圖形化通行碼認證設計-畫面拖曳式認證

Graphical Password Authentication Scheme-Screen Drag and Drop

郭文彥
輔仁大學
wykuo@csie.fju.edu.tw

楊豐源
輔仁大學
coolsealtw@gmail.com

1. 摘要

近來使用者登入認證系統的安全性日益重要，舉凡繳稅、銀行轉帳、線上刷卡、股票交易等，都是在登入後授權使用。

傳統登入方式，使用者偏向由字彙所組成的通行碼(Password)，而且登入環境可能會有木馬程式或攝影機側錄，針對傳統文字通行碼認證的缺點：安全性強度不足、容易遭受字典攻擊(Dictionary Attack)，且無法抵擋肩窺、側錄攻擊，使得整體安全性大為降低；現今有許多專家學者提出另一個替代方案：圖形化通行碼認證，此設計能夠讓通行碼更安全，且不會遭受到字典攻擊，有學者更提出能夠抵檔肩窺、側錄攻擊的圖形化通行碼認證設計。

本論文提出的畫面拖曳式通行碼認證設計(Screen Drag and Drop)，能夠確實的抵擋肩窺、側錄、和字典攻擊，並提供夠強的通行碼強度(Password Space)，相較於傳統通行碼使用者偏向設置字彙組成的通行碼，本論文選用的圖案的種類、樣式，讓每個圖案被選取的機率能夠相近，提供有如亂數般的通行碼組合。

關鍵詞：Graphical Password, Authentication Scheme, Shoulder Surfing Attack, Indirect Select.

2. 緒論

現行的傳統文字通行碼(Traditional Text-based Password)，使用者偏向於使用能夠被猜測、有意義的組合，如字彙所組成，依據使用通行碼的限制程度不同，大致可分為二種：

(一) 弱通行碼(Weak Password)：

弱通行碼是指長度較短，亂度較低，而使用者容易記憶的通行碼，由於弱通行碼容易受到字典攻擊(Dictionary attack)，且此類通行碼通常需要額外的裝置(如金融卡、提款卡)，對於使用者來說較為不方便。

(二) 強通行碼(Strong Password)：

強通行碼是指長度較長，亂度較高，較難猜測的通行碼。實際上現行許多作業系統及重要機構(如銀行)等，皆有通行碼檢查機制，杜絕使用者選擇強度過於弱的通行碼(如通行碼需包含特殊符號、數字和大小寫字母) 。但事實上對於使用者來說，因為是不熟悉的字串所組成的通行碼，不是難以記憶便是使用者傾向寫下其通行碼，反而造成了安全性上的漏洞。

使用強通行碼雖然可以抵擋字典攻擊(Dictionary Attack)，但在不使用額外輔助裝置的前提下(如 IC 金融卡、記憶卡)，強通行碼的使用將帶給使用者記憶上較重的負擔。近來，除了傳統文字通行碼外，有了另一個選項：圖形化通行碼(Graphical Password)；圖形化通行碼提供另一個實行強通行碼的一線希望。圖形化通行碼原本屬意解決在 PDA 等掌上型裝置登入的解決方式，由於此種掌上型裝置尺寸較小，要在原本就不大的觸控式螢幕面板所顯示的虛擬鍵盤上輸入由 96 種字元所組合成的通行碼，在操作上較不容易，為提供使用者更方便合適的身份認證方法，不少專家學者陸續提出各種圖

形化通行碼認證設計，其中不乏在監視器側錄(肩窺攻擊)下仍能保持安全的認證設計。

3. 相關研究

Shepard 指出，人類在記憶圖片上會比文字上有更好的記憶能力[12] ，圖形化通行碼以某些設計能夠抵擋肩窺攻擊(Shoulder Surfing Attack)及能提供強大的通行碼強度(Password Space)著名[20] 。

現今圖形化通行碼可分成兩類：認知(Recognition)類和回憶(Recall)類[20] 。認知類型(Recognition)為使用者在畫面中選取印象中的圖片，並以挑選的圖片和順序來做為使用者的圖形化通行碼來達到認證的目的；而回憶類型(Recall)則需要使用者依據當初認證時所繪出的圖形，於認證時繪製出同樣的一個或數個圖形。

