

一种对抗“肩窥”的身份认证技术研究与实践

张月红

(上海电子信息职业技术学院, 上海 201411)

✉64688613@qq.com

摘要: 本文提出了对抗“肩窥”的新型身份认证方案,设计并实现了一套智能解锁系统,在用户进行密码认证的同时进行基于按键时的压感值进行双重认证,从而有效保护移动设备的安全。进一步地,本方案随着新型的压力传感屏技术的发展,可以被移植到手机等其他带有压力传感功能的设备中,进一步地提高了本系统的应用范围。

关键词: 移动终端;身份认证;肩窥;压力特征

中图分类号: TP311.1 **文献标识码:** A

Research and Practice of an Identity Authentication Technology against *Shoulder Surfing*

ZHANG Yuehong

(Shanghai Technical Institute of Electronics & Information, Shanghai 201411, China)

✉64688613@qq.com

Abstract: This paper proposes a new identity authentication scheme against *shoulder surfing* by designing and implementing an intelligent unlocking system which conducts double authentication with the user's password and the pressure value based on keys. Therefore, this system can effectively protect the security of mobile devices. Furthermore, with the development of new pressure-sensing screen technology, this scheme can be transplanted to other devices with pressure sensing functions such as mobile phones, which further expands the application scope of the system.

Keywords: mobile devices; identity authentication; shoulder surfing; pressure characteristics

1 引言(Introduction)

《2017—2026年中国智能手机市场供需预测及投资战略研究报告》分析指出,我国智能手机普及率已高达58%,其中,安卓智能手机的市场占有率达到了83.2%,智能手机已然成为人们获取信息的重要通道。手机作为用户交换和获取信息的重要工具,存储了大量的隐私数据,这些数据的泄露必然会导致个人名誉形象的损坏和经济财产的损失。如何防止手机中敏感信息的泄露成为目前研究的热点。

当前保护手机中隐私数据最常用的方法是身份认证,传统的认证方案都是基于知识的,如IOS系统的PIN码认证方案和安卓系统的九宫格图案密码认证方案。这种认证方法很脆弱,攻击者可以通过手机屏幕上的油性残留物或者是加速度、螺旋仪传感器的数据推测出密码。

最常见的身份认证安全风险来自不怀好意者的肩窥。肩窥是一种安全领域的攻击手段,英文称为shoulder surfing,是一种社会工程学用来获取信息的方法。当用户登录系统时

输入密码和其他机密数据,攻击的实施方法通常只是通过受害者的肩膀偷看^[1]。这种攻击可以通过近距离(直接越过受害者的肩膀),也可能从一个较长的范围(通过使用一对望远镜或类似的硬件)来实现^[2]。要实现这种技术,攻击者不需要任何技术技能,只需要敏锐地观察受害者的周边环境和输入模式就足够的。这种方式在填表、在POS机上输密码,地铁上使用手机解锁等人多拥挤的场合更为适用。手机用户在解锁,登录应用时都有可能遭遇到肩窥。

因此开发一款价格低廉、便捷实用安全性高并可以防止肩窥认证方式就非常具有现实意义。

2 现状分析(Status analysis)

传统的身份识别技术包括身份标识知识(数字密码、图形密码等),在使用和安全方面都存在很多问题。身份标识知识的主要缺点为很容易被遗忘或者被盗,用户一旦遗忘用户名和密码等标识知识,给使用带来诸多不便;若是被盗,盗用者拥有与用户同等权限,这将引起更为严重的后果。



