擊鍵特徵於觸控式手持行動裝置之身分驗證

鄭培成
清雲科技大學
資訊管理系
助理教授
pccheng@cyu.edu.tw

林俊豪
彰化師範大學
數位學習研究所
研究生
m97332007@mail.ncue.edu.tw

張庭毅
彰化師範大學
數位學習研究所
副教授
tychang@cc.ncue.edu.tw

江茂綸*
朝陽科技大學
資訊與通訊系
助理教授 (通訊作者)
mlchiang@cyut.edu.tw

蔡政容
彰化師範大學
統計資訊研究所
助理教授
tsaicj@cc.ncue.edu.tw

摘要

擊鍵特徵微生物驗證的一種，本研究採用擊鍵特徵，提升系統對使用者在觸控式手持行動裝置之身分驗證能力。在特徵資料擷取過程中，除常用的時間特徵外，另新增兩項特徵，分別為使用者按觸行動裝置螢幕的壓力與按觸螢幕的面積，接著透過統計的方式建立分類器進行使用者身分驗證，並於 Android 為平台的行動裝置中進行實驗。本研究針對四種特徵組合進行比較，分別為(1)時間特徵、(2)時間特徵加面積特徵、(3)時間特徵加壓力特徵與(4)三種特徵皆有，若以(1)時間特徵驗證方式其相等錯誤率為 12%，本研究以(2)時間特徵加面積特徵或(3)時間特徵加壓力特徵相等錯誤率分別為 10%與 7%，(4)三項特徵皆使用則為 10%，實驗結果可證明增加面積或壓力皆可有效降低辨識錯誤率，其中(3)時間特徵加壓力特徵組合辨識效果為最佳。

關鍵詞：擊鍵特徵、生物特徵、身分驗證。

Abstract

Keystroke dynamic-based authentication (KDA) is one of biometric for identity authentication. Except for the original time features in KDA schemes, two novel features are proposed and found in touch screen handheld mobile devices, which are called pressure features and size features. A statistical classifier is built for authenticating the users' identities. and is implemented on Android handheld mobile devices. This paper analyzes four combinations of features: (1) time features, (2) time features and pressure features, (3) time features and size features, and (4) all of the features. The EER of four combinations are 12%, 10%, 7% and 10%, respectively. The experiment results prove that the size features or the pressure features can effectively reduce the EER. According to the results, the combination of time features and pressure features is the best for authenticating the users.

Keywords: Keystroke dynamics-based authentication, Biometric, Identity authentication.

1. 前言

近年來，資訊科技技術迅速發展，行動電話(mobile phone)與個人數位助理(Personal Digital Assistant; PDA)等行動裝置的出現，使人類可以廣泛應用這些裝置將大量的資料訊息以數位化的方式儲存於系統中，但相對衍生出如何驗證使用者身分，以保護資訊不被竊取的安全性問題。身分驗證類型分為下列三種；第一，知識為基礎的驗證，此類即為傳統利用合法使用者自行訂定的通行碼(password)進行驗證，使用個人電腦進行驗證上，使用者輸入之通行碼可包含英文字母、數字與特殊符號，在手機等行動裝置上則利用 PIN 作為使用者通行碼；第二，物件為基礎的驗證，其概念為合法使用者需要一把鑰匙打開門鎖的方式，在行動裝置上則利用加密的晶片卡；第三，以個人特徵為基礎的驗證，此方法利用每個人特殊的生理特徵進行驗證，稱之為生物特徵，如：擊鍵特徵、簽名、虹膜等皆為此類之應用[19, 21]。在手持行動裝置身分驗證方法中，傳統通

行碼驗證為利用 4 至 8 碼之數字之 PIN(Personal Identification Number)進行身分驗證，而 PIN 可能在下列情況下被竊取：首先，PIN 長度短且無法使用特殊字元增加輸入多元性，如此一來，PIN 排列組合總數則相對較少；攻擊者容易利用肩窺攻擊(shoulder surfing attack)或暴力攻擊(brute-force attack)等方式取得使用者 PIN；再者，行動裝置由於體積較小，容易遺失或被偷，歐洲每年超過一萬台行動裝置被偷竊；第三，人們常會將行動裝置借給他人，如果他人用來進行不正當的行為，此舉將會提高 PIN 被竊取的風險。

