圖形通行碼結合擊鍵特徵於觸控式行動裝置之身分驗證

林俊豪	張庭毅	蔡政容	鄭培成
彰化師範大學	彰化師範大學	彰化師範大學	清雲科技大學
數位學習研究所	數位學習研究所	統計資訊研究所	資訊管理系
研究生	副教授	助理教授	助理教授
m97332007@mail.ncue.edu.tw	tychang@cc.ncue.edu.tw	tsaicj@cc.ncue.edu.tw	pccheng@cyu.edu.tw

摘要

隨著科技的發達與行動裝置的日漸普及，可方便及簡單的透過數位化行動裝置快速存取所需資料。因 PIN-based 身分驗證法有易被破解及窺視等缺點，近年來不少學者提出結合生物特徵中之擊鍵時間特徵來加強 PIN-based 驗證安全性之方法。但由於數位行動裝置輸入設備不一致性的問題，這些結合擊鍵時間特徵的安全性驗證法應用在數位行動裝置上之並無法達到如其應用在標準鍵盤上之高準確性。為了提昇數位行動裝置身分驗證之準確性與安全性，本研究採用圖形通行碼結合擊鍵時間特徵的方法來進行身分驗證並探討新增觸控式行動裝置專屬的壓力特徵是否能更進一步改善驗證成效。本研究實驗結果顯示：(1)圖形通行碼結合擊鍵時間特徵，相等錯誤率為 7.9%，其準確性較相關文獻中以 PIN-based 驗證結合擊鍵時間特徵佳;(2)圖形通行碼結合擊鍵時間特徵與壓力特徵，可進一步將相等錯誤率降為 3.8%。換言之，本研究所採用的圖形通行碼不僅可以提升通行碼空間(password space)，在結合擊鍵時間特徵與壓力特徵後，本研究所提出之驗證方法的準確性亦優於過去結合擊鍵時間特徵的 PIN-based 驗證方法。

關鍵詞：身分驗證、生物特徵、擊鍵特徵、圖形通行碼。

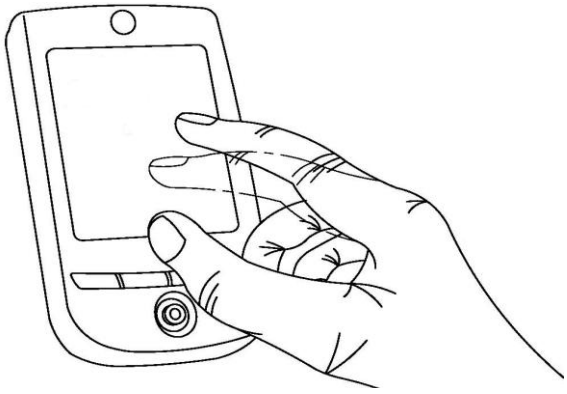
1. 前言

使用者身分認證(identity authentication)機制在電子商務及網路安全上扮演著極為重要的角色，不論是網路銀行、電子郵件、系統登入或報稅系統等，都必須先確認使用者身分，判斷是否可存取其系統上的資源。身分認證可分為下列三種[9, 32]：

- 以知識為基礎的驗證：使用合法使用者自行定義之通行碼(password)進行驗證。此類包含傳統個人電腦上由 QWERTY 鍵盤上的數字、符號及字母所組成之文字通行碼 (text-based password/alphanumeric password) 驗證、利用點擊圖片順序之圖形通行碼(graphical-based password)驗證以及行動裝置僅以數字所組成的 PIN-based(Personal Identification Number)驗證。
- 以物件為基礎的驗證：使用者需利用一把實體鑰匙打開門鎖一般，如使用者所使用的加密晶片卡。
- 以生物特徵為基礎的驗證：使用個人的特徵為身分辨識的依據。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”[21]，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。分為生理特徵與行為特徵兩類，生理特徵包含：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。

隨著網路資訊科技技術迅速發展，除了原本傳統的行動裝置外，新一代觸控式手機(touch phone)與個人數位助理等行動裝置的出現，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在網路上傳送，相對衍生出如何驗證使用者身分的安全性問題。行動裝置驗證機制僅以 4 至 8 位數字之 PIN-based 為主要方法，但其通行碼空間(password space)過小，使得 PIN 成為