图1 传统手机解锁方式

Fig.1 Traditional mobile phone unlocking method

由于传统解锁方式的固有缺陷，基于人体固有信息的生物特征识别技术应运而生，成为解决安全问题的一条新途径。生物特征识别技术是利用人的生理或者行为特征进行身份识别的技术，与传统的身份鉴定技术相比，生物特征识别技术具有不易仿造及不易丢失，可随身携带且可靠性高等优点，为用户提供极大的便利，以及更为安全的服务。生物特征包括了物理特征(如指纹、人脸、虹膜等)和行为特征(如签名、声纹、手势、步态等)，目前用于手机认证的生物特征有指纹、人脸、声音等。现有的认证方案取得了一定的成果，然而都存在一些不足，如指纹识别需要有专门的指纹采集设备，而且手指干燥或受污都会影响指纹扫描的结果；人脸和虹膜认证过程需要耗费大量的时间和设备资源，且用户在公共场合进行认证时会感到尴尬；声纹认证的扫描结果很容易受到周围环境的影响。目前，应用领域中主要的生物特征识别技术主要包括指纹识别、声音识别、人脸识别、手形识别等等，其中指纹识别份额最大，达到38.3%^[3]，但生物特征解锁同样存在一定的缺点，如生物特征智能硬件需要增加额外成本，解锁成果率有待进一步加强，使用场合受限，更加值得关注的是生物识别技术自身存在风险：(1)传输风险。在互联网环境中，生物标识必然转换为数字标识，然后通过网络进行传输。而传输过程与其他的网络应用一样，面临着窃听的风险，这降低了它神话一般的安全性。从这个角度看，它与一般的密码一样，在安全性上并无区别。(2)不可撤销性。生物识别最大的弊端是它的不可撤销性。如果发现某个密码存在风险，可以马上更改它。但如果指纹、虹膜、脸型扫描被窃取了，几乎是永远无法撤销或者追回了！它会成为互联网上你的一个器官，被打包出卖、转售；在世界各个角落的组织、黑客，会从各种角度来分析，利用和消费它，直到你个体的消亡。

出于生物特征自身的风险特点，因此不宜于在大量的中低端移动设备中大量使用。



图2 生物特征解锁方式

Fig.2 Biometric unlocking method

为解决现有解锁方案存在的问题，本文考虑将传统密码解锁方案增加一个维度：我们输入的图案或数字除了它表象

的意思，还包含了其他不为攻击者所知的内容，这样可以做到攻击者看不到全部输入信息，无法重现，无法尝试。

综合考虑各种方案，本文选择考了增按键的力度作为另一个维度，让机器记忆压感，从而增加密码强度，且第二维度密码不易察觉，安全性大大提高^[4]。具体的，本文采用的认证方案为数字密码和压力密码结合，每一位密码，都需要数字和压力值两维认证正确才通过认证，为增加系统的可靠性，本文设计的案例中，压力值密码通过划分强弱两个维度来区分，若需要增加密码安全性，则可以增加强弱维度数，进一步增加系统安全性。

同时，市面上手机大多已经配置了压感屏，增加的压力维度不增加额外模块，解锁方案成本较指纹，面部解锁等生物特征方案有着明显的优势。同时，此加密解锁方案还可适用于其他需要加密的场合，如保险箱、行李箱等。

3 硬件设计 (Hardware design)

3.1 系统总体设计

为满足本文双因素加密方案的验证和实现，本文设计了一套智能解锁装置，以验证该加密方案的可行性。本文所设计的智能解锁装置以豌豆拼为核心，通过豌豆拼中主控模块，信号模块，显示模块，扩展模块等模块的配合完成智能解锁的功能。图3为系统硬件框图。



图3 系统硬件框图

Fig.3 System hardware diagram

以下将详细介绍系统中每个模块的选型及其工作原理。

3.2 主控制器设计

本文采用的主控制器为豌豆拼夸克主控模块，其为豌豆拼系列的最新版本。豌豆拼主控模块的处理器核心是Atmel处理器，同时具有多路数字输入/输出，一个ADC转换口，多路通讯口。豌豆拼主控模块及其IO口分布如图4所示。

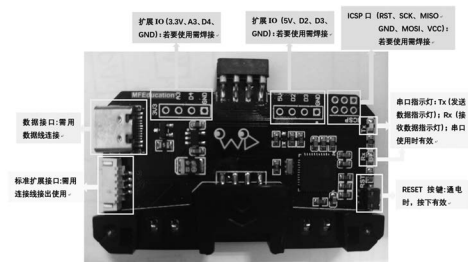


图4 夸克主控模块实物图

Fig.4 Actual photo of quark primary control module

选取豌豆拼夸克的主要原因在于其小巧而高效，符合智能解锁装置系统所要求的，小、精、准的要求。同时，豌豆拼的开发环境也较为友好，同时由于该硬件扩展性好的特性，适配的传感器和执行机构非常丰富，扩展性极强，便于多种不同类型的传感器和执行机构有机结合，在单片机内属于较合适的选型。

3.3 压力传感模块

本设计采用数字顺序和压感双重验证作为开锁密码，

因此必须选用一款可以感知按压力度的模块进行检测。豌豆拼夸克的信号模块配有压力传感器，可以用于按压强度的接受。本设计选用传感器最大量程为10kg，完全足够我们按压的范围。豌豆拼夸克的信号模块实物图如图5所示。



