手機 APP 螢幕開機鎖

The Enhanced Graphic Pattern Authentication Scheme

[1] 沈誦修　　[2] 林昇和

[1]Sung-Shiou Shen　　[2]Shen-Ho Lin

[3] 錢威　　[4] 鄭禮文

[3] Wei Chien　　[4] Zheng-Li Wen

[1] 德霖技術學院電子工程系
[1]Department of Electronic Engineering De Lin Institute of Technology,
3shubert@googlemail.com

[2] 德霖技術學院電子工程系
[2] Department of Electronic Engineering De Lin Institute of Technology,
marcular@gmail.com

[3] 寧德師範學院計算機科學系
[3] Ningde Normal University, Department of Computer Science,
air180@seed.net.tw

[4] 德霖技術學院電子工程系
[4]Department of Electronic Engineering De Lin Institute of Technology,
qwent19735@gmail.com

摘要

在現今的生活中，手機對現代人而言已經是一種必備的行動裝置[1]。智慧型手機要求使用者在開機時輸入相關密碼解開手機，方可使用手機，在使用者解鎖的時候，往往可能會被有心人士記住自己手機的密碼數字或圖形密碼，而導致被盜取個資或佔用風險增高[2]。舉例而言，螢幕圖形解鎖這項介面軟體大家並不陌生，只是簡單往上滑或是簡單執行九宮格圖形解鎖的動作而已，因此，當遭受別人記住螢幕密碼鎖圖形時，攻擊者便可自行解鎖，而導致使用者手機內的個人資訊被竊取，更進一步想，以數字、圖形密碼作為手機螢幕解鎖時，不一定能做到完善使用者身分鑑別功能，而失去儲存在手機內重要的隱私[3][4]。

本研究將開發、測試一種新的資訊保護程式，其目的在精進圖形解鎖這項 APP 程式， 透過 APP 程式修正及搭配亂碼產生以精進程式功能，目的在重新定位使用者圖控數字或圖控按鈕位置的特性，表現出圖形解鎖機制每次圖控數字或按鈕位置都會變動，促使畫出圖形或鍵入數字時每次都不同，增加竊取者不易紀錄的阻礙，間接可以達成使用者身分識別需求，提供更完善且多元的隱私權保護，藉此增加使用者安全的保障[3][5-10]。

Abstract

Smart mobile terminal are an essential device in our life today. The user usually enters in the related words or draws a simple graphic on the touch screen as passwords for unlocking the screensaver. Although this way can provide users with simple and convenient security mechanism, the process would increase the risk of words or graphic information leakage under the strict security consideration. Usually for this type of keypad lock screen app you can only customize the simple pattern or swipe-to-unlock screen with a static image on a background image that you select to unlock your phone. Therefore, the interested parties could have a chance to eavesdrop the simple graphic pattern information in order to hacking the smart device for stealing the personal information.

Due to lack of the proper identity authentication mechanism in the usually keypad lock screen app, this paper proposes a new graphic pattern protection mechanism for enhance authentication level in the keypad lock screen app field. By randomly changing the fixed position of the digital graphics that shows on the touch screen, the user can draw different graphic pattern every time based on the unique or backup PIN password to unlock the screen. Not only added the random graphic pattern authentication method indeed increase the personal secret information being stolen difficulty and complexity, it provides more security level than the traditional graphic pattern authentication in keypad lock screen as well.

Keywords: Authentication, Password, Security, Smart Phone.