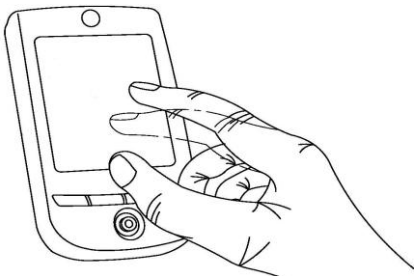
為避免上述三種 PIN 被竊取後，造成安全上的威脅，有必要在傳統 PIN 驗證上再額外提供一層安全驗證機制以改善行動裝置的安全性，其中生物特徵為廣泛運用於增強通行碼驗證之能力。生物特徵驗證定義為“運用生理或行為特徵辨識是否為正確使用者”[15]，生物特徵驗證是利用與生俱來、隨身攜帶且不易複製的個人化特徵等特性達到身分驗證，生物特徵可分為生理特徵與行為特徵兩類，在生理特徵方面包含：指紋、臉型、虹膜、視網膜等；行為特徵包含：簽名、筆跡、說話語調、擊鍵特徵等，其中擊鍵特徵優點在於不需其他昂貴設備，僅需要透過鍵盤即可取得，如此一來，其應用成本相對較低。而無論生理特徵或行為特徵皆需包含下列幾項基本條件：

1. 普遍性(universality)：人類與生俱來且每個人都有，並隨手可得的特徵。
2. 唯一性(uniqueness)：其他人不可能具備相同的特徵，且不容易進行複製，透過此特點用以驗證使用者。
3. 恆久性(permanence)：特徵不會隨著時間而有所改變。
4. 量測性(collectability)：特徵可轉換成數值的方式進行量測。

動態擊鍵特徵驗證(Keystroke Dynamics-based Authentication; KDA)屬於行為特徵的一環，在使用者於 QWERTY 鍵盤輸入通行碼時，同時記錄其輸入情況，並可動態擷取其個人所屬特徵值，如擷取各按鍵按下與放開時間，即可取得按鍵時間特徵進行使用者驗證。KDA 具有下列優點：首先，所需成本較低，直接於一般裝置中進行運算即可達到辨識功能，不像其他生理特徵驗證如：虹膜、指紋等需要額外昂貴的儀器與較多的記憶體容量進行複雜運算，相形之下，KDA 較符合成本考量需求；再者，KDA 在不影響使用者情況下進行驗證，其驗證方法是基於每個人打字型態皆有特殊的特徵，藉由擷取其特徵值作為判斷是否為使用者的依據[5, 13, 18]。因此，KDA 於使用上相對於其他生物特徵驗證方式較為容易。

由於科技的進步，各種觸碰式手持行動裝置紛紛上市，但手持式行動裝置無法如電腦一般可用 QWERTY 鍵盤進行輸入，此類裝置大多無實體按鍵可用，使用者輸入資料如圖一所示，需點擊觸碰螢幕輸入 PIN，而本研究中 KDA 之通行碼為 PIN，考量使用者無鍵盤輸入較為困難，本研究於 JAVA 環境下設計一套有如傳統手機數字鍵盤之虛擬鍵盤，讓使用者透過虛擬鍵盤輸入 PIN，如圖一；如此一來，不但解決無法取得時間特徵的問題，另外又可新增手持式行動裝置專屬特徵。

為提升使用者特徵唯一性以提高驗證之準確性，本研究所擷取之特徵值，除利用時間特徵之外，亦新增使用者按觸行動裝置螢幕之面積(size)特徵與壓力(pressure)特徵，本研究證明在觸控設備上增加面積特徵或壓力特徵後，辨識能力明顯提高，基於此目的設計實驗，分別比較(1)時間特徵、(2)時間特徵加面積特徵、(3)時間特徵加壓力特徵與(4)三種特徵皆用結果，結果顯示無論增加面積特徵亦或是壓力特徵皆可提升辨識能力，其中(3)時間特徵加壓力特徵，辨識錯誤率最低，證明壓力特徵最能有效提升辨識準確性。最後本研究將實驗應用於使用 Android 平台之觸控式手持行動裝置，實作 KDA 辨識使用者功能。



圖一：使用者透過手機進行資料輸入之示意圖

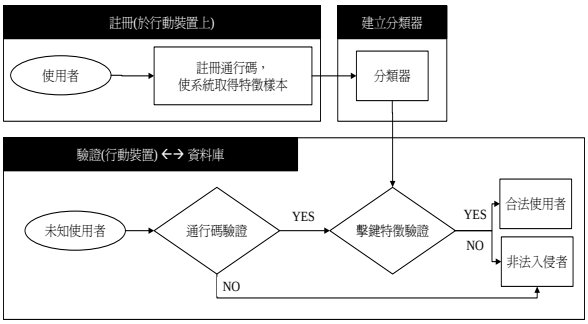
為提升使用者特徵唯一性以提高驗證之準確性，本研究所擷取之特徵值，除利用時間特徵之外，亦新增使用者按觸行動裝置螢幕之面積(size)特徵與壓力(pressure)特徵，本研究證明在觸控設備上增加面積特徵或壓力特徵後，辨識能力明顯提高，基於此目的設計實驗，分別比較(1)時間特徵、(2)時間特徵加面積特徵、(3)時間特徵加壓力特徵與(4)三種特徵皆用結果，結果顯示無論增加面積特徵亦或是壓

