**基于mini2440的声纹认证加密系统**

**作**

**品**

**测**

**试**

**报**

**告**

**2016年全国大学生信息安全竞赛**

**作品测试报告**

**作品名称： 基于mini2440的声纹认证加密系统**

**目 录**

[一、编写目的 3](#_Toc445563707)

[二、项目背景 4](#_Toc445563708)

[三、定义 4](#_Toc445563709)

[四、参考资料 5](#_Toc445563710)

[五、 测试 6](#_Toc445563711)

[5.1测试环境 6](#_Toc445563712)

[5.2 功能性测试 6](#_Toc445563720)

[5.2.1声纹数据采集模块 6](#_Toc445563721)

[5.2.2 声纹特征训练模块 6](#_Toc445563722)

[5.2.3声纹特征身份识别模块 7](#_Toc445563723)

[5.2.4文件加密解密模块 8](#_Toc445563724)

[5.2.5用户注册模块 9](#_Toc445563725)

[5.3 安全性测试 9](#_Toc445563726)

[5.3.1应用安全性测试 9](#_Toc445563727)

[5.3.2系统安全性测试 10](#_Toc445563728)

[5.3.3传输安全性测试 10](#_Toc445563729)

[5.4 稳定性测试 10](#_Toc445563730)

[5.4.1应用稳定性测试 10](#_Toc445563731)

[5.4.2系统稳定性测试 10](#_Toc445563732)

[5.4.3传输稳定测试 11](#_Toc445563733)

[六、评价 11](#_Toc445563734)

[6.1软件能力 11](#_Toc445563735)

[6.2缺陷和限制 11](#_Toc445563736)

[6.3建议 12](#_Toc445563737)

[七、测试结论 12](#_Toc445563738)

# 一、编写目的

本测试报告的测试对象是基于mini2440的声纹认证加密系统。本文档有助于实现以下目标：

1. 根据参赛作品的需求文档，确定测试范围和测试结束标准；

2. 推荐可采用的测试策略，并对这些策略加以说明；

3. 确定测试所需的资源和需投入时间；

4. 如实记录在项目执行中测试方案的变更内容和原因；

5. 通过对测试结果的分析，得到对软件质量的评价；

6. 分析系统存在的缺陷，为修复和预防bug提供建议。

本测试报告的阅读对象为项目开发人员以及信息安全竞赛评委专家，有助于项目开发人员更为系统专业地进行项目开发，也有助于信息安全竞赛评委专家通过测试报告进一步了解基于mini2440的声纹认证加密系统。

# 二、项目背景

基于mini2440的声纹认证加密系统是我们团队参加2016年全国大学生信息安全竞赛的参赛作品。本作品是我们团队在移动互联网呈现爆发性增长，个人数据和个人隐私变得越来越重要，但智能终端和移动互联网安全形势堪忧的背景下，提出的一套全新的个人数据加密系统。

基于mini2440的声纹认证加密系统由声纹数据收集模块、声纹特征训练模块、身份验证模块、文件加密解密模块以及用户界面模块组成；通过采集用户的声纹作为密钥，利用国密SM4加密算法，实现个人用户数据保密的功能。该系统无需用户输入密码，声纹特征即密钥。

# 三、定义

mini2440：Mini2440是一款真正低价实用的ARM9开发板，是目前国内性价比最高的一款；它采用Samsung S3C2440为微处理器，并采用专业稳定的CPU内核电源芯片和复位芯片来保证系统运行时的稳定性。是第一款在WindowsCE和Linux下通过简单直观的图形界面，就可设置各种程序开机自动运行的开发板。

声纹识别: 声纹识别(Voiceprint Recognition, VPR)，也称为说话人识别(Speaker Recognition)，有两类，即说话人辨认(Speaker Identification)和说话人确认(Speaker Verification)。前者用以判断某段语音是若干人中的哪一个所说的，是“多选一”问题；而后者用以确认某段语音是否是指定的某个人所说的，是“一对一判别”问题。不同的任务和应用会使用不同的声纹识别技术，如缩小刑侦范围时可能需要辨认技术，而银行交易时则需要确认技术。不管是辨认还是确认，都需要先对说话人的声纹进行建模，这就是所谓的“训练”或“学习”过程。

