**2015年全国大学生信息安全竞赛**

**作品报告**

**作品名称：基于Mini2440的声纹认证加密系统**

**电子邮箱：yijunqianshi@126.com**

**提交日期： 2016.05.28**

填写说明

1. 所有参赛项目必须为一个基本完整的设计。作品报告书旨在能够清晰准确地阐述（或图示）该参赛队的参赛项目（或方案）。

2. 作品报告采用A4纸撰写。除标题外，所有内容必需为宋体、小四号字、1.5倍行距。

3. 作品报告中各项目说明文字部分仅供参考，作品报告书撰写完毕后，请删除所有说明文字。(本页不删除)

4. 作品报告模板里已经列的内容仅供参考，作者可以在此基础上增加内容或对文档结构进行微调。

5. 为保证网评的公平、公正，作品报告中应避免出现作者所在学校、院系和指导教师等泄露身份的信息。

目录

[**摘要** 4](#_Toc452133827)

[第一章 作品概述 5](#_Toc452133828)

[1.1背景分析 5](#_Toc452133829)

[1.2相关工作 6](#_Toc452133830)

[1.2.1声纹识别： 7](#_Toc452133831)

[1.2.2SM4算法 8](#_Toc452133832)

[1.2.3mini2440介绍 10](#_Toc452133833)

[1.3特色描述 11](#_Toc452133834)

[1.4应用前景分析 11](#_Toc452133835)

[第二章 作品设计与实现 13](#_Toc452133836)

[2.1.系统整体框架 13](#_Toc452133837)

[2.1.1登陆模块 14](#_Toc452133838)

[2.1.2.RSA模块 14](#_Toc452133839)

[2.1.3.声纹识别模块 14](#_Toc452133840)

[2.1.4.SM4加密\解密模块 15](#_Toc452133841)

[2.1.5.文件存储模块 16](#_Toc452133842)

[2.1.6.文件管理模块 16](#_Toc452133843)

[2.1.7.数据包处理模块 16](#_Toc452133844)

[2.2.系统工作流程 17](#_Toc452133845)

[第三章 核心算法与模型分析 18](#_Toc452133846)

[3.1.SM4算法分析 18](#_Toc452133847)

[3.1.1SM4算法的术语说明 18](#_Toc452133848)

[3.1.2SM4算法的数学原理 19](#_Toc452133849)

[3.1.3SM4算法的实现 20](#_Toc452133850)

[3.2.声纹识别算法与模型介绍 25](#_Toc452133851)

[3.2.1声纹识别介绍 25](#_Toc452133852)

[3.2.2声纹特征值MFCC提取技术 27](#_Toc452133853)

[3.2.3 GMM模型概述 33](#_Toc452133854)

[3.3. RSA算法分析 42](#_Toc452133855)

[3.3.1 RSA算法分析 42](#_Toc452133856)

[3.3.2 RSA算法实现过程 45](#_Toc452133857)

[3.3.3 RSA算法实现核心 47](#_Toc452133858)

[第四章 作品测试与分析 50](#_Toc452133859)

[4.1测试方案 50](#_Toc452133860)

[4.2测试环境 51](#_Toc452133861)

[4.3测试用例与分析 51](#_Toc452133862)

[4.5安全性分析 55](#_Toc452133863)

[4.6测试结果 56](#_Toc452133864)

[第五章 创新性说明 58](#_Toc452133865)

[第六章 总结与展望 59](#_Toc452133866)

[参考文献 61](#_Toc452133867)

# 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**

# 第一章 作品概述

# 1.1背景分析

随着互联网的迅速发展，人们的生活走向了“数字化”，无论是个人或是机构、企业等都将信息数字化。例如在互联网时代成为潮流的电子商务，让人们可以通过互联网进行网络购物、银行转账等。同时对于商业活动如商业贸易、金融财务等，大部分已经以数字化信息的方式在网上流动，而电子银行及电子货币的研究、实施和标准化开始普及。

不仅仅在金融行业，信息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；一个是对信息传输的保护，另一个是对获取信息进行安全控制。

（一） 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。“U盾”存放用户个人的数字证书，同样银行也记录相同的数字证书。当进行网上交易时，银行发送加密后的字串A至“U盾”,“U盾”进行不可逆运算得到字串B发送至银行端，同时银行端也进行该不可逆运算，所得结果与字串B匹配，若一致则交易成功，不一致则失败。

基于“U盾”的设计思路，随着电子硬件技术的发展，类“U盾”产品的功能拓展空间日益增大。类“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。

基于以上背景分析，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。

# 1.2相关工作

基于对作品的背景分析，我们从生物识别技术、数据加密算法和硬件平台三个方面进行调查研究，确定使用声纹识别技术实现身份验证，SM4算法进行数据加密/解密，同时将系统搭载在mini2440平台。

## 1.2.1声纹识别：

进入21世纪，集光学、传感技术、超声波扫描和计算机技术等于一身的生物识别技术开始广泛作为身份验证技术被使用，用于身份验证的生物识别特征可分为固有生理特征和行为特征，主要有声纹、指纹、掌纹、虹膜、笔迹、步态等。

（一）面部识别

面部识别技术是根据人的脸面特征的唯一性特点而进行的个体识别和确认技术。人的面部特征的唯一性,可以在脸上某一单一器官 或部位上得以体现，更重要的是可在这些单一特征之间的位置、距离、 角度、数量、形状和模式等相互关系上得以体现。Windows10生物识别系统Windows Hello具有三种识别模式：面部、虹膜和指纹。但面部识别功能目前只能通过类似微软体感设备Kinect的Intel RealSense F200实感摄像头实现，该设备由三部分组成：红外线模块、3D模块、普通摄像头，因此价格较为昂贵，同时尚未能在移动设备上集成，因此还需硬件技术的提升来帮助面部识别更高质量的广泛使用。同时移动设备上的面部识别由于摄像头等硬件条件限制，安全性下降，可能通过图像等方式进行破解。

（二）虹膜识别

虹膜是眼球前部含色素的环形薄膜，由结缔组织细胞、肌纤维等构成，所含色素的多少直接决定着眼球的颜色。每个人的眼睛虹膜引起不同的精细结构而有特定性且稳定性。微软于2015年10月发布的Win10旗舰手机Lumia950、Lumia950 XL亮点之一就是支持虹膜识别，理论上只要硬件厂商为用户更新固件之后，用户就可以在升级Win10 Mobile后使用虹膜扫描登录，不过在使用虹膜识别时用户需要靠近摄像头。

(三)声纹识别

声纹识别技术是20世纪中期在美国提出的，最早进行此项技术研究的是美国贝尔实验室的劳伦斯•克斯特，他对一百多名健康人的上万个声纹图进行了分析鉴定，准确度达到99.65%。

如今在世界范围内，声纹识别技术已经应用于金融、刑侦以及其他民用安全认证系统等诸多领域。在电话勒索一类的案件中, 最容易获得的证据就是电话录音, 通过声纹识别技术, 就能根据电话录音获得线索, 缩短破案周期。声音样本在刑侦和司法上的作用已经日渐受到重视。AT&T(美国电话电报公司)研制的基于声纹识别技术的智慧卡（smart card)己应用于自动提款机。欧洲电信联盟于1998年完成了CAVE计划,并于同年又启动了IPCASSO计划,在电信网上完成了声纹识别。同时,Motorola和Visa等公司成立了V-commerce联盟,希望实现电子交易的自助化,其中通过声音确定人的身份是此项目的重要组成部分。汇丰银行和花旗银行都增加的声纹识别来加强对用户账户的安全保护。

声纹识别广泛使用的原因在于：1）其认证方式易于接受，用户只需要提供语音信息；2）语音信息获取方便、自然，涉及到的用户个人隐私信息较少，因此使用者更易接受；3）不需要昂贵易损的硬件设备，如指纹、面部、虹膜识别等都需要较高精度和较高价格的信息输入设备；4）应用推广较为方便，如基于电信网络的身份识别应用如电话银行等，和声纹识别技术结合更为方便直接。

## 1.2.2SM4算法

随着无线局域网(Wireless Local Area Network, WLAN) 的日益普及，其传输信息的安全性面临严峻的挑战。采用数据加密技术是保证用户信息在传输过程中不被暴露、盗用和篡改的有效方式。SM4算法即原SMS4算法，是由国家商用密码管理办公室于2006年1月公布的用于无线局域网产品的分组对称密码算法。SM4 密码算法是国内官方公 布的第1个商用密码算法，并且在2012年3月被国家密码 管理局批准为行业标准[1]。SM4 算法的分组长度为128 bits，密钥长度为128 bits。加密算法与密钥扩展算法都采用32 轮 非线性迭代结构，其中使用到32 bits 循环移位、S盒，解密过程与加密过程的结构相似，只是轮密钥的使用顺序相反。SM4 的安全性除密钥外，内在的是S盒的非线性特性。

（一）安全性分析

在密码学中，基于Feistel 网络的分组密码的安全性依赖于轮函数中所使用的 S 盒，因此S盒的设计至关重要。加密算法S盒良好的非线性特性，在理论上保证算法的抗线性密码分析能力，所以S盒的特性反映算法的安全性。

针对128bits加密算法 SM4、AES、Camellia 及 SEED 中S盒分析情况对比，如下表所示。

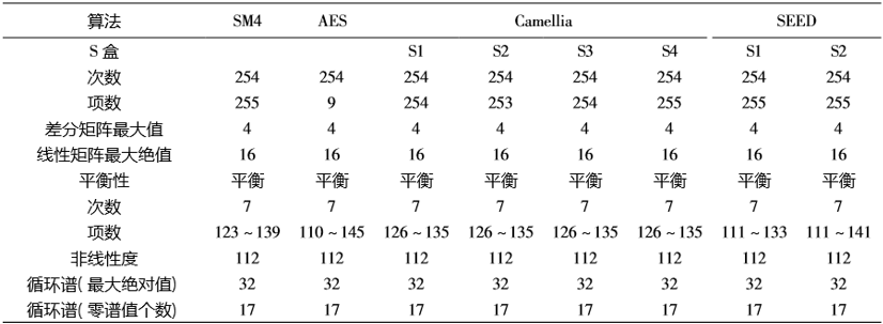


表1 S盒性质比较

从表1中可以看出 SM4 算法和 Camellia 算法的S盒代数项数为 255，而 AES 算法仅为9，可见SM4 算法和 Camellia 算法的S盒代数表达式比 AES 更复杂，从而具有更好的安全性。

（二）加解密效率

加密算法在各种软硬件平台实现的速度，反映 了它们的应用。针对 PC 和 FPGA 实现做了部分分析讨论。在软环境下，对DES、3DES、AES、SM4 等算法， 在 Windows 764 位旗舰版，CPUI5 M450 2.4 GHz，内存4GBDDR3的环境中做了简单测试，分别得出的加解密效率如表2所示。

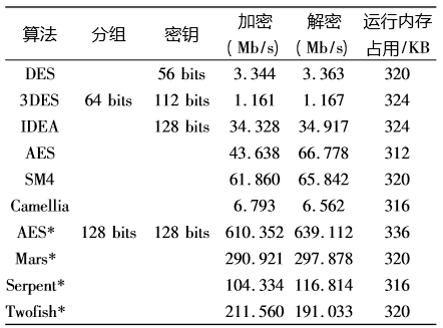


表2 各种算法加解密速度

在硬件实现中，取3个代表算法AES、SM4、Camellia 进行对比。它们均在 128 bits 分组、128 bits 密钥的情况下，加解密实现效率比较如表3所示：

