软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2013,24(Suppl.(2)):1−13

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

基于用户节奏识别的触屏解锁方式*

文 龙[1], 吴晓波[1], 王建民[1,2]

[1](中山大学 信息科学与技术学院,广东 广州 510006)

[2](中山大学 传播与设计学院,广东 广州 510006)

通讯作者: 王建民, E-mail: mcswjm@mail.sysu.edu.cn

摘 要: 触摸屏屏幕锁定设计的初衷是为了防止用户的误操作,并未考虑到安全性,为此设计了一种以安全性为核心的全新的解锁方式.该解锁方式是基于行为密码的节奏性点触输入手势,节奏识别算法能够智能地识别用户在屏幕上敲击的节奏序列,提取节奏特征,形成解锁密钥.实验结果表明,该解锁方式能够较好地匹配节奏密钥,安全性能也大为提高;并且,节奏识别以个人的乐感体会为基准,注重用户体验,具备快捷性、娱乐性、可靠性等人机交互友好的特征.

关键词: 节奏识别;屏幕锁定;手势解锁;信息安全

中文引用格式: 文龙,吴晓波,王建民.基于用户节奏识别的触屏解锁方式.软件学报,2013,24(Suppl.(2)):1−13. http://www.jos.org.cn/1000-9825/13018.htm

英文引用格式: Wen L, Wu XB, Wang JM. Touch screen unlock methods based on user's rhythm recognition. Ruan Jian Xue Bao/Journal of Software, 2013,24(Suppl.(2)):1−13 (in Chinese). http://www.jos.org.cn/1000-9825/13018.htm

Touch Screen Unlock Methods Based on User's Rhythm Recognition

WEN Long[1], WU Xiao-Bo[1], WANG Jian-Min[1,2]

[1](School of Information Science and Technology, Sun Yat-Sen University, Guangzhou 510006, China)

[2](School of Communication and Design, Sun Yat-Sen University, Guangzhou 510006, China)

Corresponding author: WANG Jian-Min, E-mail: mcswjm@mail.sysu.edu.cn

Abstract: The screen lock of touch screen devices is designed to prevent the users' misuse without taking security into account. To solve this problem, this study provides a design of a secure scheme to unlock the touch screen. Unlike the traditional modes that unlock the touch screen by sliding the sliders or identifying the graphics and images, the presented design is a method to create a rhythm key based on the tapping gestures. The rhythm recognition algorithm is able to identify the rhythm sequence tapped on the screen, extracting rhythm features and creating the keys. Through testing, the new scheme can better match the rhythm gestures and improve the information security greatly. Meanwhile, as a new unlock method and relating to the individual's sense of music experience, the rhythm recognition focus on users' experience such as convenience, entertainment and reliability, all of which are human-computer interaction-friendly features.

Key words: rhythm recognition; screen lock; unlock gesture; information security

近年来,随着科技的发展,人们对移动信息终端的依赖越来越强,带有触摸屏的移动终端作为一种新型的交互设备得到了广泛普及和应用[1−5].移动智能触摸屏设备对信息的处理能力逐渐提高,网络也带来了超乎想象的强大功能[7].应用于触摸屏上的人机交互技术直接影响了一个系统的受欢迎程度和移动终端的市场占有率[6],但同时作为信息终端,尤其是包含有大量私人信息的移动设备,信息数据的安全性十分重要,一旦设备丢失或者被他人盗用,将对个人信息与财产安全产生巨大的威胁.触屏设备锁屏的设计初衷是为了防止用户在机器

* 基金项目: 国家自然科学基金(61073132); 中央高校基本科研基金(101gpy33)
收稿时间: 2012-06-15; 定稿时间: 2013-07-22

待机时发生误操作,有代表性的一类就是苹果公司的“滑动解锁”方案.而苹果公司已经获得了“滑动解锁”方案的技术专利,意味着所有带有类似滑动解锁功能的设备都将可以被指侵权.各大设备制造商为了规避技术侵权,推出了不同的解锁方案,比如直达功能的解锁[10]、三星的滑动整张壁纸图片进行解锁、HTC 的滑动圆环解锁等等方案.但均围绕防止误操作和提升用户体验方面设计的,在设备安全性保护方面考虑不足.

目前 Android 系统内置一款图形解锁方案,使解锁首次具备了一定的安全性,但是由于手势轨迹易被窥视,也存在容易被破解的风险.通过数学计算可知,Android 图案锁定规则可以设置的锁定图案总数为 986 328 个,其密码容量甚至小于 6 位纯数字密码,使用约 50MB 的密码表在 1s 内即可完成所有图形锁定的破解[11].并且其操作界面比较单调,用户体验度欠佳,往往被忽略,而且用户也不会浪费时间设置较为复杂的轨迹.谷歌公司也意识到移动设备信息安全的重要性,于是,Android 4.0 操作系统中植入了人脸识别功能[12].但一张照片就可以轻松破解,虽然后来加入了眨眼识别,但人脸识别在夜晚或者光线不充足的地方依旧无法使用.采用 PIN 密码解锁方案也面临同样的问题,为了照顾便捷性以及记忆难度,往往将密码控制在 4 位左右,无法抗拒穷举攻击,密码也极易被人窥探,界面单调乏味.可见,目前基于安全性的解锁方案都有明显的缺点.