SM4算法: SM4算法是一个分组算法，用于无线局域网产品。该算法的分组长度为128比特，密钥长度为128比特。加密算法与密钥扩展算法都采用32轮非线性迭代结构。解密算法与加密算法的结构相同，只是轮密钥的使用顺序相反，解密轮密钥是加密轮密钥的逆序。此算法采用非线性迭代结构，每次迭代由一个轮函数给出，其中轮函数由一个非线性变换和线性变换复合而成，非线性变换由S盒所给出。

密钥: 密钥是一种参数，它是在明文转换为密文或将密文转换为明文的算法中输入的参数。密钥分为对称密钥与非对称密钥。对于普通的对称密码学，加密运算与解密运算使用同样的密钥。通常,使用的对称加密算法比较简便高效，密钥简短，破译极其困难，由于系统的保密性主要取决于密钥的安全性，所以，在公开的计算机网络上安全地传送和保管密钥是一个严峻的问题。

加密文件： 加密文件是以某种特殊的算法改变原有的信息数据，使得未授权的用户即使获得了已加密的信息，但因不知解密的方法，仍然无法了解信息的内容。在密码学中，加密是将明文信息隐匿起来，使之在缺少特殊信息时不可读。数据加密的基本过程就是对原来为明文的文件或数据按某种算法进行处理，使其成为不可读的一段代码，通常称为"密文"，使其只能在输入相应的密钥之后才能显示出本来内容，通过这样的途径来达到保护数据不被非法人窃取、阅读的目的。该过程的逆过程为解密，即将该编码信息转化为其原来数据的过程。

MFCC：Mel频率倒谱系数的缩写。Mel频率是基于人耳听觉特性提出来的，它与Hz频率成非线性对应关系。Mel频率倒谱系数(MFCC)则是利用它们之间的这种关系，计算得到的Hz频谱特征，MFCC已经广泛地应用在语音识别领域。由于Mel频率与Hz频率之间非线性的对应关系，使得MFCC随着频率的提高，其计算精度随之下降。因此，在应用中常常只使用低频MFCC，而丢弃中高频MFCC。：

# 四、参考资料

[1] SHID团队，基于mini2440的声纹认证加密系统作品简介[Z],电子科技大学,2016

[2] SHID团队，基于mini2440的声纹认证加密系统作品报告[Z],电子科技大学,2016

[3] 软件设计文档国家标准[Z],国家质量监督检验检疫总局,2006

[4] [[美] Christof Paar/Jan Pelzl 著](http://book.douban.com/search/æä¼æ¢¦%20è) , 深入浅出密码学[M], 清华大学出版社，2012

[5] [[美] Bruce Schneier 著](http://book.douban.com/search/æä¼æ¢¦%20è) , 应用密码学：协议、算法与C源程序（原书第2版）[M], 机械工业出版社，2013

[6] [李子臣，杨亚涛著](http://book.douban.com/search/æä¼æ¢¦%20è) , 典型密码算法C语言实现[M], 国防工业出版社，2013

[7] 杨阳，陈永明著，声纹识别技术及其应用，电声技术 , Audio Engineering,2007年02期

[8] 彭诗雅,基于声纹识别的身份认证技术研究, 南京航空航天大学，电路与系统，2010

# 测试

## 5.1测试环境

|  |  |  |
| --- | --- | --- |
|  | 客户端 | PC端 |
| 程序 | 基于mini2440的声纹认证加密系统硬件部分 | 基于mini2440的声纹认证加密系统软件界面 |
| 操作系统 | Linux | Windows |
| 支持平台 |  | Windows |
| 设备型号 | Mini2440 |  |

