# 面向移动平台的新型身份认证方案设计

胡 卫[1,2] 张焕国[1] 魏国珩[1,2] 周学广[2]
(武汉大学计算机学院 武汉 430072)[1] (海军工程大学信息安全系 武汉 430033)[2]

**摘 要** 各种类型的移动平台如智能手机、平板电脑、嵌入式系统快速普及,并渗透到生活和工作的方方面面,但是移动平台在带给大家丰富多彩的应用和方便快捷的生活的同时,也带来了许多新的安全问题。身份认证和接入认证是保护移动平台的第一道屏障。结合多点触控技术、重力感应技术和图形密码,设计、开发了适用于移动平台的几种身份认证方案,包括绘制曲线认证方案、图像选择认证方案、多点指划认证方案和重力感应认证方案。所设计的方案较之单纯的口令式密码,设置口令和验证口令直观方便,通过简单的操作即可产生较大的密钥空间。经分析,所提方案操作方便,安全性较高。

**关键词** 移动平台,身份认证,图形密码,多点触控,重力感应
**中图法分类号** TP302 **文献标识码** A

## Design of New Authentication Schemes for Mobile Platform

HU Wei[1,2] ZHANG Huan-guo[1] WEI Guo-heng[1,2] ZHOU Xue-guang[2]
(School of Computer, Wuhan University, Wuhan 430072, China)[1]
(Information Security Department, Navy University of Engineering, Wuhan 430033, China)[2]

**Abstract** Various types of mobile platforms such as smart phones, tablet computer, and embedded system have rapid popularized and penetrated into all aspects of life and work. The mobile platform application brings rich, colorful and convenient life, also brings many new security problems. Identity anthentication and access authentication are the first barrier protecting mobile platform. Combining with the muti-touch technology, gravity sensing technology and graphical password, several authentication schemes were designed and developed for mobile platforms, including drawing curve anthentication scheme, image choose authentication scheme, multiple point authentication scheme and gravity sensing authentication scheme. The setting and verification of password are convinient using the designed schemes, which can produce larger key space through a simple operation and possess higher security than simple password anthentication.

**Keywords** Mobile platform, Identity authentication, Graphical passwords, Multi-touch, Gravity sensing

## 1 引言

当前,随着计算机技术和移动互联网技术的飞速发展,移动平台已经拥有了强大的信息处理能力,各种类型的移动平台,如智能手机、平板电脑、嵌入式系统快速普及,并渗透到生活和工作的方方面面,特别是在新兴的物联网和云计算方面具有广阔的应用前景。但是移动平台在带给大家丰富多彩的应用和方便快捷的生活的同时,也带来了许多新的安全问题。身份认证和接入认证是保护移动平台的第一道屏障,因此有必要设计适用于移动平台且安全方便的身份认证方案。

当前移动平台的身份认证方案主要包括两种。(1)用户口令模式。用户口令认证模式是通过输入用户名和口令来实现身份认证的。这种模式的缺点在于安全强度不够,对于移动平台,信息的输入不是很方便,对于单纯的数字口令,密钥空间仅有 $10^n$,容易受到口令猜测和肩窥等威胁。(2)划动路径方式。用过 Android 手机的用户都知道,可以通过划动路径来进行屏幕的解锁。此种方案路径如果设置太少,则密钥空间不够,路径设置太多,又难于记忆,同时也容易受到口令猜测和肩窥等威胁。

移动平台的快速发展,带来了多点触控技术和重力感应技术。当前 Iphone 和 Android 手机及其平板电脑有着大量丰富的应用和游戏,将触控技术和重力感应技术发挥得淋漓尽致,但是将这两种技术用于身份认证的却不鲜见。为此,我们结合多点触控技术、重力感应技术和图形密码设计了几种适用于移动平台的新型身份认证方案。

## 2 图形密码

图形密码是利用人们对图形记忆要优于对文本记忆的特点设计的一种新型密码。用户不用记忆冗长的字符串,而是通过识别或记住图形来进行身份验证。并且,如果可能的图形数量足够大,图形密码的密钥空间可以远远超过文本密码,这样可以更好地抵抗暴力破解和字典攻击等。图形密码能够