为了真正解决移动触屏设备信息安全的问题,同时在滑动解锁这一传统交互模式上进行创新,本文设计了一种基于节奏识别的触屏手势解锁方式.手势是指人类用语言中枢建立起来的一套用手掌和手指位置、形状的特定的语言系统[8].手势可以快速传达丰富且大量的信息[9],也十分适用于触屏设备,因此便从手势开发与安全性方面展开研究.本文所设计的解锁方式不同于滑动拖拽、图形图像识别、密码匹配等传统方式,而是一种全新的、基于行为密码的节奏性点触输入手势.我们设计了一种节奏识别算法,该算法可以识别手指在屏幕上敲击出的节奏序列,提取节奏特征,形成解锁密钥.用户可以设置解锁密钥,在屏幕锁定时,敲击节奏序列,如果与预设的节奏序列相匹配,便可完成解锁.经过测试,该算法能够智能地识别用户的无级手势输入,密钥匹配率较高,安全性能也大为提高.

这种新型解锁方式不但保证了移动触屏设备的信息安全,而且兼备了手机解锁所要求的方便、快捷的特性和娱乐性,从而使用户体验大幅提升.这是以安全性为核心基于行为密码的全新解锁方式,以其所具有的方便性、快捷性、娱乐性、可靠性等人机交互友好的特征,必定会满足大量的市场需求,得到广泛应用.

1 节奏识别解锁方式

1.1 节奏识别设计思想

为了让触摸屏设备的屏锁具备安全性,根据密钥设置的基本思路,前期设计了几种预选方案.比如在屏幕上随机产生几张照片,让用户选择预先设定的那一张;或者让用户设置一串字符,解锁时在随机缺省的空位填写字符;或者把保险柜密码锁移植到屏幕上.但是各种方案都存在着以下几个方面共同的问题:

(1) 密钥空间太小,抵抗不住通过穷尽搜索的唯密文攻击;

(2) 图片或者字符容易被人偷窥,抵抗不住唯明文攻击;

(3) 提高解锁安全性就必须增加密钥长度或复杂度,这不但增加了用户记忆的负担,也必然会增大用户的操作难度.

如何设计一种解锁方法确保屏锁既具备高度的安全性,又不降低用户体验的娱乐性、快捷性.经过分析可以总结得出:指纹识别是提取指纹的细节点;人脸识别是通过不同算法从局部几何特征、面部拓扑图、线段距离等方面分辨人脸的特征;图形解锁是提取平面几何图形中轨迹的特征.于是我们想从上述方面获得启发,尝试着找到一种人类熟悉的认知方式,进行解锁方法的设计.音乐是抽象的艺术,能够调动人们的情感.人们之所以能够记住一首歌并且演唱出来是因为音乐不同于一般的声音,它的基本要素是节奏和旋律.通过对节奏和旋律的把握,人们可以准确地描述音乐.所以我们将节奏这一描述音乐的特征提取出来作为加密的突破口.每一个人都会在心里创造出不同的节奏,我们称为“心理节奏”.首先,心理节奏是深藏于人们内心的,使其不会像人脸识别或者声音识别那样被人复制而轻松击破;其次,心理节奏更倾向于一系列的“感觉”,他人可以记住你的解锁行为轨迹,可以记住你的字符密码,但是让他们精准地记住一系列的“感觉”是十分困难的.因此将节奏作为密钥,其安

全性优势十分巨大.

1.2 屏锁的技术要求

触摸屏设备的屏锁功能是面向用户的,用户经常性地使用,要求屏锁功能需具备简单实用、界面友好、稳定性高的特点;同时,由于屏锁本身的功能特点,又要求它能够具备一定的安全性,以保护触摸屏设备本身的数据安全和用户隐私.对于节奏识别的屏锁方式,为满足上述功能特点,其技术要求如下:

(1) 识别:将抽象的节奏准确地描述出来,提取其特征并构造节奏密钥,使其能够成为个人身份识别的唯一标识;

(2) 容差:节奏识别的屏锁方式要求用户预设一段节奏密钥,以后解锁时,匹配输入的节奏密钥是否与预设节奏密钥相匹配,以此判断解锁是否成功.由于用户的节奏输入每次都存在不确定性,不可能与预设的节奏序列完全一致.因此必须要求算法能够准确描述节奏,在一定的容差范围内匹配两段相近的节奏;

(3) 设防:节奏识别的主要出发点就是要提高解锁功能的安全性能,所以需要杜绝用户的胡乱输入以致解锁成功的可能,同时能够抵御各种常见的密钥攻击,诸如窥视、穷尽输入、暴力破解等.

1.3 节奏的识别与匹配

节奏的识别与匹配是本研究的重点,需要对节奏做到智能识别,提高识别成功率.无论是指纹识别、人脸识别、字符密码还是图形解锁,识别的特征或解锁密钥都是固定不变的,但是基于节奏识别的解锁方式却不同.虽然预先设置了固定的节奏序列,但是人非机器,不可能每次解锁时都能敲出与预设节奏完全一致的节奏,所以必须要考虑容差.人们敲打同一个节奏有时会稍快,有时又会稍慢,这就要求算法可以识别用户的无级输入,同一节奏的快慢皆可识别.对节奏的识别即是对节奏特征的提取,从哪个方面去识别决定着对节奏序列提取怎样的特征.前期我们尝试过各种方案.首先想到的最直接的方法就是记录两次敲击间隔时间Δt_i.这种方案能够初步描述节奏,但是只能识别所记录的固定节奏,而且容差不理想,容差所划分的区域之间无法解决边界问题,识别成功率低.为了解决用户无级输入的问题,做到快慢皆可解锁,我们引入了比例.以节奏输入序列最小间隔时间$\Delta t_{\min}$为基准,其他Δt_i与$\Delta t_{\min}$作商得到一个比例序列,并且通过算法将比值转化为正整数,做到一定容差.经过实际测试发现,虽然比例方案可以初步实现功能,但是存在着不足与漏洞.比如有时相聚很近的两点会被划分到不同比例序列,例如Δt_i=140ms,Δt_{i+1}=160ms,$\Delta t_{\min}$=100ms,虽然 140ms 和 160ms 只相差 20ms,但是它们却会被划分到两种比例中.为了更加准确地描述节奏序列的特征,我们将时间序列放到坐标系中去研究.试图通过时间序列反映在图像中的斜率去匹配,正如图 1 所示,如果序列图像与预设节奏序列很相似,即每一段的斜率误差与时间差控制在一定范围内,则认定两节奏匹配.但是经测试后发现,该方案过于灵敏.两点之间的斜率受两个端点影响,一旦两个端点都存在误差,那么对斜率影响就会比较大,超出容差的范围造成匹配失败.