图5 夸克信号模块实物图

Fig.5 Actual photo of quark signal module

豌豆拼夸克的压力传感器主要由电位计和弹簧组成。该压力传感器具有灵敏度高，呈线性变化等特性。非常适合用于本系统的应用。

3.4 人机交互设计

为了可以给用户带来优越的视觉性，本文还设计了一个专用显示屏以提供良好的人机交互。本系统中选用OLED显示屏的尺寸为豌豆拼夸克显示模块、有源阵列有机发光显示屏具有内置的电子电路系统，因此每个像素都由一个对应的电路独立驱动。OLED显示屏具备不需背光源、对比度高、厚度薄、视角广、反应速度快、可用于挠曲性面板、使用温度范围广、构造及制程较简单等优异之特性。该模块实物图如图6所示。

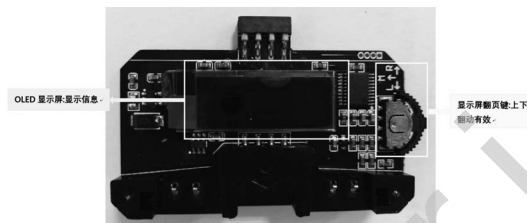


图6 夸克显示模块实物图

Fig.6 Actual photo of quark display module

显示模块的OLED显存为128*32bit，相当于32行128列点阵。将所有显示分为8页，每页16*4字节，即每页4行，纵向共32行。模块采用全量更新的策略，基于OLED128*32bit的分布，程序内部建立一个缓存数组16*4*8字节。每次修改时，先修改缓存对应的值，修改完成后，一次性写入OLED的GRAM刷新显示。

4 系统软件设计(System software design)

系统软件设计包含设置模式和解锁模式两个部分，系统软件流程图如图7所示。

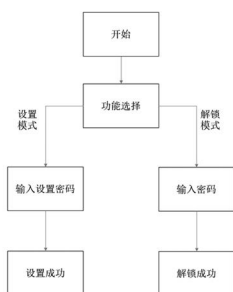


图7 系统软件流程图

Fig.7 System software flow chart

密码验证软件是整个软件设计的重点，本文设计解锁模式采用二维验证模式，即每次输入密码同时验证数字和压感值是否正确，直至四位密码全部验证通过，即确认开锁。密码验证的软件流程图如图8所示。

从流程图可以看出，整个开锁过程由以下几步组成：

- (1)模块初始化，开始运行程序，等待开始接收密码。
- (2)输入第一位密码，验证数字与压感是否正确，若正确，进入下一步，若错误，返回第一步。
- (3)输入第二位密码，验证数字与压感是否正确，若正确，进入下一步，若错误，返回第一步。
- (4)输入第三位密码，验证数字与压感是否正确，若正确，进入下一步，若错误，返回第一步。
- (5)输入第四位密码，验证数字与压感是否正确，若正确，进入下一步，若错误，返回第一步。
- (6)运行哈希验证，若正确，开锁，若错误，返回第一步。

程序初始化，从前往后输入1、2、3、4密码判断正确与否并判断压感值是否正确，若完全正确，判断是否符合哈希算法；若不正确，重新开始。若符合哈希算法，开锁成功，若不符合，返回第一步重新开始。

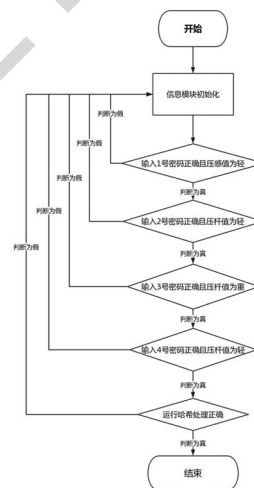


图8 密码验证流程图

Fig.8 Password verification flowchart

5 外观设计(Design)

一款好的产品，拥有一个美观的外观和牢固的机械结果也是必不可少的，本文的解锁样机要求设计一个牢固的结构以合理安排众多电子组件。

本文利用木板作为制作外壳的原材料。首先利用3D建模设计出智能解锁的CAD模型如图9所示。

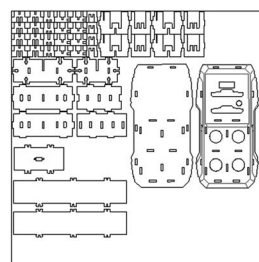


图9 主体CAD设计图

Fig.9 Main CAD design drawing

本文的外观采用CAD软件设计电路容仓，并用激光切割完成各个部件，切割对象主要材料为木材，各组件的连接采用榫结构、螺丝连接和强力胶连接，即保证了设计的精确度，和保证了外形的美观和牢固性。系统实际外观如图10所示。