## 5.2 功能性测试

### 5.2.1声纹数据采集模块

5.2.1.1 语音数据录入

|  |  |
| --- | --- |
| **测试目标** | 验证声纹数据采集模块是否能够采集用户语音数据 |
| **测试范围：** | 语音收据收集功能 |
| **测试方法：** | 安装应用，连接mini2440，打开注册功能。 |
| **预期结果：** | 该模块正常运行，在应用启动后，操作解密出现声音录入提示，当数据足够后出现声音录入终止。 |
| **实际结果：** | 与预期结果一致 |
| **需考虑的特殊事项：** | 无 |

5.2.1.2 声纹特征值提取

|  |  |
| --- | --- |
| **测试目标** | 验证声纹数据采集模块是否能够通过获取的用户语音数据得到声纹特征值MFCC |
| **测试范围：** | 声纹特征值MFCC提取功能 |
| **测试方法：** | 录入语音数据文件test.raw，经过声纹特征值MFCC提取过程将结果保存至文本文件mfcc.txt中。 |
| **预期结果：** | 该模块正常运行，在应用启动后，录入语音数据，处理语音文件test.raw，成功将声纹特征值MFCC存放至指定文件夹下声纹特征值文件mfcc.txt |
| **实际结果：** | 与预期结果一致 |
| **需考虑的特殊事项：** | 无 |

### 5.2.2 声纹特征训练模块

5.2.2.1 使用HMM算法训练模型

|  |  |
| --- | --- |
| **测试目标** | 能否使用HMM算法训练出模型 |
| **测试范围：** | 1. mfcc.txt的训练数据的输入格式 2. HMM隐马尔科夫模型训练功能 |
| **测试方法：** | 使用之前收集语音数据作为输入，将提取的声纹特征值MFCC写入mfcc.txt文件中，调用相应的HMM模型训练函数，并保存模型至模型库中。 |
| **预期结果：** | 该模块正常运行，在测试程序启动后，程序正常读入mfcc.txt文件，并且计算出相应的模型，保存在指定目录下。 |
| **实际结果：** | 与预期结果一致 |
| **需考虑的特殊事项：** | 无 |

5.2.2.2 HMM算法的正确率测试

|  |  |
| --- | --- |
| **测试目标** | 测试当前HMM算法训练出的模型的正确率 |
| **测试范围：** | 1. 训练数据的输入格式 2. 所得模型的正确率的平均值 |
| **测试方法：** | 使用小组成员所提供的训练数据集和测试数据集来训练和测试，并计算结果，记录并求正确率的平均值。 |
| **预期结果：** | 更换训练数据，每次计算所得模型都不一样，正确率也不同，但是正确率都集中在80%左右 |
| **实际结果：** | 与预期结果一致，平均正确率为82.3%。 |
| **需考虑的特殊事项：** | 无 |

### 5.2.3声纹特征身份识别模块

5.2.3.1用户的识别功能

|  |  |
| --- | --- |
| **测试目标** | 能否正确识别用户 |
| **测试范围：** | 用户的识别功能 |
| **测试方法：** | 编写测试程序，并且调用之前训练所得模型，测试人员录入声纹，观察并记录测试结果，计算测试结果。 |
| **预期结果：** | 该模块正常运行，在测试程序启动后，程序正常读入声纹特征文件，并且计算出相应的模型，保存在指定目录下。在用户进行操作时，多次判断，判断成功的概率98%以上 |
| **实际结果：** | 与预期结果一致 |
| **需考虑的特殊事项：** | 无 |

5.2.3.2 判别结果写回训练数据

|  |  |
| --- | --- |
| **测试目标** | 模型更新前的数据回写功能 |
| **测试范围：** | 判别结果写回训练数据 |
| **测试方法：** | 编写测试程序，并且调用之前训练所得模型，测试人员输入自己的语音数据。查看数据文件，观察是否有追加写入，写入结果是否与记录相符。 |
| **预期结果：** | 该模块正常运行，在测试程序启动后，程序正常读入test.raw文件，并且计算出相应的模型，保存在指定目录下。在mfcc.txt文件中又追加写入的记录，并且和实际操作相符合。 |
| **实际结果：** | 与预期结果一致 |
| **需考虑的特殊事项：** | 无 |