弱通行碼(weak password)。攻擊者經由暴力攻擊(brute force attack)或肩窺攻擊(shoulder surfing attack)[6]等手段輕易的取得使用者之 PIN，導致 PIN-based 驗證之安全性隨之瓦解。因此，許多研究將標準 QWERTY 鍵盤之擊鍵時間特徵(keystroke time feature)[1, 11, 16, 30]應用於具有 keypad 之行動裝置上[5, 8, 9, 10, 22]，擊鍵特徵驗證過程中，除驗證 PIN 的正確性外，並藉由驗證個人輸入過程中之打字型態的獨特性，如按鍵間隔時間(inter-keystroke times)及按鍵持續時間(duration-keystroke times)等擊鍵時間特徵，確認使用者身分。由於擊鍵特徵擁有成本低、不需要額外設備、可與通行碼結合使用的種種特性，因此被廣泛地用在通行碼強度的強化。如此一來，使用者身分驗證機制包含了知識為基礎的驗證與生物特徵為基礎的驗證，強化通行碼驗證之安全性。



圖一、使用者透過觸控式行動裝置進行資料輸入之示意圖

但現今行動裝置之 PIN-based 結合擊鍵特徵身分驗證除了 PIN 本身為弱通行碼的缺失外，仍存在下列問題：第一，行動輸入設備不一致(鍵盤大小或按鍵排列方式)；第二：部分行動電話與 PDA 等觸控式行動裝置無實體鍵盤可供使用者輸入，僅利用觸控螢幕(touch panel)上之虛擬鍵盤，如圖一所示。使得使用者於不同行動裝置輸入的擊鍵時間特徵有所差異，進而導致身分驗證能力之安全性及準確性降低。為改善 PIN-based 結合擊鍵時間特徵驗證後的缺失，本研究中使用者選擇圖形並記憶點擊圖形上之順序作為圖形通行碼，以圖形通行碼取代 PIN-based，提供較大之通行碼空間；結合擊鍵特徵後，不受鍵盤大小或按鍵排列方式不同之設備影響其準確性。

本研究分析(1)圖形通行碼結合生物特徵之擊鍵時間特徵辨識效果及(2)除時間特徵外，新增一項觸控裝置專有之壓力特徵(pressure feature)後驗證效果是否更加精確；最後，實作圖形通行碼結合擊鍵特徵之身分驗證於 Android 平台之觸控式手機。實驗結果說明圖形通行碼結合擊鍵時間特徵較 PIN-based 結合擊鍵時間特徵[5, 8, 9, 10, 21]之準確性高；在新增壓力這項特徵後，其辨識效果更佳。

2. 相關研究

為改善文字通行碼及 PIN-based 身分驗證之缺失，本研究結合圖形通行碼與擊鍵特徵，分別於 2.1 節與 2.2 節對圖形通行碼與擊鍵特徵相關研究進行探討。

2.1 圖形通行碼

文字式通行碼身分認證是最普遍被採用的使用者身分認證方法。以安全性而言，文字通行碼長度大於 8 字元為佳。但受制於人類長期記憶(long-term memory)，過長的文字通行碼對使用者而言有著沈重的記憶負擔，導致使用者忘記或搞混文字通行碼[35]。因此，人類為避免忘記文字通行碼通常採取下列幾種方式；第一，寫下文字通行碼；第二，於多個系統中使用相同文字通行碼；第三，使用容易記憶的文字通行碼組合(如：生日等)。如此一來；上述舉動讓文字通行碼變成弱通行碼，使得通行碼易受字典攻擊、暴力攻擊與肩窺攻擊等威脅。

為解決文字通行碼之缺失，圖形通行碼首先由 Blonder [3]提出。圖形通行碼依記憶特性之不同可分為兩類：認知(recognition)與回憶(recall)。認知型包含 Brostoff 與 Sasse [4]之 Passface 系統、Dhamija 與 Perring [12]之 Déjà Vu 系統，這

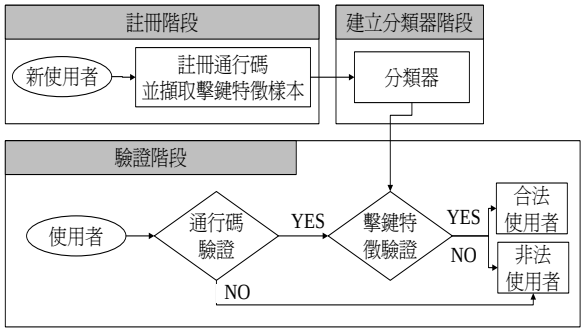
些系統皆利用挑選多個圖像區域之順序作為身分驗證的依據。但由於上述方式會遭受到肩窺攻擊，Sobrado 與 Birget [33]提出 Convex-hull Click、Movable Frame 和 Intersection 三套方式解決。Wiedenback 等人[35]以像素為基礎，使用者點擊圖像中任何點以訂定圖形通行碼，而任何點周圍有一定的寬容值；驗證時，使用者需在寬容值內點擊其圖形通行碼順序，此法其通行碼空間遠比文字通行碼大許多。回憶型圖形通行碼則以 Jermyn 等人[26]的 DAS 系統代表，其通行碼為使用者於二維網格畫出簡單的圖形，以判斷圖形與註冊時是否符合作為身分驗證的依據，而 Syukri 等人[34]認為簽名的優點在於使用者不需記憶本身的簽名且簽名很難被仿造，以簽名取代 Jermyn 等人[26]的簡易圖形繪畫，但缺點在於以滑鼠簽名對大部分人而言相當困難，以手寫的方式則需另外的裝置才可達成，此舉對使用者而言較不方便。