第一個圖形化通行碼為 Blonder 於 1996 年所提出的 Blonder，s Graphical Passwords[2] ，其認證方式乃由使用者點選預先決定的圖形順序，而圖形為一張圖片中的幾個特定區域或子圖形所組成。然而由於候選子圖形過少使得整體安全比起文字通行碼更低，並且候選子圖形中並無邊界表示，使得使用者認證時較易選錯子圖形而造成認證失敗。

之後，Jermyn 等人在 1999 年提出 Draw-A-Secret(簡稱 DAS) [3] [4] [5] [7] ，設計者強調其 DAS 設計擁有比 Blonder，s Graphical Password[2] 更佳的安全性。其特點在於認證方式使用 G x G 的網格，使用者允許在網格中畫出自己易於記憶的點、線、以及圖案，而透過重繪出正確的點、線、及圖案的順序來認證使用者。

Dhamija 與 Perrig 於 2000 提出一套名為 Déjà vu[1] 的設計，其特點為圖片的構成，並非生活中的真實圖片，而是以 hash visualization[9] 技術產生的抽象圖片。使用者不止需要記憶正確的圖片順序，並且需在每次認證中找到正確的圖片位置。此外 Déjà vu 需要一台可信任的伺服器來儲存使用者的認證資料。

sfr GmbH 公司於 2000 年在 PDA 平台上設計了一套圖形化通行碼－Visual Key[15] 。將一張預定的圖片切分為近 85 個大小不一樣的候選子圖形，而圖形化通行碼的強度根據圖片所選的候選子圖形個數成正比。雖然其候選子圖形較 Blonder，s Graphical Passwords 多，然而候選子圖形點選後並沒有設計為可見的，且每個候選子圖形為隨機切割。因此使用者點選的候選子圖形經常會是圖案中某個物件的另一小部份(如時鐘的時針、書桌的左下角、洋娃娃的眼睛)，而不是完整的物件。這將對使用者造成額外的記憶負擔，並且使用者在點選時也不能立即的發現自己的錯誤，使得使用者認證時較易選錯子圖形而造成認證錯誤。

Real User 公司於 2001 年提出的 Passfaces[13] 與 Déjà vu[1] 也非常相似，但將 Déjà vu 隨機產生的抽象圖片改為以真實的人臉來表示，其後亦有許多專家學者提出相關研究[1] [14] [21] [22] 。

PointSec 公司於 2002 年針對 Pocket PC 平台在 2002 年所提出的 PicturePIN[21] 做改良，候選子圖形可以用自己加入的圖形，但候選子圖形的總數只能夠有十個。設定圖形化通行碼時，使用者可重覆與否的挑選四到十三個候選子圖形來組合出便於自己記憶的圖形化通行碼。每次認證時候選子圖形會隨機排列，並允許使用者一個預設的錯誤登入次數，超過預設次數則封鎖使用者的登入請求。然而候選子圖形過少且子圖形的組合長度也有所限制，使得其安全強度略顯不足。

Jansen 等人於 2003 年提出的 Picture Password[23] [24] [25] ，則使用 5x6 個候選子圖形。可由一大張的風景圖片切割成 30 個網格，

在候選子圖形的點選上，能夠讓使用者選擇任意二個候選子圖形組合成為一個新的候選子圖形。其有效字元大小達到 930 個(原 30 個加上由二候選子圖形組合成的新候選子圖形)，較傳統文字通行碼的 96 個字元大小為高；而其挑選四張子圖形所提供的安全強度，約為六個字元長度的傳統通行碼強度。

Sobrado 等人於 2005 年提出 Convex Hull Click Scheme[7] 。所發展的架構能夠有效抵擋肩窺攻擊(Shoulder Surfing Attack)，登入時畫面上顯示出許多不同的小圖案，其中包含了使用者登入所需的圖形化通行碼圖案，登入時需點選由這些圖形化通行碼圖案所圍成的 Convex Hull。所提供的安全強度與其圖案的總數量相關，但是過多的圖案可能會使得尋找圖形化通行碼圖案時，造成使用者的眼花撩亂。

