

2015年全国大学生信息安全竞赛作品简介

基于Mini2440的声纹认证加密系统



SHID

**2015年全国大学生信息安全竞赛**

**作品简介**

**作品名称： 基于Mini2440的声纹认证加密系统**

**电子邮箱：**

**提交日期：**

目录

[摘 要 4](#_Toc452239826)

[一、背景 5](#_Toc452239827)

[二、设计与分析 7](#_Toc452239828)

[2.1.系统整体框架 7](#_Toc452239829)

[2.1.1登陆模块 8](#_Toc452239830)

[2.1.2. RSA模块 8](#_Toc452239831)

[2.1.3.声纹识别模块 8](#_Toc452239832)

[2.1.4. SM4加密\解密模块 9](#_Toc452239833)

[2.1.5.文件存储模块 10](#_Toc452239834)

[2.1.6.文件管理模块 10](#_Toc452239835)

[2.1.7.数据包处理模块 10](#_Toc452239836)

[2.2.系统工作流程 11](#_Toc452239837)

[三、技术点总结 11](#_Toc452239838)

[四、测试与分析 12](#_Toc452239839)

[4.1测试方案 12](#_Toc452239840)

[4.2结果分析 13](#_Toc452239841)

[五、安全评估 14](#_Toc452239842)

[六、创新点总结 15](#_Toc452239843)

[七、未来工作 16](#_Toc452239844)

摘 要

随着互联网时代的到来，无论是个人或是集体的信息都进入了“数字化”阶段，大量的文件需要存储和保护。然而传统的文件加密与存储方式都不能得到更好的加密认证与防护措施。用户设置复杂的文本密码，攻击者都可以通过肩窥攻击、暴力破解进行破解，甚至可以直接利用破解软件进行密码数据清除，无法真正有效对文件进行保护。

基于以上问题，我们提出了利用生物识别技术和文件加密算法相结合的方式对文件进行安全保护，同时将系统搭载在嵌入式设备提高系统安全性和用户体验感。通过调研，在数据存储保护方面，我们选用国密算法SM4进行加密解密；在身份验证方面，我们选用基于GMM（高斯混合模型）的声纹识别作为两道验证之一，使用MFCC（梅尔频率倒谱系数）作为说话人声音特征值。同时保留账户文本密码，使用RSA加密算法对其进行保护；在硬件平台方面，我们选用ARM9开发板mini2440作为说话人声音获取、声纹模型建立、身份验证、文件存储等几大主要功能的搭载平台。

仿真结果显示: 该算法与系统平台的设计方便可行，相应算法具有较高的识别率，认证系统便捷且安全。

**关键字：SM4算法、RSA算法、 声纹识别、GMM、MFCC、ARM9**

# 一、背景

当今社会处于一个信息时代，信息的数量日益庞大，信息的在各个行业的发展中地位不断上升，互联网让信息的流通更加便捷，这些信息时代的特征都意味着对信息的保护工作至关重要，只有保障了信息的安全，才能在竞争日益激烈的今天有立足之地，无论是对于个人还是团体。对信息的安全保护，主要从以下几个方向进行，一个是对信息本体的保护，如数据加密技术；一个是对信息传输的保护，如通信协议的制定，另一个是对获取信息进行安全控制，如身份验证。

1. 数据加密技术

随着网络通信技术和Internet的联系日益增强发展，由于一系列与网络安全相关的问题：如对主机的攻击，网络上传输的信息被截取、篡改、重发等，对网络应用的进一步推广构成了巨大威胁，因此密码体制就在这种背景下是迫切需要的。存储加密涉及大量文件、资料、新建等文档处理，需要高效，可靠的进行各种信息交换，同时对信息流转的整个过程需要有效的组织和监控。对数据的安全存储和安全传输具有较高的要求。数据加密技术不仅具有保证信息机密性的信息加密功能，而且具有数字签名、秘密分存、系统安全等性能。因而可以保障信息的机密性、完整性和准确性，防止信息被篡改、伪造和假冒。