由於行動裝置應用越來越廣泛，但受制於螢幕小且部分觸控式行動裝置僅能用手指繪畫或點擊。造成 Syukri 等人[34]、Wiedenback 等人[35]及 Sobrado 與 Birget [33]的方式並不適用於行動裝置。Jansen 等人[23, 25]提出應用於行動裝置的認知型圖形通行碼，使用者從 30 個約等於大拇指大小的圖像中挑選不重複的數個圖像，挑選圖像之順序即為註冊之圖形通行碼，驗證依據為判斷使用者點擊圖像之順序與註冊時是否相同；爾後，Jansen [24]提出改良方法，將一張具有意義的圖像(如：海洋、貓等)切割成 30 張約等於大拇指大小的區域圖，且允許使用者重複挑選某區域圖。如此一來，若挑選 3 個區域圖為通行碼，將 Jansen 等人方法之通行碼空間由 $30 \times 29 \times 28$ 擴大為 30^3；但[23, 25]仍無法有效抵擋肩窺攻擊。

由上述文獻中可得知圖形通行碼具有下列優點。第一，相較於人類對文字記憶的方式，人類對於圖像的記憶會先理解圖像，了解圖像所要表達之意義，根據圖形的含意進行記憶並記憶點擊順序；換句話說，人類的長期記憶並不會記憶整張圖像，而是記憶自己本身對圖像的解釋[28]，故具體或真實的圖像比混亂或抽象的圖像容易記憶。再者，[28, 29, 35]研究發現，證明圖像比文字或句子較容易記憶。第二，圖形通行碼之通行碼空間較 PIN 大，可抵擋暴力攻擊；以 Jansen 等人[24]的圖形通行碼為例，從 30 個區域圖中點擊 6 個區域之圖形通行碼，可提供通行碼空間為 30^6；8 位數字 PIN 則提供通行碼空間為 10^8。因此 Jansen 等人[24]之圖形通行碼可提供通行碼空間為 8 位數字 PIN 文字通行碼之 $30^6/10^8=2.7$ 倍。

2.2 擊鍵特徵

文字通行碼驗證廣泛的運用於身分認證上，一旦文字通行碼遭竊取，則系統安全性將隨之瓦解。Gaines 等人[14]提出動態擊鍵特徵驗證(Keystroke Dynamics-based Authentication; KDA)以加強身分驗證之安全性。KDA 不僅驗證使用者文字通行碼是否正確，額外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皆不盡相同之特性，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，使得傳統文字通行碼驗證多一層安全機制。



圖二、動態擊鍵特徵驗證流程圖

KDA 可分為三個階段，註冊、建構分類器及驗證，其流程如圖二所示。首先，在註冊階段中，使用者進行註冊，並擷取文字通行碼或 PIN 之擊鍵特徵樣本，所有使用者特徵將於此階段取得。[1, 3, 7, 11, 15, 16, 17, 22, 27, 30, 32]等文字通行碼的文獻中，使用者特徵樣本由按鍵持續時間、按鍵間隔時間等擊鍵時間特徵所構

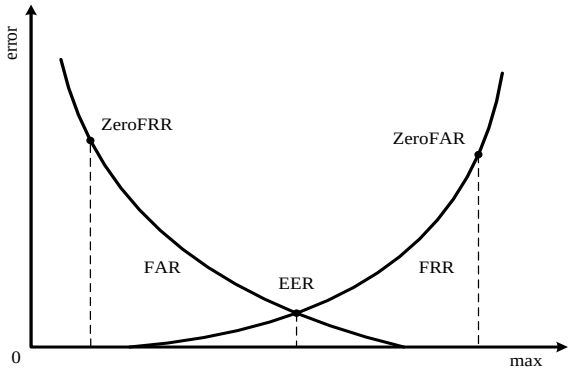
成；其中，Araújo [1]研究指出，擊鍵時間特徵的結合效果比單一種擊鍵時間較好，且建議訓練樣本以不超過 10 筆為佳，一旦超過 10 筆將會另使用者感到厭煩。Hwang 等人[22]以人工節奏的方式改善擊鍵特徵資料品質，其方法利用節拍器提醒使用者，使用者透過提示增加斷音、連音或暫停等，提高個人輸入文字通行碼時的獨特性及一致性，進而提升辨識能力。但其缺點在於使用者需記憶這些暫停的時間、位置及長度，如此一來便雖成功提升驗證安全性但卻造成使用者額外負擔。Chang 等人[7]認為須以人類與生俱來打字型態差異所產生的特徵進行辨識而非刻意使用人工節奏，其方式為利用滑鼠點擊個人的音樂節奏之時間特徵，如愛的鼓勵，以改善資料品質，如此一來；除了不會造成使用者額外負擔且較能符合生物特徵之定義。