Wiedenbeck 等人於 2005 提出了 PassPoints[6] [16] [17] [18] ，目的在於改進由 Blonder 所提出的 Graphical Passwords[2] ，能夠讓使用者點選圖片上任意的一個點，使用者也能夠提供自己所喜好的圖片來做點選。認證方式係依據使用者點選的特徵點順序，通行碼強度在圖片大小為 1024x768，網格切割大小為 14 x 14 時可以提供相當於八個字元長度的通行碼安全強度。

T. Takada 於 2008 年提出了 FakePointer[19] ，設計目的在於改進目前實行的 ATM 架構，提供更安全的登入方式。利用答案指標來做間接的選取 PIN number，登入時需利用能夠上網的工具如 PDA 等來取得答案指標並記下。

除此之外，和傳統式通行碼相比，圖形化通行碼能提供對字典攻擊更好的防禦力。若圖形化通行碼能夠被當作強通行碼來使用，則用圖形化通行碼產生的強通行碼來做使用者認證將更具有實用性。

3.1 將針對能抵擋肩窺攻擊的 Convex Hull Click Scheme 做介紹。

3.1. Convex Hull Click Scheme

Sobrado, Birget 於 2005 年所提出的 Convex Hull Click Scheme（CHC）[7] ，是一個能夠抵擋肩窺、側錄攻擊(Shoulder Surfing Attack)的設計。和 PassFace[13] 相同，CHC 需要經過數個回合 (Round) 的問題 - 回答 (Challenge-Response)，並完全回答正確。在登入過程中，使用者不需要直接點選出圖形化通行碼圖案，而是利用圖形化通行碼圖案所圍成的 Convex Hull 區域做間接的選擇。

(一) Convex Hull Click Scheme 的架構與登入方式

1. 建立通行碼：

使用者必須從一群圖案中選出數個圖案(可由使用者自己提供)，這些由使用者選出的圖案為使用者的圖形化通行碼圖案如(圖 3.1)。

圖 3.1 通行碼圖案選取範例

2. 登入：

在登入時必需經過數個 Challenge 如（圖 3.2），在每一個 Challenge 中必須找出畫面中圖形化通行碼圖案所圍成的 Convex Hull 如（圖 3.3）（圖 3.4），並 且正確的在其圍成的 Convex Hull 中做選取，便為一成功的 Round，當通過系統所設置的數個 Rounds，並全部成功的點選，便為成功的認證。

圖 3.2 CHC 認證 Challenge

圖 3.3 CHC 中 Pass-Icons 圍成的 Convex Hull

圖 3.4 CHC 中 Pass-Icons 圍成的 Convex Hull

(二)弱點分析

(1) 邊角、中間效應(Corner, Center Effect)

當使用者點選的位置接近邊角時(如圖 3.5)，即會發生邊角效應(Center Effect)，也就是說 Convex Hull 圍成的面積靠近邊角時，邊角的圖案必有一個為圖形化通行碼圖案；當這種情況發生時，便縮小了需猜測的圖案，對安全性有一定的危害。

由於圖案是隨機分佈在畫面當中，四處分散的圖形化通行碼圖案圍成的 Convex Hull 有很大的機率包含正中央(Center Effect)，也就是說攻擊者於登入時皆點選正中央，意外登入的機率便會升高。作者提出了演算法來儘量避免圖形化通行碼圖案出現在畫面的兩端和控制 Convex Hull 面積來避免中間效應(Center Effect)，也降低圖形化通行碼圖案出現在畫面的邊角來避免邊角效應(Corner Effect)，但因為如此也使得邊角的圖片和中央的圖片不會是圖形化通行碼圖片的機率增加。

圖 3.5 Convex Hull Click Scheme 邊角效應

(2) 意外登入(Accidental Login)

攻擊者不考慮使用者的圖形化通行碼圖案為何，只知道一次選取(Round)中至少會有 3 個以上的圖形化通行碼圖案，根據 Convex Hull Click Scheme[7] ，將圖形化通行碼所圍成的面積控制在約為畫面的 1/10，意外登入的機率和

