软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2018,29(Suppl.(2)):96−107

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

基于震动语义提示的智能手表文本密码输入*

王鹏程, 杨求龙, 涂华伟

(南京航空航天大学 计算机科学与技术学院,江苏 南京 211106)

通讯作者: 涂华伟, E-mail: tuhuawei09@gmail.com

摘 要: 当今社会智能手表的使用越来越广泛,其中存储了用户大量的个人信息,需要设计合适的方法对其进行保护.PIN 是密码是使用广泛的一种方式,但存在抗泄露性不足的问题.提出了一种智能手表身份认证方案,基于传统的数字密码认证设计,通过震动语义提示输入的密码位数.开展了 3 个实验来研究这种方法的表现.首先研究了能否被用户快速并且准备判别的震动时长组合.结果显示 400ms 和 100ms 的组合使用效果最好.随后设计了一组震动提示方案,并建立了震动和密码第几位的映射关系,经由实验证实了该方案能够被有效地记忆与实践.最后测试了在模拟真实情况下的密码输入.结果表明,设置 5 位密码进行 4 位输入可以导致保证较快的输入速度和较高的准确度,同时,能够保证较高的密码抗泄露性.为智能手表的身份认证设计提供了新的思路.

关键词: 智能手表;身份认证;震动;安全;穿戴设备

中文引用格式: 王鹏程,杨求龙,涂华伟.基于震动语义提示的智能手表文本密码输入.软件学报,2018,29(Suppl.(2)):96−107. http://www.jos.org.cn/1000-9825/18021.htm

英文引用格式: Wang PC, Yang QL, Tu HW. Leakage-Resilient password entry on smartwatches based on semantic tactile feedback guide. Ruan Jian Xue Bao/Journal of Software, 2018,29(Suppl.(2)):96−107 (in Chinese). http://www.jos.org.cn/1000-9825/18021.htm

Leakage-Resilient Password Entry on Smartwatches Based on Semantic Tactile Feedback Guide

WANG Peng-Cheng, YANG Qiu-Long, TU Hua-Wei

(College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 211106, China)

Abstract: Nowadays, smartwatches are increasingly used in our daily lives. Smartwatches store a large number of personal information of users and it is necessary to design appropriate ways to protect them. PIN is a widely adopted method, but it is not resistant to shoulder-surfing. This work proposes a smart-watch-based identity authentication scheme. This scheme is based on the traditional PIN authentication and prompt password entry by vibration. Three experiments have been designed to examine the performance of this method. In the first experiment, it is tested that what kind of vibration time combination is more acceptable. Results show that the vibration combination of 400 ms and 100 ms is the optimal one. In the second experiment, a set of vibration prompt scheme is designed to establish the mapping relationship between vibration and number. Results prove that the scheme can be effectively remembered and practiced. In the last experiment, the actual password input process is simulated and the traditional unlock method is compared with. Results show that inputting four digits of five-digit password can lead to an overall fast entry speed and high accuracy, while maintaining a high security. This study offers insights into identification design for smartwatches.

Key words: smart watch; identity authentication; vibration; security; wearable device

* 基金项目: 国家重点研发计划 (2017YFB0802300); 国家自然科学基金(61602236); 江苏省自然科学基金(BK20160801); 中国博士后科学基金(2016M591843); 江苏省博士后科学基金(1501053B)

Foundation item: National Key Research and Development Program of China (2017YFB0802300); National Natural Science Foundation of China (61602236); Natural Science Foundation of Jiangsu Province (BK20160801); China Postdoctoral Science Foundation (2016M591843); Jiangsu Postdoctoral Science Foundation (1501053B)

收稿时间: 2018-06-15; 采用时间: 2018-11-08

随着智能手机的普及,智能穿戴设备也随之得到了飞速发展.其中智能手表是最受厂商和消费者关注的[1].智能手表是将手表内置智能化系统,搭载智能手机系统与互联网连接,能够同步手机中的电话、短信、邮件、支付密码等用户隐私信息.智能手表在日常生活中的使用逐渐增多,同时也存储了很多用户的隐私信息.因此,要重视智能手表的安全问题,尤其是身份认证的问题.

最近的研究进一步提高了智能手表的安全性[2],但大多数认证方法与智能手机[3,4]相比,它们的安全性还有所不足.市面上主流的智能手表解锁方式一般为两种,一种是 PIN 码,用户通过输入预设的数字组合来解锁设备;另一种是图形解锁,用户在表盘显示的点阵图案上绘制预设的图形来解锁设备.尽管具有多方面的优势,但这种方法在安全性上存在很大的缺陷.图形密码非常容易被窥探[5],这使得肩窥攻击的发生率在公共场合非常高,严重威胁到了用户的隐私信息.其他还包括臭名昭著的污迹攻击[6],可以将屏幕上留下的手指痕迹用于提取密码.市面上还有一些其他认证方式,比如生物信息或者步态识别[7,8],但实现这类认证方式需要特定的硬件技术支持,限制了其使用的范围.同时还存在被伪造的风险[9].因此需要一个新的认证方式来解决这一问题.

