

信息安全工程课题研究

|  |  |
| --- | --- |
| 题目： | PINSlide |

|  |  |
| --- | --- |
| 成 员： | 任昆鹏 陈炘 马明仪 卜天童 |
| 院 系： | 软件与微电子学院 |
| 导师姓名： | 孙惠平 |

二〇一七年 十二月

# **目录**

[第一章 选题背景 2](#_Toc502703157)

[第二章 产品现状 3](#_Toc502703158)

[第三章 研究现状 4](#_Toc502703159)

[第四章 主要思路 6](#_Toc502703160)

[第五章 项目分工 7](#_Toc502703161)

[第六章 项目实现 8](#_Toc502703162)

[第七章 项目总结和收获 21](#_Toc502703163)

# 选题背景

1994 年，IBM 与 BellSouth 合作制造的具有里程碑意义的 IBM Simon 手机问世，这也是被世界所公讣的第一部智能手机。而真正被众多消费者记住，并极大的促进了行业的发展和人们生活、工作模式的转变的智能手机，则非苹果公司于2007 年推出的 iPhone 系列智能手机莫属。谷歌公司在 2008年推出的搭载 Android 系统的智能手机 G-Mobile，标志着智能手机时代的正式来临。随着智能手机操作系统功能的日益进步，处理器功能的日益强大，大屏化趋势越来越流行，智能手机不仅对非智能手机造成替代，也影响了人们办公和娱乐习惯的改变智能手机相对于功能手机来说，有更人性化的操作系统，更强大的功能，我们使用手机来进行社交、收发邮件、记录自己的行程安排，离开了智能手机几乎寸步难行。

智能手机在为我们提供便利的同时，也掌握了大量的个人隐私信息，其安全性也越来越引起人们的关注。目前主流的智能手机操作系统（IOS 和 Android）都提供了解锁机制来保护手机。IOS 的目前的解锁机制为使用指纹四位 PIN 码解锁。Android 系统的传统解锁机制除了四位 PIN 码解锁外，还有九点模式（Pattern Lock）解锁机制。然而传统的解锁模式不仅不能抵抗污渍攻击和肩窥攻击，而且存在密码空间小，容易遭到暴力攻击的问题。因此，主流手机操作系统都开发了基于生物特征的认证机制。最新的安卓和IOS系统手机都加入了指纹解锁机制。指纹解锁机制虽然用户体验方便，但是由于其安全率不高，和指纹伪造易使该机制受到攻击。同时，指纹识别由于需要额外的硬件，使得用户在不更换手机的情况下就无法使用该机制。苹果最新发布的IPhoneX手机支持FaceID人脸识别系统，这无疑是现在智能手机解锁机制的一大突破。PINSlide通过生物学认证与PIN码结合用于替代传统的PIN码机制，能够有效弥补现在的指纹解锁等机制的缺陷。

# 产品现状

1. **PIN码口令认证机制**

智能手机上传统的四位口令认证机制虽然广泛使用，但是四位口令的弱安全性是广为人知的。首先易于被人们记忆的都是弱密码，很容易被暴力破解或被攻击者进行猜。PIN码口令空间较小，容易遭受暴力攻击。对于 4 位 PIN 码，用户一般会选择与自己相关的 4 位数字（如自己和家人的生日）或简单的易于记忆的四位数（如 1234 和 0000）。因此若攻击者对用户稍作调查，猜测攻击的成功性就能大大增加。4 位 PIN 码口令机制同样面临着很大污渍攻击 （SmudgeAttack）挑战，攻击者能够通过屏幕污渍猜解口令从而达到攻击。4位PIN码在肩窥攻击防护方面也是十分薄弱的。

1. **Pattern Lock 图形口令机制**

Pattern Lock 图形口令机制是安卓操作系统用于替代4位PIN码机制的另一个广泛使用的口令机制。该机制通过滑动输入代替pin码的点击输入，大大改善了用户的认证时间和认证体验操作。Pattern Lock 图形口令机制，虽然在用户体验上面有很大的提升，但是就安全性而已相对于4位PIN码并没有太大的提高， PatternLock和PIN码一样易受到猜测攻击、污渍攻击、肩窥攻击。

1. **指纹认证机制**

苹果公司在 2014 年推出的 IPhone5s 上搭载了指纹识别器作为身份验证的工具后，指纹认证机制就成为主流手机的认证机制之一。指纹认证借助人们身体的生物特征，解决了传统的身份认证方式存在着一些问题， 如口令和密钥存在易忘记、易被攻击和易泄露。指纹认证拥有生物识別技术共有的不易遗忘和丟失、不易伪造和盗窃、可以“随身携带”、 随吋随地使用等优点每个人的指纹是独一无二的，并且相当稳定，指纹不会随年龄的增长和身体健康状况的变化而变化。而且指纹的扫描速度很快．使用非常方便。因此指纹认证在智能手机上的运用发展十分迅猛。指纹认证虽然方便且误报率低，但是用户可以用来 修改指纹的次数是极其有限的，因为指纹永久不变而每个人通常只有十指，如果攻击者能够成功复制用户的指纹，那么应用指纹认证的手机很难通过修改指纹进行预防指纹复制攻击。