到稿日期:2013-05-08 返修日期:2013-06-25 本文受国家自然科学基金(60970115),国家自然科学基金(61003268)资助。
胡 卫(1979-),男,博士生,讲师,主要研究方向为密码学与信息安全,E-mail:huwei-1212@126.com;张焕国(1945-),男,教授,主要研究方向为信息安全;魏国珩(1977-),男,博士生,副教授,主要研究方向为网络安全;周学广(1964-),男,博士,教授,主要研究方向为内容安全。

提供比文本密码更强的安全性。

鉴于人们对图形记忆要优于对文本记忆的特点，图形密码作为一种新型密码代替文本密码将是未来的一大趋势。图形密码可以分为两类：基于识别型和基于回忆型的图形密码。基于识别型的图形密码身份验证要求用户记忆预先选定的一些特定图片，在验证阶段系统从图案库中随机产生一组图片，让用户从中间选择预先设定的图片，从而实现身份验证的过程。最典型的基于识别型的身份认证方案是 Passfaces 方案（如图 1 所示）和 Pass-Objects 方案（如图 2 所示）。

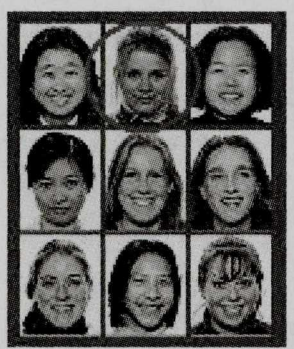

图 1　Passfaces 方案

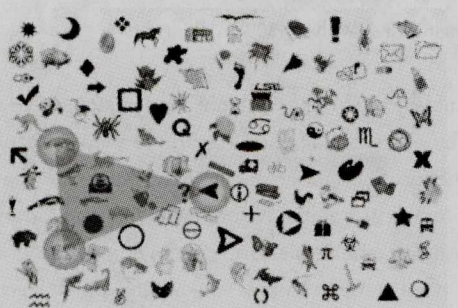

图 2　Pass-Objects 方案

基于回忆型的图形密码身份认证则是要求用户重复以前设定的过程，在设置密码的时候系统要求用户在一定的范围画出密码（图形），认证时只要用户画出设置的密码就可以通过验证。最典型的基于回忆型的图形密码方案是 DAS（Draw A Secret）方案（如图 3 所示）和 PassClicks 方案（如图 4 所示）。

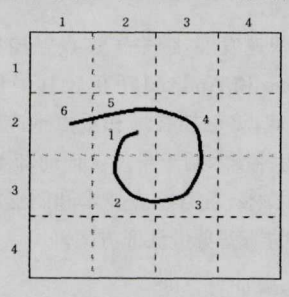


图 3　DAS 方案

图 4　PassClicks 方案

## 3　移动平台新技术

（1）多点触控技术

多点触控技术（Multi-Touch All-Point），即多点触控识别手指位置。Multi-Touch All-Point 物理上是基于互电容的检测方式，互电容是检测行列交叉处的互电容（也就是耦合电容 Cm）的变化，有手指存在时互电容会减小，就可以判断触控存在，并且准确判断每一个触控点位置。逻辑上多点触控识别引入时序来进行判断。

（2）重力感应技术

重力感应技术目前广泛用于手机和平板电脑，其硬件主要由重力感应器、速度传感器、方向感应器、轴陀螺仪组成，可根据晃动设备的动作感应出方向与重力加速度的值。通过测量内部一片重物（重物和压电片做成一体）重力正交两个方向的分力大小，来判定水平方向，内置加速计，一般采用三轴加速计，分为 X 轴、Y 轴和 Z 轴。这 3 个轴所构成的立体空间足以侦测到人在设备上的各种动作。在实际应用时，通常是以这 3 个轴（或任意两个轴）所构成的角度来计算设备倾斜的角度，从而计算出重力加速度的值。通过感知特定方向的惯性力总量，加速计可以测量出加速度和重力。