本文提出了一种智能手表身份认证方式,将震动与数字密码相结合来提高密码的抗偷窥性能,图 1 简要展示了其操作方式:手表显示出表盘,随后发出震动提示位置信息,使用者在感受到震动后选择正确的数字.因为震动的具体模式对于外部的观察者是不可知的,即使是摄像头也无法记录下震动的细节,可以有效防止信息泄露.而且如果要用于更通用的目的,兼容性很重要.比如改变银行账户的密码输入方式将会影响到所有的自动取款机和 PIN 码,以及现有的软件.此外,一些用户,特别是那些不懂技术的用户,可能会对界面的修改产生抵触.因此,新方法最好只在尽可能小地改变原有输入习惯的前提下增加认证的安全性能.该方法选择在传统的数字密码认证基础上,通过震动来提示所需要输入的密码位数,从而实现密码的乱序输入.我们设计了多种不同的震动组合,每种组合对应一个唯一的输入次序.并且偷窥者不知道用户所设置的震动的模式组合,这样即使偷窥到密码的输入过程也无法得知真实密码,以期提高智能手表的安全性.本文主要对该方案在不同的密码长度、震动组合等影响条件下的不同表现进行了实验与分析,以得出该方法的可行性和最优设置.

Fig.1 Operating schematic diagram

图 1 操作示意图

1 相关工作

本节中,我们将讨论与本文工作相关的研究内容,作为针对智能手表的用户身份验证方法,联系紧密的研究主要有 3 个方向,即如何解决肩窥问题、手表界面的设计以及触觉要素在身份认证领域的研究应用.

1.1 基于软件代码的度量

肩窥(shoulder-surfing)是指攻击者通过观察用户输入密码时的动作来窃取用户的密码,它是最常见的窃取密码的方法.使用时虽然用户的密码没有显示在屏幕上,但一个熟练的攻击者可以通过读取用户的按键顺序,复制用户的动作从而破解密码.在传统输入方式下,用户唯一的防御手段是用物体或身体遮挡键盘和输入过程对于传统的密码输入方式如何抵御肩窥问题已经有了大量的相关研究.比如 Roth 等人[10]提出了一种身份验证方案.该系统不要求用户输入显式的数字,而是通过回答问题来间接验证用户是否知道密码,因此偷窥者简单地记

住用户某一次的输入是无效的.Kwon 等人[11]对这一方法进行了更深入的研究,增加了问题的复杂度,进一步提升了抗破解难度.Bianchi 等人[12]增加了声音和触觉信息来应对肩窥攻击.Manu 等人[13]则开发了一种基于视觉跟踪的密码输入方式,用以防御肩窥和大部分录像.Von Zezschwitz 等人[14]把数字密码和手势相结合,提升了映射的复杂度.这些研究使得来自于人眼观察的肩窥攻击的抵抗能力有很大程度的提升.它们的局限之处在于,攻击者通过大量观察或是摄像头的记录依旧可以得出其中的规律,并且大多是针对智能手机设计的.因此,我们需要一种更强的认证方式(以抵挡摄像头的观察),并且要适用于智能手表.

1.2 智能手表身份认证研究

相比于智能手机,智能手表等可穿戴设备的屏幕尺寸更小,形状各异,并且佩戴的方式和智能手机也大不相同.这些可能会导致在使用触摸式的密码输入方法时,用户和设备的交互结果也有所差异.此外,由于智能手表的显示屏更小,在智能手表上的交互性能可能会受到胖手指问题[15]的影响.关于这一问题,在智能手机领域的研究已经很充分[16].

针对这一问题,Zhao 等人[17]进行了相关的研究,探究了在智能手表这一平台上,不同的认证方法、用户界面和显示尺寸对认证准确性、速度和安全性的影响.而 Nguyen 等人[18]的研究则显示,胖手指问题似乎对智能手表的身份验证影响不大.并且虽然智能手表的普通 PIN 码的错误率比智能手机要更高,但仍低于百分之十,处于可以接受的范围内.相对于常规的图形数字解锁方式,其他的认证方式也得到了一定的研究.例如,Lee 等人[19]所研究的利用智能手表传感器信息,对使用者进行持续的隐式身份认证.Lu 等人[20]的研究在此基础上,通过机器学习算法,分析用户在输入密码时的传感器数据特征,进行辅助认证.也有很多研究直接识别使用者的生物信息[7,8].

1.3 触觉在身份认证中的使用

作为人体五感之一,触觉在人机交互领域扮演着重要角色.同样地,我们也可以将其引入到身份认证领域[21,22],增加认证的维度.在上面提到的 Kwon 等人[11]的方案中,也使用了震动这一元素作为解锁的影响因素之一,大致可以表示为:手机发出震动时选择 A,发出模拟震动的音效时选择 B.Deyle 等人[23]设计了一种原型机,通过手指感受电机的细微升降来传递密码的内容.按特定手指顺序输入所感受到的升降信息.Kuber 等人[24]设计了一种更便携的设备,展现类似于盲文的触点阵列,以提供密码候选项.这些方法都是对触觉的初步应用,并且大多需要额外的硬件支持,没有利用设备本身的震动功能.但它们都有一个共同点,就是对摄像头的拍摄具有良好的抵抗能力.

2 方案设计

2.1 交互方式设计

本文所采用的具体思路如下:基于普通的方形界面数字密码解锁方式,在用户输入密码过程中,手表通过震动传达信息,提示用户输入密码的第几位.例如,假设设置的密码是“201805”,用户在开始输入时,手机给出震动,提示输入密码的第 2 位,则用户输入“0”.之后,手机再次给出震动信息,提示输入密码的第 4 位,则用户输入“8”.依此,逐步进行密码输入,图 2 展示了具体的输入流程.由于输入密码的次序是随机(提示输入密码第几位是随机的),偷窥者即使观察到输入的密码序列,也无法得知密码的真实序列,因此具有很强的抗泄露性.