力特徵皆可提升辨識能力，其中(3)時間特徵加壓力特徵，辨識錯誤率最低，證明壓力特徵最能有效提升辨識準確性。最後本研究將實驗應用於使用 Android 平台之觸控式手持行動裝置，實作 KDA 辨識使用者功能。

2. 相關研究

傳統使用者驗證方式中，最普遍是以通行碼為驗證基礎，但萬一通行碼被竊取，系統之安全性便隨之瓦解。Gaines 等人[11]提出 KDA 應用於標準 QWERTY 鍵盤上，針對使用者使用電腦存取資料時進行身分驗證，其特性在於利用每個人打字型態的獨特性以及使用者輸入其資料的一致性，基於此兩項特性擷取使用者於 QWERTY 鍵盤上輸入資料之時間特徵，並將這些特徵經量化計算後判斷是否為正確使用者，KDA 已被證明可有效改善資訊安全的問題，成功提高系統驗證使用者的能力。

近年來，觸控式手持行動裝置如：PDA、iPad 等產品相繼問世後，越來越多人使用觸控式手持行動裝置進行資料存取，但此類裝置與傳統手機差異在於此類大多無實體鍵盤。Chang 等人[4]利用點擊個人的音樂節奏之時間特徵，如愛的鼓勵，於觸控式手持行動裝置實做 KDA 系統，用以克服無鍵盤之設備。本研究除了考慮時間特徵外，將針對觸控式手持行動裝置專屬特徵－按觸螢幕之面積特徵及壓力特徵，應用於 KDA 中，提高辨識使用者之準確度。



圖二：動態擊鍵特徵驗證流程圖

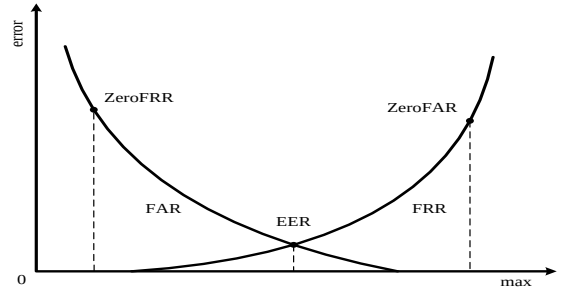
KDA 執行共有三個階段，註冊、建構分類器及驗證，其流程表示於圖二中。首先，在註冊階段中，要求使用者進行註冊，並擷取通行碼之擊鍵特徵樣本，所有使用者特徵將此階段取得。隨著行動裝置的發明，學者將 KDA 研究應用至傳統手機上，將傳統 PIN 驗證中加入 KDA 機制以提升安全性[3, 6, 15]。Hwang 等人[15]於 2009 年提出利用人工節奏特性改善資料品質，其方式為加入人工節奏提示，如使用節拍器提醒使用者，讓使用者可透過提示增加斷音、連音或暫停等，用以提高個人輸入 PIN 時的一致性進而提升辨識能力，但 Gaines 等人[11]及 Chang 等人[4]認為利用人類與生俱來打字型態差異所產生的特徵進行辨識而非刻意使用人工節奏，不會造成使用者額外負擔且較能符合生物特徵之定義；本研究以人類與生俱來打字型態的獨特性進行辨識為理論基礎，使用統計方式建構出一套用以分辨是否為合法使用者之 KDA 於觸控螢幕上。本研究新增經觀察使用者觸碰式手持行動裝置而得特徵，用以提升使用者唯一性，而非以用 Hwang 等人的人工節奏提示，達成改善資料品質的目的，進而達到提高辨識能力。

經觀察後發現，當使用者透過觸控螢幕輸入其資料時，(1)每個人用以輸入資料之手指不一定相同、(2)每個人手指粗細亦有所差異與(3)個人輸入習慣不同，有些人慣用指尖，有些人則用指腹。基於上述差異，使用者按觸觸控式手持行動裝置螢幕之面積將會有所不同；另外每個人按觸觸控式手持行動裝置螢幕的力道大小也有所差異，系統所接收到使用者按觸螢幕壓力便會有所不同。本研究假設若能加入使用者按觸行動裝置螢幕之面積特徵與壓力特徵，能提升資料品質的唯一性進而提升 KDA 辨識使用者的能力，故本研究所擷取的特徵值除時間差特徵外，並新增按觸行動裝置螢幕面積特徵與壓力特徵。