## 4　面向移动平台的身份认证方案

结合多点触控技术、重力感应技术和图形密码设计了几种适用于移动平台的新型身份认证方案，分别为绘制曲线认证方案、图像选择认证方案、多点指划认证方案和重力感应认证方案。并且基于 Android 平台进行了编程实现。

### 4.1　绘制曲线认证方案

图形密码中有一种典型的基于回忆型的图形密码方案，即 DAS（Draw A Secret）方案，如图 3 所示。此方案在设定密码时，系统要求用户在 2d 栅格上画出口令。图中从 1 到 6 对应的坐标分别为（2,2），（3,2），（3,3），（2,3），（2,2），（2,1），这 6 个坐标即为用户输入的口令。在验证阶段，系统显示同样的栅格要求用户重复原来的设定过程，如果用户画出的图形按照以前设定的顺序经过相同的方格，则通过验证。

DAS 方案的栅格为 4×4，画出的是连续曲线，其总的密钥空间为 $16 \approx 2 \times 10^{13}$，一般情况下，输入的密码远达不到 16!，在当前的运算速度下，DAS 方案的安全强度不够。我们在 DAS 方案的基础上进行了如下改进：

（1）将栅格改为 6×6。这样总的密钥空间可达到 $36! \approx 3.72 \times 10^{41}$，可以看到密钥空间得到显著提高，基本可以满足日常的安全需求。

（2）实现断续曲线密码。连续曲线会受到一些限制，而断续曲线则没有任何限制，可以随心所欲地在任何点上画线，进一步增强了方案的安全性。

（3）采用触屏技术，直接用手指在移动平台的屏幕上划动来实现画线的效果，增加了方案的便捷性。

（4）对用户名和用户画出的口令，利用 MD5 函数进行处理，将 HASH 值存储于口令数据库，从而更好地保证用户的口令安全。

在模拟器中实现的效果如图 5 所示。

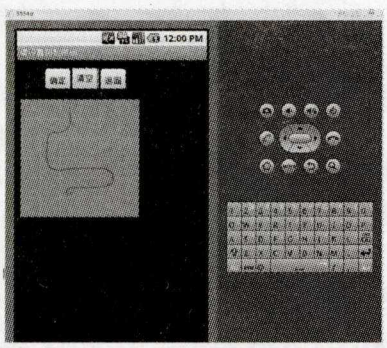


图 5　绘制曲线认证方案

### 4.2　图像选择认证方案

基于识别型的 Passfaces 方案(如图 1)利用人脸图像回忆来实现密码验证。用户在设定密码阶段,从人脸数据库挑选出多幅图像作为口令。验证阶段,用户看到一个由 9 张人脸组成的 3×3 网格,包括 1 幅口令图像和 8 幅迷惑图像。这个过程持续多次,用户全部选对预先设定的人脸图像就可以通过验证。因为人们对人脸记忆更容易,识别更迅速,所以缩短了验证时间。

但是 Passfaces 方案的密钥空间为 $9^N$($N$ 为口令图像个数),显然密钥空间较小,安全强度不够。我们在移动平台上实现时进行了如下改进:

(1)选择 6×8 的网格放置图片。用户可在其中随意选取图片。选取图片的个数、顺序无限制,亦可重复选取,选取的图片序列即为用户密码。方案的密钥空间可以达到 $48^N$($N$ 为选取图片的个数)。