为了提高密码的抗暴力破解性,本方案提出了“多设置,少输入”的策略,即设置 n 位密码,但只需要输入其中的 k 位($k<n$).在该策略下,最多需要 $A_n^k 10^{n-k}$ 次才能破解密码.例如,6 位密码,如果输入 6 位,则所需尝试破解的最多次数为 720 次.但如果只输入 4 位,则所需次数为 36 000,因此极大地提高了密码的安全性.

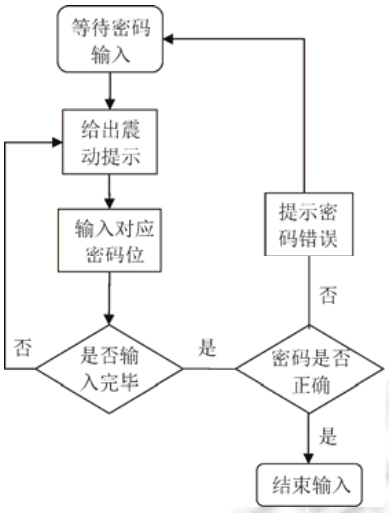

Fig.2 Password input process

图 2 密码输入流程

2.2 震动提示设计

该方案的技术关键是震动提示的设计.设计的原则是使用较为简洁的信息.

用户能够较好地记忆和回忆元素的组合,以便快速定位到对应的密码位并输入.基于摩尔斯电码,本方案设计了如下震动语义方案.以短震动和长震动的不同组合来提示密码位,震动间的间隔为 200ms.表 1 展示了密码位 1~9 的编码组合,更多的密码位可根据表 1 来设计.在实际的使用中,也可以由用户自定义特殊的编码组合,进一步确保安全性能.

Table 1 Vibration combination mapping table

表 1 震动组合对照表

震动提示位置	震动形式	说明
1	▬	
2	▬▬▬	
3	▬ ▬	
4	▬ ▬▬▬	▬ 短震
5	▬▬▬ ▬	▬▬▬ 长震
6	▬▬▬ ▬▬▬	间隔 200ms
7	▬ ▬ ▬	
8	▬ ▬ ▬▬▬	
9	▬ ▬▬▬ ▬	

但由于震动本身有一定的声音,可能会泄露震动的组合信息,因此需要设计掩饰技术来消除这种影响.本研究拟通过播放和震动声音相近的音频文件,覆盖整个震动提示过程,以防止密码的泄露.

3 实验 1

该方案的核心是采用规律的长短震动来传递密码位置信息,因此需要探讨该方案在智能手表上实现的合理配置(短震和长震的震动时长选取)和可行性(实际操作的速度与成功率).

主要针对如下的研究问题:什么样的震动时间长短组合最适合实际使用?不同的长短组合会在很大程度上影响震动的辨识的准确度和速度.本实验主要调查的是,该如何选取一个合理的值,使得本方案能够在两者上取得最佳的均衡效果.

3.1 实验设备

为了实现解锁界面的模拟,我们选择华为的 HUAWEI WATCH 2 作为实验平台,系统版本为 Android 7.1.1,屏幕为 1.2in 圆形 AMOLED 显示屏,分辨率为 390×390,具有震动和扬声器功能.在其上编写了多个 Android Wear 应用程序,可以实现数据的记录和解锁界面的模拟,满足了不同实验的需求.

3.2 实验者

实验招募了 10 名志愿者(5 男 5 女),都为 20 岁~24 岁的学生,所有人都是右手为惯用手,其中 7 人使用过 PIN 码作为手机的解锁方式,所用的密码长度 4 位~6 位不等,有 4 人使用过智能手表或手环等穿戴设备,所有参与者都表示不希望他人能够访问他们的智能手机或手表.

3.3 实验设计

本实验中只有 1 个自变量,就是不同震动时长的组合.因变量为实验者完成的时间和准确度.为了探究什么样的震动时间长短组合能够在辨识度、准确度和速度上取得最佳的均衡效果,我们选择了 5 种不同的震动长短组合进行测试,分别为(100,300),(100,400),(100,600),(200,400),(200,600)(单位:ms),括号内第 1 个数字表示短震动的时间长度,第 2 个代表长震动的时间长度.所有组合的震动间隔都是 200ms(我们做了一个前期实验,证明了 200ms 是最合适的间隔时间,100ms 就会令用户难以分辨).实验中,每种时长都要做 4 组输入,每组组内所有独特的震动模式都会出现 2 次.

考虑到震动本身存在声音,我们录制了一段手表震动的音频作为掩饰音效,完整地覆盖到整个震动的过程,前期实验证明,即使在安静的办公室环境下也可以有效遮盖震动本身的声音,并且也可以防止使用者是依靠辨别震动发出的声音而不是感受震动本身来获取信息.

震动模式出现的顺序都是随机的,每种长短组合共有 72 次输入.5 种震动短长组合出现的次序通过两个 5×5 的拉丁方进行平衡(一共 10 名实验者).记录了判断的用时和准确率.判断时间是从震动提示结束后,到实验者点击按钮为止.准确率为实验者判断错误的次数除以所有实验次数.

3.4 实验过程

实验场地为一个安静的办公室,所有实验者所处的环境都相同,他们被要求坐在桌前又好又快地完成实验任务.所有实验的顺序都采用了拉丁方进行平衡,实验的长度都在 20min 左右.为了避免疲劳对结果的影响,实验期间允许用户休息一段时间.实验分为练习阶段和测试阶段.在练习阶段,实验者坐在椅子上,练习上述实验过程,感受相关操作,直到确保参与者操作熟练后再进行正式实验.