# 第三章 研究现状

**1、智能手机解锁机制面临的威胁**

智能手机解锁机制面临的威胁主要有猜测攻击或暴力攻击、污渍攻击、肩窥攻击。

猜测攻击或暴力攻击：是四位口令和 9 点 Pattern Lock 机制最容易遭受到的攻击。4 位 PIN 码机制和 Pattern Lock 图形口令机制都是基于用户记忆的口令机制，即“What You Know”的模式。两个机制都存在口令空间较小的弱点，容易遭受暴力攻击。对于 4 位 PIN 码，用户一般会选择与自己相关的 4 位数字（如自己和家人的生日）或简单的易于记忆的四位数（如 1234 和 0000）。因此若攻击者对用户稍作调查，猜测攻击的成功性就能大大增加。同样，对于 Pattern Lock 机制，用户为了记忆方便趋向于设置简单的图形，因此增大了攻击者猜测攻击的成功率。

污渍攻击 （SmudgeAttack）：指攻击者通过用户手指在手机屏幕滑动时留下的污渍辨别用户输入的内容。对于使用传统的 4 位 PIN 码作为手机解锁机制的用户，由于键盘的位置是固定的，攻击者很容易根据用户手指点击留下的污渍猜测用户输入的 4 位 PIN 码进行攻击。而对于使用 Pattern Lock 解锁机制的，污渍攻击也是很有效的攻击方法。攻击者同样可以根据屏幕上留下的滑动痕迹猜测用户设置的密码图案。

肩窥攻击：是一种利用直接观察就可以得到所需要信息的攻击技术。肩窥攻击可分为一次发现攻击和多次发现攻击。攻击者进行一次发现攻击时，可以通过直接偷窥用户的合法输入后进行攻击。而在多次发现攻击中，攻击者可以多次直接偷窥用户合法输入并回放用户输入进行攻击。

2、智能手机上的生物学认证

生物识別技术是借助人们身体的某种特征．如指纹，声音、眼睛的虹膜，甚至身体的气味进 行身份识别的技术。生物识別技术共有不易遗忘和丟失、不易伪造和盗窃、可以“随身携带”、随吋随地使用等优点，广泛应用于身份认证、出人口管理、电子商务、电子政务等领域。目前生物学认证主要分为两大领域：基于生理特征的认证（如声音特征、面部特征 等）以及基于行为特征的认证（如击键特征、滑动特征和手势特征等）。

生理特征认证即通过人的生理特征，如指纹和面部特征等识别个人身份。指纹识别

和需要特殊的硬件支持。苹果公司在 2014 年推出的 IPhone5s 上搭载了指纹识别器作为身份验证的工具，安卓手机厂商随后也推出了支持指纹认证的手机。指纹指的是指端表面的纹路。其中凸起的纹线称为脊（ridge），脊之间的部分称为谷 (VaⅡey) 。指纹的纹路并不是连续，平滑流畅的，而是经常出现中断、分叉或转折等，这样就形成了一系列的特征点，而这些特征点对每个人均是不同的 、与生俱来的、终身不变的，因而提供了身份识别的信息。

与基于生理特征的认证机制不同，智能手机上基于行为特征的认证机制是根据用户

与手机交互的行为特征进行判断。该机制不需要使用额外的硬件支持，仅通过手机屏

幕和其他手机搭载的传感器收集用户的动作数据，并使用机器学习算法学习用户的行

为特征用作认证。

前对基于行为特征的认证的研究方向主要包括击键特征认证、滑动特征认证以及手势特征认证。击键特征认证是指用户点击键盘的行为特征作为认证因子进行认证。滑动特征认证机制根据手指在屏幕上进行滑动动作时产生的特征数据进行认证。比如利用用户在屏幕上滑动时产生的压力、按压面积以及滑动的轨迹等特征作为认证因子。由于每个人的手掌都有一定的生理特征，因此在做手势的过程中，会产生因人而异的行为特征。

3、智能手机上的滑动输入

滑动输入，即 Word-Gesture Keyboard 最早由 Montgomery 在 1982 年提出。传统的输入方式为通过手指点击需要输入的字母或数字进行输入，称为点击输入。而滑动输入就是在触摸屏的软键盘上以滑动的方式，在滑动轨迹上将需要输入的内容都包含进去。相比较传统的点击输入方式，滑动输入只需在一次动作中即可完成输入，有着更高效的优点。