特徵值成功取得後，由所收集的特徵樣本建構分類器，此分類器目的是用來分辨是否為合法使用者。Shih[21]與 Killourhy[17]指出 KDA 有許多建構分類器的方法，如：統計(statistics)[3, 12, 21]、模糊邏輯(fuzzy logic)[2, 9]與類神經[13, 14, 20]等；Campisi 等人[3]提出多種正規化的方法，如：Z 分數、中位數等可用來讓單一系統結合多種分類器進行驗證。Clarke 等人[7, 8]於傳統手機上，利用 4 位數 PIN，分別使用前饋式多層感知器(Feed Forward Multi-Layer Perceptron; FF-MLP)、半徑式函數(Radial Basis Function; RBF)網路與廣義迴歸類神經網路(Generalized Regression Neural Network; GRNN)等類神經網路(neural network)建構分類器，但此方法建立之分類器需要非法使用者訓練樣本來訓練類神經網路，而蒐集非法使用者訓練樣本較不符合現實情況；相較之下，統計分類器具有下列優點：首先，此方法較不需高運算量的計算，且辨識使用者身分之時間較短；其次，此方法不需非

法入侵者資料當訓練樣本；最後，此方法驗證效果多數比類神經或模糊理論較佳；基於上述優點，本研究採用統計方法進行分類器建構，以 PIN 為基礎加上新增觸控式手持行動裝置專屬特徵之 KDA，進行使用者驗證。

在驗證階段中，系統首先會如同傳統的 PIN 驗證機制一般，針對使用者登入時所輸入 PIN 進行判斷，如果與註冊時的 PIN 相同則進行 KDA 流程，透過已建構的分類器進行辨識，如果通過辨識系統即為正確使用者，則允許其登入，反之，系統將拒絕入侵者登入，以保障資訊可安全的被存取。



圖三：五種評估準則關係圖

評估 KDA 系統的優劣，可由正確率及錯誤率進行分析，圖三為評估準則關係圖，常用的評估方式說明如下：

錯誤拒絕率(False Rejection Rate; FRR)，用以表示使用者登入系統卻被拒絕的比例，意即將合法使用者誤認為入侵者，此種錯誤在統計稱之為型Ⅰ錯誤(Type Ⅰ Error)。

錯誤接受率(False Acceptance Rate; FAR)，用以表示入侵者登入攻擊卻被系統接受，意即將入侵者誤認為合法使用者，此種錯誤在統計稱之為型Ⅱ錯誤(Type Ⅱ Error)。

相等錯誤率(Equal Error Rate; EER)：錯誤拒絕率與錯誤接受率相等時的情況，可用來評估系統優劣。

ZeroFRR(Zero False Rejection Rate)：當錯誤拒絕率為零時，此時錯誤接受率定義為 ZeroFRR，用以評估合法使用者可以完全登入情況，被非法使用者入侵的機率。

ZeroFAR(Zero False Acceptance Rate) 當錯誤接受率為零時，此時錯誤拒絕率定義為 ZeroFAR，用以評估可完全排除非法使用者入侵的情況下，合法使用者登入的成功率多寡。

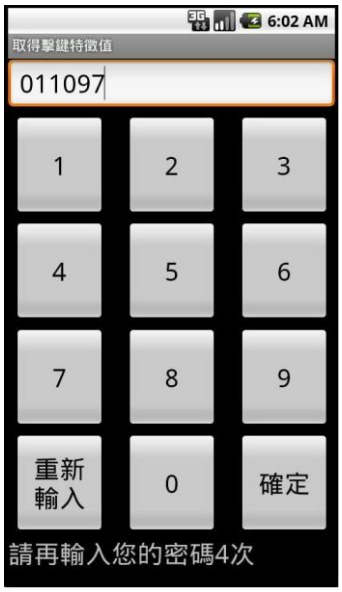
以上這些評估準則在越接近零表示系統成效越佳，其中錯誤拒絕率與錯誤接受率存在著負相關關係，當錯誤拒絕率降低時，錯誤接受率相對提升，意即提升系統安全性時，則合法使用者登入會較為困難；反之，若欲使合法使用者登入較為容易，則安全性將會變低。其中，錯誤拒絕率或錯誤接受率分別僅針對合法使用者或非法入侵者進行評估，而相等錯誤率則可用以評估系統包含使用者與入侵者所有錯誤，本研究使用相等錯誤率為系統評估準則，用以評估系統整體驗證之能力。