在建構分類器階段中，分類器由所收集的特徵樣本建構，用以分辨是否為合法使用者。Shih [32]與 Killourhy [27]指出，建構 KDA 分類器的方法有很多，包含統計(statistics)[1, 2, 5, 15, 16, 18, 29, 32]、模糊邏輯(fuzzy logic)[11, 16, 19]、K 位最近鄰居法(K Nearest Neighbor; KNN)[20, 31]與類神經(neural network)[7, 8, 9, 10, 16, 17]等方式。其中，Haider 等人[16]利用統計、模糊邏輯與類神經等方法建構分類器應用於文字通行碼驗證上，並進一步分析建構方法的各種組合驗證效果。類神經網路之分類器需要利用非法使用者訓練樣本訓練網路，此舉較不符合實際應用；雖然 KNN 分類器不需利用非法使用者訓練樣本，但其缺點在於驗證階段須將使用者特徵需與其他所有使用者特徵進行比較，使用者數量增加會讓系統運算時間變長，導致使用者需花費較多時間等待驗證完成。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，亦不需與其他使用者特徵比較；最後，此方法之驗證效果多數比類神經或模糊理論較佳。

隨著行動裝置的普及，許多研究[5, 8, 9, 10, 21]將 KDA 的觀念延伸至 PIN-based 驗證於具有 keypad 之行動設備上，改善其驗證之安全性。Hwang [21]將其改善資料品質的方式延伸至行動裝置上，以提升 PIN-based 驗證之安全性，但此研究[21]與其應用於 QWERTY 標準鍵盤之研究[22]有相同的缺點，其方式仍然會造成使用者額外的負擔。Clarke [8, 9, 10]與 Campisi [5]則著墨於分類器建構；其中，Clarke [8, 9, 10]利用多種類神經方式於行動裝置上建構分類器，但此缺點與傳統之類神經網路分類器一樣需要利用非法樣本訓練網路且不適用於低運算功能之行動設備，不符合實際應用。Campisi [5]則利用多種統計方式正規化分類器，有助於多分類器整合，但其實驗是利用文字訊息為輸入字串，但由於行動裝置的輸入設備並不一致，若使用不同行動裝置進行實驗，其結果將會有所差異。

由於具觸控螢幕之行動裝置的出現，Saevanee 等人[31]以筆記型電腦之觸控板(touch pad)模擬行動裝置之觸控螢幕，並以 KNN 為分類器。而其缺點在於僅用 10 名使用者進行實驗，受測者過少且註冊時要求使用者多達 20 次的輸入當為訓練樣本。Saevanee 等人[31]及 Chang 等人[7]分別利用筆記型電腦之觸控板及滑鼠模擬手指在觸控螢幕上點擊，但並不足以反應至行動裝置上之成效。

在驗證階段中，系統先判斷使用者之通行碼是否正確，倘若與註冊時不同，系統先行拒絕登入；如與註冊時相同則透過已建構的分類器對特徵值分析，若特徵值分析結果符合所設定之門檻值則允許登入，反之；系統予以拒絕登入。



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

本研究將圖形通行碼結合擊鍵特徵並使用統計分類器運用於觸控式行動裝置上進行使用者身分驗證，用以改善 PIN-based 驗證之安全性以及防止圖形通行碼遭肩窺攻擊。另外，經由觀察使用者透過點擊螢幕輸入資料的情況發現，使用者點擊觸控式手持行動裝置螢幕的力道大小不盡相同，系統所接收到使用者按觸螢幕壓力便會有所差異。因此，本研究假設若能加入使用者按觸行動裝置螢幕之壓力特徵以提升資料品質，進而提升 KDA 辨識使用者的能力，故本研究進一步分析除擷取時間特徵值之外，新增按觸行動裝置螢幕壓力特徵後，其辨識準確性是否提升。

本節中以 KDA 流程介紹本研究之研究方法，其中 3.1 節詳細說明特徵值收集過程之註冊階段；3.2 節介紹利用統計方法之建構分類器階段；3.3 節敘述判斷使用者身分的過程之階段驗證。