1. 研究動機與目的

現今，智慧型手機解鎖常以輸入數字密碼或是繪出圖形密碼進行開鎖，此類使用者身分識別技術容易遭受盜錄，而導致使用者個人資訊外流，常見的防犯方式，大多都是增加數字密碼的長度、複雜性，或者是定期更換密碼或密碼圖形來加以防犯，但是在本質上仍未完全有效的解決問題。

由於智慧型手機的流行，美觀要求，以將傳統手機按鍵由觸控螢幕取代，導致其他人機介面功能推陳被新，以目前的智慧型手機來說雖然提供許多功能廣為大眾喜愛，不過還是存在些個人隱私保護的問題，例如 Line 或一些聊天程式可直接透過解開手機螢幕鎖直接聊天，一般使用者解鎖時，將滑動螢幕、輸入數字密碼或是在九宮格上滑入圖形密碼進行解鎖動作。一般使用者在進行開鎖時較不會注意身旁是否有他人偷看，而導致密碼遭人盜取，諸如此類情境導致密碼可能被盜取或是被記取下來，而威脅自己的隱私權。為增加安全性，手機上已有指紋或是臉型當作身分鑑別輸入資料，相對於通行密碼輸入方式安全的多，但是，這些機制的輸入資料並非無法複製，因此這類以指紋或是臉型當作輸入密碼的機制其安全性依然存在挑戰，若能搭配其他安全機制做配合，將可提升使用者個人隱私的保護[1]-[5]。

在生活實例，使用者常以生日等一些個人相關資訊作為手機防盜之密碼，這些密碼極容易被猜測，當此密碼被他人知道時，一樣可以侵入並竊取手機內的一切資訊，更何況手機上的身分辨識條件通常只以單一條件作為身分辨識的依據，反觀將此單一條件加入一些參數，使辨識條件更嚴謹，即使個人密碼被測錄、盜取時，會因為輸入密碼的參數不同而無法開啟，可以有效防犯個人隱私被盜取[5][6]。

本專題研究 APP 手機螢幕鎖主要操作如下，在開啟螢幕時會將數字、圖形鎖的位置隨機更換，每次的位置會依亂碼演算法去設定數字或圖形符號的位置，使每一次數字或圖形符號的位置不同，在隨機更換的同時也決定數字或圖形符號彼此之間的相對位置，並計算出最佳路徑對應輸入數字或圖形符號列，在輸入數字密碼或圖形符號時，也記錄輸入數字之間的時間間隔作為輸入密碼參考依據[6]-[9]。當使用者密碼輸入時，錯誤的密碼、順序及時間差，此安全系統將會自動重新定義數字密碼或圖形符號的位置，直到使用者輸入正確密碼或超過預定重複次數，就鎖住手機系統，必須特殊開啟程序才可重啟手機功能[10]。而透過本專題研究所提新機制，呈現使用者手機的螢幕鎖圖形排列為亂碼的方式顯示，藉此，增加數字密碼或圖形符號輸入的隨機變動特性，提升防犯密碼被測錄的效能，來保障使用者的權益。

2. 軟硬體架構與設計流程

軟體設計流程

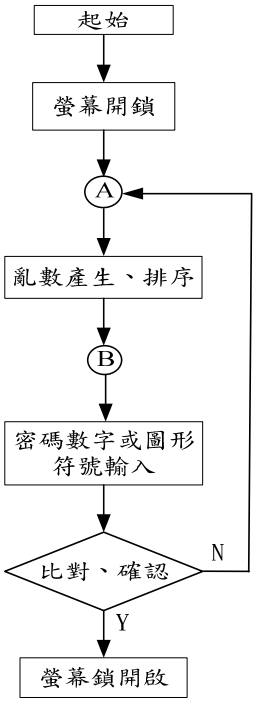

圖2-1系統軟體流程圖

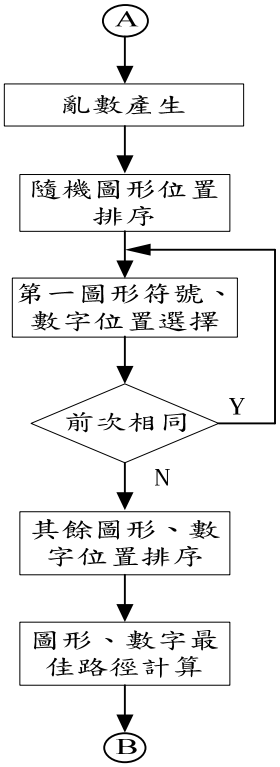

圖2-2 亂數產生位置排序流程圖

2.1. 軟體設計流程

圖 2-1 是整個系統軟體設計流程，基本軟體程式碼部分可參考或搜尋網路上開放程式碼取得可用資源加以修改以節省設計開發時間，配合圖 2-1 系統軟體流程，程式執行程序如下：