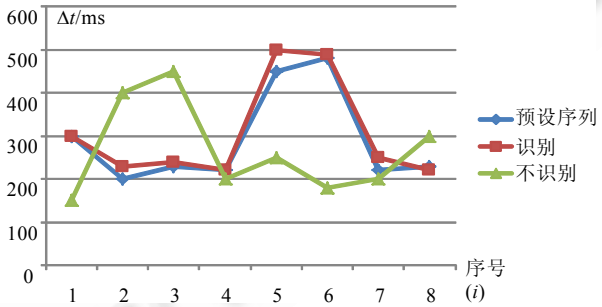

Fig.1 The show of rhythm recognition algorithm based on slope

图 1 基于斜率的节奏识别算法图示

前面几种方案都存在识别成功率低的致命问题,为了解决这一问题,我们设计了聚类方案,如图 2 所示,具体算法见第 3 节算法实现部分.经测试发现,识别成功率明显提升,接近 90%.经过进一步测试发现,有些明显不同的

节奏序列也可以通过匹配.说明聚类不当,导致识别过于模糊.

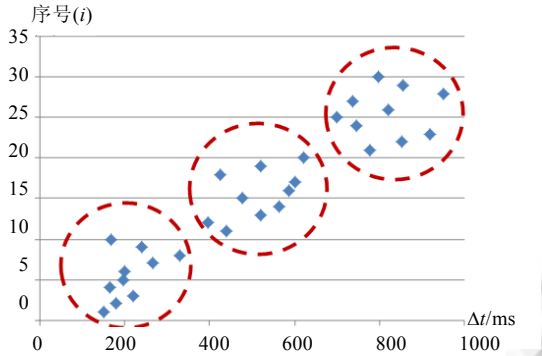

Fig.2 The show of rhythm recognition algorithm based on clustering

图 2 基于聚类的节奏识别算法图示

通过分析比较上述各种方案我们发现两个极端,一个是由于聚类粗糙导致识别过于模糊,成功率高但是失去了安全性;另一个是对于节奏序列每一段都进行特征提取,导致识别过于灵敏,虽然保证了安全性但是识别成功率不高.这是一对矛盾,也许将来通过算法的改进会在某一端产生突破,目前我们所给出的节奏识别算法就是取长补短,寻找最优的折中方案,既能保证解锁的成功率又能确保不失安全性.最终确定为聚类方案和特征识别相结合,并且进行了算法改进和参数调整,使得识别成功率和安全性都得到保障.详细算法过程见第 3 节.

1.4 节奏密钥的构造

节奏识别算法的任务便是完成对节奏的识别,并构造节奏密钥,用以形成触摸屏的解锁密钥.在节奏识别算法中,对节奏序列的密钥构造分 3 方面进行:

(1) 对用户在触摸屏设备屏幕上的节奏敲击序列,提取其所敲击触点的个数,用以形成密钥长度 *length*;

(2) 对用户在触摸屏设备屏幕上的节奏敲击序列,提取其所敲击触点的位置属性,用以形成位置序列 *location*[*length*];

(3) 对用户在触摸屏设备屏幕上的节奏敲击序列,提取其所敲击触点的节奏特性,具体使用敲击序列的时间间隔序列 *time*[*length*−1],用以形成节奏序列 *rhythm*[*length*−1].

解锁时,屏锁系统会针对用户输入的节奏敲击序列,提取密钥长度、位置序列和节奏序列这 3 个参数,分别与预先设置的节奏密钥的相关参数进行匹配,任何一项不匹配,就判断节奏密钥错误,解锁失败.如图 3 所示.

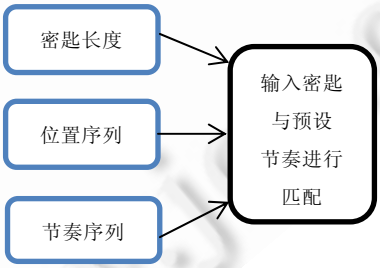

Fig.3 The rhythm key matching process

图 3 节奏密钥匹配过程

从对节奏密钥的构造方式来看,解锁者需要对节奏敲击序列的触点个数、位置属性和节奏特性 3 方面都完全熟知才能解锁成功.这些是节奏敲击的一系列的“感觉”,只有本机用户自己知道,因此非本机用户想要破解节奏密钥是非常困难的,就算知道触点个数和位置属性,对于节奏敲击的“感觉”也是很难复制的.

2 节奏识别屏锁应用框架

基于上述讨论,本文设计了一种基于节奏识别的触屏解锁方式.该方式不同于其他基于移动拖曳、图形图像识别、数字密码等传统的触屏解锁方式,而是把节奏特征与行为密码结合起来,是一种全新的交互模式.即在触摸屏设备上实现一种节奏识别算法,把用户在屏幕上通过一定方式敲击的节奏序列作为密钥,通过判断用户输入的节奏序列与预设节奏序列是否匹配,从而判断解锁是否成功,完成对用户身份的识别.

