保護。

15. 我認為名片交換過程所等待的時間是短暫且可接受的。



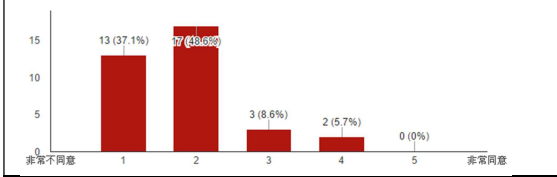
分析：雖然同意者仍占多數，但是也有不少人表示不同意，因此，名片交換過程所等待的時間或許可以在進行加強。

16. 我認為此系統的使用不受時間與空間限制，符合我的需求。



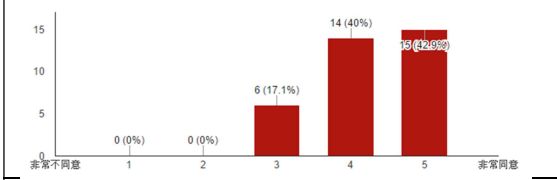
分析：多數人同意此系統的使用不受時間與空間限制，符合需求。

17. 就算有需要，我也不願意使用此系統來保存名片、交換或新增聯絡人。



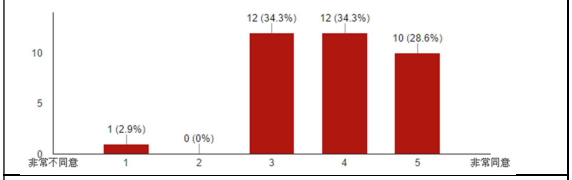
分析：此題是反面敘述之題目，多數人非常不同意。

18. 我認為即使沒有人教導，我還是能自己學習來使用此系統。



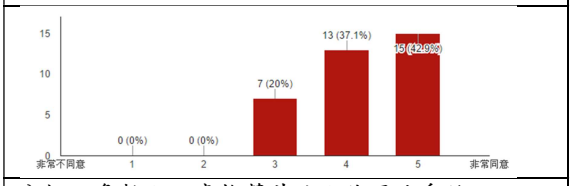
分析：多數人表示同意，即使沒有人教導，還是能自己學習來使用此系統；但有少數表示不同意，因此，對於系統的使用，或許能新增使用手冊。

19. 我認為此系統對於個人隱私保護的技術是值得信賴的。



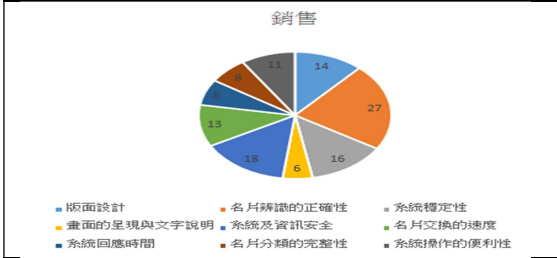
分析：多數人同意系統對於個人隱私保護的技術是值得信賴的。

20. 我願意推薦其他人使用此系統。



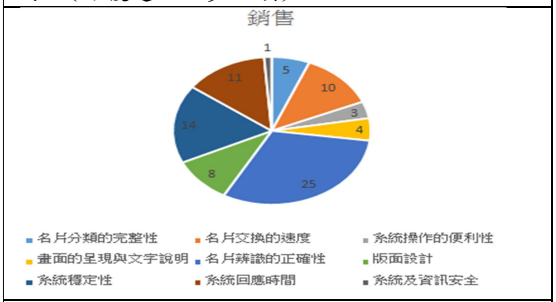
分析：多數人願意推薦其他人使用此系統。

21. 使用此系統時，您最重視的是哪些項目？(可複選，至多三項)



分析：由圖表可知多數人重視的前三項目為名片辨識的正確性(27)、系統及資訊安全(18)、系統穩定性(16)

22. 您認為此系統目前哪些功能是最需要改進的。(可複選，至多三項)



分析：由圖表可知多數人認為最需要改進的前三項目為名片辨識的正確性(25)、系統穩定性(14)、系統回應時間(11)

對於此系統的問卷調查結果，可分析出在未來要面對的擴充功能上，外部見到的 NFC 技術，探討是否能有更快速的傳輸方式;OCR 辨識功能上，對中、英文的同步辨識，期望能有更高效率的辨識度;而 Google Contact 的同步，希望能增加對 Google Contact 的寫入功能，例如：刪除、編輯、新增群組等，而內部最重要的便是各式卡片與使用者的個人資料安全性了，因此，「資訊安全」是極力研究的部分，一個好的系統，便是讓使用者在使用上安全無虞。

而從上述所提到的學生證，我們更延伸出是否能透過除了學生證的資訊，另外儲存其他個人資料，使之成為專屬的個人名片，藉以成為各大專院校學生之間互動的橋樑，除此之外，透過系統連結 Facebook、Twitter 等社群網站，讓我們的最新動態能同步更新並顯示於我們的個人名片上。

六、結論

目前透過論文研究之成果，將管理卡片的麻煩事延伸到現今人手一台的智慧型裝置。首先在初利用系統時，須先申請個人帳號，接著登入後即可開始使用系統功能，如下：我們利用裝置之拍照功能拍攝後進行 OCR 辨識，並藉由 NFC 感測器技術使之更便利的交換資訊，而交換的資訊利用加解密技術 AES 與 RSA 保障個資安全，同時，在有網路的環境下，可將卡片上的資訊同步到個人 Google Contacts 帳號中，如此一來，我們就可以隨時新增聯絡人資料，當然，也可選擇只新增至裝置的聯絡人，完全取決於使用者需求。另外，對於卡片的管理，我們會進行卡片分類，有利使用者取得需要的名片資訊，還可查看目前卡片的儲存狀況或對卡片進行編輯。

而在未來，穿戴式裝置及 NFC 等應用定是更加蓬勃發展，期望未來能把目前智慧型手機上所具備的功能融合至系統中，讓這種NFC、感測器感應、和文字辨識的方式，能激盪出更多的應用。

* 本研究接受科技部編號：MOST 104-2221-E-017 -014 -研究計畫經費補助

參考文獻

[1] 資策會，資訊工業策進會研究顯示：智慧型行動裝置普及，估 2016 年市場將飽和，2014/12/29 21:25

[2] DAF 2014 行動支付技術與應用論壇，NFC 技術趨勢與行動支付未來 http://www.digitimes.com.tw/tw/b2b/Seminar/shwnws_new.asp?CnlID=18&cat=99&product_id=051A30515&id=0000379872_3IF93Y976OJOX13CTTNYZ#ixzz3Pwzlxe7s，http://www.google.com.tw/ig

[3] NFC。2012。維基百科。網址 : http://zh.wikipedia.org/wiki/近場通訊

[4] OCR。2013。維基百科。網址 : http://zh.wikipedia.org/wiki/光学字符识别

[5] Online OCR API。2015。Smart Mobile Software。網址 : http://ocrapiservice.com/

[6] Making a Simple OCR Android App using Trsseract。2011。GAUTAM。網址 : http://gaut.am/making-an-ocr-android-app-using-tesseract/

[7] ABBYY Cloud OCR SDK。2015。ABBYY。網址 : http://ocrsdk.com/

[8] Google Contacts API version 3.0。2012。GOOGLE。網址 : https://developers.google.com/google-apps/contacts/v3/

[9] RSA 加密演算法。2014。維基百科。網址:http://zh.wikipedia.org/wiki/RSA 加密演算法

[10] DDOS 阻斷服務攻擊。2014。維基百科。網址: http://zh.wikipedia.org/wiki/阻斷服務攻擊