(1) 使用者碰觸使用手機螢幕時，螢幕圖形鎖開啟

(2) 配合亂數產生演算法將數字或圖形符號的位置打亂重新排序並顯示在螢幕上，詳細程序圖 2-2 所示。

(3) 使用者輸入密碼數字或圖形連線。

(4) 依最佳路徑判斷使用者輸入之密碼數字或圖形列，假如使用者密碼輸入錯誤手機將會自動重新進入步驟(2)產生一個新的數字或圖行排列，讓使用者重新輸入密碼。若使用者密碼輸入正確既開啟解鎖。

(5) 當使用者解鎖密碼後並可以正常運用手機，使用者使用完手機，都將會再次鎖螢幕，基於程式設計，將先黑屏在重新開起螢幕鎖，每次的數字或圖形排序確定不會跟上次一樣，依個人的密碼設計不同，可以確保手機的資訊安全與隱私。

2.2. 亂數產生位置排序流程

圖 2-2 是針對圖 2-1 流程圖裡的亂數產生與圖形排列的步驟進階分析及說明。

(1) 如圖 2-1 的設計流程第一項所表示螢幕觸控開啟時將致能亂數產生演算法。
(2) 由亂數產生演算法搭配位置定位以決定密碼數字與圖形符號位置。
(3) 確定第一個密碼數字或圖形符號位置。
(4) 比對第一個密碼數字或圖形符號位置與前一次位置是否相同，若相同必須重新定位數字或圖形位置排列。
(5) 確定第一個密碼數字或圖形符號位置後在進行其他密碼數字或圖形符號位置確定。
(6) 將依密碼數字或圖形符號位置決定最佳路徑的數字密碼或圖形輸入列。

根據圖 2-1 與圖 2-2 說明，將造成使用者在輸入密碼數字或圖形符號列時每次長度與內容都不同，增加竊取密碼困難度。

3. 軟體研究步驟

因手機 APP 的開發系統 Android 是以開放式的型式做為應用化

(1) 在網路上搜索相關 Android 的相關程式及應用方面資訊，參考相關書籍。
(2) 搜尋相關亂數產生、涵數與相關排序的方法、演算法，圖形或數字的順序演算。
(3) 搜尋相關比對演算法的資料以演算法的排序，測是亂數產生的圖形、數字是否會自動產生亂數，並不重複　執行同樣的亂數產生。
(4) 已將亂數產生的圖形及數字在經程式設計、排序密碼的比對，來加以控制圖形及數字的隨機亂數排序位置。
(5) 將確定第一個密碼數字或圖形符號位置，隨機固定排序，比對第一個密碼數字或圖形符號位置與前一次位置是否相同，若相同必須重新位置排序。當使用者解碼時系統必須比對圖形、數字密碼是否為最佳路徑位置。
(6) 由程式判斷是否為最佳路徑位置，當判斷為正確　時，使用者將能操作手機，當判斷錯誤時，系統自動重新產生一個新的數字、圖行排序，讓使用者重新輸入密碼。

4. 測試結果

如圖 4-1 為螢幕開鎖圖，密碼設定為 168，每當螢幕開啟時，首先執行亂數產生演算法產生亂數用以決定螢幕上每一個數字按鈕位置的排列，如圖 4-1 顯示出來的畫面，將會使數字按鈕位置排列不同於一般數字按鈕位置排列形式。