Swype 是目前用户数量最多的一款以滑动输入代替点击输入的智能手机输入法。它只需要用户在需要输的单词所组成的字母间滑动，既可根据词库和单词的使用频率挑选出用户最有可能输入的单词。

Pattern Lock是安卓手机采取一个滑动输入验证机制。Schaub F 等人证明了通过滑动方式输入的 9 点 Pattern Lock 比点击输入的 4 位 PIN码更能抵御肩窥攻击。

# 第四章 主要思路

1. 主要思路概述

PINSilde的主要设计思路是两条，一是通过滑动替代击键作为输入手段，可以增加输入的速度以及抵抗肩窥攻击的能力。二是添加用户滑动的生物特征作为第二验证因子，进一步提高安全性。

PINSlide 的口令构成形式为:(Password, 滑动输入特征)。PINSlide 要求用户使 用滑动的方式输入口令，不仅要求用户滑动序列中包含 Password1，并且要求滑动输 入特征也符合口令。

PINSlide的工作过程分为两个阶段：

**注册/更新阶段(Setting/Updating Phase)**:在注册及更新阶段中，用户需要设定 4 位 PIN 码，并重复输入一次以确认 4 位 PIN 码的正确性。在完成 4 位 PIN 码的设置 后，需要在固定的数字键盘上以用户习惯的滑动轨迹反复滑动输入 4 位 PIN 码。系统 将收集该阶段的滑动特征数据作为训练集数据。

**认证阶段(Unlock Phase)**:在该阶段中，用户只需重新滑动输入设定的 4 位 PIN 码，SlideAuth 即可根据滑动输入的序列及滑动特征判断输入的用户是否为合法用户。 SlideAuth 首先判断用户滑动输入的序列中是否包含设定的 4 位 PIN 码，若不包含， 则判定为非法输入。若包含，则对用户滑动输入过程中产生的滑动特征进行验证。若 滑动特征与合法用户类似为同一类，则判定为合法输入;否则，判定为非法输入。

1. 滑动特征选取

滑动特征数据主要包括原始数据和 加工数据两种。滑动过程中产生的原始数据主要有:滑动轨迹的坐标(x，y)、手指接 触屏幕的面积、手指按压屏幕的压力以及动作发生的绝对时间等数据。由于滑动是一 个运动的过程，因此可以根据原始数据计算得出一些加工数据，如滑动的速度、加速 度、滑动的持续时间、滑动轨迹的曲率等。

结合相关研究及 PINSlide本身的特性，PINSlide初步所选取的滑动特征包括滑动持续时间、X轴起始坐标和终止坐标、Y 轴起始坐标和终止坐标、手指按压压力平均 值、手指按压面积平均值、X 轴方向和 Y 轴方向上的速度平均值，共9项特征。

# 第五章 项目分工

卜天童：负责APP的设计和用户特征数据的预处理，以及用户实验的实施和数据分析。

马明仪：负责APP的设计，滑动特征、口令注册、滑动输入的验证等功能的设计与实现。

任昆鹏：负责用户生物特征算法的优化，以及用户实验的具体设计和实施。

陈炘：用户滑动特征数据种类的指定，以及使用机器学习方法对滑动特征建模。

# 第六章 项目实现

１、pinslideApp设计与实现

PinslideApp是我们实现基于生物特征的滑动解锁机制的一种实验应用。该应用用于基于生物特征的滑动解锁的实验室、用户实验，攻击实验的实施。应用包含：设置密码、预览、查看信息、生物特征认证设置等功能。具体的实现如下：

1. 设置密码--默认密码为1234
2. 预览--可以在app内滑动测试，并且下面会显示posx posy等信息
3. 查看信息--可以查看历史滑动信息，可以将信息删除，也可以点击同步/上传按钮将数据上传（当后台服务器设置为添加到元数据之后时为同步，覆盖原数据为上传），另外上传的时候是上传以前没有上传的滑动。
4. 设置--可以在本页面设置测试者的姓名使用手和是否显示滑动的轨迹。
5. 生物学认证--可以查看当前机器学习的参数版本和上次训练模型的时间。可以点击重新训练样本进行重新训练，点击更新生物热嗯真参数，获取服务器设置的机器学习参数，点击上传生物认证信息上传模型的模板和阈值等。
6. 可以点击下部按钮设置开启生物学认证和开启锁屏
7. 本app可以记录滑动数据，训练的模板数据，开启生物认证后每次的滑动时候的阈值比较等