3. 方法

本節中將針對在觸控式手持行動裝置中執行 KDA 流程各階段進行說明。3.1 節將詳細說明特徵值收集過程；3.2 節介紹本研究利用統計的方式建立分類器；3.3 節則說明身分驗證過程。

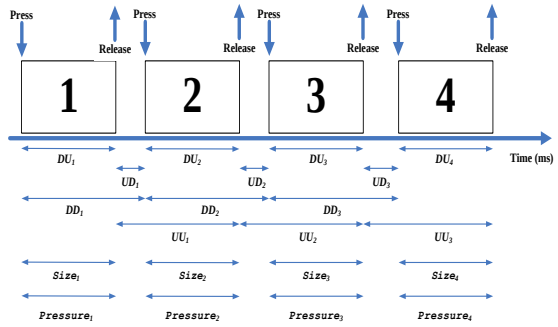
3.1 特徵值收集

本研究將 KDA 應用於觸控式手持行動裝置上，故以 4 至 8 碼數字之 PIN 為使用者驗證之通行碼，考量觸碰式手持行動裝置大多無實體鍵盤，設計虛擬鍵盤讓使用者透過虛擬鍵盤進行 PIN 輸入，如圖四所示。其中最上面方框中顯示使用者輸入之數字；中間 12 個按鍵為虛擬鍵盤，各按鍵大小為 90×100 像素，按鍵間上下間隔 5 像素、左右為 20 像素，虛擬鍵盤除輸入 PIN 之 10 個數字鍵外，若使用者 PIN 輸入錯誤則可按重新輸入鍵重新輸入，輸入完成後按確定鍵送出；最下方則提示使用者尚需輸入多少次。



圖四：使用者輸入 PIN 時螢幕畫面

當手指按下(Press)螢幕至手指離開(Release)螢幕後，這段時間間隔中將會產生 4 種分別為 DU, UD, DD, UU 時間特徵之時間特徵與面積特徵及壓力特徵。圖五為表示使用者 PIN 為 1234 之時間 4 種特徵、面積特徵與壓力特徵示意圖；由圖五中可知，四種時間特徵值存在著一定的關聯性。



圖五：各種擊鍵特徵示意圖

- Down-Up (DU)時間： 同一個字元 *i* 的按鍵按下與放開之時間間隔，稱 DU_i
- Up-Down (UD)時間： 第 *i* 個字元的按鍵放開到下一個鍵按下之時間間隔，稱 UD_i
- Down-Down (DD)時間： 第 *i* 個字元的按鍵按下到下一個字元的按鍵按下之時間間隔，稱 *DDi*
- Up-Up (UU)時間： 第 *i* 個字元的按鍵放開到下一個鍵放開之時間間隔，稱 UU_i
- Size： 同一字元 *i* 的按鍵按下到放開螢幕所受之面積，稱 $Size_i$
- Pressure： 同一字元 *i* 的按鍵按下到放開螢幕所受之壓力，稱 $Pressure_i$

Araújo[1]指出，時間特徵值取 DU, UD 與 DD 的辨識效果最佳，本研究除採用 DU, UD 與 DD 三個時間特徵值之外，另新增新提出的面積特徵值與壓力特徵值；當使用者按觸螢幕 *K* 次則總共產生 5*K*-2 個特徵，其中包含 *K* 個 DU 特徵之 DU 集合、*K* 個面積特徵之 *S* 集合與 *K* 個壓力特徵之 *P* 集合及 *K*-1 個 UD 特徵之 UD 集合與 *K*-1 個 DD 特徵之 DD 集合，表示如下：

$DU = \{DU_1, DU_2, \ldots, DU_K\}$
$UD = \{UD_1, UD_2, \ldots, UD_{K-1}\}$
$DD = \{DD_1, DD_2, \ldots, DD_{K-1}\}$
$P = \{P_1, P_2, \ldots, P_K\}$
$S = \{S_1, S_2, \ldots, S_K\}$

求出時間特徵、面積特徵與壓力特徵集合後，使用者所有特徵 *feat* 集合，如下所示：

$feat = \{DU, UD, DD, P, S\}$

特徵值收集時，Araújo[1]建議使用者輸入訓練樣本筆數以不超過 10 次為佳，若超過 10 筆則使用者會感到厭煩，本研究以不造成使用者負擔為考量，每位使用者於註冊時，僅輸入 5 筆訓練樣本。