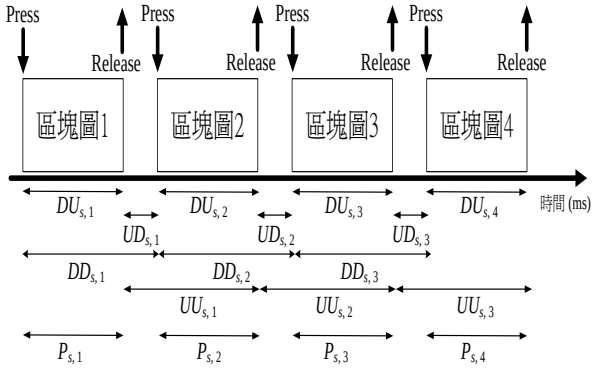
3.1 註冊階段

本研究之圖形通行碼以 Jansen 等人[24]為基礎進行改良，使用者先行挑選喜愛之 325 × 432 pixel 大小圖像，系統將此圖像切割成 30 個大拇指般之 65 × 72 pixel 大小區域圖，使用者透過點擊觸控式行動裝置螢幕挑選可重複之 3 至 6 個區域圖，此挑選順序即為其註冊之圖形通行碼，

圖四為模擬器執行時之使用者介面。其中，上方提示使用者仍需輸入幾次圖形通行碼，下方功能鍵中，使用者分別可用以重新圖形通行碼及確認送出圖形通行碼。本研究之圖形通行碼所用之圖像並無邊界，為讓使用者察覺是否有點擊到該圖像，本研究以震動的方式提醒使用者，若點擊到圖片則震動 100 毫秒。

圖四、於模擬器呈現使用者輸入圖形通行碼介面

當使用者點擊螢幕的同時，系統記錄其點擊位置、時間特徵與壓力特徵。使用者手指按下(Press)到離開(Release)螢幕這段期間產生 4 種時間特徵及壓力特徵，其相互關聯性如下，其中圖五表示第 s 筆訓練樣本中使用者點擊第 1、2、3、4 個區域圖時，所產生各項特徵。



圖五、各項擊鍵特徵示意圖

- Down-Up (DU)時間：第 *s* 筆訓練樣本中，同一個區域圖 *i* 按下到放開之時間間隔，稱 $DU_{s,i}$。
- Up-Down (UD)時間：第 *s* 筆訓練樣本中，從第 *i* 個區域圖放開到下一個區域圖按下之時間間隔，稱 $UD_{s,i}$。
- Down-Down (DD)時間：使用者第 *s* 筆訓練樣本中，從第 *i* 個區域圖按下到下一個區域圖按下之時間間隔，稱之為 $DD_{s,i}$。
- Up-Up (UU)時間：第 *s* 筆訓練樣本中，從第 *i* 個區域圖放開到下一個區域圖放開之時間間隔，稱 $UU_{s,i}$。
- Pressure：第 *s* 筆訓練樣本中，區域圖 *i* 按下時螢幕所受之壓力，稱 $P_{s,i}$。

時間特徵有 DU、UD、DD 及 UU。Araújo[1]指出，時間特徵值中取 DU、UD、UU 組合辨識效果最佳，本研究採用這三種時間特徵並新增一項壓力特徵。使用者第 s 筆訓練樣本中，當使用者點擊螢幕 *k* 個區域圖，則總共可收集到 4*k*-2 個特徵，其中包含 *k* 個 DU 特徵之 DU_s 集合與 *k* 個壓力特徵之 P_s 集合、*k*-1 個 UD 特徵之 UD_s 集合與 *k*-1 個 UU 特徵之 UU_s 集合，如下：

$DU_s = \{DU_{s,1}, DU_{s,2}, \ldots, DU_{s,k}\}$
$UD_s = \{UD_{s,1}, UD_{s,2}, \ldots, UD_{s,k-1}\}$
$DD_s = \{DD_{s,1}, DD_{s,2}, \ldots, DD_{s,k-1}\}$
$P_s = \{P_{s,1}, P_{s,2}, \ldots, P_{s,k}\}$

得到時間特徵及壓力特徵後，則使用者第 *s* 個樣本之所有的特徵集合表示為 $feat_s$：

$feat_s = \{DU_s, UD_s, DD_s, P_s\}$
$= \{X_{s,1}, X_{s,2}, \ldots, X_{s,f}\}$

其中 f=4*k*-2 為特徵值個數。

在收集特徵樣本的過程中，本研究以不造成使用者負擔為考量，僅要求使用者於註冊階段輸入 5 筆訓練樣本(s=1 to 5)，低於 Araújo 等人建議[1]。

3.2 建構分類器階段

因應低運算量之行動設備，本研究採用 Gláucya 等人[15]的統計方法建構分類器。使用者在註冊階段所輸入之 5 筆訓練樣本分別透過等式(1)及等式(2)計算各項特徵值之平均數(mean)與標準差(standard deviation)。

$$\mu_f = \frac{1}{5}\sum_{s=1}^{5} X_{s,f} \quad \text{for } f\text{=1 to } 4k\text{-2} \quad (1)$$

$$\sigma_f = \frac{1}{5-1}\sum_{s=1}^{5} \left| X_{s,f} - \mu_f \right| \quad \text{for } f\text{=1 to } 4k\text{-2} \quad (2)$$