(2)Passfaces 方案需要切换多个界面来完成用户的密码验证过程。我们设计的方案可以在一个界面中完成所有密码的设置和验证过程。

(3)方案中的图片可以由用户定制,更加灵活和便捷。

在模拟器中实现的效果如图 6 所示。

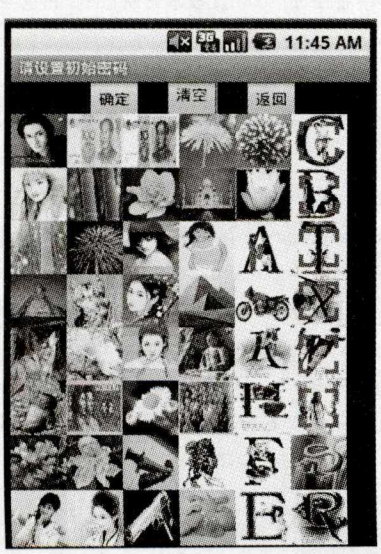


图 6　图像选择认证方案

### 4.3　多点指划认证方案

支持触控功能的移动设备越来越多,其应用也日趋广泛。结合流行的多点触控,选择多点指划的方向作为身份认证的口令,构思了一种利用多点指划技术来实现身份认证的方案。

认证界面为 9 个可触屏划动的圆球,每个圆球预设 8 个划动方向即东、南、西、北、东南、西北、东北、西南。当手指触控到圆球时,8 个方向凸显出来,手指离开屏幕,圆球的 8 个方向隐藏。将手指的滑动方向作为身份口令,口令设定过程是两个手指同时滑动任意两个球的 16 个方向中的任两个方向为一步,将这两个球的划动方向作为口令,可以通过多次操作设置多位口令。在进行口令验证时,要求用户选择正确的两个圆球,同时划出正确的方向。

实现的效果如图 7 所示。

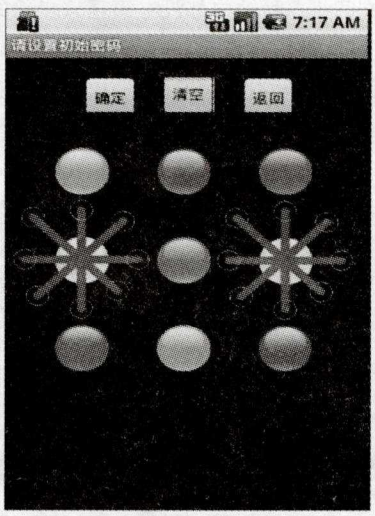


图 7　多点指划认证方案

当设置 $N$ 位口令时,方案密钥空间计算公式为:$(9\times8\times8\times8)^N$。通过简单的 3 次划动(即设置 3 位口令),密钥空间即可达到 97844723712,安全性较高。

### 4.4　重力感应认证方案

现代智能移动平台都具有重力感应的功能,重力感应功能可以解放手指,通过直接摇晃设备,即可实现操作。为此我们结合图形密码的 PassClicks 方案(如图 4),设计了基于重力感应的认证方案。

(1)口令设置

用户口令设置界面主要由一张风景图片组成。用户设置密码是通过在该风景图片上用手指点触选择几个特殊点,以其坐标作为密码。选取时界面会以红色小圆点为标记指出已选的特殊点,如图 8 所示。验证的有效区域处于以手指选择点为圆心、半径为 40 个像素的圆内。这个圆形区域即是口令验证容忍度,半径越小,安全性越高,验证容忍度小;半径越大,安全性越低,验证容忍度高。

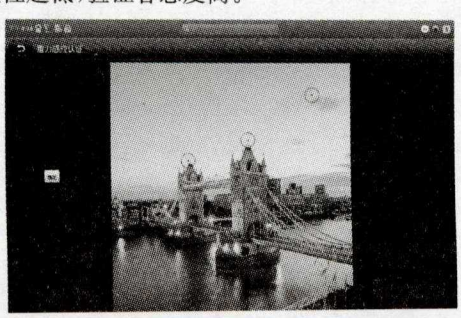

图 8　重力感应认证方案设置口令

(2)口令验证

用户身份认证界面仍然由这一张风景图片作为背景。与口令设置界面不同,用户不能用手指点触界面,而是通过滚动位于屏幕中央的重力感应小球来实现口令的验证。用户通过摇晃所持设备,使小球按顺序通过在口令设置时所设点的有效区域。验证步骤如下:首先判断滚动球与第一个所选点有效区域的位置。当滚动球经过该有效区域时,第一步验证成功。继续判断滚动球与第二个所选点有效区域的位置,以此类推。例如当判断第二个有效区域时,滚动球经过第三个有效区域,则不处理,直到滚动球经过第二个有效区域则继续判断。若用户在间隔5秒钟内都没有滚至该步骤的有效区域,则认为验证失败,退出身份验证环节。当用户认为滚动球操作有误时,可将球滚至右上角的区域,执行重新验证操作,清空已操作的步骤,等待下次重新验证。验证口令效果如图9所示。