3.2 分類器建立

分類器的建立是為了讓註冊階段所得到的特徵值資料轉換成辨識是否為正確使用者的關鍵，驗證階段透過分類器辨識使用者，以決定是否讓使用者登入進行資料存取，相關研究中文獻[16, 17, 21]可得知，建立分類器種類眾多，但以單一方法建立分類器而言，類神經、模糊邏輯等人工智慧的方法需要較多的訓練時間與複雜的運算；相較之下，統計的方式有下列幾項優點：計算所需成本較低、計算時間短使得驗證速度快，且辨識效果佳[13, 17]，由於手機對資料處理速度相對於電腦較慢，如此一來，為使驗證時間不至於過久，本研究採用統計的方式；透過公式(1)、(2)求出建構分類器所需之平均數(Mean)μ_{feat}集合與標準差(Standard deviation)σ_{feat}集合，其中 $feat_i$ 為使用者之第 *i* 筆訓練樣本之特徵集合(*i*=1 to 5)，公式(1)為平均數公式，公式(2)則為標準差公式，透過公式(1)、(2)所計算出來的μ_{feat}集合與σ_{feat}將是分類器用來辨識使用者的依據。

$$\mu_{feat} = \frac{1}{5}\sum_{i=1}^{5} feat_i \qquad (1)$$

$$\sigma_{feat} = \frac{1}{5-1}\sum_{i=1}^{5} |feat_i - \mu_{feat}| \qquad (2)$$

3.3 身分驗證

使用者輸入的 PIN 與註冊的 PIN 相比較，如果相同即進行 KDA 流程，若不同則先予以拒絕登入；KDA 過程中，首先，未知使用者輸入的 PIN 測試(登入)樣本 $feat_v$ 集合透過公式(3)求出使用者各項特徵與訓樣本特徵間之差距 *D* 集合，接著將 *D* 集合除以特徵值個數 *P*=5*K*-2，至此可得出使用者各項特徵與訓樣本各項特徵之平均 *result*，最後設定門檻值(threshold)判斷該使用者是否為合法使用者，若 *result* 小於或等於門檻值則為正確使用者，允許登入系統進行資料存取；反之則拒絕登入。

$$D = \frac{feat_v - \mu_{feat}}{\sigma_{feat}} \qquad (3)$$

$$result = D/P \qquad (4)$$

4.實驗與結果

本研究使用觸控式手持行動裝置為 Motorola Milestone 觸控式手機，內建 ARM Cortex A8 550 MHz 處理器、動態記憶體 256MB，並於 Android 平台進行開發實作 KDA；每位使用者訓練樣本為 5 筆；所有實驗對象總共有 25 位，使用者年齡介於 19 至 40 歲；各使用者輸入 5 筆自訂之 PIN 用以合法使用者驗證，非法使用者之入侵情況則由 10 位具有資訊背景人員針對每組 PIN 進行攻擊 5 次；輸入之通行碼為使用者自行訂定 4 到 8 位數字 PIN，使用者個人特徵值個數為 5*K*-2。時間特徵資料利用 Android API 中 MotionEvent 函式庫中所提供之 getDownTime() 與 getEventTime()分別求出按鍵按下時間與離開按鍵時間，在經由計算求得實驗所需之 DU、UD 與 DD，所用時間精確度單位則毫秒(ms)；壓力特徵資料與面積特徵資料分別藉由 MotionEvent 函式庫提供之 getPressure()與 getSize()取得，單位分別為公斤 Kgf/cm^2 及 pixel。

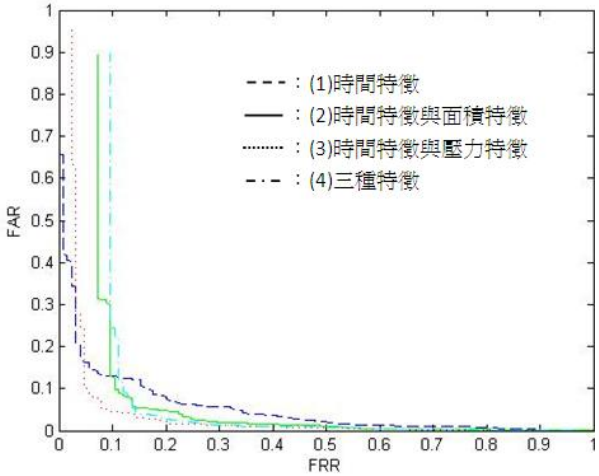
本研究所收集資料如表一所示，表中詳列各年齡、性別、4 至 8 碼數字之 PIN 字元數與輸入 PIN 之手指等特性之人數。