2.1 屏锁系统结构模型

触摸屏设备包括智能手机、平板电脑、个人数字助理、数码相框、数码播放器等移动终端,这些设备的共性是具有一个触摸屏,用户可以通过对触摸屏的触压、敲击、滑动等操作,完成对设备数据的查看、编辑、存储、删除等处理.

为了把本节奏识别屏锁方式应用到触摸屏设备上,我们设计了相应的触屏系统结构模型,如图 4 所示.该系统包括获取模块、运算模块、解锁模块和设置模块 4 个基本模块,其中,运算模块可分为位置运算模块和节奏运算模块,具体模块功能说明如下:

(1) 获取模块,具备位置传感器和计时器功能,以获取位置信息和时间信息,用于当触摸屏设备处于锁定工作模式时,获取用户连续敲击触摸屏所形成的一组触点序列的位置信息 *location*[*length*]和时间信息 *time*[*length*].获取模块还具备判断敲击的触点序列是否结束的功能,通过设置一个时间阈值,若超过该时间阈值再无敲击动作,则判定触点序列敲击完毕.

(2) 运算模块,用于根据触点序列的位置信息和时间信息,通过节奏识别算法,提取所述触点序列的位置属性和节奏特性.运算模块包括位置运算模块和节奏运算模块,位置运算模块根据获取模块提供的触点序列的位置信息,分析每一个触点在所述触摸屏上的相对位置关系,以标记触点序列的位置属性;节奏运算模块以获取模块提供的触点序列时间信息作为输入,采用一定的识别算法,计算出一组数据,以标记触点序列的节奏特性.

(3) 解锁模块,进行判断操作和解锁操作,用于当解锁的敲击触点序列的位置属性和节奏特性与预先设定的解锁触点序列的位置属性和节奏特性相符合时,执行解锁操作,以使所述触摸屏终端切换为非锁定工作模式.

(4) 设置模块,用于使用户通过连续敲击触摸屏对经获取模块以及运算模块获得的触点序列进行多次确认,以设定或者更改触摸屏设备的解锁敲击触点序列.

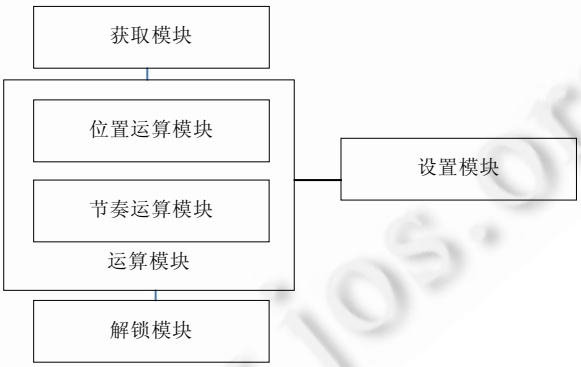

Fig.4 The structure model of screen lock system

图 4 屏锁系统结构模型

2.2 节奏密钥构造模型

在实际应用中,在触摸屏上设置左右两个感应区域,用户可以通过手指在屏幕上敲击左右两个感应区域,形成左右顺序、快慢不同的敲击节奏序列.节奏识别算法以敲击屏幕锁形成的节点时间间距序列作为输入,通过一定的策略,提取节奏特征,包括上文所述的密钥长度 *length*、位置序列 *location*[*length*]和节奏序列 *rhythm*[*length*−1],形成节奏密钥,该密钥标记了敲击序列的节奏属性.节奏密钥构造模型如图 5 所示.

Fig.5 The structure model of rhythm key

图 5 节奏密钥构造模型

2.3 屏幕解锁模型

用户首先预设触摸屏设备的解锁密钥,解锁时,触摸屏设备针对用户输入的节奏序列进行密钥匹配,判断是否解锁成功.屏幕解锁模型如图 6 所示.

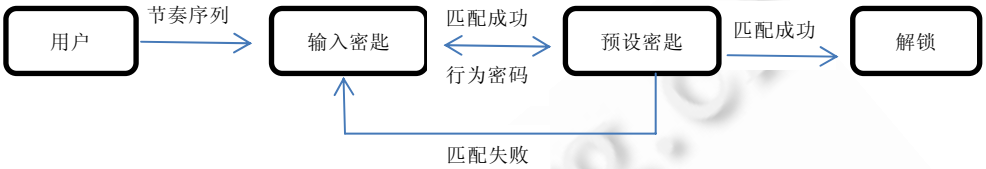

Fig.6 The model of unlocking screen

图 6 屏幕解锁模型

3 节奏识别算法

用户输入节奏序列后形成节点时间间距序列,通过节奏识别算法,可以构造节奏密钥.设整数 *length* 记录节点序列长度,数组 *time*[*length*−1]记录节点时间间距(以毫秒计),*time*[*length*−1]反映的是节点敲击的快慢程度.

节奏识别算法的任务是使用适当的方法,把这个时间序列 *time*[*length*−1]表示成节奏密钥,以匹配特征相同或近似的时间序列.我们曾实验过比例、划分区间、函数斜率等方式,但都出现匹配过于灵敏或边界划分不合理等问题,不能很好地反映时间序列的离散聚合程度.经过反复实验,我们最终设计了一种基于聚类思想的节奏识别算法,能够较好地划分聚类,把时间节点归类到合适的类别中去.作为对聚类算法的辅助补充,另外设计了一种时间突变算法,有效地增强了对时间序列的特征描述和密钥的抗攻击性.

3.1 聚类算法

聚类算法的基本思想是选取若干个聚类中心,采用一定的聚类策略,把时间点归类到聚类中心去,用数字“1,2,3...”标记每个时间点的聚类结果,形成节奏序列.