（二）身份验证

身份验证在人类的社会生活中自古有之。传统的身份认证方法(如使用身份证、护照、钥匙、智能卡、密码、口令等)存在携带不便,易伪造、遗失,因使用过多、使用不当而损坏或不可读、密码易被破解等诸多问题,安全性、可靠性差。每个人所固有的生物特征,具有与其他人不同的惟一性和在一定时期内不变的稳定性,而且不会丢失,不易伪造和假冒,所以被认为是终极的身份认证媒介。

生物特征识别技术是通过计算机和光学、声学、生物传感器和生物统计学原理等高科技手段密切结合，利用人固有的生理特征（指纹、人脸、虹膜、声音等）来进行个人身份的鉴定。生物特征识别技术比传统的身份鉴定方法更具安全性、保密性、方便性和防伪性好等优点。生物识别系统对生物特征进行取样，提取其唯一的特征并且转化成数字代码，并进一步将这些代码组成特征模板。由于微处理器及各种电子元器件成本不断下降，精度逐渐提高，生物识别系统逐渐应用于商业上的授权控制如门禁、企业考勤管理系统安全认证等领域。

(三)“U盾”

U盾是用于网上银行电子签名和数字认证的工具，它内置微型智能卡处理器，采用非对称密钥算法对网上数据进行加密、解密和数字签名，确保网上交易的保密性、真实性、完整性和不可否认性。类似“U盾”的产品日益增多，功能拓展空间随着电子硬件技术的发展也逐渐增大。类似“U盾”的产品不仅在软件层面进行加密工作，还可以通过硬件的保护达到双重保险，同时将功能集中归一化，更有助于确保安全。

基于以上调查，我们团队提出了基于mini2440的声纹认证加密系统，本系统由声纹数据收集模块、数据建模训练模块、身份识别模块、SM4加密/解密模块、登录与注册模块、文件管理模块，达到了利用声纹验证、加密算法保护用户信息和文件。

# 二、设计与分析

# 2.1.系统整体框架



图2-1 系统框架

整个系统包含了登陆模块(包括：普通登陆与注册模块、声纹数据收集模块)、声纹识别模块（包括：数据建模训练模块、身份识别模块）、RSA模块、文件存储模块、SM4加密\解密模块、文件管理模块。

## 2.1.1登陆模块

登陆模块包括了普通登陆与注册模块。普通登陆模块这一部分主要实现的是用户在使用这个系统的时候能够有普通的设置账号、设置普通密码，以及与一些常用社交账号绑定的功能。同时为了与整个系统的安全性和功能性接轨，还有一个第一次登陆的声纹数据收集模块，一般而言用户在此处的操作为进行录音存储（在系统中一般为录音5s，可以进行回放确认操作）。在用户第一次注册的时候需要进行相应的录音操作，同时在用户需要提取重要存储文件时，需要进行相关的验证，此时的模型和算法需要被处理过的在这个模块存储的信息与数据。同时，音频有Mini2440端进行录制并回放，账户的密码须符合6-24位，大小写字母与数字，首字符为字母。登陆成功后将进入到文件操作模块。

这样双重的登陆系统是方便用户能够使用并尽快熟悉系统，同时也提高了安全性，为整个系统的安全性和功能性做出相应的操作与应用。

## 2.1.2. RSA模块

当Mini2440硬件启动后，将由RSA模块随机生成RSA密钥对，一旦PC端与Mini2440相连接，硬件就把对应的RSA公钥传递给PC端。当用户在硬件注册是，PC将用RSA公钥对MD5（用户账号+用户密码+盐）处理后的账户密码进行加密后传输到硬件上，硬件再对其用RSA私钥解密后保存在板子内部。同理，在登陆时可以解密后与账户的密码进行对比验证。这样可以保证硬件与PC端用户的登陆与账户的安全性，提升了整个系统的安全性能。