選取次數成次方關係，在面積為 1/10，選取次數數為 5 的情形下，意外登入的機率約為 $1/10^5$（在排除 Center Effect 的情況下）。

4. 畫面拖曳式認證

為了能夠更間接的選取，避免使用鍵盤輸入或滑鼠直接點選遭受側錄或木馬程式錄製下來而危害到安全性，本論文提出一個更能夠抵擋肩窺攻擊的圖形化通行碼認證設計：畫面拖曳式認證。

4.1. 設計概念

若用一個面積範圍取代直接性的點選取通行碼，便能抵擋肩窺、側錄攻擊。本論文提出的拖曳式設計利用三角形區域和拖曳整個畫面來做選取。

4.1.1. 三角形

使用三角形來做間接的選取通行碼，能夠提供以下特性：

(1) 簡單

三角形是圍成一個面積最簡單的組合。

(2) 面積絕不大於畫面 1/2

三個點能夠圍成的三角形區域的面積，大至畫面二分之一，小至三點成一直線。

(3) 降低中間效應(Center Effect)

四個以上的點圍成的多邊形面積，會出現大於畫面二分之一的情形(中間效應)，也就是在選取面積大於畫面的二分之一的情況下，使用滑鼠點選畫面正中央會發生成功選取的情形(一定包含中間點)；而三個點所圍成的面積最大為畫面的二分之一，能夠有效的降低中間效應(仍會發生)。

4.1.2. 畫面拖曳

在點選的目標沒有不確定因素下，使用滑鼠或鍵盤直接做點選無法抵擋肩窺攻擊。然而在有不確定因素下(如 Convex Hull 的範圍)使用滑鼠或鍵盤做直接點選，依然會洩露出些許資訊。例如如果在 Convex Hull Click Scheme[7] 下被滑鼠點選到的圖案不為圖形化通行碼圖案(見 3.1 節)，在點選邊角的情形下，邊角的圖案必有一為通行碼圖案(邊角效應)。在此提出一個能夠消除使用滑鼠或鍵盤直接點選會洩露出資訊的方法，即是使用拖曳(Drag and Drop)畫面，拖曳畫面能提供的優點如下。

(1) 拖曳畫面

當使用者移動單一圖案，或者輸入單一文字，使用者和攻擊者的注意力便會集中在這一個圖案或文字上，此圖案或文字可能為圖形化通行碼圖案或文字。換句話說，此圖案或文字和圖形化通行碼圖案兩者必定有著某種關聯。反之當使用者拖曳的是整個畫面，攻擊者所見到的是所有的圖案同時移動，無法得知使用者專注的圖案為何。

(2) 更間接的點選：

在這裡利用二個畫面的重疊，來達到選取圖形化通行碼圖案的目的。兩層畫面各含有圖形化通行碼圖案或文字，藉由一個畫面中的圖形案通行碼圖案或文字所圍成的三角形區域，和另一個畫面中的圖形案通行碼圖案或文字，經過拖曳後圖案和三角形重疊達到選取的目的。

藉由三角形的間接性區域選取，加上拖曳畫面的間接性重疊選取，兩者同時配合，使得肩窺、側錄攻擊很難取得有用資訊。

4.1.3. 登入規則

登入時藉由兩個獨立的層來做重疊選取，一層為三角形層(Triangle Layer)，一層為通行碼圖案層。

(1) 三角形層可重新產生

由於三角形層中的圖案為隨機放置(這裡使用數字圖案)，會發生圖案所圍成的三角形面積過小或是成一直線的情況如(表 4-1)，使用者可以依情況重新產生三角形層；也就是說重新產生的情形有可能是三角形面積過小或是三點成一直線，攻擊者無法得知為何種情形。

表 4-1 不同圖案數平均面積和組合數

總圖案數	三角形平均面積	總組合數	一直線組合數	小於畫面 0.1 組合數（不含共線)	介於畫面 0.1~0.2 間組合數(不含共線)
3 x 3	0.2083	84	8	0	32
4 x 4	0.1515	560	44	124	236
5 x 5	0.1282	2300	152	1052	664
6 x 6	0.1157	7140	372	3744	1644
7 x 7	0.1079	18424	824	9888	4848
8 x 8	0.1027	41664	1544	22624	11476
9 x 9	0.0989	85320	2712	49344	22460
10x10	0.0961	161700	4448	98200	40056