实验协调者首先给实验者介绍掩饰方法下的震动提示,并让实验者感受每一种震动组合,等到熟练后再进行正式实验.开始后手表发出有规律的震动,实验者在屏幕上点击对应的按钮.如果能够判断,就选择“Yes”,再填写判断出的震动组合类型.如果没有感受清楚,就选择“UNCLEAR”按钮,填写自己猜测的组合类型(如图 3 所示).如果不能,则直接选择“NO”,开始下一个测试.

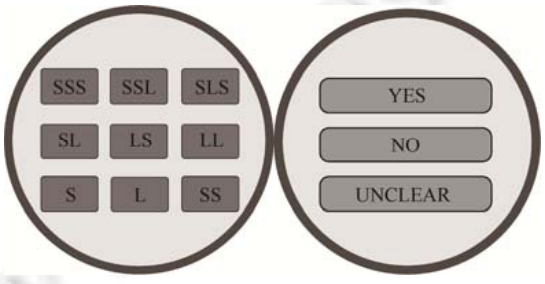

Fig.3 Experiment 1 interface

图 3 实验 1 界面

当完成实验后安排实验者填写问卷调查,根据速度和准确度表达对两种输入方式的偏爱程度(7 表示最喜欢,1 表示最不喜欢).

3.5 结果分析

我们选择了重复度量方差分析法进行分析,并将不同模式之间的数据进行两两比较,意图得出不同组间的数据差异和模式对实验者各方面表现的影响程度大小.

3.5.1 学习效果分析

首先进行的是实验者的学习效果分析,因为每个实验者在 5 种输入方式下都做了 4 组实验,所以首先分析 4 组实验中的输入时间,分析从第几组开始实验者的输入达到了稳定的水平.

分析结果显示,第 1 组比其余 3 组的输入时间明显更长(p<0.05),但是后 3 组的输入时间无明显差异(p>0.05).因此我们可知,实验者从第 2 组开始就可以实现稳定的输入过程.因此,将学习效果考虑在内后,我们选择后 3 组的实验数据来作为后续分析的对象,而舍弃掉第 1 组的数据.

3.5.2 正确率分析

我们主要分析的是不同的震动时长组合对用户输入效果的影响大小,震动时长组合的不同在时间上有很强的主效应($F_{4,36}$=13.673,p<0.01).表 2 展示了震动时长组合间正确率的两两对比结果,其中,p_1 为正确率,p_2 为时间.可以看到,(200,400)的组合与其他几组存在着显著差异(p<0.05).图 4 展示了不同时长组合的平均正确率,其中,误差线表示 95%的置信区间.可以看出,其他 4 种时长组合的正确率都在 95%左右(p>0.05),而(200,400)组合的正确率只有 79%.并且根据用户的主观评价表可知,它也是实验者反映的最难以分辨的类型.因此首先排除了这一组合.

Table 2 Comparisons of statistical p value of accuracy rate and time between different vibration combinations

表 2 不同震动组合之间正确率和时间的统计 p 值差异比较

Mode	(100,300)	(100,400)	(200,400)	(100,600)	(200,600)
(100,300)	–	p_1=1/p_2=1	p_1=0.063/p_2=0.099	p_1=1/p_2=1	p_1=1/p_2=0.718
(100,400)	p_1=1/p_2=1	–	p_1=0.017/p_2=0.037	p_1=0.51/p_2=1	p_1=1/p_2=0.396
(200,400)	p_1=0.063/p_2=0.099	p_1=0.017/p_2=0.037	–	p_1=0.09/p_2=0.284	p_1=0.014/p_2=1
(100,600)	p_1=1/p_2=1	p_1=0.51/p_2=1	p_1=0.09/p_2=0.284	–	p_1=1/p_2=0.536
(200,600)	p_1=1/p_2=0.718	p_1=1/p_2=0.396	p_1=0.014/p_2=1	p_1=1/p_2=0.536	–

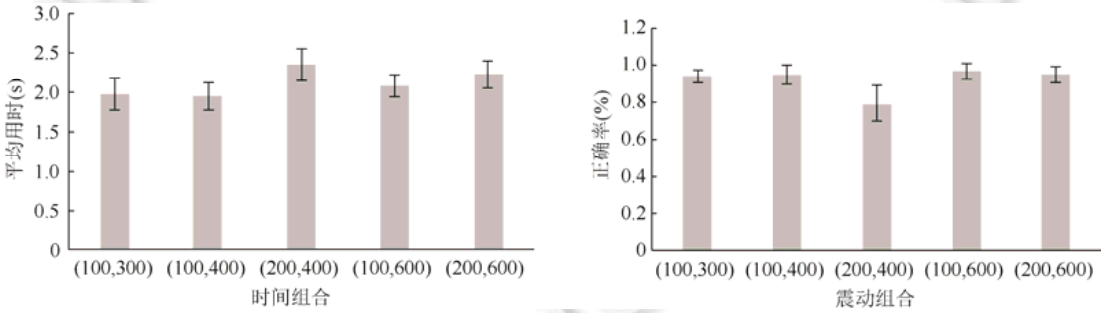

Fig.4 Comparison of average time and accuracy rate of different vibration combinations

图 4 不同震动组合的平均用时和正确率比较

3.5.3 用时分析

震动时长组合的差异在时间上的主效应也十分显著($F_{4,36}$=5.305,p=0.02),表 2 展示了不同震动时长组合之间时间的两两对比结果.图 4 展示了用户从手表开始震动到分辨出震动组合平均所需时间的长短.可以看出,(200,400)的平均用时是最长的,剩余几种的用时则差不多(p>0.05),这也符合我们之前的结论.一方面是因为 400ms 比 600ms 本身就要短一些,另一方面是因为(100,400)的组合清晰度要优于(100,300)的组合.