聚类算法以时间节点长度 *length* 和时间间距序列 *time*[*length*−1]作为输入.记聚类中心个数为 *centerNum*,聚类中心为 *groupCenter*[*centerNum*],时间宽度为 *wide*,节奏序列为 *rhythm*[*length*−1],相关公式如下:

$$wide = \mathrm{Max}(time[i]) - \mathrm{Min}(time[i]) \tag{1}$$

$$centerNum = \begin{cases} wide/R_2 + 1, & wide\%W_2 \leqslant R_2 - R_1 \\ wide/R_2 + 2, & wide\%W_2 > R_2 - R_1 \end{cases} \tag{2}$$

$$rhythm[i] = \begin{cases} 1, & centerNum = 1 \\ j+1, & centerNum \neq 1 \end{cases} \tag{3}$$

其中,

$$i \in [0, length-2], j \in [0, centerNum], groupCenter[j+1] - groupCenter[j] \geqslant R_2,$$

$$|time[i] - groupCenter[j]| < R_1 \text{ OR } |time[i] - groupCenter[j]| \leqslant |time[i] - groupCenter[j+1]|.$$

在上述公式中,R_1=50,R_2=250 是聚类约束参数,R_1 表示聚类半径,R_2 表示聚类间距,聚类算法步骤如下:

输入:节点个数 *length*,时间序列 *time*[*length*−1].

Step 1. 初始化整型数组 *rhythm*[*length*−1];

Step 2. 对 *time* 进行从小到大排序

Step 3. *wide*=*time*[*length*−2]−*time*[0], if *wide*<=R_2−R_1 goto Step 4;

else goto Step 5;

Step 4. for i=0 to $length-2$, $ryhthm[i]$=1, 结束算法;

Step 5. 对 $time$ 进行聚类

Step 5.1. $centerNum=wide/R_2+1$, if $wide\%R_2>R_2-R_1$, $centerNum$++;

Step 5.2. $groupSum=setSum=j=0$, $groupCenter[j]=time[j]$;

Step 5.3. for i=0 to $length-2$, if $|time[i]-groupCenter[j]|<R_1$

then $groupSum+=time[i]$, $setSum$++, $rhythm[i]=j+1$;

Step 5.4. $groupCenter[j]=groupSum/setSum$;

Step 5.5. for i=0 to $length-2$, if $time[i]-groupCenter[j]>R_2-R_1$

then $groupCenter[j++]=time[i]$, $groupSum=setSum=0$, goto Step 5.3;

Step 5.6. 没有聚类新的聚类中心, if 所有点已聚类 then 结束算法;

else goto Step 6;

Step 6. 对未聚类的节点进行聚类($rhythm[i]=0$)

Step 6.1. for i=0 to $length-2$, if $time[i]>groupCenter[j]$ then $rhythm[i]=j$;

Step 6.2. for k=0 to j, loop Step 6.3~Step 6.4;

Step 6.3. for i=0 to $length-2$, if $groupCenter[k]<time[i]<groupCenter[k+1]$

and $time[i]-groupCenter[k]<groupCenter[k+1]-time[i]$ then $rhythm[i]=k+1$;

else goto Step 6.4;

Step 6.4. $mid=(groupCenter[k]+groupCenter[k+1])/2$,

if $rhythm[i-1]=k+1$ and $time[i]-time[i-1]<=R_1$ and $time[i]-mid<=W_1/2$;

then $rhythm[i]=k+1$;

else $rhythm[i]=k+2$;

输出:$rhythm[length-1]$.

3.2 突变算法

聚类算法很好地实现了对节点进行归类的功能,能够描述一个节点序列的离散聚合程度,但另一方面,却忽略了节点序列的函数特性,而描述这类特性能够有效地增强密钥的抗攻击性.根据时间序列的增减特性,针对前后两个时间构成突然增大或突然减小,定义时间正突变和负突变.设时间突变序列为 $change[length-2]$,其取值为 1,−1 和 0,分别表示正突变、负突变和无突变.

时间突变算法相关计算公式如下:

相邻时间间隔:

$$\mathrm{d}t[i]=time[i+1]-time[i],\ i=0,1,2,\ldots,length-3 \tag{3}$$

平均正增长:

$$posiAver=\frac{\sum \mathrm{d}t[i]}{N_1},\ \mathrm{d}t[i]>0 \tag{4}$$

平均负增长:

$$negeAver=\frac{\sum \mathrm{d}t[i]}{N_2},\ \mathrm{d}t[i]<0 \tag{5}$$

$$change[i]=\begin{cases}1, & \mathrm{d}t[i]>posiAver\ \&\&\ \mathrm{d}t[i]>W_1\ \|\ \mathrm{d}t[i]>W_2\\ -1, & \mathrm{d}t[i]<negeAver\ \&\&\ \mathrm{d}t[i]<-W_1\ \|\ \mathrm{d}t[i]<-W_2\\ 0, & \text{其他}\end{cases} \tag{6}$$

其中,W_1=100,W_2=200 是突变约束参数,W_1 表示突变至少满足条件,W_2 表示突变直接触发条件.

时间突变算法步骤如下:

输入:节点个数 *length*,时间序列 *time*[*length*−1].

Step 1. 初始化整型数组 *change*[*length*−2]和 d*t*[*length*−2],

$posiSum=negeSum=N_1=N_2=0$;

Step 2. for i=0 to *length*−3, do d$t[i]=time[i+1]-time[i]$;

Step 3. for i=0 to *length*−3, if d$t[i]>0$ then $posiSum$+=d$t[i]$, N_1++;

else if d$t[i]<0$ then $negeSum$+=d$t[i]$, N_2++;

Step 4. $posiAver=posiSum/N_1$, $negeAver=negeSum/N_2$,

for i=0 to *length*−3, if d$t[i]>posiAver$ and d$t[i]>W_1$ or d$t[i]>W_2$

then $change[i]=1$;

else if d$t[i]<negeAver$ and d$t[i]<-W_1$ or d$t[i]<-W_2$

then $change[i]=-1$;

else $change[i]=0$;

输出:*change*[*length*−2].