(2) 通行碼圖案有順序關係

通行碼圖案層中的通行碼圖案選取必須有順序關係，假使沒有順序會發生設置的圖案越多，而意外登入的機率卻越大，因為三角形面積在沒有順序的情況下包含一個以上的點的機率隨圖案數越多而增高如(表 4-2)。

表 4-2 成功選取機率表

總圖案數	通行碼圖案數	三角形平均面積	平均三角形內 Icon 數	包含 1 個通行碼圖案機率	包含 2 個以上通行碼圖案機率	成功選取機率
5 x 5	4	0.12820	3	0.3652	0.0565	0.4217
5 x 5	5	0.12820	3	0.4130	0.0814	0.4944
5 x 5	6	0.12820	3	0.4460	0.1326	0.5786
10 x 10	4	0.09612	9	0.2788	0.0395	0.3184
10 x 10	5	0.09612	9	0.3195	0.0628	0.3823
10 x 10	6	0.09612	9	0.3511	0.0897	0.4408

將圖形化通行碼圖案設置順序的主因，是為了降低意外登入的成功率，舉例如下：

在 5 x 5 個數字下，圍成三角形平均面積約 0.128，在圖形化通行碼圖案數為 4 的情況下，無順序成功選取的機率為 0.421(1 Round)，有順序成功選取機率則為 0.128 如(表 4-2)。

在 10 x 10 個數字下，圍成三角形平均面積約 0.096，在圖形化通行碼圖案數為 4 的情況下，無順序成功選取的機率為 0.318(1 Round)，有順序成功選取機率則為 0.096 如(表 4-2)。

相對的，有順序增加使用者不少記憶上的負擔，但在安全性和實用性上的衡量下，加入圖案的順序才能確保此設計的安全性。

4.2. 設計實作

設計中登入畫面分為二層，一層為三角形層，另外一層為通行碼圖案層，藉由三角形的範圍來做選取通行碼圖案

(1) 三角形層：

此層使用數字的圖案，使用者須從數字圖案中選擇 3 個來作為三角形層的通行碼圖案。

(2) 通行碼圖案層：

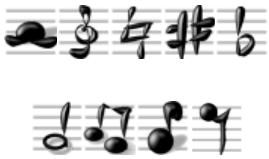
此層圖案供使用者認證時選取，圖案的選擇和整個設計的安全度相關；這裡藉由日常生活中常看到的事物做為圖形化通行碼圖案，增加使用者熟悉度，減少記憶上的負擔。

以下為適合做為圖形化通行碼圖案的類別：

交通號誌

水果

音符



花卉

等

4.2.1. 登入架構

1. 註冊階段：

(1)使用者選出三個數字為其通行碼數字如(圖 4.1)。

(2)使用者選出數個圖案為其通行碼圖案如(圖 4.2)，並決定圖形化通行碼圖案選取順序。

圖 4.1 選取通行碼數字階段

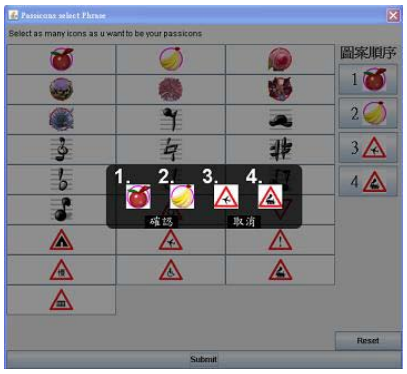


圖 4.2 選取通行碼圖案階段

2. 登入階段：

根據註冊階段所設置的通行碼數字和通行碼圖案，在登入時可以分為以下的三個步驟。

(1)找出通行碼數字圍成的三角形選取區域

(2)找出通行碼圖案

(3)將三角形選取區域和通行碼圖案重疊做選取

3. 練習模式：

假設使用者對於本認證設計並不熟悉，這裡提出了練習模式，讓使用者熟悉此設計，並藉由通行碼數字和通行碼圖案的位置提示，來讓不熟悉的使用者了解如何選取，進而成功登入。

(1) 找出三角形選取區域

從三角形層中找出通行碼數字所圍成的三角形，練習模式中，三角形層會自動繪出三角形選取區域，讓使用者熟悉如(圖 4.3)。

(2) 找出通行碼圖案

於圖形化通行碼圖案層依順序找出圖形化通行碼圖案，並記住此圖形化通行碼圖案位置如(圖 4.4)。

(3) 選取通行碼圖案

將通行碼數字圍成的三角形選取區域和通行碼圖案重疊做選取如(圖 4.5、圖 4.6、圖 4.7、圖 4.8)所示。

(4) 選取完成

依順序重覆選取圖形化通行碼圖案完成後按“ENTER”登入。

圖 4.3 圖形化通行碼數字提示(6,13,15)