## 2.1.3.声纹识别模块

声纹识别模块主要是由数据建模训练模块、身份识别模块两个模块组成的。

1. 数据建模训练模块

数据建模训练模块主要实现的是接收来自用户提供的个人信息与数据，并将原始的数据进行去噪、清洗以及相关其他处理后传入该模块进行训练。

对于声纹识别的数据建模训练模块，我们主要采用了声纹特征MFCC系数模型来进行建模的处理。首先是语音信号预处理后，接着是特征参数的提取，同时选取的特征必须能够有效地区分不同的说话人，且对同一说话人的变化保持相对稳定。基于人耳的听觉机理，反映听觉特性，模拟人耳对声音频率感知的特征参数，如美尔倒谱系数等。很多研究证明，由于Mel频率特性反映了人耳的听觉特性，常用于代替人耳来分析语音，其性能和鲁棒性都是最符合实际听音效果的。MFCC参数与线性预测倒谱分析相比，突出的优点是不依赖全极点语音产生模型，因此，在该系统为与文本无关的说话人识别时，MFCC参数能够更好地提高系统的识别性能。步骤如下图所示：



图2-2 数据建模训练模块

1. 身份识别模块

通过上述的数据建模训练模块后，身份识别模块实现的则是在再次需要进入时，对用户进行生物特征的验证与识别。这里主要是一个特征值匹配以及对上述模型进行解模型的过程。我们采用的是SAX算法来进行相应的时间序列间间隔计算从而得到匹配的程度。当数据训练达到一定程度后，对预先设定的阈值进行调整。从而达到声纹识别算法在该系统中能够结合实际精准的应用。并将该系统的安全性因为声纹识别的属性而提高，将该模块在系统中更好的运行。

## 2.1.4. SM4加密\解密模块

本模块主要实现，当文档在Mini2440与PC端传输时，需要防止外来的拦截与解密。文件被SM4算法进行加密后，传入Mini2440中，在个过程里该算法主要是负责对文件在传输中遭遇拦截或者丢失进行负责。当传入后加密的文件需要被用户提取出来时，需要用户通过身份验证后得到相应的密钥，再利用该模块对加密的文件进行解密。这样可以保证文件在两个硬件上相互传输的安全性与可靠性。

同时，SM4模块是保证文件存储于Mini2440中，硬件丢失后文件的安全性。其密钥需要声纹识别的身份验证后才能够获得，也避免了暴力破解的危险，极大提高了整个文件的安全性。

## 2.1.5.文件存储模块

本模块主要实现了用户需要安全性高的存储文件的功能。文件被sm4模块加密后传入Mini2440上，并存储在其中。该Mini2440由用户自身保管，相当于U盾的概念，从而使得文件能够安全存储，并且当Mini2440丢失时，由于存储模块中是存储的加密后的文件，不会在没有得到认证和密钥的情况下破解。同时，SM4模块与声纹识别模块也有效的防止了暴力破解，极大提高了系统的安全性能。

## 2.1.6.文件管理模块

该模块放在电脑端的应用中，实现了用户能够更加方便的传输和选择文件。并且有界面友好性，操作简单的特性。为的是让系统使用与操作更加的简单与友好。

## 2.1.7.数据包处理模块

数据包处理模块是用于处理PC端与Mini2440之间的数据处理，为数据进行解（打）包帧头，帧头的内容以此为指令、数据长度、数据校验和指令校验。其中，指令用于PC与硬件之间的通信，通过自己定义可用于登陆、注册、录音、文件操作等；数据长度和数据校验用于帧头后面所携带的数据，数据校验采用CRC16；指令校验用于校验帧头中的指令，采用与全一异或的方式。

# 2.2.系统工作流程



# 三、技术点总结

* 使用mini2440作为系统搭载平台，进行用户声音信息获取、身份验证、文件存储、文件加密解密操作。
* 使用QT作为用户界面开发框架，在PC端和mini2440端均实现用户交互界面。
* 使用RSA非对称加密算法对用户的账户文本密码进行保护，由mini2440端生成公钥和私钥，公钥发送至PC端对文本密码进行加密，私钥存放在mini2440端用于身份验证。
* 使用SM4算法对用户的文件进行进行加密解密，文件存放在mini2440端。
* 使用MFCC梅尔频率倒谱系数，作为后续的建立和训练声纹模型以及身份验证中的说话人特征参数。
* 使用GMM(高斯混合模型)作为声纹识别模型，利用说话人的声音特征参数进行建立声纹模型，用不同参数的高斯分布的概率统计模型来表征不同的说话人身份。
* 使用EM(最大期望)算法来训练说话人模型，即得到说话人GMM模型的参数。
* 使用K-means（K均值聚类）算法进行EM算法的初始化，即获得高斯混合模型的阶数和初始化参数。