本研究使用統計建構分類器，故不需使用非法使用者樣本進行訓練，符合實際應用；且系統不需複雜運算適用於低運算量之行動設備。

3.3 驗證階段

首先系統針對未知使用者點擊圖形密碼之位置順序與註冊時點擊之位置順序比對，若不同則先予以拒絕登入。比對結果若相同則繼續進行下個步驟，使用者所點擊的登入樣本 $feat_v=\{DU_v, UD_v, DD_v, P_v\}=\{X_{v,1}, X_{v,2}, \ldots, X_{v,f}\}$ 集合透過等式(3)求出該使用者登入樣本與註冊時的訓練樣本之各項特徵值差距之平均 D；最後設定門檻值(threshold)以判斷該使用者是否為正確使用者，若 D 小於或等於即為合法使用者，允許登入系統進行資料存取；反之則拒絕登入。

$$D = \frac{1}{4k-2}\sum_{f=1}^{4k-2} \frac{X_{v,f} - \mu_f}{\sigma_f} \quad (3)$$

本研究中,僅針對該使用者之登入樣本與訓練樣本進行分析比對，即使系統使用者增加亦不影響建構分類器與驗證時使用者之等待時間。

4.實驗與結果

本研究將圖形通行碼結合擊鍵特徵實作於採用 Android 系統之 Motorola Milestone 觸控式手機，其內建 ARM Cortex A8 550 MHz 處理器及 256 MB 動態記憶體。實驗對象總共有 25 位，年齡介於 19 至 25 歲；本研究要求每位使用者輸入 5 次自訂之圖形通行碼當作訓練樣本以建構分類器；合法使用者由各使用者對自己的通行碼進行 5 次驗證,每組通行碼則總共有 150 筆樣本進行非法使用者驗證。

本研究中使用的時間特徵由 Android API 中 MotionEvent() 函式庫提供之 getDownTime()與 getEventTime()分別求出按下與離開螢幕時間，而後透過各特徵間之間的關聯性，經計算分別求出實驗所需之 DU、UD 與 DD，時間精準度單位為毫秒(ms)。壓力特徵則透過 MotionEvent()函式庫提供之 getPressure()直接取得，單位為平方公分公斤力。

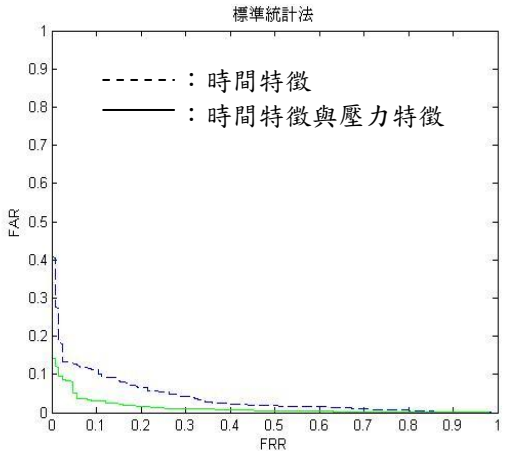
表一、與相關文獻結果比較

	通行碼	通行碼空間	訓練樣本數	分類器建構方法	相等錯誤率 (%)
Clarke & Furnell [8, 9, 10]	4 位數字 PIN	1×10^4	30	類神經	9~16
	11 位數字電話號碼	1×10^{11}	30	類神經	5~13
	6 字元文字訊息 (text massage)	$26^6 \cong 3\times10^8$	30	類神經	15~21
Campisi 等人[5]	10 字元文字字母 (letter)	$26^{10} \cong 1.4\times10^{14}$	6	統計	13
Hwang 等人[21]	4 位數字 PIN	1×10^4	5	統計	4
本研究(時間特徵)	3 至 6 個點擊區域	$30^6 = 7.29\times10^8$	5	統計	7.9
本研究(時間特徵與壓力特徵)	3 至 6 個點擊區域	$30^6 = 7.29\times10^8$	5	統計	3.8