圖 4.4 圖形化通行碼圖案位置(蘋果、香蕉、飛機、火車)

圖 4.5 三角形重疊選取蘋果

圖 4.6 三角形重疊選取香蕉

圖 4.7 三角形重疊選取飛機

圖 4.8 三角形重疊選取火車安全分析

(1) 暴力攻擊(Brute-force attack)

暴力攻擊為攻擊者根據所有的可能性去做猜測，不考慮三角形過小或三點成一直線的機率，攻擊的 成功率和通行碼強度(password space)

有關，此設計的通行碼強度和三角形層、通行碼圖案層的圖案成正比；通行碼數字沒有順序，圖形化通行碼圖案有順序關係，故通行碼強度為 $C(n \times n, 3) \times (n \times n)^m$ 。(n 為每邊的圖案數，m 為通行碼圖案數)(表 4-3、表 4-4)

表 4-3 畫面拖曳提供的通行碼強度(10 x 10)

文字總數	通行碼文字數	圖案總數	通行碼圖案數	通行碼強度
10 x 10	3	10 x 10	3	1.61×10^{11}
10 x 10	3	10 x 10	4	1.61×10^{13}
10 x 10	3	10 x 10	5	1.61×10^{15}
10 x 10	3	10 x 10	6	1.61×10^{17}
10 x 10	3	10 x 10	7	1.61×10^{19}
10 x 10	3	10 x 10	8	1.61×10^{21}

表 4-4 畫面拖曳提供的通行碼強度(5 x 5)

文字總數	通行碼文字數	圖案總數	通行碼圖案數	通行碼強度
5 x 5 (25)	3	25	3	3.59×10^{7}
5 x 5 (25)	3	25	4	8.98×10^{8}
5 x 5 (25)	3	25	5	2.24×10^{10}
5 x 5 (25)	3	25	6	5.61×10^{11}
5 x 5 (25)	3	25	7	1.40×10^{13}

表 4-5 Convex Hull Click Scheme 通行碼強度

圖案總數	通行碼圖案數	通行碼強度，
100	5	7.5×10^{7}
100	6	1.1×10^{9}
100	7	1.6×10^{10}
200	5	7.5×10^{9}
200	6	8.2×10^{10}
200	7	2.2×10^{12}

本設計在圖案總數（文字總數+圖案總數）、通行碼圖案數(通行碼文字數+通行碼圖案數)和 Convex Hull Click Scheme 同樣的情況下，能夠提供更強的通行碼強度，如在本設計中文字總數和圖案總數加起來為 200，通行碼文字數和通行碼圖案數加起來為 7 時，能提供的通行碼強度為 1.61×10^{13}，較 Convex Hull Click Scheme 中，圖案總數為 200，通行碼圖案數為 7 時，提供的通行碼強度 2.2×10^{12} 來得高，且圖形化通行碼認證乃為互動式認證：一個請求(Request)，一個回應(Response)，使得暴力攻擊在此認證設計下所需時間大幅增加。

(2) 邊角、中間效應(Corner, Center Effect)

本設計的登入方式為利用通行碼數字圍成的三角形區域來選取通行碼圖案，而選取的方式為拖曳整個通行碼圖案層，所以攻擊者並不會知道使用者是否利用邊角圖形化通行碼數字做選取，所以能夠有效的抵擋邊角效應。

同理此設計是利用拖曳通行碼圖案層來做選取，攻擊者在不知通行碼圖案的情形下，無法將其拖曳至畫面中間做登入，也無法得知使用者是否選取中間的圖案做登入，且使用三角形的選取面積不會大於畫面二分之一，所以此設計能夠有效抵擋邊角和降低中間效應產生的弱點。