# 四、测试与分析

# 4.1测试方案

本团队制定了详细的测试计划，并且将应用移植到真机与Mini2440操作板上，演练各项功能操作，以下是各项功能测试及预期结果：

|  |  |  |
| --- | --- | --- |
| 测试类型 | 测试内容 | 预期结果 |
| 功能性测试 | 声纹数据采集模块 | 能够成功录入声音和采集特征值 |
| 声纹特征训练模块 | 能够使用HMM算法成功得到训练模块 |
| 声纹特征身份识别模块 | 能够成功声纹识别 |
| 文件加密解密模块 | 能够成功用SM4算法加密解密 |
| 用户注册模块 | 能够成功注册并得到响应信息 |
| 安全性测试 | 应用安全性测试 | 加密文件解密后仍然为乱码或身份认证失败。 |
| 系统安全性测试 | PC端无法查找到模型文件，mini2440端模型库存在模型文件 |
| PC安全性测试 | 存储和取回文件的身份控制已启用 |
| 稳定性测试 | 应用稳定性测试 | 应用稳定运行，无BUG出现 |
| 系统稳定性测试 | 系统无异常 |
| PC端稳定测试 | PC端能够正常运行并处理文件操作 |

表5-1-1 系统功能测试方案

# 4.2结果分析

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

该系统由登陆模块(包括：普通登陆与注册模块、声纹数据收集模块)、声纹识别模块（包括：数据建模训练模块、身份识别模块）、RSA模块、文件存储模块、SM4加密\解密模块、文件管理等模块组成。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四道有效的安全防护。首先是对用户的账户安全与数据信息用RSA模块采取了安全保护。其次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，同事系统是由各个模块组成，做到了整个系统模块间有较高的解耦性，模块内有较高的耦合度，整个系统可靠性高。

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。

# 五、安全评估

基于Mini2440的声纹认证加密系统的设计理念是本系统通过收集用户的声纹特征，利用声纹识别相关技术，进行用户身份识别，同时利用了SM4算法加密与解密技术、RSA加密解密模块来保证文件与账户信息在两个硬件平台中传输的安全性。在这个过程中，没有显式密码，也没有直接可观察的身份认证操作；而针对本系统可能存在的攻击方式，主要有：肩窥攻击、暴力破解、字典攻击、数据泄漏、生物特征伪造等。

对于本系统对于各种攻击安全性分析如下：

1. 肩窥攻击：

本系统的解锁密码为用户的“操作习惯”，这便无法通过视线观测获取解锁密码，因此，本系统可以抵抗肩窥攻击。

2. 暴力破解：

与肩窥攻击相同，由于本系统不存在显式的密码，所以攻击者无法穷举构造伪造密码，对本系统进行解锁。因此，本系统可以抵抗暴力破解。

3. 字典攻击：

攻击者无法穷举构造本系统的解锁方式，同样更难于特定的字典来攻击本系统。因此，本系统可以抵抗字典攻击。

4. 数据泄漏：

至于数据泄漏问题，攻击者也许可以通过读取电脑信息获取到用户的电脑与Mini2440交互数据信息。但是，一方面本系统收集的数据已通过SM4算法进行加密。同时，攻击者即便破获了我们的数据，也很难获得文件实际的内容，只能获得文件加密后的内容因此，本系统可以抵抗数据泄漏。

另一方面，本系统加入了RSA加密，RSA加密模块在Mini2440启动后便开始运行，保证了PC端与Mini2440之间账户信息的安全性，有效防止了数据泄露的问题。

5. 生物特征伪造：

本系统所采用的生物特征并不像虹膜识别、人脸识别有一个固定的可以直观显示的特征，用户的声纹是无法用机器或是模仿来简单的得到识别。由于每个人个人的声音与发声时的震动都有所不同，获得的特征值也不同。因此，本系统可以抵抗生物特征伪造。