表一為與同樣以行動裝置進行研究之相關文獻比較，由於圖形通行碼尚未有結合擊鍵特徵之研究，相關研究以 PIN-based 驗證結合擊鍵時間特徵於行動裝置比較，其中 Clarke & Furnell[8, 9, 10]針對每位使用者皆進行相等錯誤率評估，故其相等錯誤為區間。從表一結果可發現，本研究雖僅以 5 筆訓練樣本完成 KDA 訓練,身分驗證準確度比 Clarke & Furnell[8, 9, 10]與 Campisi 等人[5]佳;圖形通行碼結合時間特徵結果雖較 Hwang 等人[21]略差，但本研究優點在於不會額外增加使用者負擔，且若增加壓力特徵後，本研究準確性皆較過去相關研究佳。實驗結果證明圖形通行碼結合擊鍵特徵確實可改善 PIN-based 結合即鍵時間特徵之驗證安全性，尤其在新增壓力特徵後，EER 由 7.9%降至 3.8%。在通行碼空間比較中，雖然較 Clarke & Furnell [9, 10]之 11 數字電話號碼與 6 字元文字訊息及 Campisi 等人[5]之 10 字元文字字母小，但這些方式存在著會造成使用者沉重記憶負擔且會受到鍵盤大小與樣式不同等因素影響，故這些方式並不適用於行動裝置上。與 Hwang 等人[21]及 Clarke & Furnell [8, 9]所使用的 PIN 相比，本研究僅需點擊三個區域圖為 $30^3=2.7\times10^4$ 即可大於其 1×10^4。綜觀上述比較，本研究可在不造成使用者記憶負擔的情況下，增加通行碼空間，進而改善 PIN-based 驗證之安全性。

透過 Fawcett[13]使用 ROC 圖以評估系統驗證準確性,本研究以 Fawcett 所提之方法，使用錯誤拒絕率與錯誤接受率分別繪出圖形通行碼僅結合時間特徵以及結合時間特徵、壓力特徵之 ROC 圖，並經由相等

錯誤率分別找出最佳門檻值。圖六為本研究兩項實驗之 ROC 圖，若曲線越接近原點則代表辨識準確性越佳，以下針對圖六中兩條曲線說明：(1)虛線為圖形通行碼結合時間特徵，當門檻值為 1.92 時，相等錯誤率為 7.9%；(2)實線為圖形通行碼結合時間特徵與壓力特徵，當門檻值為 1.98 時，相等錯誤率為 3.8%。由以上結果足以佐證新增壓力特徵後，辨識準確率的確明顯獲得改善。



圖六、兩項實驗之 ROC 比較圖

效能方面，在建構分類器階段所需時間為 8 毫秒；使用者輸入圖形通行碼後，在身分驗證階段則花費 3 毫秒，可適用於低運算量之行動設備。除此之外，由於本研究讓使用者採用點擊的方式輸入其圖形通行碼，此方式讓本研究執行 KDA 運作時可不受行動裝置鍵盤大小與排列方式等因素影響。

5. 結論

本研究將圖形通行碼結合擊鍵特徵實作於支援 Android 平台之觸控式行動裝置，用以改善 PIN-based 驗證之安全性。利用點擊的方式使得時間特徵與壓力特徵的取得，不受鍵盤大小與樣式之影響。與 PIN-based 身分驗證相比，通行碼結合擊鍵特徵確實不僅提供較大的通行碼空間且提升行動裝置對身分驗證的安全性，加入壓力特徵後效果更佳，足以佐證壓力特徵的確是一項觸控式行動裝置可用來提升驗證能力的新特徵。實驗結果進一步發現，使用者等待建構分類器與完成驗證的時間相當短暫；換句話說，系統對於使用者身分驗證極具效率。基於科技發展日新月異，各式的觸控式行動裝置功能越來越強大，相對行動裝置感知器亦越來越精確，未來可朝向尋找更多類獨一無二並隨身攜帶且成本低廉之生物特徵，以提升身分驗證準確性之目標努力。

致謝

國科會計畫編號: NSC99-2221-E-018-018 及 NSC99-2221-E-018-021 贊助此研究。

參考文獻

[1] Araújo L. C. F., L. H. R., S., M. G., L., L. L., L., and J. B. T., Y.-U., "User authentication through typing biometrics features," ***IEEE Transactions on Signal Processing***, Vol. 53, No. 2, pp. 851-855, 2005.

[2] Bleha S. A., C., S., and B., H., "Computer-access security systems using keystroke dynamics," ***IEEE Transactions on Pattern Analysis and Machine Intelligence***, Vol. 12, No. 12, pp. 1217-1222, 1990.

[3] Blonder G. E., ***Graphical Passwords***. 1996, United States Patent 5559961.

[4] Brostoff S. and M. A., S., "Are Passfaces more usable than passwords: a field trial investigation," ***in People and Computers XIV – Usability or Else: Proceedings of HCI,*** Sunderland, UK, pp. 405-424, 2000.