### 5.2.4文件加密解密模块

5.2.4.1 文件加密解密

|  |  |
| --- | --- |
| **测试目标** | 验证加密算法以及密钥扩展算法的正确性 |
| **测试范围：** | 测试生成的加密文件能否识别，并解密后与原文件内容一致。 |
| **测试方法：** | 输入声纹特征值与待加密文件，进行加密与解密操作。 |
| **预期结果：** | 经过加密后的文件为乱码文件。经过解密后的文件与原文件内容一致。 |
| **实际结果：** | 实际结果与预期结果一致 |
| **需考虑的特殊事项：** | 无 |

### 5.2.5用户注册模块

5.2.5.1 用户注册和登陆功能

|  |  |
| --- | --- |
| **测试目标** | 验证系统的用户注册和登陆功能 |
| **测试范围：** | 1. 测试用户在PC端注册和登陆 |
| **测试方法：** | 在PC端注册页面和登陆页面按照界面提示录入数据，根据提示信息判断结果。 |
| **预期结果：** | 注册时，进入注册页面，设置自己的用户名和密码，并录入声纹。登录时，输入自己用户名和密码，点击登陆按钮，登陆成功。 |
| **实际结果：** | 实际结果与预期结果一致 |
| **需考虑的特殊事项：** | 无 |

## 5.3 安全性测试

### 5.3.1应用安全性测试

|  |  |
| --- | --- |
| **测试目标** | 应用安全性测试 |
| **测试范围：** | 测试本应用在应用级别是否安全 |
| **测试方法：** | 首先内置一定的数据到数据文件，然后开始用不正确的声纹进行解密操作。 |
| **预期结果：** | 加密文件解密后仍然为乱码或身份认证失败。 |
| **实际结果：** | 实际结果与预期结果一致 |
| **需考虑的特殊事项：** | 无 |

### 5.3.2系统安全性测试

|  |  |
| --- | --- |
| **测试目标** | 系统安全性测试 |
| **测试范围：** | 测试本应用在系统级别是否安全 |
| **测试方法：** | 声纹录入后，查找PC端是否存储的模型文件，mini2440端模型库是否生成模型文件。 |
| **预期结果：** | PC端无法查找到模型文件，mini2440端模型库存在模型文件。 |
| **实际结果：** | 实际结果与预期结果一致 |
| **需考虑的特殊事项：** | 无 |

### 5.3.3 PC端安全性测试

|  |  |
| --- | --- |
| **测试目标** | PC端安全性测试 |
| **测试范围：** | 测试本应用在PC端级别是否安全 |
| **测试方法：** | 查看在PC端是否要通过身份验证才能进行文件的存储和取回 |
| **预期结果：** | 存储和取回文件的身份控制已启用 |
| **实际结果：** | 实际结果与预期结果一致 |
| **需考虑的特殊事项：** | 无 |

## 5.4 稳定性测试

### 5.4.1应用稳定性测试

|  |  |
| --- | --- |
| **测试目标** | 应用稳定性测试 |
| **测试范围：** | 测试本应用在应用级别是否稳定 |
| **测试方法：** | 常时间使用本应用，看是否出现BUG |
| **预期结果：** | 应用稳定运行，无BUG出现 |
| **实际结果：** | 实际结果与预期结果一致 |
| **需考虑的特殊事项：** | 无 |

### 5.4.2系统稳定性测试

|  |  |
| --- | --- |
| **测试目标** | 系统稳定性测试 |
| **测试范围：** | 测试本应用在系统级别是否稳定 |
| **测试方法：** | 在使用本应用时，同时开启其他应用，查看本应用及系统是否有异常出现 |
| **预期结果：** | 系统无异常 |
| **实际结果：** | 实际结果与预期结果一致 |
| **需考虑的特殊事项：** | 无 |

### 5.4.3 PC端稳定测试

|  |  |
| --- | --- |
| **测试目标** | PC端稳定测试 |
| **测试范围：** | 测试本应用在PC端是否稳定 |
| **测试方法：** | 多次在PC端进行文件的存储和取回，查看对文件管理的功能是否正常运行 |
| **预期结果：** | PC端正常运行并处理文件操作 |
| **实际结果：** | 实际结果与预期结果一致 |
| **需考虑的特殊事项：** | 无 |