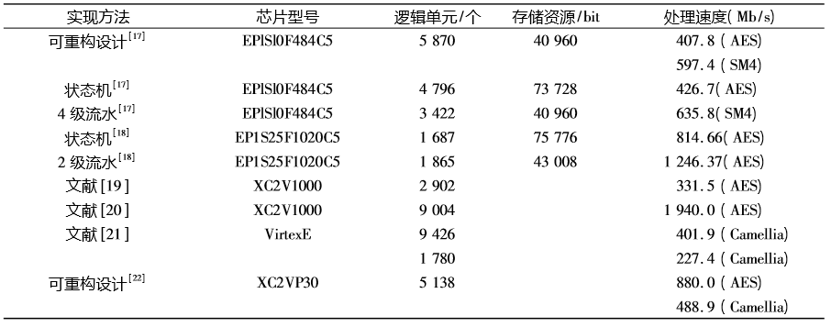


表3 AES、SM4、Camellia算法硬件实现比较

表3 中可见，SM4 算法在使用逻辑单元和存储资源上比 AES 要少得多，但加解密速度要快不少。在文献［1］中，使用相同资源的可重构设计表明了Camellia 算法比AES算法要慢不少，这也说明 Camellia 算法结构要比 AES 算法复杂。

综合上述调研，SM4 算法作为分组密码算法，与公钥密码算法相比不仅数据吞吐率高，消耗的硬件资源也相对较少，且由于其实现简单，SM4 算法非常适合在智能数据卡、物联网传感节点等对面积和成本要求比较严格的场合使用。因此我们选择SM4算法搭载在mini2440上对文件进行加密解密。

## 1.2.3mini2440介绍

Mini2440是一款低价实用的ARM9开发板，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。mini2440的PCB采用沉金工艺的四层板设计，专业等长布线，保证关键信号线的信号完整性。

ARM9系列处理器是英国ARM公司设计的主流嵌入式处理器，采用5级流水线的哈佛结构。增加的流水线设计提高了时钟频率和并行处理能力。相比ARM7改进了指令周期对于处理器性能的提高有很大的帮助。ARM9一般是有MMU(内存管理单元), MMU单元是大型操作系统必需的硬件支持，如LINUX;WINCE等，一般的操作系统都可以移植。

# 1.3特色描述

* 安全性：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。
* 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。
* 透明性：本系统的声纹识别和文件加密解密过程完全在硬件平台运行，PC前端界面仅显示响应获得的文件，不会让用户感受到任何认证存在的迹象。
* 便携性：将身份验证和文件存储集成在mini2440嵌入式处理器中，便于用户携带，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。

# 1.4应用前景分析

在处于信息时代的今天，任何交流的信息可以转换成对应形式的数据进行传输、存储、处理，因此掌握数据无论对个人还是团体都是掌握竞争力的体现之一。大数据研究的先河之作《大数据时代》中，维克托·迈尔·舍恩伯格前瞻性地指出，大数据带来的信息风暴正在变革我们的生活、工作和思维，大数据开启了一次重大的时代转型，并用三个部分讲述了大数据时代的思维变革、商业变革和管理变革。因此除了处理好数据之外，对数据进行安全性保护的重要性也上升到了新的地位。

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。

我们团队的系统以安全性为第一要务，围绕这个，对于数据本体加密，通过国内外加密算法的比较，我们选择了我国发布的SM4算法进行数据的加密，SM4算法有密钥长度长不易被破解，在软硬件平台实现速度快等优点。对于数据获取途径的安全控制，我们从生物特征识别技术入手，比较了当今主流的识别技术，选定了性能较好且用户接受度高的声纹识别技术。同时，对于用户账户密码的传输和保护，我们使用了非对称加密算法RSA，使用户的身份验证有了双重防线。

除了把握安全性的性能提高，我们将系统的实现搭载在mini2440ARM处理器上，实现了系统的产品化，有便携性、功能集成度高等优点，同时mini2440结合SM4、RSA加密算法和声纹识别技术的使用从某些程度上降低了产品的成本。综上所述，我们团队的作品有较好的应用发展前景。

# 第二章 作品设计与实现

# 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



图2-3 系统工作流程图

# 第三章 核心算法与模型分析

# 3.1.SM4算法分析

国密算法即国家密码局认定的国产密码算法，即商用密码。

商用密码，是指能够实现商用密码算法的加密、解密和认证等功能的技术。（包括密码算法编程技术和密码算法芯片、加密卡等的实现技术）。商用密码技术是商用密码的核心，国家将商用密码技术列入国家秘密，任何单位和个人都有责任和义务保护商用密码技术的秘密。

商用密码的应用领域十分广泛，主要用于对不涉及国家秘密内容但又具有敏感性的内部信息、行政事务信息、经济信息等进行加密保护。比如：商用密码可用于企业门禁管理、企业内部的各类敏感信息的传输加密、存储加密，防止非法的第三方获取信息内容；也可用于各种安全认证、网上银行、数字签名等。

为了保障商用密码安全，国家商用密码管理办公室制定了一系列密码标准，包括SSF33、SM1（SCB2）、SM2、SM3、SM4、SM7、SM9、祖冲之密码算法等等。其中SSF33、SM1、SM4、SM7、祖冲之密码 是对称算法；SM2、SM9是非对称算法；SM3是哈希算法。

SM4算法作为国密算法的一种，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。

## 3.1.1SM4算法的术语说明

1.字与字节

用表示e比特的向量集，用中的元素表示字，中的元素称为字节。

2. S盒

S 盒为固定的8比特输入8比特输出的置换，记为*Sbox*(.)。

3. 基本运算

在本算法中采用了以下基本运算：

(1)⊕： 32 比特异或  
(2) <<<i：32 比特循环左移i位

4.密钥及密钥参量

加密密钥长度为 128 比特，表示为，其中为字。

轮密钥表示为其中为字。轮密钥由加密密钥生成。  
为系统参数，为固定参数，用于密钥扩展算法，其中、 为字。

## 3.1.2SM4算法的数学原理

1.轮函数 F

本算法采用非线性迭代结构，以字为单位进行加密运算，称一次迭代运算为一轮变换。设输入为，轮密钥为，则轮函数F为：

2.合成置换

，是一个可逆变换，由非线性变换 τ 和线性变换 L 复合而成，T(.)=L(τ(.))

1. 非线性变换τ

τ 由 4 个并行的 S 盒构成。设输入为 ,输出为入为,则

1. 线性变换L

非线性变换 τ 的输出是线性变换L的输入。设输入为 ，输出为 ，则

3.S盒

S盒中数据均采用16进制表示。

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | a | b | c | d | e | f |
| 0 | d6 | 90 | e9 | fe | cc | e1 | 3d | b7 | 16 | b6 | 14 | c2 | 28 | fb | 2c | 05 |
| 1 | 2b | 67 | 9a | 76 | 2a | be | 04 | c3 | aa | 44 | 13 | 26 | 49 | 86 | 06 | 99 |
| 2 | 9c | 42 | 50 | f4 | 91 | ef | 98 | 7a | 33 | 54 | 0b | 43 | ed | cf | ac | 62 |
| 3 | e4 | b3 | 1c | a9 | c9 | 08 | e8 | 95 | 80 | df | 94 | fa | 75 | 8f | 3f | a6 |
| 4 | 47 | 07 | a7 | fc | f3 | 73 | 17 | ba | 83 | 59 | 3c | 19 | e6 | 85 | 4f | a8 |
| 5 | 68 | 6b | 81 | b2 | 71 | 64 | da | 8b | f8 | eb | 0f | 4b | 70 | 56 | 9d | 35 |
| 6 | 1e | 24 | 0e | 5e | 63 | 58 | d1 | a2 | 25 | 22 | 7c | 3b | 01 | 21 | 78 | 87 |
| 7 | d4 | 00 | 46 | 57 | 9f | d3 | 27 | 52 | 4c | 36 | 02 | e7 | a0 | c4 | c8 | 9e |
| 8 | ea | bf | 8a | d2 | 40 | c7 | 38 | b5 | a3 | f7 | f2 | ce | f9 | 61 | 15 | a1 |
| 9 | e0 | ae | 5d | a4 | 9b | 34 | 1a | 55 | ad | 93 | 32 | 30 | f5 | 8c | b1 | e3 |
| a | 1d | f6 | e2 | 2e | 82 | 66 | ca | 60 | c0 | 29 | 23 | ab | 0d | 53 | 4e | 6f |
| b | d5 | db | 37 | 45 | de | fd | 8e | 2f | 03 | ff | 6a | 72 | 6d | 6c | 5b | 51 |
| c | 8d | 1b | af | 92 | bb | dd | bc | 7f | 11 | d9 | 5c | 41 | 1f | 10 | 5a | d8 |
| d | 0a | c1 | 31 | 88 | a5 | cd | 7b | bd | 2d | 74 | d0 | 12 | b8 | e5 | b4 | b0 |
| e | 89 | 69 | 97 | 4a | 0c | 96 | 77 | 7e | 65 | b9 | f1 | 09 | c5 | 6e | c6 | 84 |
| f | 18 | f0 | 7d | ec | 3a | dc | 4d | 20 | 79 | ee | 5f | 3e | d7 | cb | 39 | 48 |

例：输入‘ef’，则经S盒后的值为表中第e行和第f列的值，*Sbox*(‘ef’)= ‘84’。

4.加/解密算法

定义反序变换R为。

设明文输入为，密文输出为，轮密钥为。则本算法的加密变换为：

本算法的解密变换与加密变换结构相同，不同的仅是轮密钥的使用顺序。加密时轮密钥的使用顺序为：（*rk*0, *rk*1, …, *rk*31）；解密时轮密钥的使用顺序为：（*rk*31, *rk*30, …, *rk*0）

## 3.1.3SM4算法的实现

1、加密过程实现：

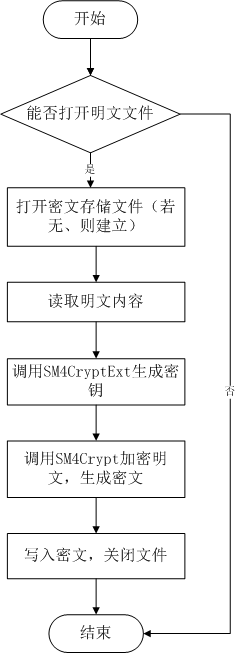


图3-1 加密实现流程图

2、解密过程实现：

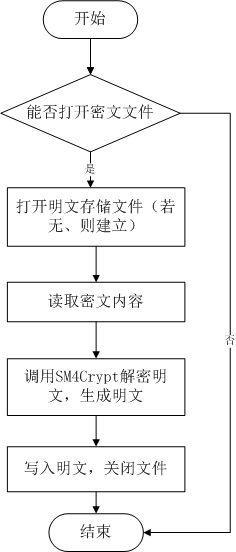


图3-2 解密实现流程图

3、SMS4的加解密函数

参数说明：Input为输入信息分组，Output为输出分组，rk为轮密钥

void SMS4Crypt(muint8 \*Input, muint8 \*Output, muint32 \*rk)

{

muint32 r, mid, x0, x1, x2, x3, \*p;

p = (muint32 \*)Input;

x0 = p[0];

x1 = p[1];

x2 = p[2];

x3 = p[3];