(3) 意外登入(Accidental Login)

意外成功登入的機率和三角形的面積和通行碼圖案相關，當通行碼圖案個數為 n，便需經過 n 次的選取，也就是登入機率平均為三角形平均面積的 n 次方(表 4-9)，對使用者來說三角形面積越高越好，而就安全性來說越小越好，Convex Hull Click Scheme 中將面積控制在約為畫面的 0.1，而本設計中面積自然的落於 0.1~0.2 左右(隨著圖案數增多，平均面積越小)。

計算三角形平均面積方式(表 4-6，表 4-7，表 4-8)：

表 4-6 面積演算法使用參數

參數	定義	參數	定義
n	邊長能夠放置的點個數	ab, ac, bc	三角形圍成之三邊
a ,b ,c	三角形圍成之三座標	total	所有面積總合
ratio	三角形和畫面面積比	m	n x n,畫面中點的個數
avarea	三角形平均面積		

表 4-7 面積演算法使用方法

參數	定義
Distance()	算出兩點之間距離
Triangle()	用海龍公式算出三角形面積

表 4-8 面積演算法

```
for (int i=0; i<m-2;i++){                    //
    for (int j=j+1;j<m-1;j++){          //將 n x n 中三個點可能性都排出來
        for (int k=j+1;k<m:k++){        //
            a.x = i % n;                              //計算點 a 的 x 座標
a.y = i / n;                                  //計算點 a 的 y 座標
b.x = j % n;                                  //計算點 b 的 x 座標
b.y = j / n;                                  //計算點 b 的 y 座標
c.x = k % n;                                  //計算點 c 的 x 座標
c.y = k / n;                                  //計算點 c 的 y 座標
```

```
ab = distance(a,b);                    //計算 a 點到 b 點長度
ac = distance(a,c);                    //計算 a 點到 b 點長度
bc = distance(b,c);                    //計算 a 點到 b 點長度
//三角形面積比：三角形面積/畫面面積
ratio = Triangle(aa, bb, cc)/((n-1) x (n-1));
total += ratio;                        //累加三角形面積
count++;                               //累加三角形面積次數
        }
    }
}
avarea = total / count;      //平均面積：總面積除以面積數
```

表 4-9 畫面拖曳認證意外登入機率

圖案數	三角形平均面積	通行碼圖案數	意外成功選取機率
3 x 3	0.2083	n	$(0.2083)^n$
4 x 4	0.1515	n	$(0.1515)^n$
5 x 5	0.1282	n	$(0.1282)^n$
6 x 6	0.1157	n	$(0.1157)^n$
7 x 7	0.1079	n	$(0.1079)^n$
8 x 8	0.1027	n	$(0.1027)^n$
9 x 9	0.0989	n	$(0.0989)^n$
10x10	0.0961	n	$(0.0961)^n$

5. 結論與未來工作

5.1. 結論

生活各種事物慢慢趨向網路化，舉凡水費、電費、繳稅，至網路商店，銀行轉帳等皆和金錢相關，更顯得登入安全的重要性。若攻擊者仿冒成功登入，輕者造成個資的洩露，重則造成金錢上的損失。隨著科技越來越進步，木馬在使用者無意間被植入，還有與真實網站看似無異的釣魚攻擊，小到使用者無法察覺的偷窺側錄，使得任何的情況下皆有曝露通行碼(Password)的危險性。

因此更增加了登入安全的重要性，必須假設在曝露的空間下登入也能夠安全的進行，在最壞的情況下洩露最少的機密資訊，本文所提出的畫面拖曳認證設計，確實能更有效的抵擋肩窺、側錄攻擊。

5.2. 未來工作

希望能夠針對此設計的實用性和未來性做改進，以下提出增強實用性和記憶性的未來方向：

(1) 實用性：

在 5 x 5 的設計下，使用者能夠迅速的搜尋出數字和圖案；在 10 x 10 的設計下，使用者要在 100 個數字中找出三個，並不容易，在一群數字中，數字和數字間很相似，使用者看來很模糊，可以改為使用不同類型文字：如英文，日文，文字符號或是抽象圖片等來分類增加可辨識度。

(2) 記憶性：

圖案可記憶性和種類相關，圖案間要能夠明辨分明，並且為了增加可記憶性，這些圖案要是使用者所熟悉的生活周遭事物，但哪些事物做為圖案能夠提供較好的可記憶性，仍需要經過使用者的測試使用後才知道。

6. 參考文獻

[1] D. Davis, F. Monrose, and M. K. Reiter, “On user choice in graphical password schemes,” in *Proceedings of the 13th USENIX Security Symposium.* San Diego, CA, 2004.