# 六、评价

## 6.1软件能力

本团队对基于mini2440的声纹认证加密系统完整的功能测试、稳定性测试与安全测试，并完成该测试报告，证实了本系统软件在mini2440测试环境下通过了用户身份认证功能、文件加密解密功能；同时，在windows 系统PC端测试环境下，本系统实现了用户存储文件至mini2440功能、用户从mini2440取回文件功能。通过PC端和mini2440端的通信管理文件，使得用户的信息、数据得到更有效的安全保护。

基于mini2440的声纹认证加密系统已完成系统测试，运行流畅、功能都良好实现。但是，可能由于实际运行环境与测试环境的不同，带来一定影响，这一点我们会对不同环境进行测试，并进行调试。

## 6.2缺陷和限制

尽管我们的参赛作品基于mini2440的声纹认证加密系统已实现所有功能并进行了性能的优化；但是，经过本次系统化的测试，我们还是发现了该系统的几点缺陷：

1、缺陷描述：由于需要较大量的用户语音数据训练来提高模型的精确度，声纹数据采集时间较长。

缺陷影响：对于用户在进行第一次登陆既注册时，耗费时间较长，用户体验不够完善。

2、缺陷描述：将文件存储放于mini2440端，mini2440存储空间有限，需要多个硬件设备供用户使用。

缺陷影响：无法满足用户需要存放大量数据的需求。

## 6.3建议

针对本次基于mini2440的声纹认证加密系统测试中发现的两点缺陷，我们提出了相应的建议并将尽快完善。

1、缺陷描述：由于需要较大量的用户语音数据训练来提高模型的精确度，声纹数据采集时间较长。

建议：通过提高硬件设备的采样率达到声纹特征值的独一性强，来降低所需的用户语音数据量，缩短语音录入的时间。

2、缺陷描述：将文件存储放于mini2440端，mini2440存储空间有限，需要多个硬件设备供用户使用。

建议: 将文件存储部分放置云端，通过制定传输协议来达到文件传输过程的安全保护。

# 七、测试结论

我们团队制定了详细的测试计划，并对“基于mini2440的声纹认证加密系统”进行了全面、严格、规范的测试。本次测试完全依照现有的功能模块进行功能、稳定性和安全测试，功能测试覆盖率100%，稳定性测试全面，安全性测试具有系统性。

测试结果表明：“基于mini2440的声纹认证加密系统”在当前的mini2440设备软硬件、PC端软硬件系统功能符合参赛作品需求中的要求，稳定性测试与安全性测试结果也达到相应标准。同时，也验证了该系统具有以下特点：

1、功能全面

该系统由声纹数据采集模块、声纹特征训练模块、文件加密解密模块等模块组成。该系统完美实现了对使用者的身份认证，以及让使用者安全存储、查看个人文件信息。

2、系统安全性较好

该系统对用户的信息数据进行了三道有效的安全防护。首先是用户对文件进行操作的访问控制，我们使用错误接受率和错误拒绝率均低的声纹识别来进行身份验证。其次通过使用国密算法SM4算法，利用SM4算法密钥长度长不易被破解等优点，对文件进行加密。最后我们将身份验证和文件加密解密过程搭载在硬件设备mini2440上，做到硬件层面的防护，极难被破解获取信息。同时，我们对该系统进行的详细的安全性测试已全部通过。作为一个信息安全竞赛作品，我们进行了安全评估分析，也验证了系统的安全性。

3、系统可靠性高

本系统将主要的身份验证和文件加密解密功能集中在硬件设备上，在确认文件传输之前与PC端仅用指令进行通信，因此具有良好的用户文件保护机制，系统可靠性高。

4、系统用户体验性好

本系统设计产品化，利用mini2440功能完整且体积较小的优点，将用户所需的身份验证和文件存储集中在硬件设备，使用户可以随时随地进行文件的查看和管理。

综上所述测试结论: 通过。