#ifdef LITTLE\_ENDIAN

x0 = Rotl(x0, 16); x0 = ((x0 & 0x00FF00FF) << 8) ^ ((x0 & 0xFF00FF00) >> 8);

x1 = Rotl(x1, 16); x1 = ((x1 & 0x00FF00FF) << 8) ^ ((x1 & 0xFF00FF00) >> 8);

x2 = Rotl(x2, 16); x2 = ((x2 & 0x00FF00FF) << 8) ^ ((x2 & 0xFF00FF00) >> 8);

x3 = Rotl(x3, 16); x3 = ((x3 & 0x00FF00FF) << 8) ^ ((x3 & 0xFF00FF00) >> 8);

#endif

for (r = 0; r < 32; r += 4)

{

mid = x1 ^ x2 ^ x3 ^ rk[r + 0];

mid = ByteSub(mid);

x0 ^= L1(mid);

mid = x2 ^ x3 ^ x0 ^ rk[r + 1];

mid = ByteSub(mid);

x1 ^= L1(mid);

mid = x3 ^ x0 ^ x1 ^ rk[r + 2];

mid = ByteSub(mid);

x2 ^= L1(mid);

mid = x0 ^ x1 ^ x2 ^ rk[r + 3];

mid = ByteSub(mid);

x3 ^= L1(mid);

}

#ifdef LITTLE\_ENDIAN

x0 = Rotl(x0, 16); x0 = ((x0 & 0x00FF00FF) << 8) ^ ((x0 & 0xFF00FF00) >> 8);

x1 = Rotl(x1, 16); x1 = ((x1 & 0x00FF00FF) << 8) ^ ((x1 & 0xFF00FF00) >> 8);

x2 = Rotl(x2, 16); x2 = ((x2 & 0x00FF00FF) << 8) ^ ((x2 & 0xFF00FF00) >> 8);

x3 = Rotl(x3, 16); x3 = ((x3 & 0x00FF00FF) << 8) ^ ((x3 & 0xFF00FF00) >> 8);

#endif

p = (muint32 \*)Output;

p[0] = x3;

p[1] = x2;

p[2] = x1;

p[3] = x0;

}

4、SMS4的密钥扩展算法

参数说明：Key为加密密钥，rk为子密钥，CryptFlag为加解密标志

void SMS4KeyExt(muint8 \*Key, muint32 \*rk, muint32 CryptFlag)

{

muint32 r, mid, x0, x1, x2, x3, \*p;

p = (muint32 \*)Key;

x0 = p[0];

x1 = p[1];

x2 = p[2];

x3 = p[3];

#ifdef LITTLE\_ENDIAN

x0 = Rotl(x0, 16); x0 = ((x0 & 0xFF00FF) << 8) ^ ((x0 & 0xFF00FF00) >> 8);

x1 = Rotl(x1, 16); x1 = ((x1 & 0xFF00FF) << 8) ^ ((x1 & 0xFF00FF00) >> 8);

x2 = Rotl(x2, 16); x2 = ((x2 & 0xFF00FF) << 8) ^ ((x2 & 0xFF00FF00) >> 8);

x3 = Rotl(x3, 16); x3 = ((x3 & 0xFF00FF) << 8) ^ ((x3 & 0xFF00FF00) >> 8);

#endif

x0 ^= 0xa3b1bac6;

x1 ^= 0x56aa3350;

x2 ^= 0x677d9197;

x3 ^= 0xb27022dc;

for (r = 0; r < 32; r += 4)

{

mid = x1 ^ x2 ^ x3 ^ CK[r + 0];

mid = ByteSub(mid);

rk[r + 0] = x0 ^= L2(mid);

mid = x2 ^ x3 ^ x0 ^ CK[r + 1];

mid = ByteSub(mid);

rk[r + 1] = x1 ^= L2(mid);

mid = x3 ^ x0 ^ x1 ^ CK[r + 2];

mid = ByteSub(mid);

rk[r + 2] = x2 ^= L2(mid);

mid = x0 ^ x1 ^ x2 ^ CK[r + 3];

mid = ByteSub(mid);

rk[r + 3] = x3 ^= L2(mid);

}

if (CryptFlag == DECRYPT)

{

for (r = 0; r < 16; r++)

mid = rk[r], rk[r] = rk[31 - r], rk[31 - r] = mid;

}

}

# 3.2.声纹识别算法与模型介绍

## 3.2.1声纹识别介绍

当今社会处于一个信息时代，信息安全尤其重要。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。

在生物识别领域中，声纹识别也称为说话人识别以其独特的方便性、经济性和准确性等优势受到世人瞩目,并日益成为人们日常生活和工作中重要且普遍的安全认证方式。说话人识别是一种根据说话人语音波形中反映说话人生理和行为特征的语音参数自动识别说话人身份的技术。说话人识别可以看作是语音识别的一种,是指通过对说话人语音信号的特征分析与参数提取,从而能对说话人身份进行辨认和确认。

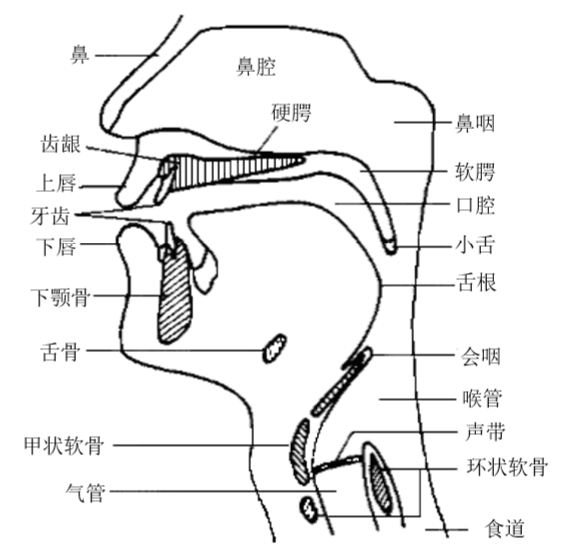


图3-3

由于每个人的声音器官，诸如声带、口腔、鼻腔、舌、齿、 唇、肺等，在发音时呈现千姿百态，抑或有着哪怕是微小 的差异，以及年龄、性格、语言习惯等多种原因，再加上 发音容量的大小不一，发音频率的不尽相同，因而导致这 些器官发出的声音必然有着各自的特点，形成每个人独具一格的声纹(Voiceprint)，可用语谱图观察出来。

基于声纹识别系统的不同应用，声纹识别系统的技术实现基本上可以分归两类，即说话人确认技术和说话人辨认技术。本系统所运用到的是说话人辨认技术，用于辨认未知说话人是否是已记录的说话人中的哪一位。

从声纹识别系统的使用场合来看，需要判别的声音其来源基本可分为3种情况，即文本提示型、文本相关型和文本无关型。文本无关型的声纹识别系统的技术含量要求比较高，它不仅仅需要解决匹配判断问题，还需要预先提取说话人的语音特征，才能进行判断识别。本系统所运用到的是文本无关型声纹识别技术，预先提取梅尔倒谱系数作为语音的特征。

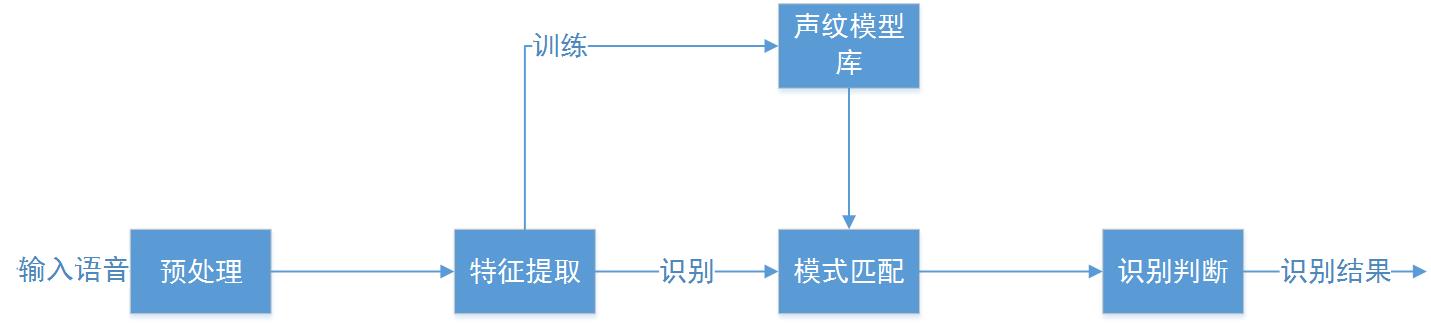


图3-4声纹识别处理流程

## 3.2.2声纹特征值MFCC提取技术

1、梅尔倒谱系数提取流程

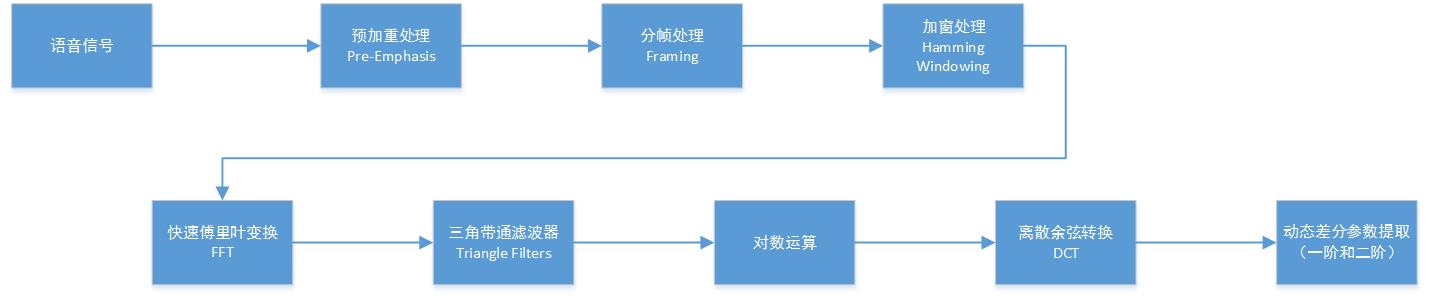


图3-5梅尔倒谱系数提取流程图

所得的维MFCC参数



下图是处理8000Hz采样频率单通道的录音文件所得到的MFCC 特征值结果

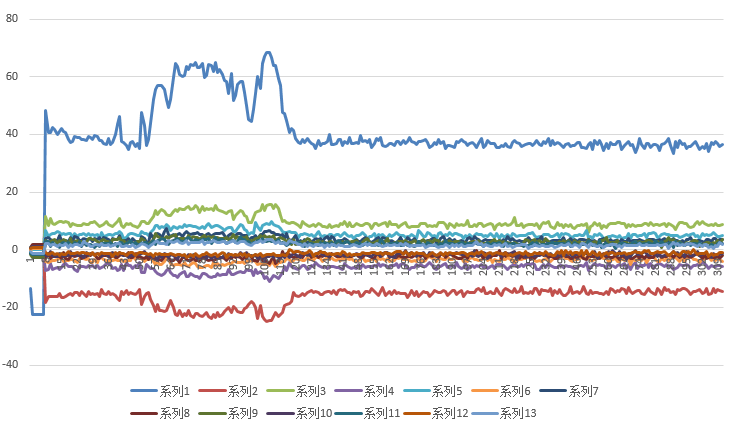


图3-6 MFCC特征值（条数：维度，横轴：组数，纵轴MFCC特征值）

2、语音数据序列预处理

(1)预加重处理

预加重处理其实是将语音信号通过一个高通滤波器，公式中μ的值介于0.9-1.0之间，我们通常取0.97。预加重的目的是提升高频部分，使信号的频谱变得平坦，保持在低频到高频的整个频带中，能用同样的信噪比求频谱。同时，也是为了消除发生过程中声带和嘴唇的效应，来补偿语音信号受到发音系统所抑制的高频部分，也为了突出高频的共振峰。