4 应用与测试

4.1 算法测试

为了进行有效的算法分析,使用 MFC 编写了一个节奏识别算法程序,由键盘左右方向键输入节奏序列,测试节奏识别算法对输入节奏序列的响应(生成密钥).

如图 7 所示,为 MFC 测试节奏识别算法图.

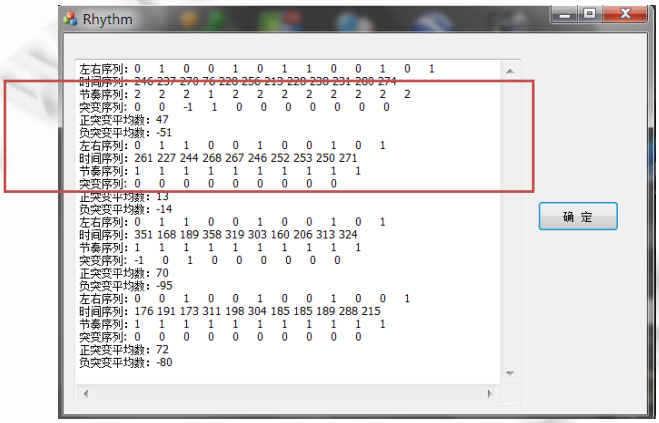

Fig.7 The MFC rhythm recognition algorithms testing program

图7 MFC节奏识别算法测试程序

4.1.1 聚类算法测试

分别敲击两次大致的快、中、慢 3 种节拍的节奏序列,形成 *time* 数组,见表 1.

Table 1 The first group testing data

表 1 测试数据 1

序号 i / $time[i]$	1	2	3	4	5	6	7	8	9	10
序列1	120	123	145	150	136	370	350	324	400	354
序列2	720	699	800	750	723	754	726	220	234	241
序号 i / $time[i]$	11	12	13	14	15	16	17	18	19	20
序列1	600	645	623	390	405	123	145	162	150	142
序列2	258	246	300	305	250	460	450	464	705	745

经过聚类算法,可以发现两个序列分别被聚成了 3 类,如图 8 所示.

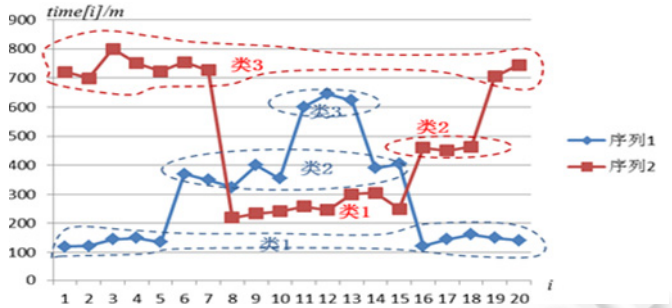

Fig.8 The clustering results
图8 聚类结果

4.1.2 突变算法测试

分别敲击 3 段节奏序列,形成 *time* 数组,见表 2.

Table 2 The second group testing data
表 2 测试数据 2

序号 *i* / *time*[*i*]	1	2	3	4	5	6	7	8	9	10
序列1	254	242	253	250	259	256	267	259	261	254
序列2	124	132	124	162	150	123	147	158	162	148
序列3	620	587	568	657	588	578	300	320	321	350
序号 *i* / *time*[*i*]	11	12	13	14	15	16	17	18	19	20
序列1	261	256	284	265	281	261	274	267	256	247
序列2	430	450	444	421	468	520	479	500	510	495
序列3	344	120	140	125	130	145	121	420	430	140

经过突变算法,可以发现序列 1 中各序列起伏不大,没有突变;序列 2 中有一个正突变,序列 3 分别有 1 个正突变和 3 个负突变.如图 9 所示.

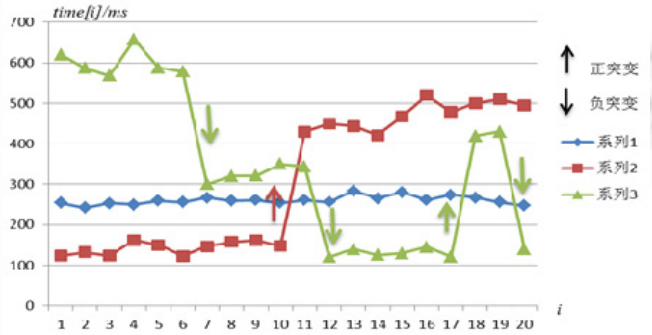

Fig.9 The mutation results
图9 突变结果

随机敲击一段快慢不一的序列,得到 *time* 数组,见表 3.

综合使用聚类算法和突变算法,得到的结果如图 10 所示.