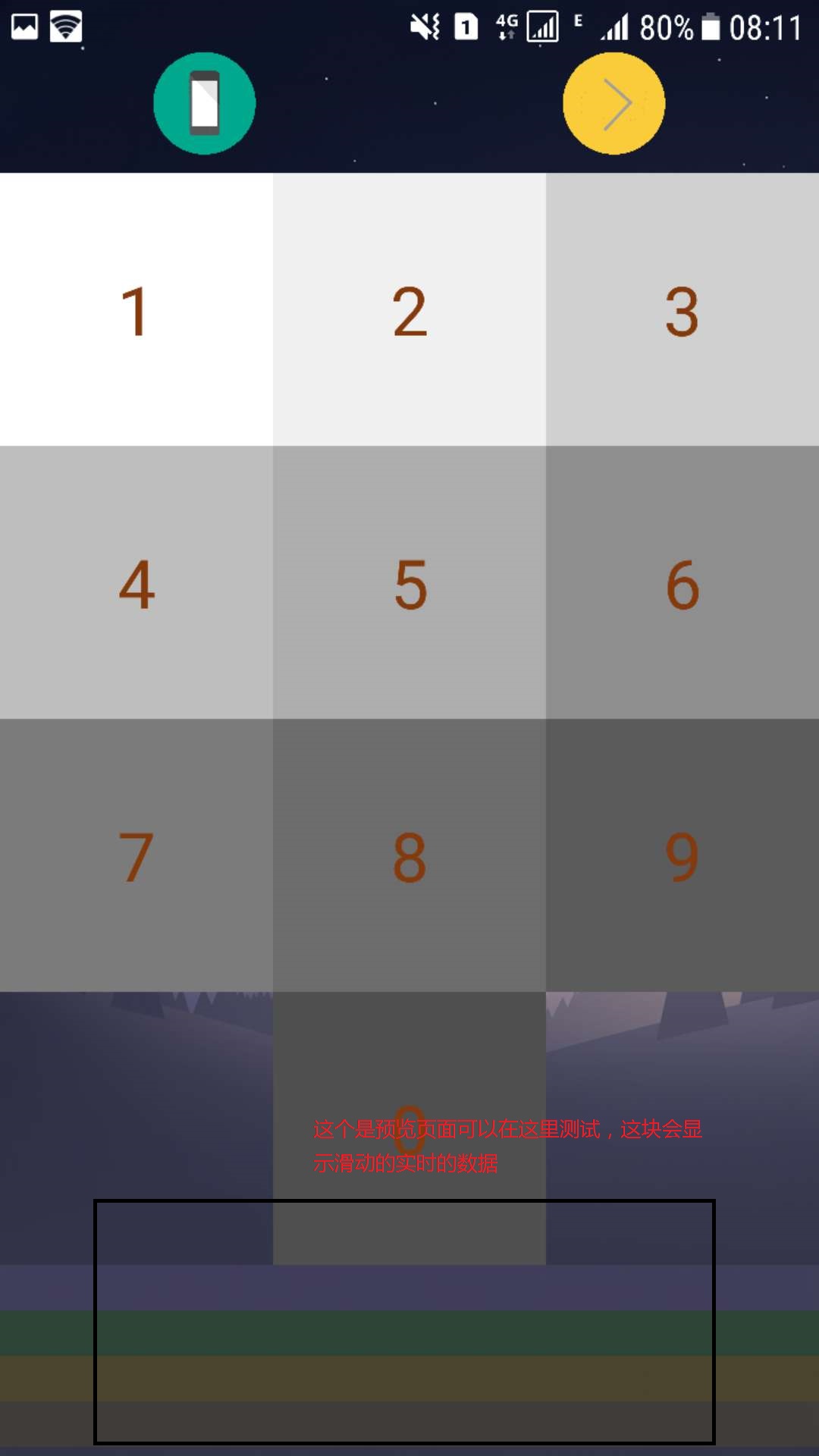
**图片：**

****

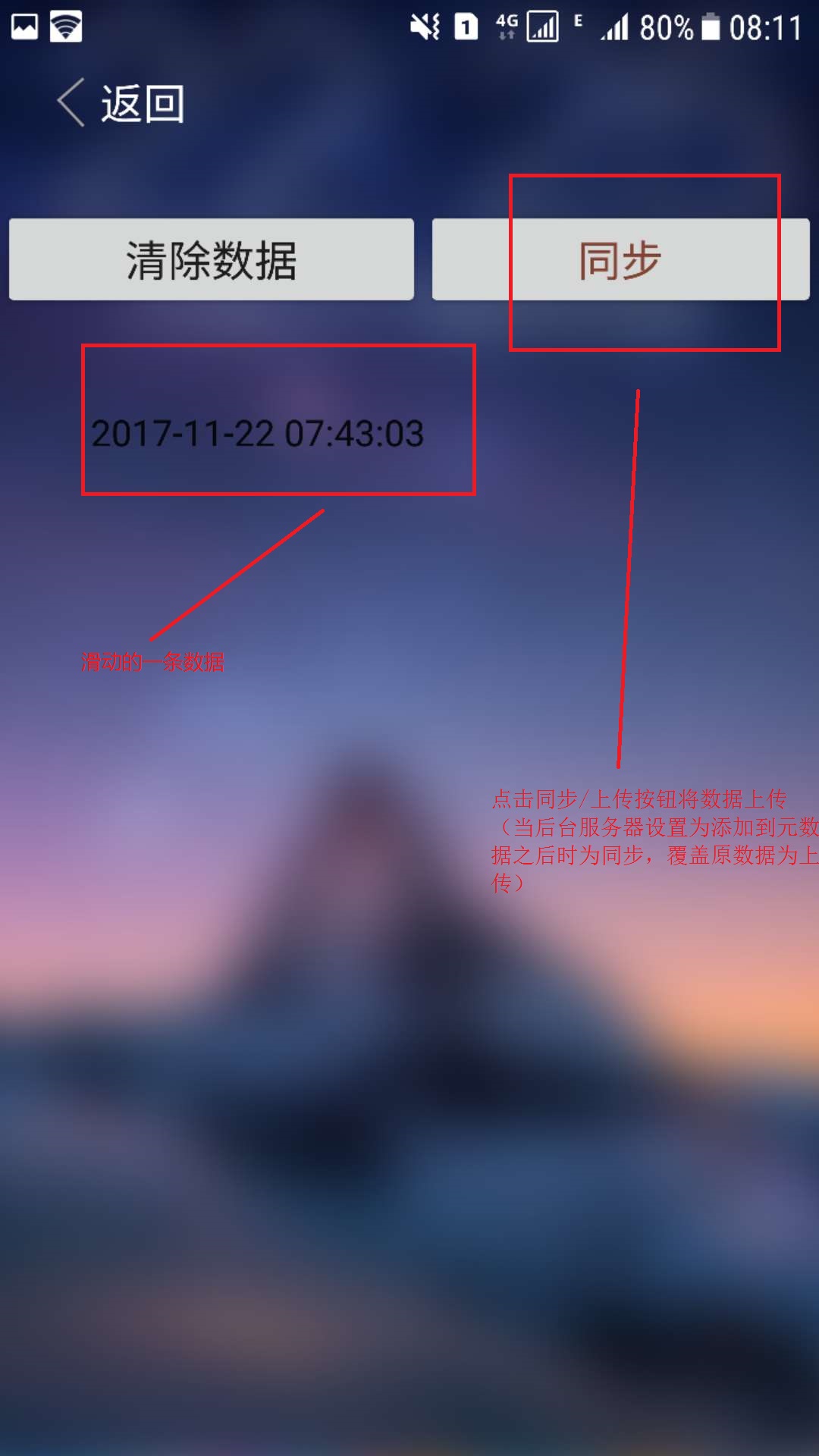
**主界面**

****

**设置密码**

****

**预览页面**