[2] G. E. Blonder, “Graphical passwords,” in *Lucent Technologies, Inc., Murray Hill, NJ*, U. S. Patent, Ed. United States, 1996.

[3] J. Goldberg, J. Hagman, and V. Sazawal, “Doodling Our Way to Better Authentication,” presented at Proceedings of Human Factors in Computing Systems (CHI), Minneapolis, Minnesota, USA., 2002.

[4] J. Thorpe and P. C. v. Oorschot, “Towards Secure Design Choices for Implementing Graphical Passwords,” in *Proceedings of the 20th Annual Computer Security Applications Conference.* Tucson, Arizona, 2004.

[5] J. Thorpe and P. C. v. Oorschot, “Graphical

Dictionaries and the Memorable Space of Graphical Passwords," in *Proceedings of the 13th USENIX Security Symposium*. San Deigo, USA: USENIX, 2004.

[6] J.-C. Birget, D. Hong, and N. Memon, "Robust discretization with an application to graphical passwords," Cryptology ePrint archive 2003.

[7] Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The Design and Analysis of Graphical Passwords." In *Proceedings of the 8th USENIX Security Symposium*, 1999.

[8] L. Sobrado and J.-C.Birget, "Graphical passwords," *The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research*, vol. 4, 2002..

[9] Perrig and D. Song, "Hash Visualization: A New Technique to Improve Real-World Security," in *Proceedings of the 1999 International Workshop on Cryptographic Techniques and E-Commerce*, 1999.

[10] Pointsec for Pocket PC, Pointsec Mobile Technologies, Nov. 2002, (http://www.pointsec.com//news/download/Pointsec_PPC_POP_Nov_02.pdf).

[11] R. Dhamija and A. Perrig, "Déjà Vu: A User Study Using Images for Authentication," in *Proceedings of 9th USENIX Security Symposium*, 2000.

[12] R. N. Shepard, "Recognition memory for words, sentences, and pictures," *Journal of Verbal Learning and Verbal Behavior*, vol. 6, pp. 156-163, 1967.

[13] RealUser, "www.realuser.com".

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

[15] Sfr, "www.viskey.com/tech.html.".

[16] S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: Basic results," in *Human-Computer Interaction International (HCII 2005)*. Las Vegas, NV, 2005.

[17] S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: Effects of tolerance and image choice," in *Symposium on Usable Privacy and Security (SOUPS)*. Carnegie-Mellon University, Pittsburgh, 2005.

[18] S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system," *International Journal of Human Computer Studies*, to appear.

[19] T. Takada, "FakePointer: An Authentication Scheme for Improving Security against Peeping Attacks Using Video Cameras," in *Mobile Ubiquitous Computing. Systems. Services and Technologies (UBICOMM)*. Sep, 2008.

[20] T. Y. Suo, Y. Zhu, Owen, "Graphical passwords: a survey," in *Computer Security Applications Conference, 21st Annual*. Dec, 2005.

[21] T. Valentine, "An evaluation of the Passfaces personal authentication system," Technical Report, Goldsmiths College, University of London 1998.

[22] T. Valentine, “Memory for Passfaces after a Long Delay,” Technical Report, Goldsmiths College, University of London 1999.

[23] W. Jansen, “Authenticating Mobile Device Users Through Image Selection,” in *Data Security,* 2004.

[24] W. Jansen, S. Gavrila, V. Korolev, R. Ayers, and R. Swanstrom, “Picture Password: A Visual Login Technique for Mobile Devices,” National Institute of Standards and Technology Interagency Report NISTIR 7030, 2003.

[25] W. A. Jansen, “Authenticating Users on Handheld Devices,” in *Proceedings of Canadian Information Technology Security Symposium,* 2003.