Table 3 The third group testing data

表3 测试数据3

序号 i / $time[i]$	1	2	3	4	5	6	7	8	9	10
序列1	240	320	220	150	170	220	480	560	580	500
序号 i / $time[i]$	11	12	13	14	15	16	17	18	19	20
序列1	580	240	210	310	350	450	800	950	808	818
序号 i / $time[i]$	21	22	23	24	25	26	27	28	29	30
序列1	858	488	588	600	520	500	550	500	440	900
序号 i / $time[i]$	31	32	33	34	35					
序列1	980	560	550	520	560					

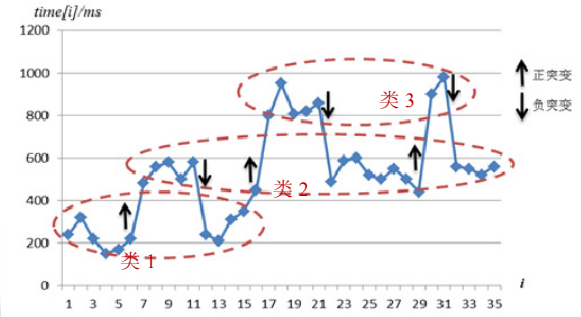

Fig.10 The clustering and mutation results

图10 聚类和突变结果

4.1.3 密钥匹配测试

首先敲击预设序列,通过聚类和突变算法,得到节奏序列为 *rhythm*={2,1,1,2,1,1,2,1,1,2,2},突变序列为 *change*={–1,0,1,–,1,0,0, –1,0,0,0},然后再敲击其他序列,测试密钥匹配情况,得到 *time* 数组,见表 4.

Table 4 The forth group testing data

表4 测试数据4

序号 i / $time[i]$	1	2	3	4	5	6	7	8	9	10	11
预设	469	185	277	452	198	334	448	220	331	500	443
序列1	424	198	252	414	197	280	418	191	309	492	444
序列2	473	226	263	486	231	296	511	237	305	528	462
序列3	253	122	169	351	145	202	347	150	240	397	364
序列4	719	435	527	702	448	584	698	470	601	750	693
序列5	191	248	491	204	267	504	209	287	537	204	271
序列6	380	350	352	384	394	320	464	250	340	320	325

经过节奏识别算法发现,序列 1~序列 3 与序列 4 均能匹配,而序列 5 和序列 6 不能匹配.如图 11 所示.

序列 1 和序列 2 可以匹配,是因为与预设序列较为接近,而序列 4 和序列 5 能够匹配,是因为它们的节奏特征是一致的(同一种节奏可以有快慢),序列 5 和序列 6 不匹配是因为节奏特征不符合.可见算法对节奏特征相似的时间序列都能匹配,但对于节奏特征不符合的序列,则有效摒除.

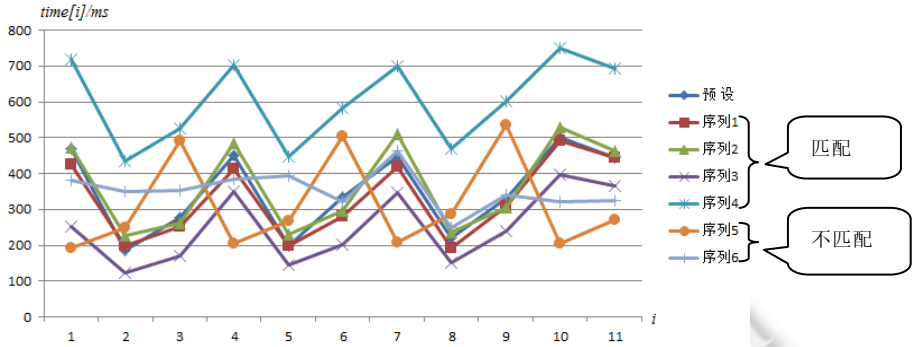

Fig.11 The showing of key match

图11 密钥匹配图示

4.2 解锁性能测试

为了验证节奏识别的解锁性能,在 Android 2.2 手机平台上,开发了一个节奏识别屏锁软件,该软件的锁屏界面上有两个左右分布的鼓形图案(如图 12 所示),手指敲击鼓形图案可以形成左右顺序、快慢不一的节奏序列.使用节奏识别算法提取敲击序列的节奏特征,形成解锁密钥,测试其解锁性能.

Fig.12 The interface of Android screen lock software

图12 Android屏锁软件界面

4.2.1 用户体验测试

使用搭载 Android 2.2 操作系统的智能触屏手机,先后让 10 位使用者进行测试,让其自行设置节奏密钥,在屏幕锁定后进行解锁,统计密钥长度、解锁成功与失败次数,见表 5.

Table 5 The unlock users' experience datas

表 5 解锁用户体验数据

密钥长度	解锁成功	解锁失败	成功率(%)
4	483	22	95.64
5	473	32	93.66
6	469	39	92.32
7	463	43	91.50
8	460	46	90.90
9	457	48	90.49
10	454	50	90.07

随着密钥长度的递增,解锁成功率呈略微下降之势,但仍接近 90%,可见节奏识别稳定性较高,用户体验良好.

4.2.2 安全性能测试

用户自己预先设置密钥,只告诉密钥长度,让他人来进行暴力解锁,统计解锁成功与失败的次数,见表 6.

Table 6 The violent unlock users' experience datas

表 6 暴力解锁用户体验数据

密钥长度	解锁成功	解锁失败	成功率(%)
4	14	492	2.77
5	11	494	2.19
6	9	496	1.78
7	5	502	0.99
8	3	510	0.58
9	2	548	0.36
10	1	574	0.17

可见,对于暴力解锁,成功率非常低,节奏识别的安全性较高.

5 总结与展望

随着信息时代的飞速发展,人们对移动智能终端的依赖性越来越强.移动终端上大量的数据与私人信息的安全性也日益凸显.目前,种类繁多的解锁方式都不具备安全性,几种具备安全性的解锁方式也各有不足,其中还夹杂着激烈的专利之争.基于这种情况,根据市场需求,本文设计了一种基于节奏识别的触屏解锁方式,采用行为密码的思想,提取用户敲击屏幕的节奏特征,生成一种描述节奏特征的密钥.该解锁方式构思新颖,使用方便,在提升用户体验的同时大大增强了屏锁安全性.