(2)分帧处理

先将N个采样点集合成一个观测单位，称为帧。通常情况下N的值为256或512，涵盖的时间约为20~30ms左右。为了避免相邻两帧的变化过大，因此会让两相邻帧之间有一段重叠区域，此重叠区域包含了M个取样点，通常M的值约为N的1/2或1/3。通常语音识别所采用语音信号的采样频率为8KHz或16KHz，以8KHz来说，若帧的长度为256个采样点，则对应的时间长度是256/8000×1000=32ms。

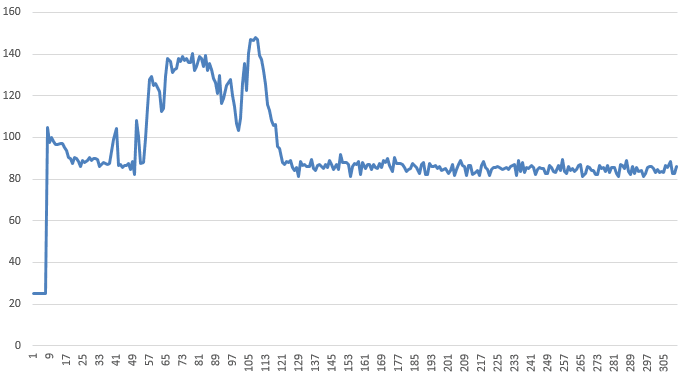


图3-7 帧能量图（横轴表示帧数，纵轴:频域下一帧的积累能量）

(3)加窗处理

语音信号一般在10ms到30ms之间，我们可以把它看成是平稳的。为了处理语音信号，我们要对语音信号进行加窗，也就是一次仅处理窗中的数据。因为实际的语音信号是很长的，不能也不必对非常长的数据进行一次性处理，解决办法就是每次取一段数据，进行分析，然后再取下一段数据，再进行分析。

仅取一段数据的方式就是构造一个函数，这个函数在某一区间有非零值，而在其余区间皆为0。汉明窗就是这样的一种函数，它主要部分的近似sin（x）在0到pi区间的形状，而其余部分都是0。这样的函数乘上其他任何一个函数f，f只有一部分有非零值，也就是提取出了我们所需要提取的一段数据。

汉明窗之所以这样提取数据因为之后我们会对汉明窗中的数据进行FFT快速傅里叶变换，它假设一个窗内的信号是代表一个周期的信号，也就是说窗的左端和右端应该大致能连在一起。而通常一小段音频数据没有明显的周期性，加上汉明窗后，数据形状就类似有周期性。因为加上汉明窗，只有中间的数据体现出来了，两边的数据信息丢失了，所以等会移窗的时候，只会移1/3或1/2窗，这样被前一帧或二帧丢失的数据又重新得到了体现。

假设分帧后的信号为S(n), n=0,1…,N-1, N为帧的大小，那么乘上汉明窗函数:

后,W(n)形式如下，不同的a值会产生不同的汉明窗，一般情况下a取0.46:

3、快速傅里叶变换

(1)傅里叶变换原理

对于任何一个函数的曲线，傅立叶认为任何一个复杂的曲线都可以分解为正弦函数与余弦函数的叠加，下图公式表现实值函数的傅立叶级数:

利用傅里叶级数思想，我们可以把复杂的函数进行分解进而处理：

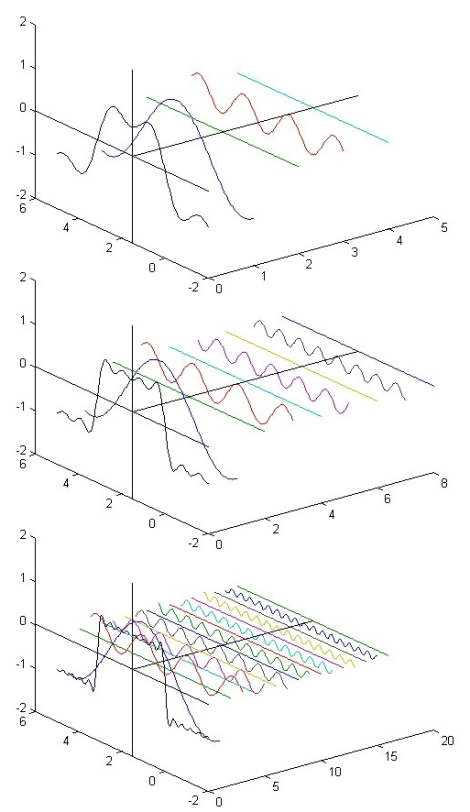


图3-8 分解复杂函数

傅里叶变换就是把时域中的函数转换成了频域中的函数，以方便我们做数据的处理，处理完之后，用同样的原理再做一次傅立叶逆变换就得到了我们所需的结果。

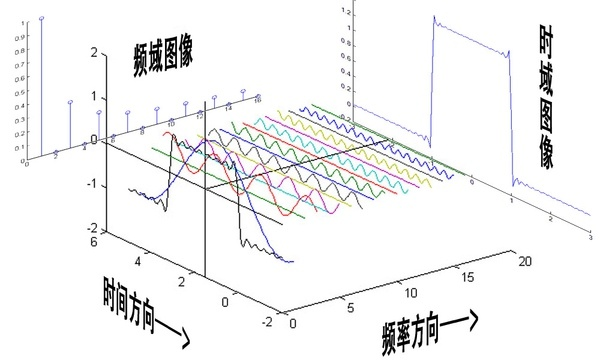


图3-9 时域图像和频域图像的关系

时域和频域间转换主要利用傅里叶级数和傅里叶变换，由于快速傅里叶变换FTT有计算量小的优点，结合高速硬件就能对信号进行实时处理，因此我们在本系统中通过快速傅里叶变换FTT进行时域和频域的转换。

（2) FFT的具体计算方法

FFT的计算方法被称为蝶形计算：

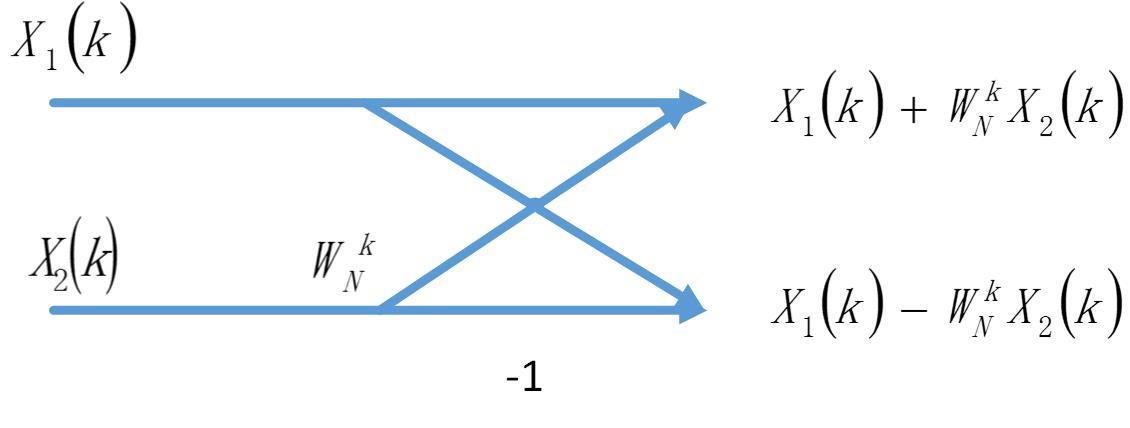


图3-10

以8点FFT（8个数的）为例：

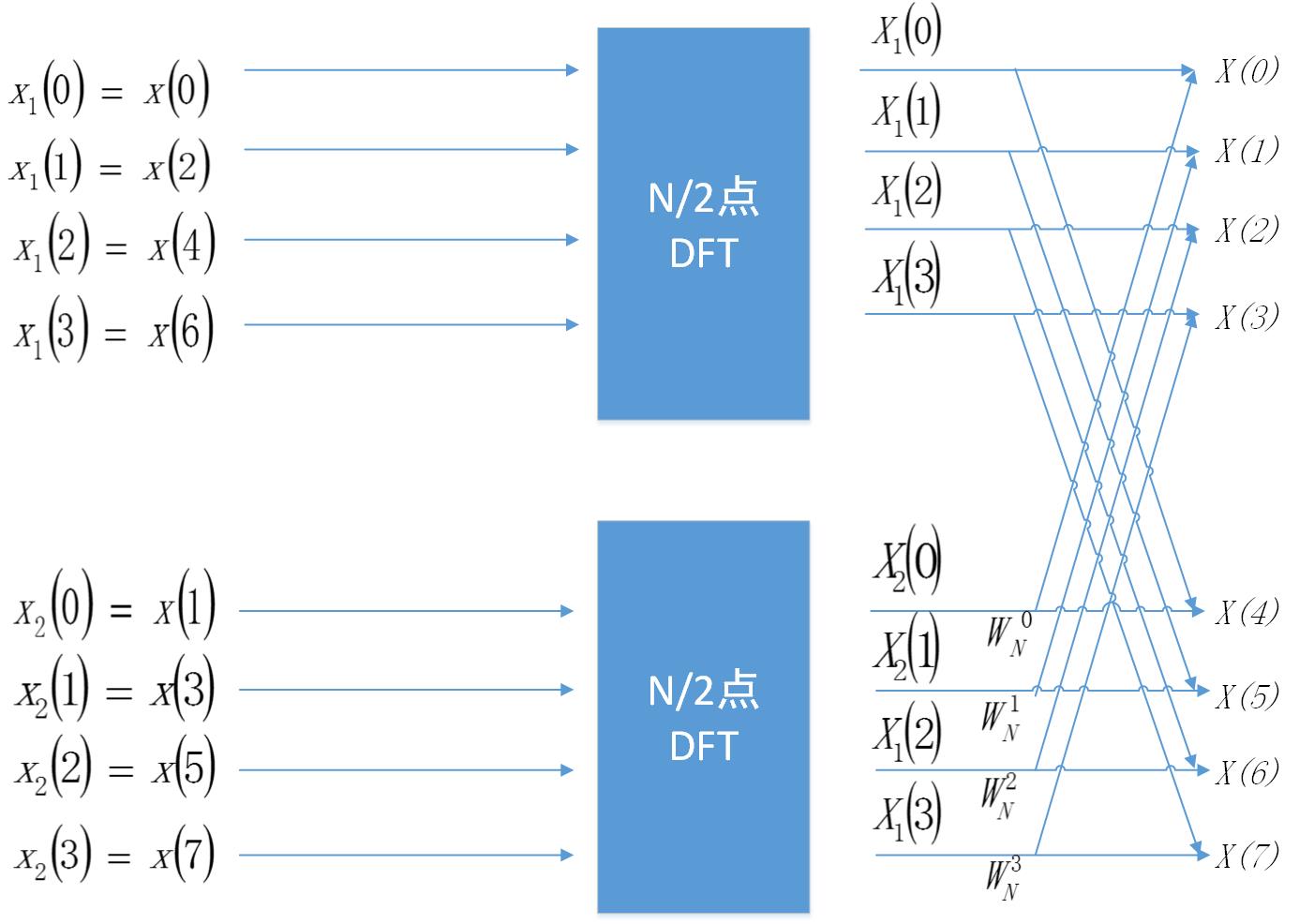


图3-11

4、三角带通滤波器

三角带通滤波器有两个主要作用：对频谱进行平滑化，便于后续计算以及提取MFCC特征值，并且消除谐波，突显原先语音的共振峰。因此一段语音的音调或音高，是不会呈现在 MFCC 参数内，换句话说，以 MFCC 为特征的语音辨识系统，并不会受到输入语音的音调不同而有所影响。此外，还可以降低运算量。