3.5.4 主观评价

在主观评价表中,我们发现速度上有差异性($F_{4,36}$=64.636,p<0.01).实验者对于(200,400)的组合评价最低,平均只有 4.8 分,而(100,300)的组合得到了 5.7 分,其余 3 种都在 6 分以上.用户更喜欢震动组合内长震和短震时间差差异更大的组合.

3.5.5 小 结

在平均错误率上来看,只有一种组合显示出了相对较大的劣势.在保证正确率的前提下,为了尽量缩短输入的总时长,优先选择时间较短的组合.再综合用户的主观评价表,我们认为(100,400)的组合是最好的选择.

4 实验 2

经过实验 1 的研究,我们可以初步确定一个最佳震动时长组合(在本次实验中为(100,400)的组合).但是仅知道最适合辨认的时长组合是不够的,实验者对震动提示所表示信息的识别与记忆也会影响密码输入速度.因此,在本实验中我们要调查实验者对不同震动组合的记忆与分辨能力究竟如何,不同组合之间是否存在区别.相对普通密码输入方式,本方案引入了震动语义提示这一要素,需要了解用户对这一新要素的实际接受程度.

4.1 实验设备和实验者

同实验 1.

4.2 实验设计

由于不同震动模式对应的是待输入数字在整个密码中所处的位置,所以我们只设计了 9 种不同的组合(预期长度不会超过 9 位数字),在键盘上排列为 3×3 的方格,还原了真实的数字键盘,排除了键盘位置对操作的影响.每个实验者需要进行 4 组实验,每组实验都是 2 轮,每轮 9 个震动的随机顺序序列,同样添加了掩饰音效.一共有 72 次输入.

4.3 实验过程

实验开始后,与实验 1 类似,首先感受每一种震动组合,等到熟练后再进行正式实验.实验者需要感受手表发出的震动,并判断每一次震动对应表示的位置,根据之前所背诵的表格内容,在键盘上选择相应的数字.记录下每一次震动形式下,实验者所花的时间、错误率等信息,并在实验结束后填写主观评价表.

4.4 结果分析

5.4.1 学习效果

分析收集到的时间和正确率信息可知,实验组别的差异对用时有强烈的主效应($F_{3,27}$=9.201,p<0.01),但是在正确率方面的效应却并不显著($F_{3,27}$=2.571,p=0.75).对组间的时间度量两两对比结果见表 3.其中,p_1 为时间,p_2 为正确率.数据显示,第 1 组和最后两组的差异较大(p<0.05),而第 3 组和第 4 组的时间特征则几乎没有差别(p=1),并且由图 5(图中误差线表示 95%的置信区间)可以发现,后两组的数据的平均时间明显优于前者,并且误差值也较小,而正确率的变化则不大($F_{3,27}$=2.571,p=0.75).因此我们可以认为,在经过了两组实验的学习与训练过程后,实验者就可以熟练地掌握这一输入方式,形成震动和数字的映射关系.并且猜测是因为实验的条件比较安静,实验者都可以在充分的思考后再做出选择,因此不同组间的差异多反映在时间上,而正确率都较高.

Table 3 Comparisons of statistical p values of time and accuracy rate between different blocks

表 3 不同 Block 之间时间和正确率的统计 p 值差异比较

Block	1	2	3	4
1	–	p_1=0.636/p_2=0.727	p_1=0.054/p_2=0.234	p_1=0.041/p_2=1
2	p_1=0.636/p_2=0.727	–	p_1=0.059/p_2=1	p_1=0.016/p_2=0.918
3	p_1=0.054/p_2=0.234	p_1=0.059/p_2=1	–	p_1=1/p_2=0.45
4	p_1=0.041/p_2=1	p_1=0.016/p_2=0.918	p_1=1/p_2=0.45	–

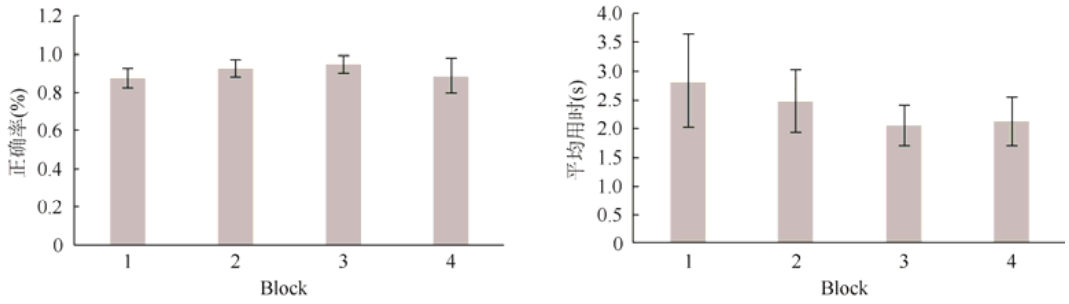

Fig.5 Comparison of accuracy rate and average time of 4 blocks

图 5 4 个 Block 的平均正确率和用时比较

5 实验 3

在确认了方法的可行性和可靠程度之后,我们所需调查的是,在真实情况下的连续密码输入效果究竟如何.通过设置不同的密码长度,获取效率最高、安全性能最好的设置,并与传统的输入方式作对比来调查该方案的实际连续操作情况.在实验的过程中记录相关的数据,并通过测试后的调查问卷来获取用户的主观偏好.