本研究目的在於評估時間特徵增加壓力特徵或面積特徵後，辨識效果是否較佳，透過 Fawcett[10]介紹得知可用 ROC 圖用來評估系統辨識效果，本研究利用 Fawcett [10] 所提之方法，使用錯誤拒絕率與錯誤接受率分別求出分類器中 4 種特徵組合之 ROC 圖，並經由相等錯誤率找出最佳門檻值，圖六以 ROC 圖方式呈現本研究實驗結果，圖中可分別看出錯誤拒絕率、錯誤接受率，若曲線越接近左下角原點則表示該方法越佳，以下分別針對 4 條曲線進行說明；只利用(1)時間特徵值當門檻值 1.82 時，其相等錯誤率為 12%；使用(2)時間特徵與面積特徵當門檻值 1.85 時，則相等錯誤率為 10%；(3) 時間特徵與壓力特徵當門檻值 1.82 時，相等錯誤率從 12%降至 7%；(4)三種特徵都使用則相等錯誤率為當門檻值 1.95 時，11%；從以上結果可證明，新增壓力特徵或面積特徵皆可提升辨識能力，但壓力特徵效果最佳，面積特徵較無壓力特徵班顯著改善，表二為本研究成果與其他文獻比較[3, 5, 6, 7]。

從表二與同樣使用行動裝置進行研究之相關文獻比較，其中 Clarke & Furnell [5, 6, 7] 針對每位使用者皆進行相等錯誤率評估故其相等錯誤率有區間；訓練樣本數方面，本研究僅需 5 筆訓練樣本即可完成 KDA 訓練，實驗

表一：各項實驗對象資料

年齡	20 歲以下	8
	21-25 歲	10
	26 歲以上	7
性別	男生	12
	女生	13
4 至 8 碼數字之 PIN 字元數	4	14
	5	3
	6	4
	7	3
	8	1
輸入 PIN 之手指	右大拇指	5
	右食指	13
	右中指	3
	左中指	1
	右食指與右中指	1
	右大拇指與左大拇指	2



圖六：各種特徵之 ROC 比較圖

表二：相關文獻結果比較

	輸入字串	訓練樣本數	相等錯誤率(%)
Clarke & Furnell[5, 6, 7]	4 位數字 PIN	30	9~16
	11 位數字電話號碼	30	5~13
	6 位元文字訊息	30	15~21
Campisi [3]	10 位元數字	6	13
本研究(時間與壓力)	4 至 8 位數字	5	7
本研究(時間與面積)	4 至 8 位數字	5	10

結果證明在利用較少的訓練樣本數訓練的情況下，新增面積特徵或壓力特徵後，可降低辨識錯誤情況發生。

本研究於手機上進行測試，建立分類器所需時間為 3 毫秒，使用者輸入 PIN 後的身分驗證則花費 2 毫秒，此兩項數據足以證明本研究驗證使用者相當具有效率，使用者在極少等待時間下即可完成身分驗證。

5. 結論

由於行動裝置的進步與發展，人類對行動裝置的應用越來越廣泛，為使資訊安全更受保障，本研究使用支援 Android 平台之觸控式手持行動裝置，以時間特徵、面積特徵與壓力特徵實作 KDA，用以提升系統安全性；研究結果發現，僅採用(1)時間特徵時相等錯誤率為 12%；(2)面積特徵後相等錯誤率降為 10%；而(3)時間特徵與壓力特徵結合後更可降低至 7%，此結果足以佐證新增面積特徵或壓力特徵確實可以有效降低辨識錯誤產生，提升辨識使用者能力。

基於科技發展日新月異情況下，各種觸控式手持行動裝置的出現改變人類儲存重要訊息的方式，而有些觸控式手持行動裝置設計並無實體鍵盤，本研究以此考量設計虛擬鍵盤擷取使用者時間特徵、面積特徵與壓力特徵進行研究。有鑑於行動裝置帶給人類相當多的方便性，而人類使用行動裝置將越來越頻繁，未來可朝向透過尋找更多人類獨一無二且應用成本較低之生物特徵進行使用者驗證，進而提升系統驗證能力之目標努力。

誌謝

國科會計畫編號：NSC99-2221-324-041-MY3、NSC99-2221-E-018-018 及 NSC 99-2221-E-018-021 贊助此研究。

參考文獻

[1] Araújo, L. C. F., Sucupira, L. H. R., Liza´rraga, M. G., Ling, L. L., and Yabu-Uti, J. B. T., "User Authentication through Typing Biometrics Features," ***IEEE Transactions on Signal Processing***, Vol. 53, No. 2, pp. 851-855, 2005.