所以，在防御外来攻击方面，本作品提出的基于Mini2440的声纹认证加密系统目前已有的加密系统与方式更加可靠。

目前，我们团队已对本系统进行了一套完整的系统测试，进一步改进了算法的准确度，确保了本作品的安全性。

# 六、创新点总结

* + **功能集成增加安全性**

我们将文件的加密解密、文件的存储、声纹特征的存放、模型训练及模型库的生成、模型的匹配过程均搭载在硬件平台mini2440上，不易被破解读取用户信息和文件，同时将功能与PC端隔离，使用户的相关数据集成存储、使用时形成的动态信息存放集中得到更好的保护。同时，本系统将声纹识别和SM4加密算法、RSA加密算法结合，使用从数据存储和数据获取两个方向进行双重保护，使数据的安全性大大增加，用户的信息数据得到有效的保护。

* + **声纹特征结合文件加密多维保护**

我们将由用户的语音提取出的声纹MFCC特征值通过转换作为加密文件的密钥，声纹特征值存放于硬件平台不易被获取，同时声纹的特征性和独一性为文件加密提供了第一道防线。

* + **双重密码保护**

我们在使用用户的声纹作为身份验证的方式的同时，还添加了普通的文本密码作为第一道密码保护，与普遍性的密码输入结合，使得在声纹识别过程之前有另一层保护，并且双重的保护降低任一密码出现失误造成的风险，更加保障了用户的个人数据安全。

* + **产品化设计提高用户体验**

我们的初衷是以安全性为主导产品化为辅助的设计方案，利用mini2440的体积小性能全的优点，借鉴“U盾”的设计思想，并且拓展功能，将用户使用系统的主要流程搭载在硬件平台，与声纹的“便携性”结合，大大提升了用户的使用体验质量，同时，将验证与PC机分离，使用户可以随时随地进行文件获取查看，同时集成度高将功能分离又保证用户在使用中的安全性。

* + **产品成本低**

sm4加密算法在软硬件的运行速度快不消耗过多资源，节省了开发成本，同时mini2440功能齐全且价格较低，声纹识别技术所需的设备支持仅为一个麦克风，在实现功能的情况下成本要求较低，从硬件角度降低了开销。

# 七、未来工作

通过对数据安全性保护的分析，我们团队将保护过程分为对数据本体的加密、数据传输的保护和数据获取途径的安全性控制，经过调研，从数据本体加密和数据获取途径的安全性控制来开发系统。

我们团队提出了基于mini2440的声纹认证加密系统，本系统由声纹数据收集模块、数据建模训练模块、身份识别模块、SM4加密/解密模块、登录与注册模块、文件管理模块，在本系统中，用户利用声纹和普通文本密码进行对文件查看的双重保护，同时文件经过加密，成为文件的更加有力防线。将系统搭载在mini2440上，便于用户携带和功能的分隔保护。

基于以上的系统研发，我们还需要做以下方面的工作：

1）硬件优化方面：

在声纹识别过程中，需要提高采样率来获得更高的识别精确度，但提高采样率需要一定的硬件支持，我们计划选择效率更高的硬件平台，达到集成滤波器、采样精度高等硬件支持。

2）降低能耗方面：

目前我们的硬件平台使用的是mini2440，性价比十分高且系统运行稳定，但存在运载本系统耗电量的较高的情况。未来我们在条件允许下计划选择运载相同系统的情况下耗电量更低的硬件设备，达到更好的用户体验。

同时，我们还需要在以下多方面降低能耗，优化算法提高运算效率，提高识别准确率，使识别精度，数据加密解密过程与系统能耗三方面的关系，达到平衡，实现最优方案。

3）产品化方面：

我们在研发系统时就立足于以安全性为中心产品化为辅助的方案，将系统搭载在mini2440是我们对产品化做出的第一步，但是为了用户有更好的使用体验，未来我们计划将文件的存储放置云端，同时结合传输协议的制定，对数据传输过程进行安全控制，使得用户的数据量有更好的拓展空间，也使系统的适用对象范围更大化。