三角滤波器的频率响应定义为:

式中：

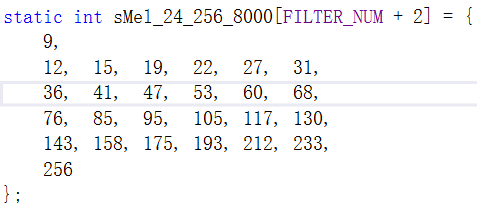


图3-11 在采样率8000Hz下计算的三角带通滤波器频率数组

对数能量即一帧的音量（即能量），也是语音的重要特征，而且非常容易计算。因此，通常会再加上一帧的对数能量（定义：一帧内信号的平方和，再取以10为底的对数值，再乘以10）使得每一帧基本的语音特征就多了一维，包括一个对数能量和剩下的倒频谱参数。若要加入其它语音特征以测试识别率，也可以在此阶段加入，这些常用的其它语音特征包含音高、过零率以及共振峰等。计算每个滤波器组输出的对数能量为：

5、离散余弦转换

离散余弦变换（Discrete Cosine Transform，简称DCT变换）是一种与傅立叶变换紧密相关的数学运算。在傅立叶级数展开式中，如果被展开的函数是实偶函数，那么其傅立叶级数中只包含余弦项，再将其离散化可导出余弦变换，因此称之为离散余弦变换。

经过离散余弦变换可以得到MFCC系数，将上述的对数能量带入离散余弦变换，求出L阶的Mel-scale Cepstrum参数。L阶指MFCC系数阶数，通常取12-16。这里M是三角滤波器个数。：

,

6、动态查分参数提取（一阶和二阶）

标准的倒谱参数MFCC只反映了语音参数的静态特性，语音的动态特性可以用这些静态特征的差分谱来描述。实验证明：把动、静态特征结合起来才能有效提高系统的识别性能。差分参数的计算可以采用下面的公式：



## 3.2.3 GMM模型概述

**一、GMM模型的理论依据和数学定理**

GMM 模型也称高斯混合模型（Gaussian Mixture Model）,它是一种概率统计模型。GMM 模型应用于声纹识别中主要有两点依据:其一，说话人的语音可以认为是由不同的音素构成的，而同一音素则可以归为一类。故由一系列语音帧提取出来的特征参数序列可以根据不同的音素而进行分类。从概率分布的角度来讲，一个说话人的特征参数在特征空间中的分布是由表征其发不同音素的特征矢量序列的分布集合而成的，而某一类特征矢量服从同一高斯分布。其二，在统计学中，一个任意分布可以由多个高斯分布的线性组合来表示。因此，高斯混合模型从理论上可以描述各种语音特征的统计分布。

基于GMM 模型的声纹识别的基本原理就是为每一个说话人建立一个GMM 模型，模型参数是由特征矢量的分布决定的。由于表征每一个说话人个性特征的特征矢量服从的概率分布是不一样的，故 GMM 模型参数也是不同的。因此可以用参数不同的高斯分布的概率统模型来表征说话人的身份。

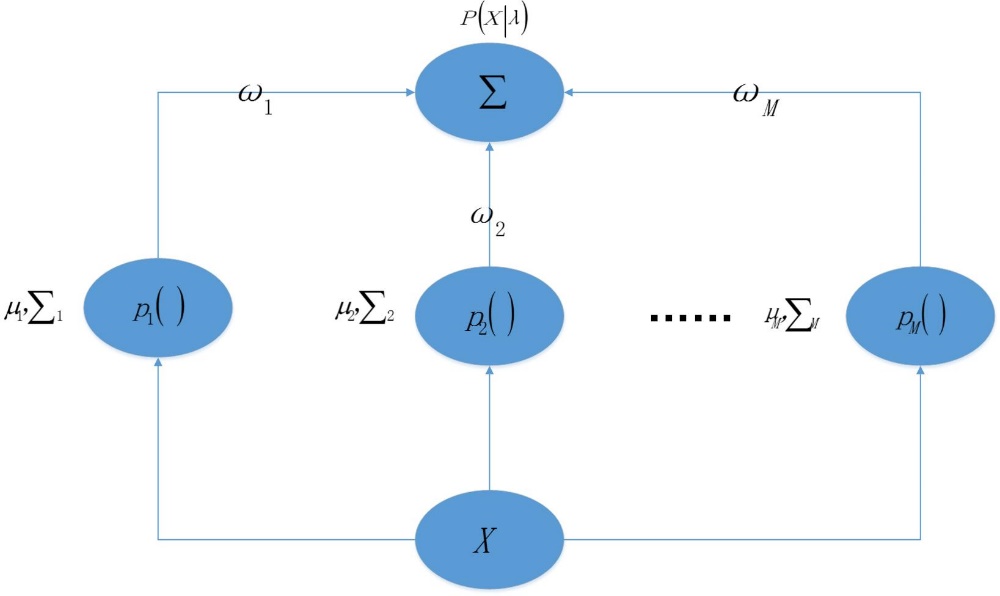


图3-12 GMM模型示意图

由GMM模型示意图可知，一个阶的高斯混合模型是由个高斯概率密度函数按照一定的加权系数 叠加而成的。对于任一测试的特征矢量 与通过特征矢量样本训练后得到的GMM模型匹配的概率输出为：

式中，表示单个的高斯概率密度函数的个数，即高斯混合模型的阶数，表示特征矢量的帧数，表示第帧特征矢量，表示第个高斯概率密度函数的加权系数，且有：

对于任一个子分布，它是一个D维的高斯概率密度函数，表示为：



其中，D表示特征矢量的维数，表示第个高斯子分布的均值，表示第个高斯子分布的方差，为的对角阵：



式中，是GMM 模型中第个子分布对应的特征矢量的第个分量的方差。

综上所述，一个阶的高斯混合模型可由下列参数来描述：

(1) :高斯混合模型的阶数或是模型中子高斯概率密度函数的个数。

(2) ，:每个子高斯概率密度函数的均值和方差。

(3) :表示每个子高斯概率密度函数的加权系数。

于是把一个GMM模型简记为：



**二、GMM模型的参数估计**

一个GMM模型是由四个参数来表征，这四个参数即代表了一个说话人模型。我们在作品设计中选择最大期望算法（Expectation Maximization Algorithm，EM）作为参数估计的方法。