[2] Bazrafshan, F., Javanbakht, A., and Mojallali, H., "Keystroke identification with a genetic fuzzy classifier," in ***2nd International Conference on Computer Engineering and Technology (ICCET)***, pp. V4-136-V4-140, 2010,

[3] Campisi, P., Maiorana, E., Bosco, M. L., and Neri, A., "User authentication using keystroke dynamics for cellular phones," ***IET Signal Processing***, Vol. 3, No. 4, pp. 333-341, 2009.

[4] Chang, T.-Y., Yang, Y.-J., and Peng, C.-C., "A personalized rhythm click-based authentication system," ***Information Management & Computer Security***, Vol. 18, No. 2, pp. 72-85, 2010.

[5] Clarke, N. L. and Furnell, S. M., "Authentication of users on mobile telephones - A survey of attitudes and practices," ***Computers & Security***, Vol. 24, No. 7, pp. 519-527, 2005.

[6] Clarke, N. L. and Furnell, S. M., "Advanced user authentication for mobile devices," ***Computers & Security***, Vol. 26, No. 2, pp. 109-119, 2007.

[7] Clarke, N. L. and Furnell, S. M., "Authentication mobile phone users using keystroke analysis," ***International Journal of Information Security***, Vol. 6, No. 6, pp. 1-14, 2007.

[8] Clarke, N. L., Furnell, S. M., Lines, B. M., and Lreynolds, P., "Keystroke dynamics on a mobile handset: a feasibility study," ***International Journal of Information Security***, Vol. 11, No. 4, pp. 161-166, 2003.

[9] De Ru, W. G. and Eloff, J. H. P., "Enhanced password authentication through fuzzy logic," ***IEEE Expert***, Vol. 12, No. 6, pp. 38-45, 1997.

[10] Fawcett, T., "An introduction to ROC analysis," ***Pattern Recognition Letters***, Vol. 27, No. 8, pp. 861-874, 2006.

[11] Gaines, R. S., Lisowski, W., Press, S. J., and Shapiro, N., *Authentication by keystroke timing: Some preliminary results*. 1980.

[12] Gláucya, C. B., Jeneffer, C. F., Edson, C. B., and Carvalho, F., "Authentication Personal," in ***International Conference on Intelligent and Advanced Systems***, pp. 254-256, 2007.

[13] Haider, S., Abbas, A., and Zaidi, A. K., "A Multi-Technique Approach for User Identification through Keystroke Dynamics," ***IEEE International Conference on Systems, Man, and Cybernetics***, Vol. 2, pp. 1336-1341, 2000.

[14] Harun, N., Woo, W. L., and Dlay, S. S., "Performance of keystroke biometrics authentication system using artificial neural network (ANN) and distance classifier method," in ***International Conference on Computer and Communication Engineering (ICCCE)***, pp. 1-6, 2010,

[15] Hwang, S., Cho, S., and Park, S., "Keystroke dynamics-based authentication for mobile devices," ***Computers & Security***, Vol. 28, No. 1-2, pp. 85-93, 2009.

[16] Karnan, M., Akila, M., and Krishnaraj, N., "Biometric personal authentication using keystroke dynamics: A review," ***Applied Soft Computing***, pp. 2010.

[17] Killourhy, K. S. and Maxion, R. A., "Comparing Anomaly-Detection Algorithms for Keystroke Dynamics," in ***39th Annual International Conference on Dependable Systems and Networks (DSN-2009)***, pp. 125-134, 2009.

[18] Monrose, F. and Rubin, A. D., "Keystroke dynamics as a biometric for authentication," ***Source, Future Generation Computer Systems archive***, Vol. 16, No. 4, pp. 351-359, 2000.

[19] Shabtai, A., Kanonov, U., and Elovici, Y., "Intrusion detection for mobile devices using the knowledge-based, temporal abstraction method," ***Journal of Systems and Software***, Vol. 83, No. 8, pp. 1524-1537, 2010.

[20] Shanmugapriya, V. and Padmavathi, G., "Keystroke Dynamics Authentication Using Neural Network Approaches," ***Information and Communication Technologies***, Vol. 101, Part 3, pp. 686-690, 2010.

[21] Shih, D. H. and Lin, T. C., "User authentication system by using keystroke dynamics," in ***International Conference on Pacific Rim Management 18th Annual Meeting***, pp. 102-115, 2008.