图9 重力感应认证方案验证口令

(3)密钥空间

该方案中背景为800×800像素的图片,而有效区域为半径40个像素的圆。

选择1个特殊点时,密钥空间约为$[800^2/(40^2)]=400$;

选择2个特殊点时,密钥空间约为$[800^2/(40^2)]\times([800^2/(40^2)]-1)=159600$;

选择3个特殊点时,密钥空间约为$[800^2/(40^2)]\times([800^2/(40^2)]-1)\times([800^2/(40^2)]-2)=63520800$。

对于背景为$M\times N$像素的图片,有区域半径为$R$,设置$n$个点作为口令时的密钥空间计算公式为:$[M\times N/R^2]!/([M\times N/R^2]-n)!$。此公式计算的密钥空间为估算值,实际的密钥空间将比公式计算的略大。

**结束语** 本文所提出的身份认证方案在设计时都摒弃了文本形式的密码认证模式,通过图像选择、绘制曲线、多点指划、重力感应等组合形式完成密码口令的设置和认证,方案具有一定的新颖性和吸引力。并且在认证过程中密码口令不会以明文形式出现,从而增强了认证方案的安全性。我们针对Android平台的智能手机和平板设备,利用Java语言和Eclipse编程软件进行了编程实现,下一步将扩展至其他主流的移动平台操作系统,以满足不同用户的需要。

## 参考文献


[1] Hu Wei, Wu Xiao-ping, Wei Guo-heng. The Security Analysis of Graphical Passwords [C]// 2010 International Conference on Communications and Intelligence Information Security. ICCIIS2010. 2010:200-203

[2] 胡卫,吴晓平,张昌宏,等. 图形密码身份认证方案设计及其安全性分析[J]. 计算机工程与设计,2009,30(14):3284-3287

[3] Suo X, Zhu Y, Owen G S. Graphical passwords: A survey[C]// 21st Annual Computer Security Applications Conference (ACSAC'05). 2005:463-472

[4] Chiasson S, Biddle R, van Oorschot P C. A Second Look at the Usability of Click-Based Graphical Passwords[C]// Symposium On Usable Privacy and Security (SOUPS) 2007. Pittsburgh, PA, USA, 2007:18-20

[5] Birget J C, Hong D, Memon N. Graphical Passwords Based on Robust Discretization [J]. IEEE Transactions on Information Forensics and Security, 2006, 1(3):395-399

[6] 汪永松. Android平台开发之旅[M]. 北京:机械工业出版社,2010

[7] 丰华,于松波. Eclipse开发技术详解[M]. 北京:中国铁道出版社,2010


(上接第85页)


[8] Khanna G, Beaty K, Kar G, et al. Application Performance Management in Virtualized Server Environments [C]// Proc. of Network Operations and Management Symp. 2006

[9] Wood T. Black-box and Gray-box Strategies for Virtual Machines Migration[C]// Proceedings of the 4th Int'l Conference on Networked Systems Design & Implementation. IEEE Press, 2007

[10] Bobroff N, Kochut A, Beaty K. Dynamic Placement of Virtual Machines for Managing SLA Violations[C]// Proc of the 10th IFIT/IEEE International Symp. on Integrated Network Management. 2007

[11] Montresor, et al. Messor: Load-Balancing through a Swarm of Autonomous Agents[C]// Proc. of 1st Int. Workshop on Agents and Peer-to-Peer Computing. Italy, 2002

[12] Calheiros R N, Ranjan R, De Rose C A F, et al. Cloudsim: A Novel Framework for Modeling and Simulation of Cloud Computing Infrastructures and Services [R]. GRIDS-TR-2009-1. Grid Computing and Distributed Systems Laboratory, The University of Melbourne, Australia, March 2009