**(1)EM算法原理**

EM算法是一种估计GMM模型参数的经典迭代算法，该算法分为两个步骤：E步（E-step）和M步（M-step）。如下图所示：

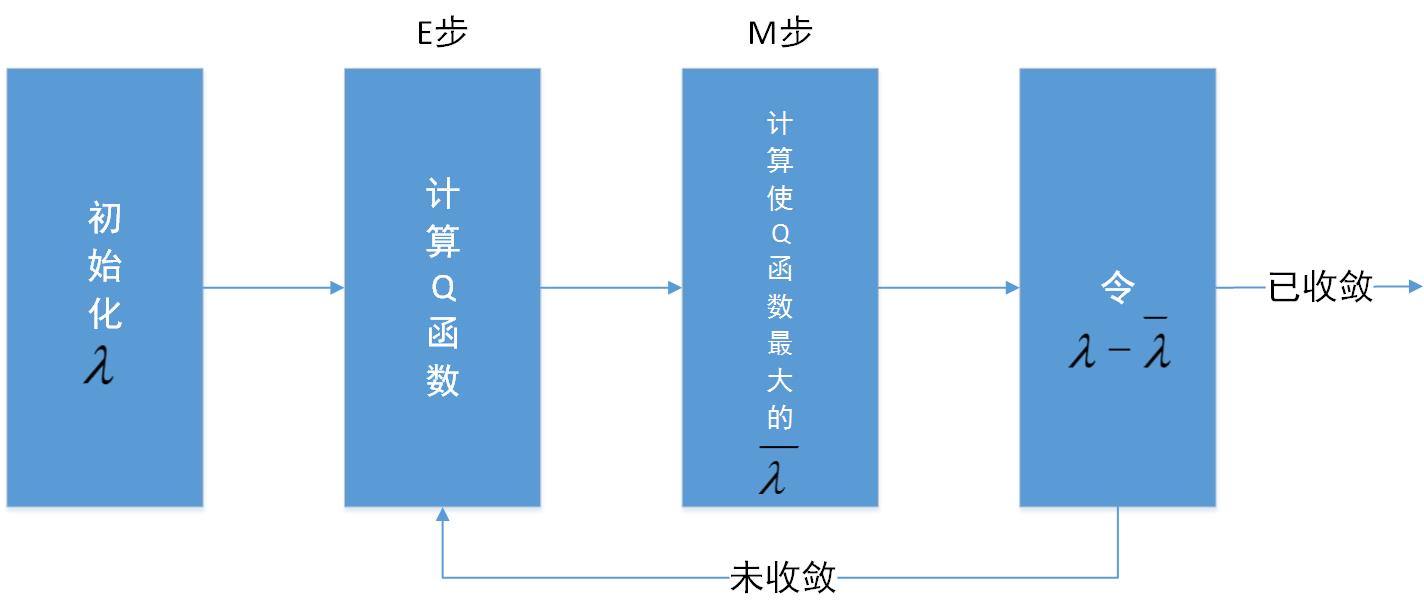


图3-13 EM算法流程图

设为可观测数据，服从参数为的某种概率分布，为不可知数据，和一起构成完整数据集，则其联合概率密度函数可表示为：



定义似然函数为，和是常量，未知且服从参数为的某一概率分布：



算法中的E步就是求完整数据集中的未知量的对数似然函数的数学期望，即定义函数：



上式中，是当前参数值，是新的参数值，是迭代次数。通过E步去掉了变量。算法中的M步就是对E步的数学期望进行最大化，从而得到新的参数值：



E步和M步反复迭代，直至似然函数收敛到局部极大值。

**(2)用EM算法估计GMM参数**

根据EM算法的基本原理，并结合具体的语音高斯混合模型来求GMM参数。GMM模型的概率密度函数：

则非完整样本集的对数似然函数表示为：



由于上式中的似然函数是对数的和的形式，很难求极值。然而是可观测的非完整样本数据集，假定存在未知数据项，则和一起构成完整数据集,完整数据集的对数似然函数表示为：



由E步计算上述完整数据集的对数似然函数的数学期望：



展开得：



其中，表示在模型参数和样本集合已知的情况下，样本属于第个子高斯分布的后验概率，该后验概率有下式计算，其中表示第次循环。



通过EM算法的M步找到使似然函数最大化的模型参数。由可知，是由两项相加得到，对第一项进行最大化即可估计加权系数，对第二项最大化即可得到均值与协方差矩阵。

特征矢量落入状态的概率为：



由此得到GMM模型三个参数的重估公式。

第个子高斯子分布的加权系数重估公式为：



第个子高斯子分布的均值矢量重估公式为：



第个子高斯子分布的方差矩阵重估公式为：



**三、GMM模型的初始化**

使用EM算法首先要获得高斯混合模型的阶数和初始化参数，我们在作品设计中选择K-means（K均值聚类）算法将特征矢量分为个聚类，进行初始化。

设训练数据集为,GMM模型的阶数为，数据集相应的分为类，模型的初始化即是对这个数据进行聚类分析，并求出每一类的均值和方差。

步骤1：在训练数据集中，任意选取个特征矢量，通常选取样本集中最开始的个特征矢量，作为初始聚类中心，记为：，其中上标表示迭代次数。

步骤2：逐个将需分类的模式样本按最小距离准则分配给个聚类中心中的某一个，若满足

 且

则属于第类。

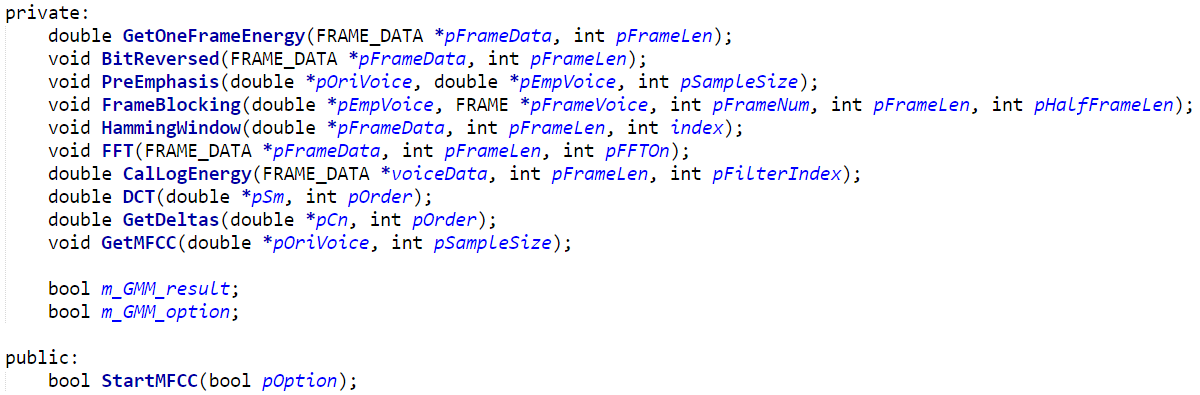
步骤3：重新计算各类的聚类中心，正式中为第个聚类域中所包含的样本数据的个数。

步骤4：若，则返回至步骤2，若，则算法收敛，计算结束。

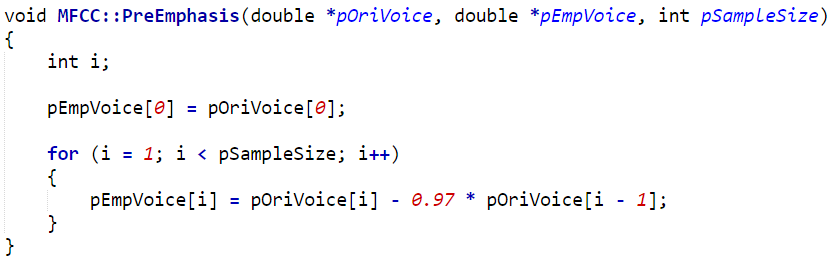
**四、GMM模型的实现**

**(一)MFCC模块主要函数**

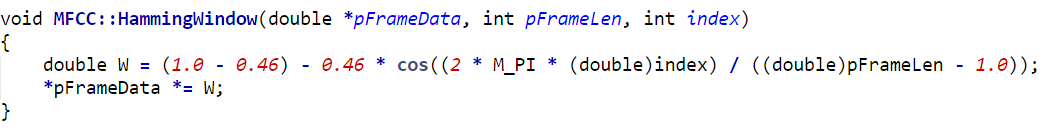


下面为按照MFCC声纹特征值提取的流程具体函数的实现：

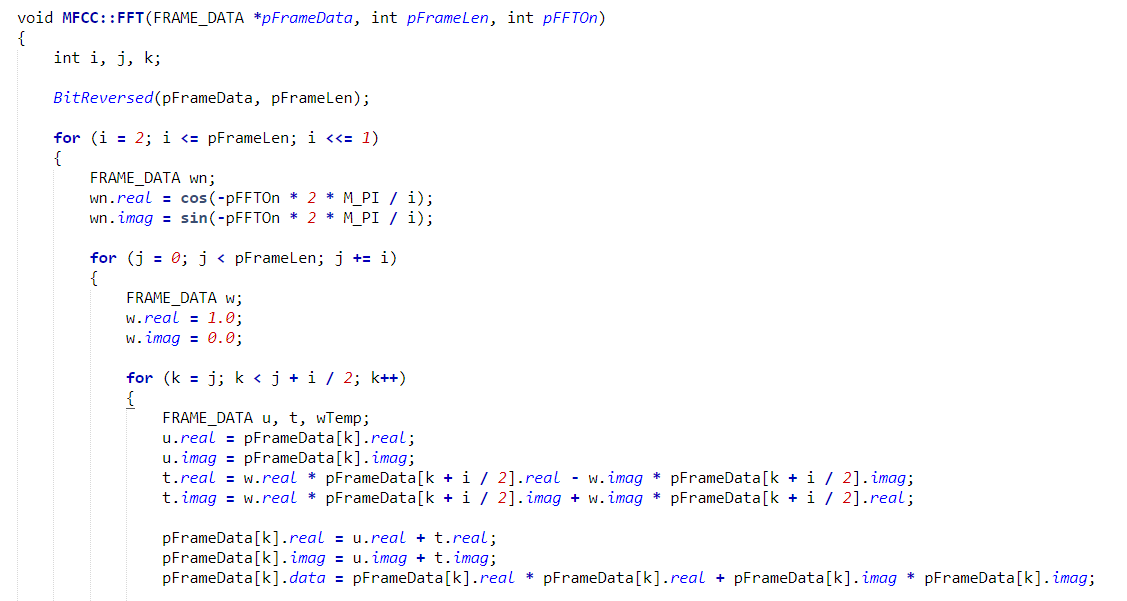
(1)预加重处理函数：

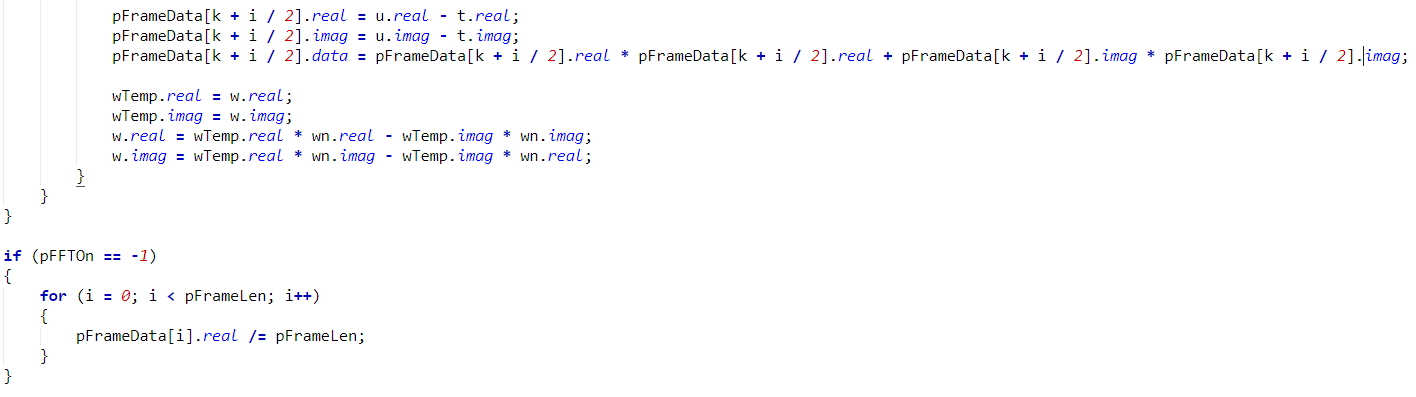


(2)汉明窗化函数：

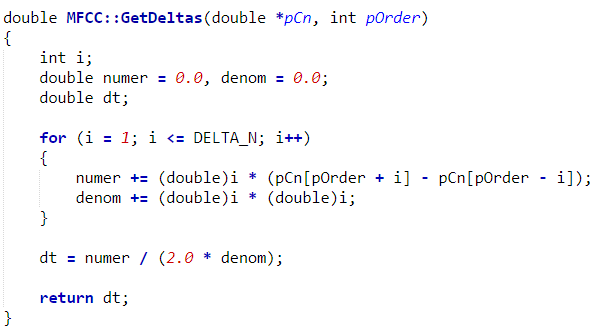


(3)快速傅里叶变换函数：

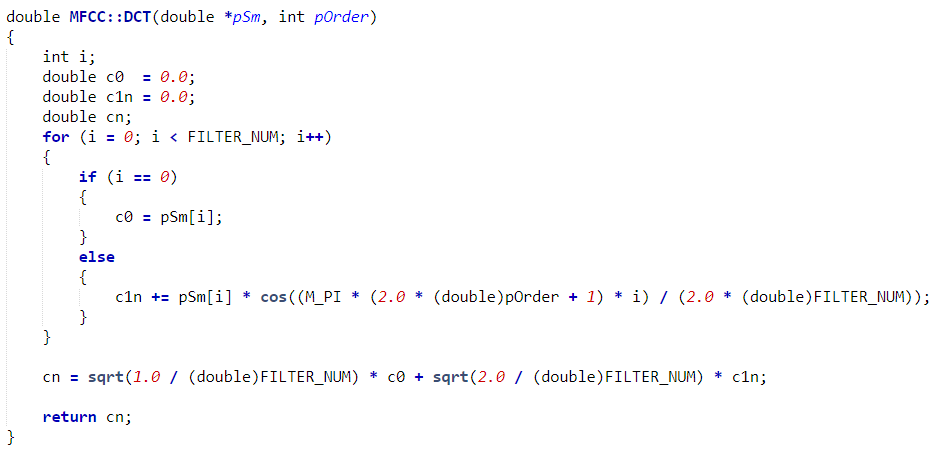


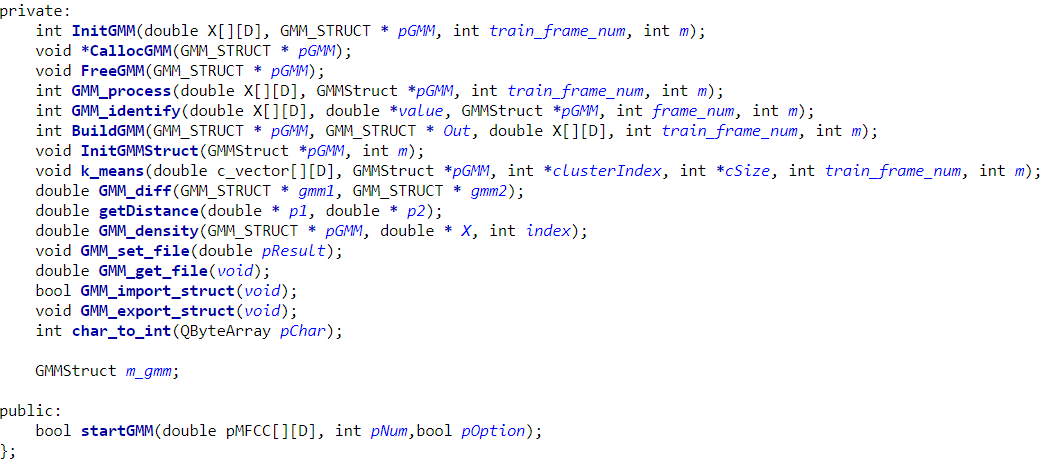


(4)三角滤波处理函数：



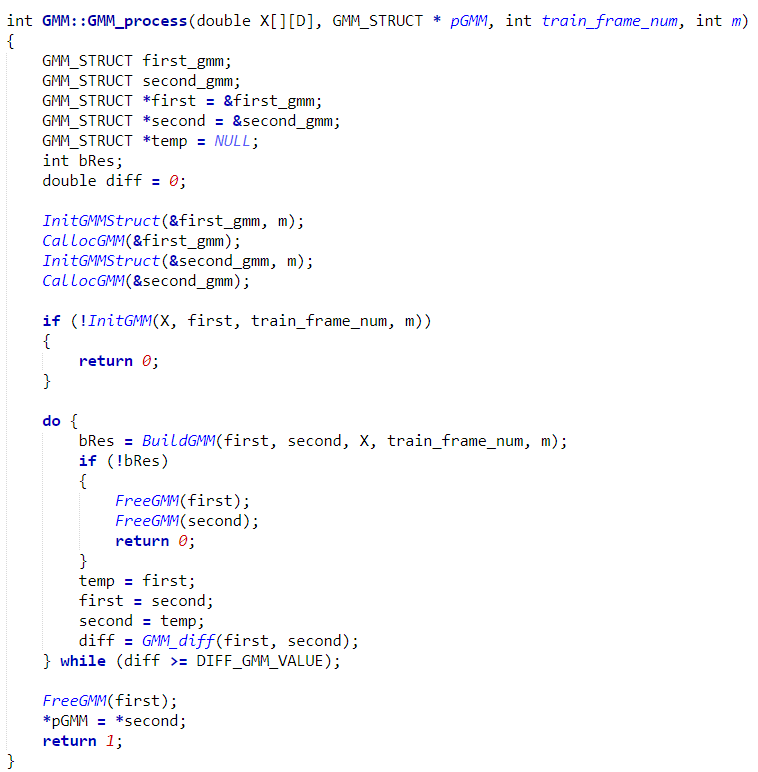
(5)离散余弦转换函数：

**(二)GMM模块主要函数**

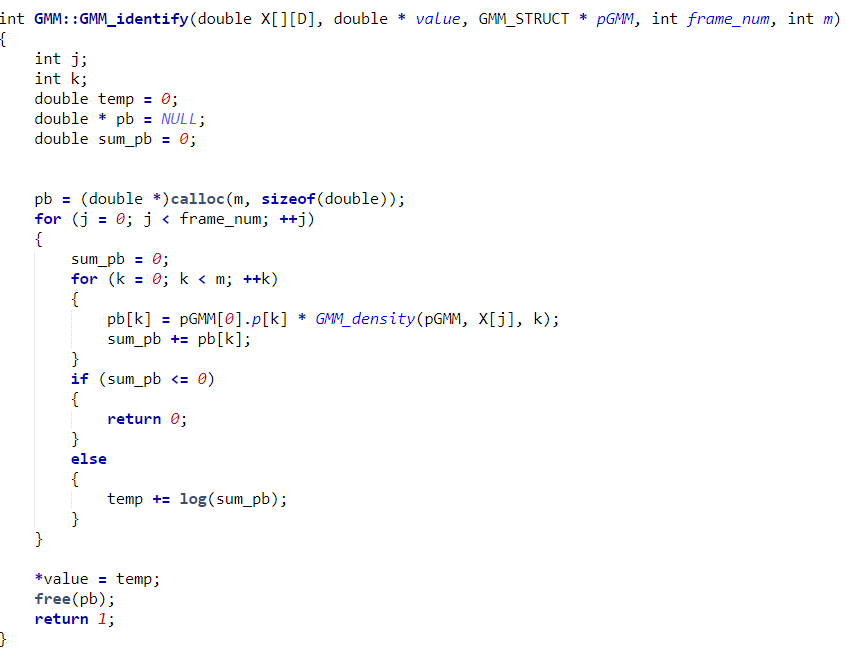


下面为按照GMM声纹模型建模、训练、识别的流程具体函数的实现：

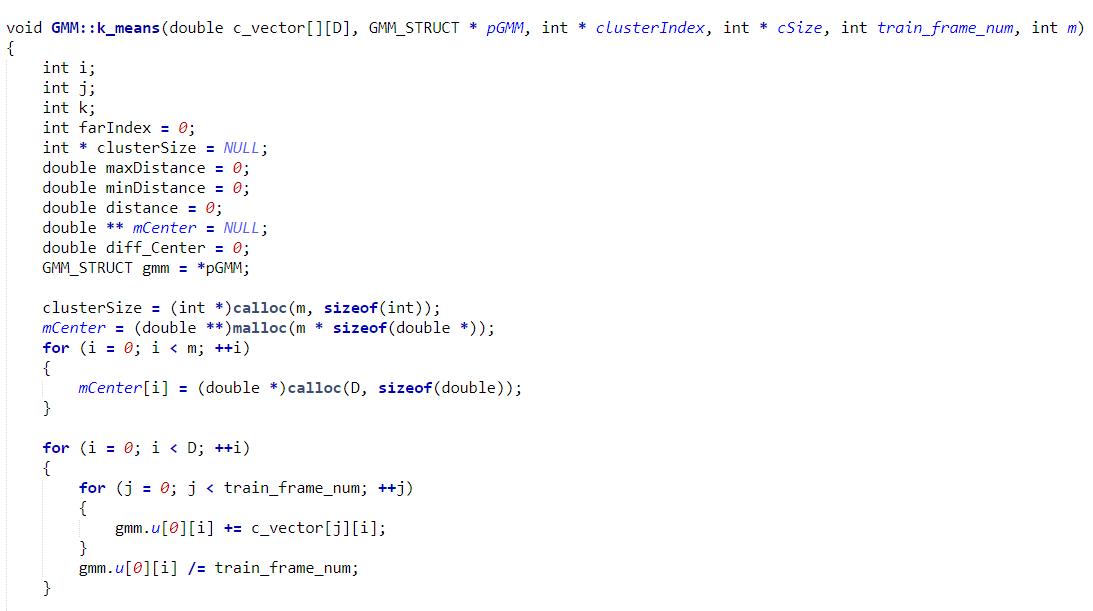
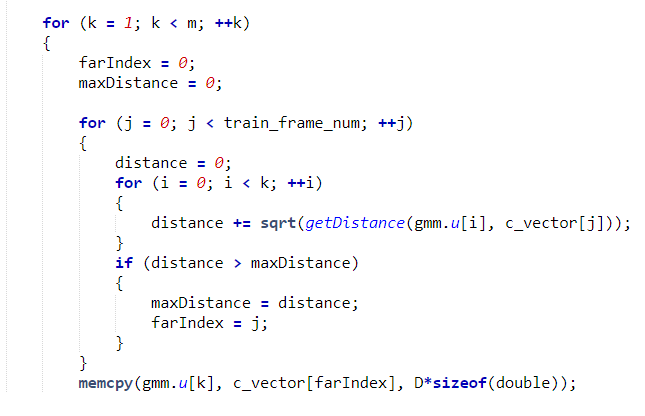
1. GMM模型建立函数：