5.1 实验设备和实验者

同实验 1.

5.2 实验设计

本实验的目的是比较无震动密码输入和我们提出的密码输入技术的在时间和错误率上的表现差异,还要调查在仅输入 4 位密码的情况下,应如何设置密码位数以达到高安全性和相对好的输入效率果.因此本实验的自变量为密码的长度和震动的有无.实验者在无震动和有震动情况下输入 4 位密码.在无震动情况下,密码长度为 4 位.在有震动情况下,密码长度为 4 位、5 位、6 位、7 位.为了区分无震动和有震动的 4 位密码,屏幕上会给出明显的提示.

对于每一种独特的密码长度,都有 5 个随机生成的密码,其中无震动情况和有震动情况下的 4 位密码数字是一样的,以确保对照组的统一.每个实验者都被要求做 3 组实验,每次输入时都有声音掩饰.由于实验流程较长,我们允许实验者中途进行休息,以避免疲劳产生的影响.同时,为了消除学习效应的影响,不同实验者进行输入时的密码种类出现顺序遵循 5×5 的拉丁方平衡.

我们没有要求实验者记住密码,因为短时间内记住全部 25 种密码是不可能的,所以待输入的密码都被明文显示在屏幕的右侧,共 5 种密码形式.考虑到进一步提高密码输入的安全性,我们提出了“多设置,少输入”的方案:在密码长度大于 4 位的情况下,也只需要输入其中 4 位.

考虑到可能存在误触,在提交完整的密码之前可以删除已经输入的部分,若有没感受清楚的震动也可以进行重震,所有的这些操作都会被记录下来.为了保证每次输入的独立性,最小化学习效果的影响,实验者在提交错误的结果后并没有修正的机会,而是直接进入下一个密码的输入.此外,也记录了完成时间、错误率和主观评价,所有的数据都会参与到最后的数据分析阶段.

5.3 实验过程

协调者首先给实验者介绍震动语义提示输入的流程,在经历了前两个实验之后,实验者对其也有了一定的了解,等到熟练后再进行正式实验.开始后手表发出有规律的震动,屏幕右侧会出现待输入的密码,实验者根据震动的内容和对照实验者背诵的表格来选择正确的数字.

例如,图 6 中显示的数字为 5920371,手表以短-长(S-L)的形式震动,参照表 1 内容可知,我们需要输入右边密码的第 4 位,也就是数字“0”.以此类推,经历 4 次震动,输入完全部的 4 位密码.

Fig.6 Experiment 3 interface

图 6 实验 3 界面

结果正确或错误都会得到提示,并开启下一轮的输入.中途允许撤销输入和重复本次震动提醒.在每一组的结束时也有提示,给实验者休息的时间.当完成实验后安排实验者填写问卷调查,根据速度和准确度表达对两种输入方式的偏爱程度(7 表示最喜欢,1 表示最不喜欢).

5.4 结果分析

5.4.1 学习效果

我们对实验所得的数据进行了重复度量方差分析,数据显示,测试组的先后顺序对正确率有一定的主效应($F_{3,12}$=4.824,p<0.05),而对时间的效应要强得多($F_{3,12}$=10.682,p<0.05).可以看出,第 1 组和后两组的数据效果存在显著差异(p<0.05),第 2 组和后两组的差异则并不显著(p>0.05).这说明,即使前期做了充分练习,并且有前置实验,也依然存在较为明显的学习效果学习效果,因此我们舍弃了第 1 组数据,选取后 3 组的数据来进行下一步分析工作.

5.4.2 用时分析

重复度量方差分析法的结果表明,密码(有震动)的长度对输入的速度有显著影响($F_{3,27}$=20.703,p<0.01).表 4 展示了有震动情况下的不同长度密码输入之间的时间和正确率两两比较的差异(p 值),其中,p_1 为时间,p_2 为正确率.可以看出,长度为 4 的密码和长度为 6 位、7 位的密码在使用效果上存在显著差异(p<0.05),但后两者之间的差异却并不明显(p=1).5 位密码和双方都存在显著性差异,因此 4 种密码长度可以分为 3 类.

Table 4 Comparisons of statistical p values of time and accuracy between different password lengths with vibration

表 4 有震动情况下不同长度密码输入间时间和正确率统计 p 值差异比较

Length	4	5	6	7
4	–	p_1=0.053/p_2=0.906	p_1=0.001/p_2=0.168	p_1=0.001/p_2=1
5	p_1=0.053/p_2=0.906	–	p_1=0.090/p_2=0.322	p_1=0.06/p_2=0.906
6	p_1=0.001/p_2=0.168	p_1=0.090/p_2=0.322	–	p_1=1/p_2=0.223
7	p_1=0.001/p_2=1	p_1=0.06/p_2=0.906	p_1=1/p_2=0.223	–

图 7 展示了不同输入方式的平均用时对比,横坐标的 1 代表 4 位的无震动密码,2、3、4、5 分别依次代表了 4 位、5 位、6 位、7 位的有震动密码输入,误差线表示 95%的置信区间.可以发现,随着输入的密码的长度的增加,用时也越来越长.总用时在 7 位时最大,接近了 15s,但总体相对于 6 位密码的区别并不大(p=1).4 位有震动密码的平均用时则是 11s,是无震动密码的 3 倍,毫无疑问,该方案增加了时间的开销.