****

**查看信息**

****

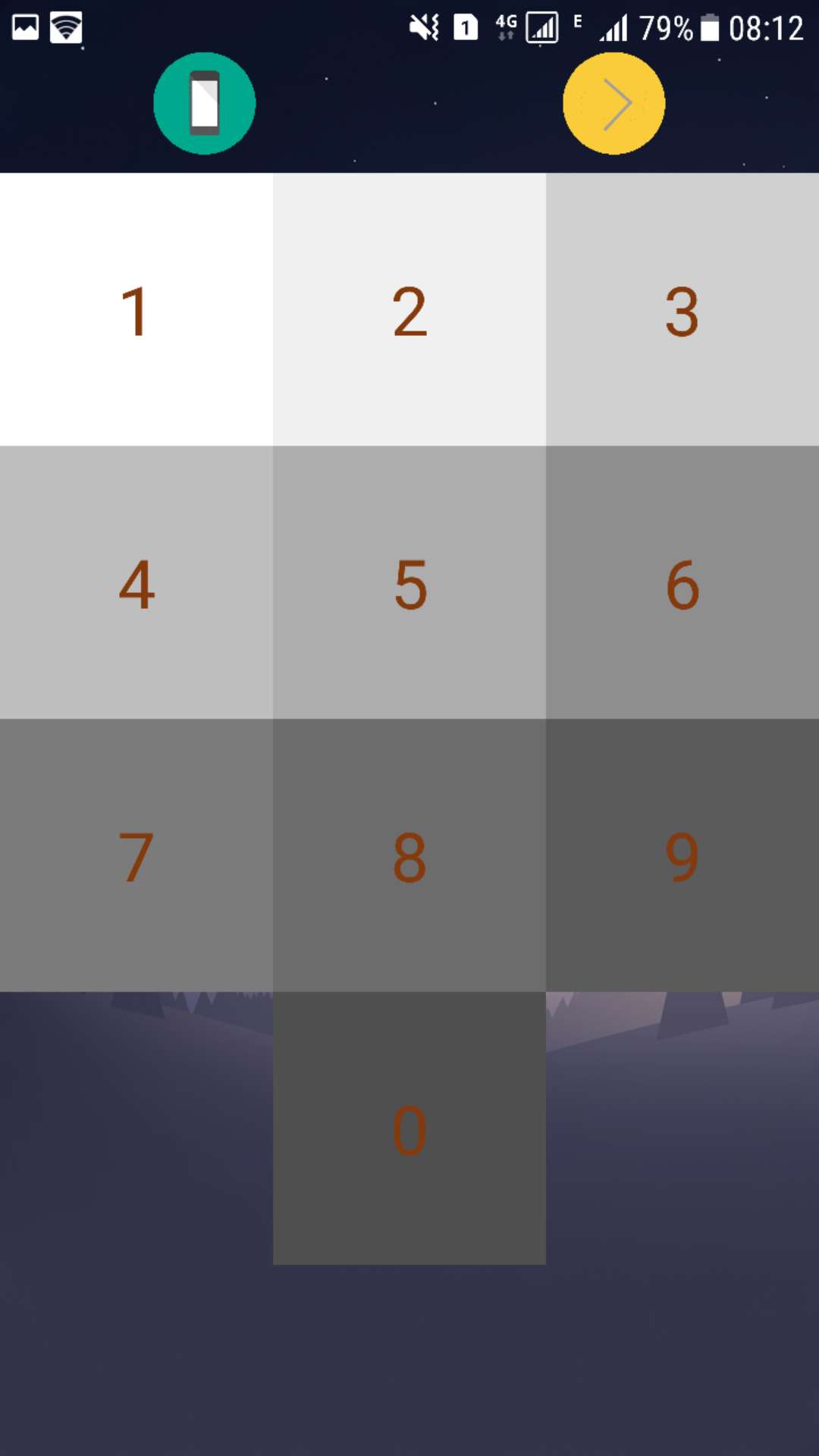
**轨迹信息**

****

**设置页面**

****

**生物认证页面**

****

**锁屏时候的页面**