1. 计算后验概率，GMM模型识别函数：



(3)K-means算法函数（部分）：

# 3.3. RSA算法分析

## 3.3.1 RSA算法分析

RSA密码体制是美国麻省理工学院（MIT）Rivest、Shami和Adleman于1978年提出来的，它是第一个理论上最为成功的公开密钥密码体制，它的安全性基于数论中的Euler定理和计算复杂性理论中的下述论断：求两个大素数的乘积是很容易计算的，但要分解两个大素数的乘积，求出它 们的素数因子却是非常困难的，它属于NP—完全类，是一种幂模运算的加密体制。除了用于加密外，它还能用于数字签字和身份认证。下面将从各个方面来详细对 RSA公钥体制进行研究。

1、RSA的构成

RSA系统由以下几部分组成：

(1) 随机选取的在素数和，还有 ，其中，和保密，公开。

(2) 任取，其中表示比小的素数的个数，任取, 且为加密密钥，公开。

(3) 计算，使称为对模的逆，其中为解密秘钥，保密。

在RSA系统中，设为明文，且明文块的数值大小小于为,密文，则其加密和解密算法如下：

加密算法

加密算法

在RSA系统中构成加密秘钥，即公钥，构成解密秘钥，即私钥。

2、RSA思想的证明

RSA是基于数论中的Euler定理和其它同余性质的，在证明RSA系统思想正确性之前，先给出Euler定理和同余式相乘的性质：

Euler定理：设即和 互素，则有:

同余式相乘性质,设有:

则有:

证明RSA系统思想正确性主要是看能否从密文和解密秘钥恢复明文,即由和,计算出:

下面就证明是否能从密文和解密密钥恢复明文,

因为

所以,其中为任意整数。

由解密公式有：

又由Euler定理有:

同样由同余式相乘性质有:

由于明文块数值大小小于,则有:

故RSA中，能利用和恢复明文,则RSA的系统思想证明是正确的。但众所周知RSA是基于整数因子分解的密码体制，它利用的是：求两个大素数的乘积是很容易计算的，但分解密两个大素数的乘积，求出它们的素数因子却是非常困难的，这样一个数学难题，它属于NP-完全类。因此RSA的安全性完全信赖于因子分解的困难性，只要被因子分解，则RSA便被击破，这样在RSA系统中怎样选取大的素数，才是关键所在。

3、RSA中素数的选取

在RSA中，因,若，被知道，即能将*N*因子分解，则由可以算出。由于*e*是公开密钥，且解密秘钥*D*关于*E*满足

则*D*也不难求得，这样RSA系统便被完全攻破。

RSA中的素数都是上面位的十进制数，怎样才能选择好的*P*和*Q*，怎样才能生成这样的数，并且判断它是否为素数，这是一个RSA系统关键的问题。针对素数*P*和*Q*的选择，1978年Rivest等人在正式发表的RSA公开密钥的论文中，就建议对素数*P*和*Q*的选择应当满足：

(1) *P、Q*要足够在，在长度上应相差几位，且二者之差与*P、Q*位数相近；

(2) *P-1*与*Q-1*的最大公约数GCD(*P-1,Q-1*)就尽量小；

(3) *P-1*与*Q-1*均应至少含有一个大的素数因子。

并把满足这些条件的素数称为安全素数。

4、RSA安全性分析

在公布RSA算法之后，在使用RSA密码体制和分析RSA算法发现了一系列的算法本身脆弱性及其存在的问题。

（1）RSA公钥密码体制在加密或解密变化中涉及大量的数值计算，其加密和解密的运算时间比较长，这比数据加密标准DES的计算量开销大，在一定程度上限制了它的应用范围，以致于实际使用RSA密码体制无法用软件产品，必须用超大规模集成电路的硬件产品。

（2）虽然提高N=P\*Q的位数会大大提高RSA密码体制的安全性，但其计算量呈指数增长，以致使其实现的难度增大，实用性降低。

（3）RSA公钥密码体制的算法完整性（指密钥控制加密或解密变换的唯一性）和安全性（指密码算法除密钥本身外，不应该存在其它可破译密码体制的可能性）沿有等进一步完善。

（4）RSA算法面临着数学方法的进步和计算机技术飞跃发展带来的破译密码能力日趋增强的严重挑战。因子分解问题有了长跑的发展，1995年人类成功地分解了128位十进制数RSA密码算法，破译512位长的RSA指日可待。

尽管如此，自1978年RSA算法公布以来，公开密钥密码已从理论研究进入实际应用研究阶段。RSA公开密钥密码算法在信息交换过程中使用比较广泛，安全性比较高。以当前的计算机水平，如选择1024位长的密钥（相当于300位十进制数字）就认为是无法攻破的。