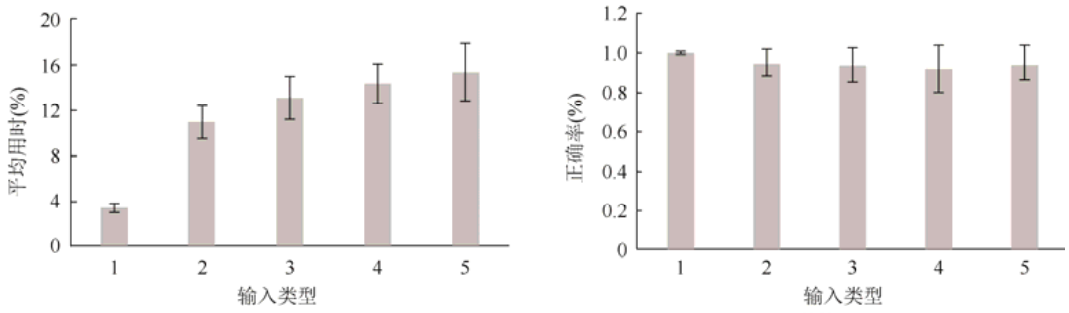

Fig.7 Comparison of average time and accuracy rate of different input types

图 7 不同类型输入方式的用时和正确率对比

5.4.3 正确率分析

图 7 展示了几种不同模式下的平均错误率信息.横坐标的 1 代表 4 位的无震动密码,2、3、4、5 分别依次代表了 4、5、6、7 位的有震动密码输入.

当我们把目光集中在有震动的 4 组上时,首先我们发现,与实验 2 的结果类似,不同的密码长度在错误率的方面影响并不明显($F_{3,27}$=0.637,p=0.598),具体到不同长度的两两对比时,根据表 4,所有组间的差异值 p 都大于 0.05,也就是说,密码长度并不显著影响正确率.从图 7 提供的平均正确率来看,有震动输入的 4 种方式正确率都在 94%左右.其中,6 位密码的正确率最低,为 92%,但仍处于一个较高的值.而在传统的无震动密码输入下,用户的正确率为 100%.

5.4.4 主观评价

用户的主观评价表显示在速度上存差异性($F_{3,27}$=27,p<0.01).接受度最高的是 4 位的有震动密码,平均评分达到了 6.2,随着密码长度的增加,用户感受到的输入难度也随之增加,平均评价也在降低.经口头访问得知,偏好的原因是最后一位数字可以不感受震动,直接输入剩下的那个即可,简化了输入过程.

但是和数据分析不同的是,在输入准确度的主观评价上也存在明显的影响($F_{3,27}$=5.18,p=0.06).我们猜测出现这一现象的原因可能是因为实验者下意识地排斥更长的密码,从而导致评价出现了偏差.

5.4.5 小 结

实验者在使用本文设计的方案时,正确率可以稳定在 90%以上,证明了该方案的可行性.但该方案也比普通的 PIN 码输入更加耗时,并且密码位数会显著影响解锁时间($F_{3,27}$=20.703,p<0.01).4 位密码因为存在只需要感受 3 位的缺陷,增加了信息泄露的可能性.6 位和 7 位之间用时和正确率的差距都不大(p>0.05).因此我们认为,如果追求解锁速度可以使用 5 位的密码,想要尽可能地提高安全性能则是 7 位的密码更加符合要求.

6 总 结

针对这一新的解锁方式,我们做了一系列实验,通过对实验数据的记录和分析,我们得出以下结论.

(1) 总体来说,长短差异较大的组合表现得会更好,差异较大的组合在正确率上有明显优势.另一方面,震动的时长也会影响输入所需要的时间,长震动达到 600ms 的组合在平均总用时上明显比长震动为 400ms 和 300ms 的组合要多.因此,综合上述两点,我们认为(100,400)的组合最适合实际使用.

(2) 实验者在记忆震动组合方面表现出了很大的个体差异性,但在较短的时间内就可以熟练地掌握其操作方式.由实验 2 的学习情况可知,平均两组实验任务之内的学习时间就可以获得很好的记忆效果,也即两组实验任务之内熟练掌握这一映射关系,证明了方法的可行性.同时,我们发现实验者对某几种特定的组合分辨能力明显较差,可能与人的记忆模式有关,可以为以后的模式设计作指导.

(3) 在真实的连续密码输入情况下,该方案的在各种条件下的正确率都可以达到 90%以上,证明该方案使用熟练后也不会影响解锁的正确率,会在一定程度上增加解锁的总用时.由主观评价可知,用户更喜欢较短、较

简单的密码,但考虑到时间成本和安全性能的平衡,我们认为设置 5 位密码进行 4 位输入可以保证较快的输入速度和较高的准确度,同时能够保证较高的密码抗泄露性.

以上结论总结了本方案的优缺点和实现价值.本文也存在一些局限,例如,没有提供给使用者自定义密码映射的机会,并且本文研究的是较安静环境下的密码解锁表现,未来可以在多种不同的环境下研究使用情况.

References:

[1] Rawassizadeh R, *et al*. Wearables: Has the age of smartwatches finally arrived? Communications of the ACM, 2015,58(1):45−47.