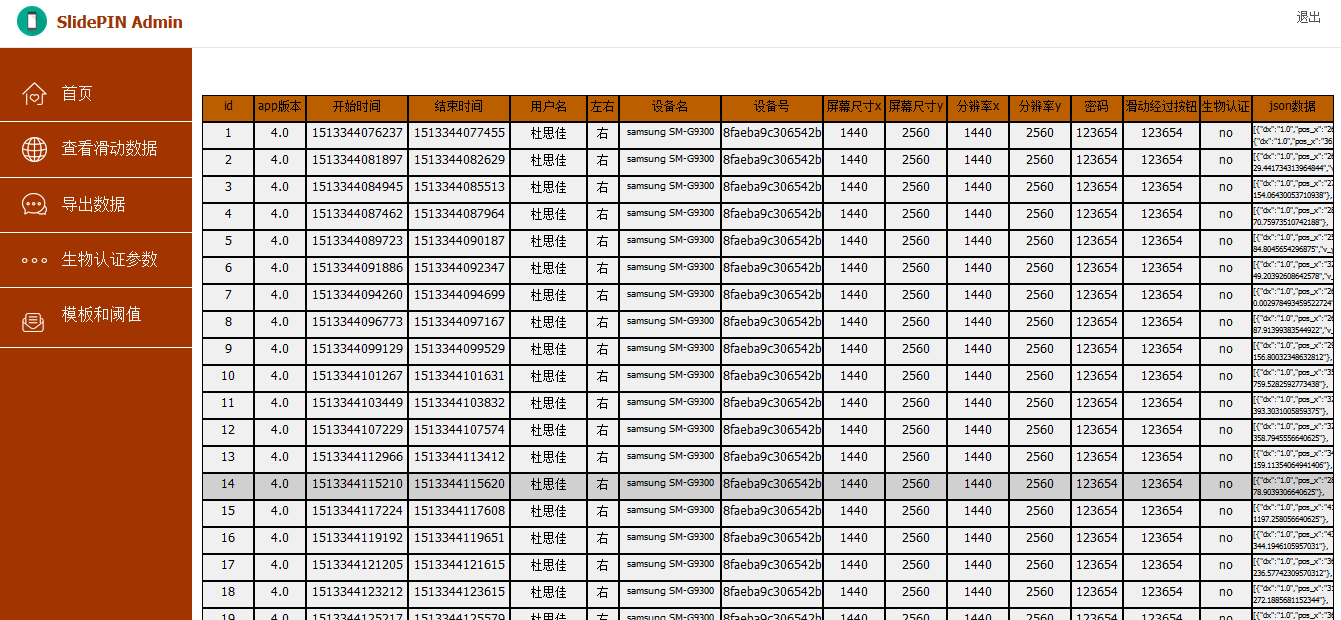
**上面的2个按钮分别是直接进入和到拨号页面**

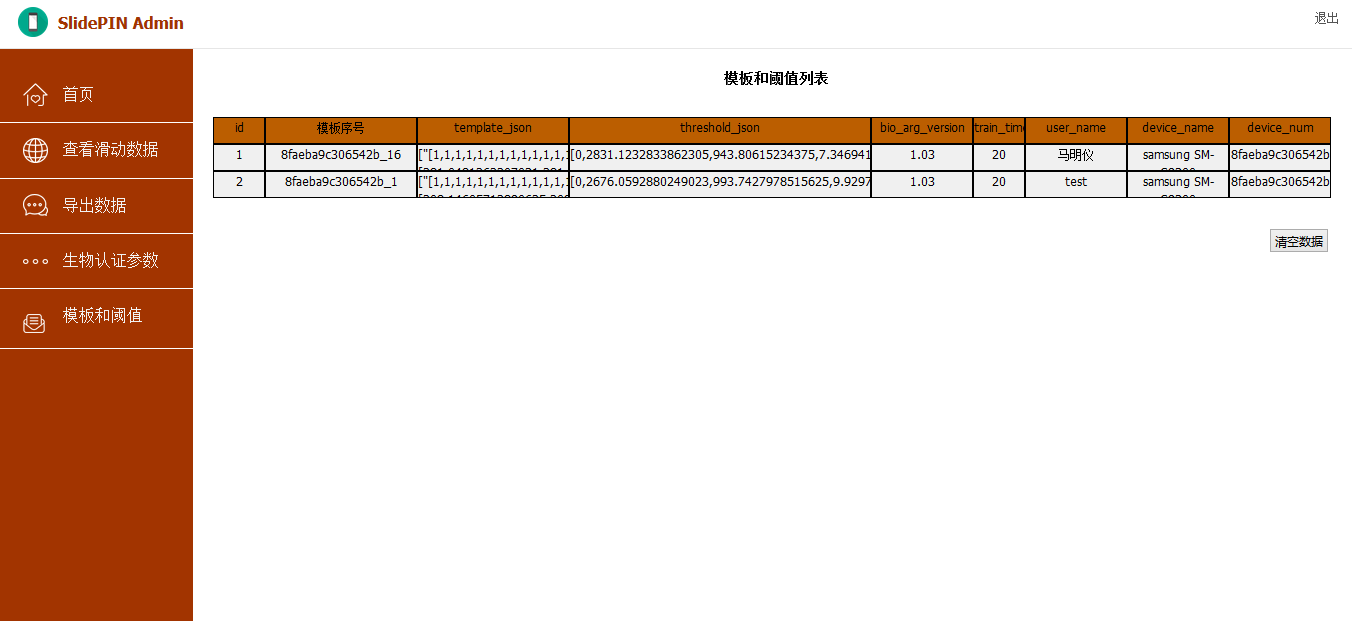
2、后台管理系统

后台管理系统，用于收集PINSlideAPP端用户的训练数据和生物特征参数。

主要包括：查看滑动数据，导出数据，生物认证参数，模板和阈值功能模块。

查看滑动数据：用于显示用户每条的滑动数据，包含id、app版本、开始时间、结束时间、用户名、左右手、设备名、设备号、屏幕尺寸、分辨率、密码、滑动经过按钮、生物认证等参数。