## 3.3.2 RSA算法实现过程

首先产生密钥，过程如下：

(1) 随机产生两个长度为位的素数*P*和*Q*

(2) 计算公钥 (publicKey 是*k*位的长度)

(3) 随机产生一个加密密钥 *keyE*,其中; 注意这是保证解密密钥=1有解的充要条件， 称为*n*的欧拉函数,值为:

(4) 求解解密密钥,为解密密钥*keyD*的逆元，此公式原方程为

由此公钥，加密密钥，解密密钥全部产生。

其次 对明文加密或对密文进行解密,过程如下:

(1) 加密:，其中*M*表示明文,*C*表示密文

(2) 解密:，其中*M*表示明文,*C*表示密文

具体流程如下图所示：

图3-14 加密或解密流程图 图3-15 总的流程图 图3-16 产生密钥流程图

## 3.3.3 RSA算法实现核心

1. 产生两个素数
2. 求解公钥，以及使用公钥的欧拉函数。同时求加密密钥
3. 求解密密钥

求解密密钥实际上是如何去解一次同余方程。根据费马定理与欧拉定理给出了同余方程的解为:

由此可得出

即

1. 数据的加密解密

产生密钥后，下一步所要做的就是进行加密和解密，首先我们看一下加密解密的公式：

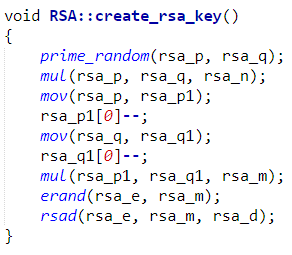
其中*C*表示明文，*M*表示密文，*keyE*表示加密密钥,*KeyD*表示解密密钥,*publicKey*表示公钥。由此公式可以看出，难点是如何做高次模，先做指数运算，再求模，显然是行不通的，因为*keyE*通常比较大,M的指数次方运算后所得的值可能会越界，这样求模后的值肯定不正确，(M=CkeyD mod publicKey同理),而且这样做的效率也十分的低。在说明如何做高次模运算时，我们先看一下这个公式:

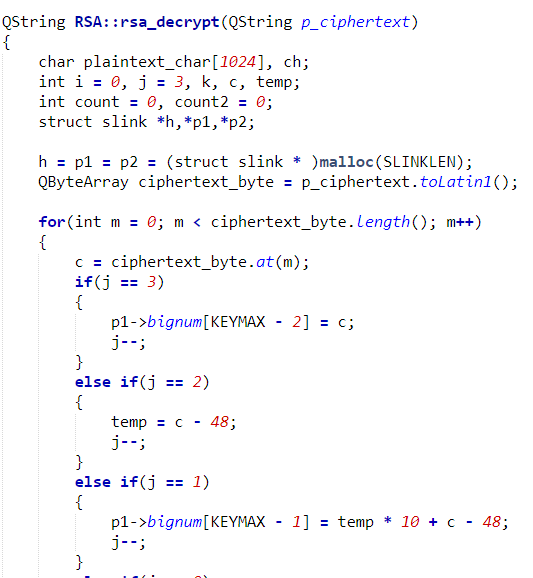
当a=b时,这个公式就是

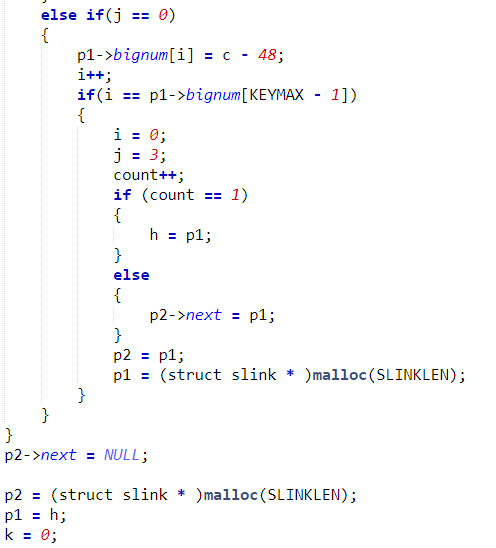
……

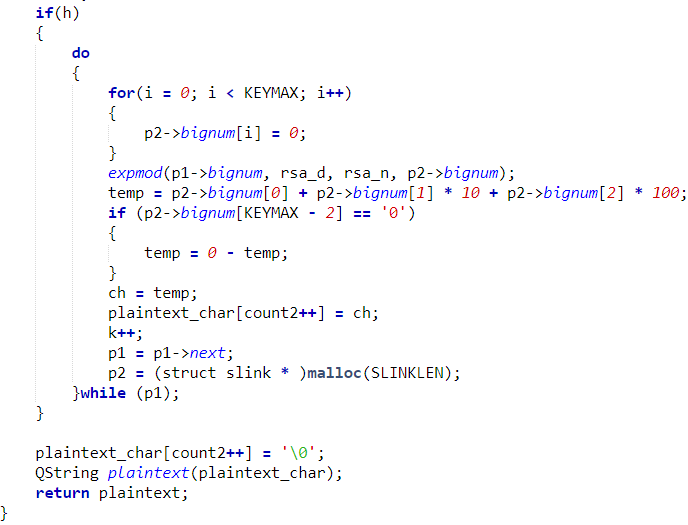
在实际编程时，我们不需要按一个一个底数分解因子，而是以2次方的形式迭代计算高次模。

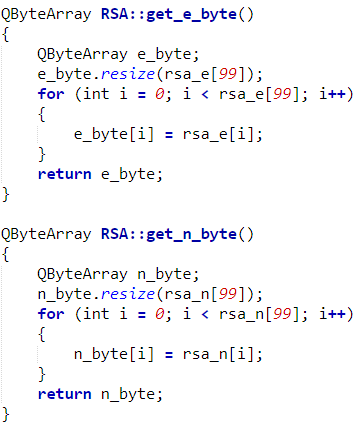
根据以上的主要算法步骤，在程序中实现的核心程序源码为：











# 第四章 作品测试与分析

# 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 |
| 声纹模型建立训练模块 | 能够使用GMM算法成功建立并训练得到声纹模型 |
| 声纹特征身份识别模块 | 能够成功声纹识别说话人 |
| 文件加密解密模块 | 能够成功用SM4算法加密解密 |
| 文件管理模块 | 身份验证通过后可以导入文件存入板子或者查看指定文件 |
| 用户认证模块 | 能够成功注册并得到响应信息  能够成功登陆并得到响应信息 |
| 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 |
| 认证安全性测试 | 存储和取回文件的身份控制已启用，并且账户密码和文件数据经过加密处理。 |
| 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 7 64位旗舰版  CPU 15  m450 2.4GHz  内存4G DDR3 |
| 设备型号 | Mini2440 |  |

# 4.3测试用例与分析

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：** | 语音数据收集功能 |
| **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 |

2、语音数据回放

|  |  |
| --- | --- |
| **测试目标** | 验证声纹数据采集模块是否能够回放采集到的用户语音数据 |
| **测试范围：** | 语音数据回放功能 |
| **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，录音结束后，点击界面回放按钮，回放收集到的语音数据。 |
| **实际结果：** | 与预期结果一致 |
| **需考虑的特殊事项：** | 无 |

3、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raw文件，经过声纹特征值MFCC提取过程将结果保存至MFCC文件。 |
| **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raw文件，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内 |
| **实际结果：** | 与预期结果一致 |
| **需考虑的特殊事项：** | 无 |

4、使用GMM算法训练模型

|  |  |
| --- | --- |
| **测试目标** | 能否使用GMM算法训练得到说话人声纹模型 |
| **测试范围：** | 1. 声纹特征值MFCC文件的训练数据的输入格式 2. GMM高斯混合模型训练功能 |
| **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写入对应文件中，调用相应的GMM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，程序正常读入声纹特征值MFCC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、GMM算法的正确率测试

|  |  |
| --- | --- |
| **测试目标** | 测试当前GMM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 |

6、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 |

7、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，程序正常读入语音数据raw文件，并且计算出相应的模型，保存在指定目录下。在MFCC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 |

8、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 |

9、 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：** | 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 |

10、 文件管理功能

|  |  |
| --- | --- |
| **测试目标** | 验证系统的文件管理功能 |
| **测试范围：** | 测试用户在PC端文件管理功能 |
| **测试方法：** | 在PC端登录页面登录成功通过身份验证后，向mini2440端导入指定文件和从mini2440端导出指定文件。 |
| **预期结果：** | 进入登录界面，输入账户密码，并在mini2440端录音，通过声纹识别身份验证成功，在PC端进入文件管理界面，选择文件导入选项导入指定文件，选取指定文件导出进行查看编辑。 |
| **实际结果：** | 实际结果与预期结果一致 |
| **需考虑的特殊事项：** | 无 |

# 4.5安全性分析

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来保证文件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、中间人攻击、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，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。

5. 中间人攻击：

由于本系统存在PC与Mini2440之间的串口通信机制，若采用明文方式，易被中间人获取传输信息。故本系统采用RSA算法将数据加密进行加密传输，若被截获，也不易得到明文。故可抵抗中间人攻击。

6. 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。

# 4.6测试结果

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。

# 第五章 创新性说明

**1.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。

**2.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。

**3.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意一个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同时提高用户使用接收度。

在注册时使用RSA算法对账户密码即文本密码进行加密，提高注册时账户密码在PC端和mini2440端之间传输的安全性。同时登陆时利用RSA进行解密实现高强度的账户信息保护。

**4.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，同时能将系统随身携带也辅助提高了信息的防护效果。

# 第六章 总结与展望

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。

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，性价比较高且系统运行稳定，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）安全性能提高方面:

本系统着重在数据本体的保护和获取数据途径的安全控制上进行研发，未来我们计划针对数据的传输进行安全性能的提升，拓展硬件设备和PC端之间串口通信的协议制定的参数，达到整个数据交互流程的较全面保护。

4）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。

# 参考文献

[1] 杨宏志，韩文报，李光松．AES和Camellia算法的可重构硬件实现[J]. 计算机工程，2010，36(16):18-20.

[2] 王晨光，乔树山，黑勇. 分组密码算法SM4的低复杂度实现[J]. 计算机工程，2013，39(7):177-180.

[3] 李湘锋,赵有健,全成斌. 对称密钥加密算法在 IPsec 协议中的应用[J]. 电子测量与仪器学报，2014，28(1):75-83.

[4] 方植彬. 信息与通信网络安全技术——生物识别技术[J]. 电子产品可靠性与环境试验，2014，32(5):55-61.

[5] 杨阳, 陈永明. 声纹识别技术及其应用[J]. 电声技术，2007，31(2):45-46,50.

[6] 石燕. 声纹识别技术研究[D]. 南京：南京航空航天大学，2004.

[7] 林珊. 谈谈生物识别技术[J]. 科教前沿，2011，(13):25,34.

[8] TAN Li- li, WEI Gang. Blind signal separation of convolution mixture signals via minimum mutual information (MMI) method [J]. Journal of China Institute of Communications, 1999, 20(10):49- 55.

[9] TAN Li- li, WEI Gang. Multi- input and multi- output (MIMO) blind convolution via maximum entropy (ME) method [J]. Act Electronica Sinica, 2000, 28(1):114- 116.

[10] ARAKI S, MUKAI R, MAKINGO S, et al. The fundamental limitation of frequency domain blind source separation for convolution mixtures of speech [J]. IEEE Tran .On Speech and Audio Processing, 2003, 11 (2):109- 116.