[2] Shukla D, *et al*. Beware, your hands reveal your secrets! In: Proc. of the 2014 ACM SIGSAC Conf. on Computer and Communications Security. ACM, 2014. 904−917.

[3] Shin KI, Park JS, Lee JY, Park JH. Design and implementation of improved authentication system for android smartphone users. In: Proc. of the 26th Int'l Conf. on Advanced Information Networking and Applications Workshops (WAINA). 2012. 704−707.

[4] Truong KN, Thariq S, Daniel W. Slide to X: Unlocking the potential of smartphone unlocking. In: Proc. of the SIGCHI Conf. on Human Factors in Computing Systems. ACM, 2014. 3635−3644.

[5] De Luca A, Denzel M, Hussmann H. Look into my eyes! Can you guess my password? In: Proc. of the SOUPS 2009. ACM Press, 2009. 7:1−7:12.

[6] Aviv AJ, Gibson KL, Mossop E, Blaze M, Smith JM. Smudge attacks on smartphone touch screens. In: Proc. of the 4th USENIX Conf. on Offensive Technologies (WOOT 2010). 2010. 1−7.

[7] Johnston AH, Weiss GM. Smartwatch-Based biometric gait recognition. In: Proc. of the 2015 IEEE 7th Int'l Conf. on Biometrics Theory, Applications and Systems (BTAS). IEEE, 2015.

[8] Lu CX, Du B, Kan X, Wen H, Markham A, Trigoni N. VeriNet: User verification on smartwatches via behavior biometrics. In: Proc. of the 1st ACM Workshop on Mobile Crowdsensing Systems and Applications. 2017. 68−73.

[9] Johnston AH, Weiss GM. Smartwatch-Based biometric gait recognition. In: Proc. of the IEEE Int'l Conf. on Biometrics Theory, Applications and Systems. IEEE, 2015. 1−6.

[10] Roth V, Richter K, Freidinger R. A PIN-entry method resilient against shoulder surfing. In: Proc. of the 11th ACM Conf. on Computer and Communications Security. ACM, 2004. 236−245.

[11] De Luca A, Hertzschuch K, Hussmann H. ColorPIN: Securing PIN entry through indirect input. In: Proc. of the SIGCHI Conf. on Human Factors in Computing Systems. ACM, 2010. 1103−1106.

[12] Bianchi A, Oakley I, Kostakos V, Kwon DS. The phone lock: Audio and haptic shoulder-surfing resistant PIN entry methods for mobile devices. In: Proc. of the 5th Int'l Conf. on Tangible, Embedded, and Embodied Interaction. 2011. 197−200.

[13] Kumar M, Garfinkel T, Boneh D, Winograd T. Reducing shoulder-surfing by using gaze-based password entry. In: Proc. of the 3rd Symp. on Usable Privacy and Security. 2007. 13−19.

[14] Von Zezschwitz E, De Luca A, Brunkow B, Hussmann H. Swipin: Fast and secure pin-entry on smartphones. In: Proc. of the 33rd Annual ACM Conf. on Human Factors in Computing Systems. 2015. 1403−1406.

[15] Siek KA, Rogers Y, Connelly KH. Fat finger worries: How older and younger users physically interact with pdas. In: Proc. of the IFIP Conf. on Human-Computer Interaction. Berlin, Heidelberg: Springer-Verlag, 2005. 267−280.

[16] Harbach M, De Luca A, Egelman S. The anatomy of smartphone unlocking: A field study of android lock screens. In: Proc. of the 2016 CHI Conf. on Human Factors in Computing Systems. 2016. 4806−4817.

[17] Zhao Y, Qiu Z, Yang Y, Li W, Fan M. An empirical study of touch-based authentication methods on smartwatches. In: Proc. of the 2017 ACM Int'l Symp. on Wearable Computers. 2017. 122−125.

[18] Nguyen T, Memon N. Smartwatches locking methods: A comparative study. In: Proc. of the Symp. on Usable Privacy and Security (SOUPS). 2017.

[19] Lee WH, Lee R. Implicit sensor-based authentication of smartphone users with smartwatch. In: Proc. of the Hardware and Architectural Support for Security and Privacy. 2016.

[20] Lu CX, Du B, Kan X, Wen H, Markham A, Trigoni N. VeriNet: User verification on smartwatches via behavior biometrics. In: Proc. of the 1st ACM Workshop on Mobile Crowdsensing Systems and Applications. 2017. 68−73.

[21] Bianchi A, Oakley I, Kwon DS. Spinlock: A single-cue haptic and audio PIN input technique for authentication. In: Proc. of the Int'l Workshop on Haptic and Audio Interaction Design. Berlin, Heidelberg: Springer-Verlag, 2011. 81−90.

[22] De Luca A, Von Zezschwitz E, Huβmann H. Vibrapass: Secure authentication based on shared lies. In: Proc. of the SIGCHI Conf. on Human Factors in Computing Systems. 2009. 913−916.

[23] Deyle T, Roth V. Accessible authentication via tactile pin entry. Computer Graphics Topics, 2006,2:24−26.

[24] Kuber R, Yu W. Feasibility study of tactile-based authentication. Int'l Journal of Human-Computer Studies, 2010,68(3):158−181.

王鹏程(1996－),男,安徽天长人,硕士生,CCF 学生会员,主要研究领域为人机交互.

杨求龙(1993－),男,硕士生,CCF 学生会员,主要研究领域为人机交互.

涂华伟(1984－),男,博士,副教授,CCF 专业会员,主要研究领域为人机交互,智能计算.