滑动数据显示

生物特征参数：用于设置app中使用的机器学习参数版本以及是否使用生物特征。



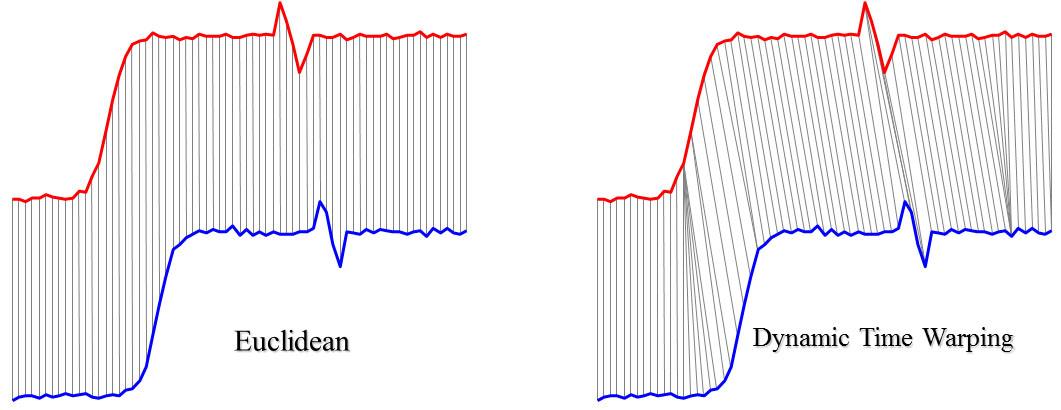
模板和阈值：用于显示用户上传的特征模板和所使用的阈值。



3、生物特征识别算法

使用动态时间规整(Dynamic Time Warping, DTW)算法 验证可行性

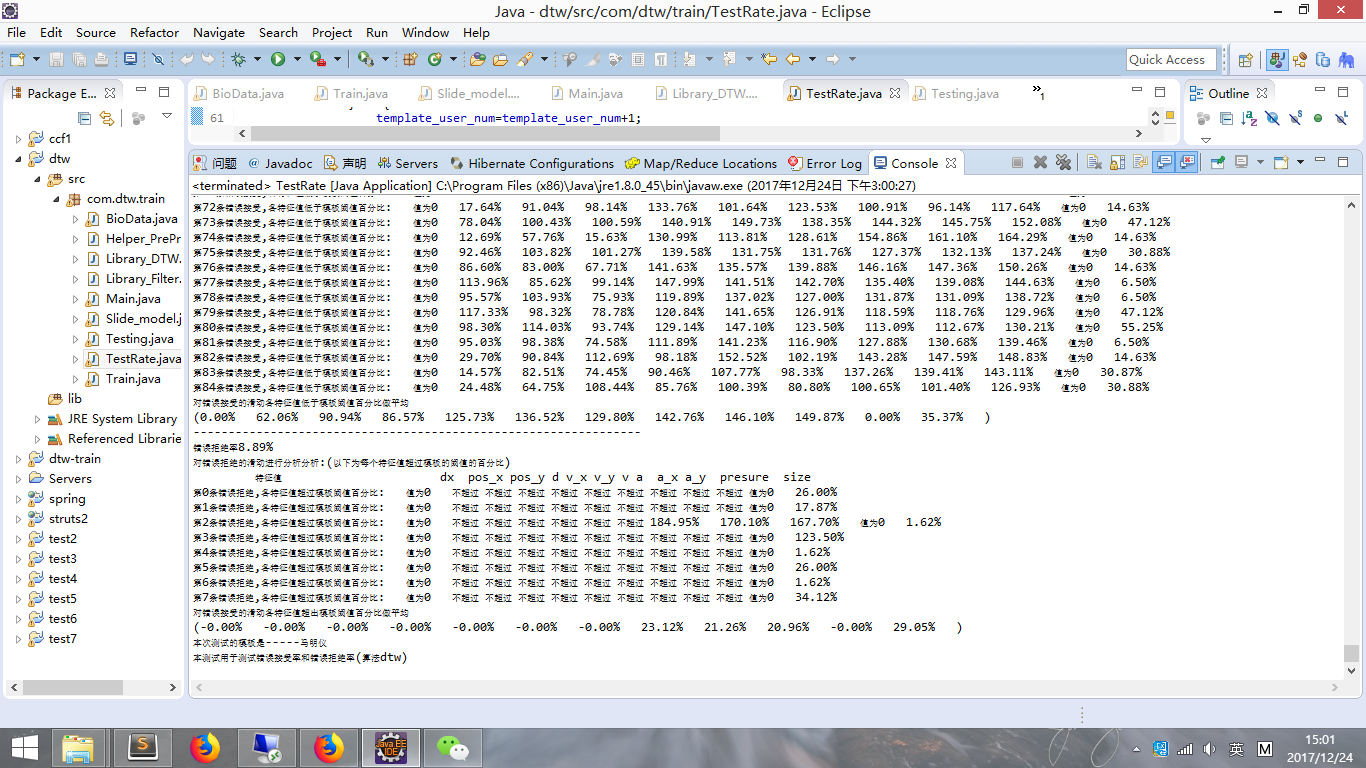
DTW算法是一种把时间规整和距离计算结合起来的非线性规整技术，具有概念简单、算法鲁棒性强的优点。



4、用户实验实施

实验实施：该实验共取10名实验者，每个人每天收集有效滑动数据30条，总共实验三天。共收集900条数据。

实验算法测试：取出1位测试者每天10条数据，组合生成3组20条数据，生成测试模板。使用所有900条数据，测试模板，计算出错误拒绝率和错误接受率。做平均值。



算法测试截图

# 第七章 项目总结和收获

这个项目的收获颇丰，有

1） 了解了正规严谨的人机交互实验流程和注意事项，如何设计实验流程，如何进行试验以及试验过程和数据搜集分析过程中应该注意的事项。

2） 学习了机器学习的基本理论以及DTW、GMM等几个算法的详细内容、数学原理以及具体的应用。

3） 在实验过程中摸索出了一套高效搜集、分析数据的方法，知道了应该如何在安全性和可用性之间做权衡。

4） 对人机交互中的安全有了更深一步的了解。