该解锁方式的核心是节奏识别算法,我们通过大量的测试,最后采用了基于聚类和提取函数特征的思想,构造出聚类算法与时间突变算法,该算法对于用户输入的无级时间序列,能够有效地提取聚类特征和时间突变特性,在兼顾模糊识别与灵敏识别的同时,对特征相似的时间序列能够有效匹配,对不符合特征的序列则能有效屏蔽.

目前,该解锁方式已在 Android 手机平台上通过了测试,解锁软件的性能稳定,用户体验良好,用户在敲击节奏序列体验到方便快捷、娱乐有趣的同时,也增强了屏锁的安全性,不同人有不同的节奏体验,他人即使看到密钥输入过程,也很难破解.

下一步,我们打算在节奏识别密钥的构造、存储和识别上加以深入研究,加进校验码冗余的思想,从信息存储的角度来完善对密钥的管理,允许密钥在比对上存在一定的差错;在密文存储过程中对明文进行 SHA-1 散列,以增强安全性.

致谢 在此,我们向对本文研究提供过帮助的老师和同学表示感谢.

References:

[1] Dong SH. Progress and challenge of human-computer interaction. Journal of Computer-Aided Design & Computer Graphics, 2004, 16(1):1−13 (in Chinese with English abstract).

[2] Zhang GH, Heng XA, Ling YX, Lao SY. Interaction gesture analysis and design based on multi-touch surface. Application Research of Computers, 2010,27(5):1737−1739, 1752 (in Chinese with English abstract).

[3] Ling YX, Zhang GH, Li R, Ye T. Research on natural gesture recognition method based on multi-touch. Journal of National University of Defense Technology, 2010,32(1):127−132 (in Chinese with English abstract).

[4] Du D. Design and realization of human-machine interface based on touching screen of duplicator stencil duplicator. Chinese Journal of Liquid Crystals and Displays, 2007,22(2):217−221 (in Chinese with English abstract).

[5] Li WS, Deng CJ, Lü Y. Interaction gesture analysis based on touch screen. Chinese Journal of Liquid Crystals and Displays, 2011, 26(2):194−199 (in Chinese with English abstract).

[6] Yu YN. Research and implementation of man-machine interaction based on android platform [MS. Thesis]. Beijing: Beijing University of Posts and Telecommunications, 2011 (in Chinese with English abstract).

[7] Wu YH. 3G Era of mobile media development advantages. News World, 2010,(5):161−162 (in Chinese with English abstract).

[8] Ye ZP, Wang XY. A directly to function interface of mobile phone unlock method. Chinese Invention Patent, CN101827172A, 2010-09-08 (in Chinese).
[9] Sun Y. Android security protection mechanism and decryption. Netinfo Security, 2013,(1):71−74 (in Chinese with English abstract). [doi: 10.3969/j.issn.1671-1122.2013.01.019]
[10] Wang Y, Pan R. The gesture design principles of the mobile terminal interaction design. Modern Decoration (Theoretical), 2012, (8):178−179 (in Chinese with English abstract).
[11] Gu YH, Shi Y. Treatise on the development trend of mobile phone interface design. Journal of Huaiyin Institute of Technology, 2010,19(1):54−57 (in Chinese with English abstract).
[12] Peng EH. Face recognition to unlock the phone. Chinese Invention Patent, CN202009428U, 2011-10-12 (in Chinese).

附中文参考文献:

[1] 董士海.人机交互的进展及面临的挑战.计算机辅助设计与图形学学报,2004,16(1):1−13.
[2] 张国华,衡祥安,凌云翔,老松杨.基于多点触摸的交互手势分析与设计.计算机应用研究,2010,27(5):1737−1739,1752.
[3] 凌云翔,张国华,李锐,叶挺.基于多点触摸的自然手势识别方法研究.国防科技大学学报,2010,32(1):127−132.
[4] 杜德.基于触摸屏的数码一体机人机界面设计与实现.液晶与显示,2007,22(2):217−221.
[5] 李文生,邓春健,吕燚.基于触摸显示屏的人机交互手势分析.液晶与显示,2011,26(2):194−199.
[6] 郁亚男.基于 Android 平台的人机交互的研究与实现[硕士学位论文].北京:北京邮电大学,2011.
[7] 吴义辉.#G 时代我国手机媒体发展优势.新闻世界,2010,(5):161−162.
[8] 叶志平,王先毅.一种使手机解锁后直接到达功能界面的方法.中国专利,CN101827172A,2010-09-08.
[9] 孙奕.Android 安全保护机制及解密方法研究.信息网络安全,2013,(1):71−74. [doi: 10.3969/j.issn.1671-1122.2013.01.019]
[10] 王垚,潘荣.移动终端交互设计中手势设计原则初探.现代装饰(理论),2012,(8):178−179.
[11] 顾炎辉,石莹.手机人机交互界面设计趋势探究.淮阴工学院学报,2010,19(1):54−57.
[12] 彭恩厚.人脸识别解锁的手机.中国专利,CN202009428U,2011-10-12.

文龙(1990－),男,黑龙江哈尔滨人,学士,主要研究领域为人机交互技术与可用性,嵌入式媒体技术,数字娱乐软件技术.
E-mail: wenhenlongsysu@gmail.com

王建民(1973－),男,博士,教授,CCF 会员,主要研究领域为人机交互技术与可用性,嵌入式媒体技术,数字娱乐软件技术.
E-mail: mcswjm@mail.sysu.edu.cn

吴晓波(1989－),男,学士,主要研究领域为人机交互技术与可用性,嵌入式媒体技术,数字娱乐软件技术.
E-mail: wxboston@gmail.com