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

[6] Chang T. Y., M. S., H., and W. P., Y., "A Communication-Efficient Three-Party Password Authenticated Key Exchange Protocol," ***Information Sciences***, Vol. 181, No. 2, pp. 217-226, 2011.

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

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

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

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

[11] de Ru W. G. and J. H. P., E., "Enhanced password authentication through fuzzy logic," ***IEEE Expert: Intelligent Systems and their Applications***, Vol. 12, No. 6, pp. 38-45, 1997.

[12] Dhamija R. and A., P., "Déjà Vu: User study using images for authentication," in ***the 9th Usenix Security Symposium***, pp. 2000.

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

[14] Gaines R. S., W., L., S. J., P., and N., S., ***Authentication by keystroke timing: Some preliminary results***. 1980.

[15] Gláucya C. B., C. F., J., C. B., E., and F., C., "Authentication Personal," in ***International Conference on Intelligent and Advanced Systems***, pp. 254-256, 2007.

[16] Haider S., A., A., and A. K., Z., "A multi-technique approach for user identification through keystroke dynamics," ***IEEE International Conference on Systems, Man, and Cybernetics***, Systems, Man, and Cybernetics, 2000 IEEE International Conference on, Vol. 2, pp. 1336-1341, 2000.

[17] Harun N., W. L., W., and S. S., D., "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.

[18] Hocquet S., J. Y., R., and H., C., "User classification for keystroke dynamics authentication," ***Advances in Biometrics, Lecture Notes in Computer Science***, Vol. 4642, pp. 531-9, 2007.

[19] Hosseinzadeh D., S., K., and A., K., "Keystroke Identification Based on Gaussian Mixture Models," in ***IEEE International Conference on Acoustics, Speech and Signal Processing***, Vol. 3, pp. 1144-1147, 2006.

[20] Hu J., D., G., and A., S., "A k-Nearest Neighbor Approach for User Authentication through Biometric Keystroke Dynamics," in ***IEEE International Conference on Communications***, pp. 1556-1560, 2008.

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

[22] Hwang S. S., H. J., L., and S., C., "Improving authentication accuracy using artificial rhythms and cues for keystroke dynamics-based authentication," ***Expert Systems with Applications***, Vol. 36, No. 7, pp. 10649-10656, 2009.

[23] Jansen W., "Authenticating Users on Handheld Devices," in ***Canadian Information Technology Security Symposium***, pp. 2003.

[24] Jansen W., "Authenticating Mobile Device Users through Image Selection," in ***Data Security***, pp.

2004.

[25] Jansen W., S., G., V., K., R., A., and R., S., "Picture Password: A Visual Login Technique for Mobile Devices," in ***National Institute of Standards and Technology Interagency Report***, pp. 2003.

[26] Jermyn I., A., M., F., M., M. K., R., and A.D., R., "The Design and Analysis of Graphical Passwords," in ***the 8th USENIX Security Symposium***, pp. 1999.

[27] Killourhy K. S. and R. A., M., "Comparing anomaly-detection algorithms for keystroke dynamics," in ***International Conference Dependable Systems & Networks***, Lisbon, Portugal, pp. 125-134, 2009.

[28] Mandler J. M. and G. H., R., "Long-Term Memory for Pictures," ***Journal of Experimental Psychology: Human Learning and Memory***, Vol. 3, No. 4, pp. 386-396, 1977.

[29] Revett K., S. T., d. M. e., and H. M. D., S., "Enhancing login security through the use of keystroke input dynamics," in ***Advances in Biometrics, Lecture Notes in Computer Science***, Lecture Notes in Computer Scienc, pp. 661-667, 2005.

[30] Rick J. and G., G., "Identity authentication based on keystroke latencies," ***Communications of the ACM***, Vol. 33, No. 2, pp. 168-176, 1990.

[31] Saevanee, H. and Bhatarakosol, P., "User Authentication Using Combination of Behavioral Biometrics over the Touchpad Acting Like Touch Screen of Mobile Device," in ***Computer and Electrical Engineering***, pp. 82-86, 2008.

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

[33] Sobrado L. and J. C., B., "Graphical passwords," ***The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research***, Vol. 4, pp. 2002.

[34] Syukri A. F., E., O., and M., M., "A User Identification System Using Signature Written with Mouse," in ***the 3rd Australasian Conference on Information Security and Privacy***, pp. 403-441, 1998.

[35] Wiedenbeck S., J., W., J. C., B., A., B., and N., M., "Authentication using graphical passwords: Basic Results," in ***Human-Computer Interaction International***, Las Vegas, NV, pp. 2005.