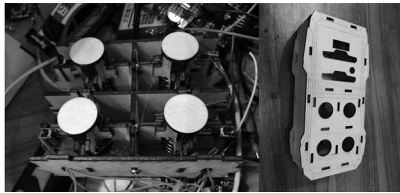


图10 系统实际外观图

Fig.10 Actual appearance of the system

6 系统的测试和结果分析(System test and result analysis)

6.1 压力维度测试

为验证本文采用的压力值强弱维度划分的合理性，本文首先对压力值进行了测试，并根据手感、压感值和输出维度进行对比验证。验证中，由于采用的为12位ADC，故压力输出值为0—4095，以2048位分界线对二者进行了区别，高于该值为强，低于该值为弱，验证结果如表1所示。

表1 压力实验结果记录

Tab.1 Record of pressure test results

项目	组别一	组别二	组别三	组别四
手感	轻	较轻	较重	重
压力值	358	1033	2875	3502
输出结果	轻	轻	重	重

由以上实验结果可以看出，本文采用的二维度强弱划分法，输出结果与手感值对应，且离边界值较远，不易出现读取值与手感值对应错误的情况。

6.2 解锁功能测试

在完成智能门锁的硬件和服务平台搭建之后，为验证其有效性，对系统功能进行测试。测试的目的是检测设计的双重加密系统是否能实现对应加密的功能^[5]。

实验过程有以下几个步骤：

- (1)预先设置好数字顺序和压感值作为密码；
- (2)依次输入正确或错误的密码；
- (3)验证是否正常解锁；
- (4)重复多次试验。

设定密码为“轻轻重重”的，实验结果如表2所示。

表2 实验结果记录

Tab.2 Record of test results

统计数量	按键1	按键2	按键3	按键4	解锁状态
共1100次	轻	轻	重	轻	失败
共1300次	重	轻	轻	轻	失败
共1500次	轻	重	轻	重	失败
共1200次	轻	轻	重	轻	成功
共1100次	轻	重	轻	重	失败

可以看到，实验过程中，系统能够识别输入的密码是否正确，并在数值顺序和压感值配对成功后开启解锁，在识别失败后不进行动作，结果基本达到预期设想。

6.3 测试结果分析

实际试验结果表明：

(1)本设计中的智能解锁方式识别率较高，能够准确识别输入的密码是否正确。

(2)加入的压感密码后，双重加密具有良好的加密效果，不易被偷窥、复制，具有良好的安全性。

(3)整个系统的测试后可知，系统获得了良好的效果，且总体成本较低。

通过以上结果可以看出，本文设计的加密系统有望进一步完善后推向市场。基于此技术原理，可以轻易开发出可用于保险箱，行李箱等各种可以增加实体“锁”的需求场合。还可以被应用在配备了压感屏的手机中。在未来会有越来越多的设备有条件使用这个技术，以获得更高的安全性。

7 结论(Conclusion)

本设计方案中双重验证智能解锁方式的设计，结合软硬件一起来实现加密、解锁功能。在实际的测试中有良好的效果。本项目基本功能已经完成，当时仍然有许多的不足之处。未来在一下方面有望得到改善。

本文压感加密采用了二值化处理，加密程度较低，未来在条件允许的情况下，需进一步提高压力值分布区域，进一步提高压感加密的程度；本文由手机解锁衍生，虽其后设计目的不仅仅服务于手机，但相应的手机端加密APP日后也需进行相应的开发，以提高整个系统的完整性；可以根据需求的不同，设置不同的安全等级和密码的难度，这样可以提高用户自主性，是用户根据场合设置相应的密码，提升可用性；对硬件进行一定的保护，防止恶意破坏、拆卸。

参考文献(References)

- [1] V.Roth,K.Richter,R.Freidinger.A PIN-Entry Method Resilient Against Shoulder Surfing[C].Proceedings of the 11th ACM Conference on Computer and Communications Security,2004(10):236-245.
- [2] Luca,A.D.,Hertzschuch,K.,Hussmann,H.ColorPIN-securing PIN entry through indirect input[C].CHI2010,2010(4):1103-1106.
- [3]曹巍,赵滢.一种基于双因素认证的移动支付安全技术研究[J].网络空间安全,2014,5(2):10-12.
- [4] 林兴志.物流统一信息系统双因素认证安全策略分析[C].全国密码学与信息安全教学研讨会,2010.
- [5] 林亮亮,陈洋,徐璐.一种基于手动输入的手机解锁方法[J].西安石油大学学报(自然科学版),2016,31(4):122-126.

作者简介：

张月红(1975-)，女，硕士，副教授.研究领域：渗透测试，漏洞挖掘，WEB安全。