圖 4-1 螢幕開鎖圖

由於數字按鈕位置排列關係，使用者在輸入密碼時必須加入冗餘數字，才可以將密碼數字的順序呈現，在經過最佳路徑演算判別輸入數字按鈕序列決定輸入序列合法性，由圖 4-1，使用者要輸入密碼 168 必須加入冗餘數字“9”得到密碼數字的順序呈現，如圖 4-1 紅線所示。隨著螢幕鎖數字排列隨機改變，既使在密碼不變條件下，每次輸入密碼數字總數與軌跡都不相同，已達成改變一般圖形輸入數字排列順序與軌跡不變容易被破解問題。也因為每次輸入密碼數字總數與軌跡都不相同，因此必須有一最短路徑判決演算法決定輸入密碼合法性。圖 4-2 說明最佳路徑計算方法，圖示中，方框內數字以列、行直接代表數字按鈕所在位置所屬的權重，紅線上所註示與數字按鈕位置框外小數字為每個數字按鈕位置框與鄰近數字按鈕位置框權重差異與斜邊不須經過其他數字按鈕位置框之權重差異將之稱為差異權重，最佳路徑決定將所輸入數字按鈕對應權重與路徑所經過的差異權重一並輸入，經比對路徑與差異權重決定最短路徑判斷密碼合法性。

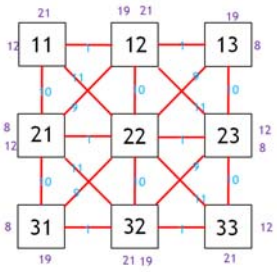

圖 4-2 差異權重：數字按鈕位置框與其他數字按鈕位置框權重差異

圖 4-3 最短路徑輸入5位數圖

依前文所述，圖 4-3 最短路徑密碼 5 位數圖,此圖密碼為“14698”但實際密碼依然是 168。為避免習慣上輸入時的第一數字與最後數字為密碼所屬數字，演算法允許第一數字與最後數字為冗餘數字，不會影響最短路徑判別。圖 4-4 所示以最短路徑為 6 個字數的序列，目的在於不被讓人看到密碼的第一個密碼與最後一個密碼，故以設計前後面可以增加數個冗餘的數字並去錯亂旁人偷偷側錄密碼，所以可增加多數個冗餘的密碼來增加密碼的長度，並且不管長度多少一樣都可以解碼。

圖 4-4最短路徑輸入6位數圖

5. 參考文獻

[1] Andrew Nusca, “Smartphone vs. feature phone arms race heats up; which did you buy?,” ZDNet. Retrieved December 15, 2011.

[2] McAfee, “Mobility and Security: Dazzling Opportunities, Profound Challenges,” Technical report, May 2011.

[3] W. Jeon et al., “A Practical Analysis of Smartphone Security,” Proc. Int'l Conf. Human Interface and the Management of Information—Part I, Springer-Verlag, pp. 311-320, 2011.

[4] N. Husted, H. Saïdi, and A. Gehani, “Smartphone Security Limitations: Conflicting Traditions,” Proc. 2011 Workshop on Governance of Technology, Information, and Policies, ACM, pp. 5-12, 2011.

[5] P. Andriotis, T. Tryfonas, G. Oikonomou, “A Pilot Study on the Security of Pattern Screen-Lock Methods and Soft Side Channel Attacks,” Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks, WiSec’13, Pages 1-6, April 17-19, 2013.

[6] K. I. Shin, J. S. Park, J. Y. Lee, J. H. Park, “Design and Implementation of Improved Authentication System for Android Smartphone Users,” IEEE Computer Society, 2012 26th International Conference on Advanced Information Networking and Applications Workshops, pp 704-707, 2012.

[7] Pierre L'Ecuyer, “Efficient and Portable Combined Random Number Generators, ” Communications of the ACM, Vol. 31, No. 6, pp. 742-774, June, 1988.

[8] Dr. Paul Coddington, “Parallel Random Number Generators in Java,” The University of Adelaide, Australia, November 2, 2003.

[9] Stephen K. Park and Keith W. Miller, “RANDOM NUMBER GEUERATORS: GOOD ONES ARE HARD TO FIN,” Communications of the ACM, Vol. 31, No. 10, pp. 1192-1201, October 1988.

[10] M. R. Henzinger, P. Klein, S. Rao, S. Subramanian, “Faster Shortest-Path Algorithms for Planar Graphs,” Journal of computer and system sciences, 1997.