



(12) 发明专利

(10) 授权公告号 CN 110659468 B

(45) 授权公告日 2022. 02. 15

(21) 申请号 201910773435.2

CN 109802942 A, 2019.05.24

(22) 申请日 2019.08.21

Bin Hao等.Voiceprint-based Access

(65) 同一申请的已公布的文献号

Control for Wireless Insulin Pump

申请公布号 CN 110659468 A

Systems.《网页在线公开:https://

(43) 申请公布日 2020.01.07

ieeexplore.ieee.org/stamp/stamp.jsp?tp=&

(73) 专利权人 江苏大学

arnumber=8567568》.2018,第1-9页.

地址 212013 江苏省镇江市京口区学府路
301号

龚雪等.基于动态可变参数的复合混沌系统
的语音加密算法研究.《声学技术》.2017,第35卷
(第6期),第542-549页.

(72) 发明人 郑志燊 何洋 施雨 毛启容

Hua-Hong Zhu等.Voiceprint-Biometric
Template Design and Authentication Based

(51) Int.Cl.

on Cloud Computing Security.《网页在线公

G06F 21/32 (2013.01)

开:https://ieeexplore.ieee.org/stamp/

G06F 21/60 (2013.01)

stamp.jsp?tp=&arnumber=6138538》.2012,第1-

(56) 对比文件

7页.

CN 110070895 A, 2019.07.30

车念等.融合多重加解密算法的保密通信系

CN 109119063 A, 2019.01.01

统.《信息安全技术》.2017,第38卷(第4期),第

CN 102073829 A, 2011.05.25

936-940页.

US 2013253919 A1, 2013.09.26

审查员 杨怡睿

CN 103391201 A, 2013.11.13

权利要求书4页 说明书6页 附图4页

CN 108922559 A, 2018.11.30

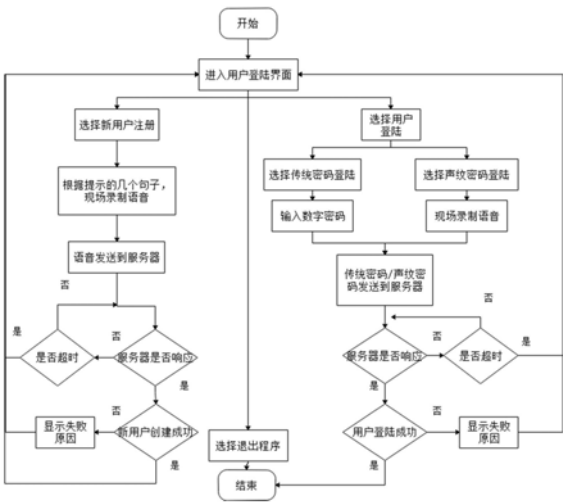
(54) 发明名称

供友好、便利的操作环境,同时也保证用户的文
件数据的安全。

基于C/S架构和说话人识别技术的文件加密
解密系统

(57) 摘要

本发明公开了基于C/S架构和说话人识别技术的文件加密解密系统,用户使用传统数字密码或生物特征的声纹密码远程登录系统,当用户提出对文件加密或解密请求时,系统根据说话人现场采集语音信息进行声纹提取,最后进行判决处理和进行对文件的加密或解密操作。加密或解密操作时,首先确认现场说话人的身份,只有通过时才使用加密算法或对应的解密算法对文件进行加密或解密,加密时把加密标志追加至文件头部,解密时把文件头部中的加密标志去除并使用解密算法进行文件解密。本发明将人随身携带的声纹密码和文件加密解密操作进行结合,同时使用远程服务器来使客户端轻量化,不仅为用户提



1. 基于C/S架构和说话人识别技术的文件加密解密系统,包括客户端和服务端;其特征在于,

所述客户端包括:用户登录界面模块、新用户注册模块、老用户登录模块、文件加密和解密模块、现场语音采集模块;所述用户登录界面模块提供友好的用户交互界面,让用户选择登录或注册;所述新用户注册模块包括用于采集用户声纹的提示性语句和发送注册信息到服务器功能,并且包括提示用户操作过程中出现的问题的可能原因;所述老用户登录模块包括用户选择使用传统密码或声纹密码登录系统,登录成功提示或登录失败的可能原因提示;所述文件加密和解密模块能使用加密算法和解密算法对用户的文件进行加密或解密;所述现场语音采集模块能调用用户设备上的麦克风进行语音录制;

所述服务端包括:用户验证模块、语音降噪模块、模型训练模块、模型识别判决模块、数据库存储模块;所述语音降噪模块连接到所述模型训练模块,所述语音降噪模块连接到模型识别判决模块,所述模型识别判决模块连接到所述用户验证模块;所述语音降噪模块是所有用户传输到服务器的语音都必经的预处理模块,用于提高用户语音的质量;所述模型训练模块是用于采集用户的语音进行提取用户的声纹特征并保存,所述声纹特征用于模型识别判决;所述用户验证模块包括用户输入密码登录的验证和用户用声纹密码登录的验证,以模型识别判决模块的判决结果作为验证结果;所述模型识别判决模块是采用说话人识别技术,把用户传输到服务器的语音进行说话人识别,同时结合用户的操作请求来进行判决,最后把判决结果反馈到客户端;所述数据库存储模块是存储用户的基本信息和密码信息,用于用户的验证;

所述模型识别判决模块能够:

A. 提取梅尔频率倒谱系数MFCC

提取梅尔频率倒谱系数的过程为预加重、分帧加窗、短时傅里叶变换STFT、Mel频率滤波和离散余弦变换DCT,具体如下:

(a) 预加重:将语音的低频范围预加重处理,提高语音信号高频段的信噪比;

(b) 分帧加窗:语音信号在一个短时间范围内,其特性基本保持不变即相对稳定,将语音信号分成若干段,每一段为一帧,每帧的时长设置为20ms;

为了保证帧与帧之间的平滑过渡,保持连续性,每个语音帧乘一个窗函数保证两端能平滑过渡;

(c) 短时傅里叶变换:把语音从时域变换到频域,在频域中进行分析;

(d) Mel频率滤波:把离散频谱用序列三角滤波器进行滤波得到一组系数;

(e) DCT变换:在经过一次变换,最后求得MFCC倒谱系数;

B. 使用高斯混合模型GMM进行计算概率

将上述提取的MFCC倒谱系数,作为一批观察数据

$$X = \{x^{(1)}, x^{(2)}, \dots, x^{(s)}\}$$

单高斯模型用多位高斯正态分布概率密度函数表示:

$$N(x; \mu, \Sigma) = \frac{1}{\sqrt{(2\pi)^d |\Sigma|}} \exp\left(-\frac{1}{2}(x - \mu)^T \Sigma^{-1}(x - \mu)\right)$$

其中 x 是维数为 d 的样本向量; μ 是模型期望; Σ 是模型方差;
数据的概率分布函数通过概率加权函数表示

$$P(x^{(i)}) = \sum_{j=1}^m \alpha_j N_j(x^{(i)}; \mu_j, \Sigma_j)$$

上式为高斯混合模型,其中 α_j 表示第j个单高斯模型在混合模型中占的比例, $N_j(x^{(i)}; \mu_j, \Sigma_j)$ 表示第j个单高斯模型, μ_j 是均值向量, Σ_j 是协方差矩阵;

通过最大后验概率来辨认语音的说话人身份,最大后验概率表示为

$$p(\theta_i|x) = \frac{P(x|\theta_i)P(\theta_i)}{P(x)}$$

假设数据库中说话人的可能性相等,则 $p(\theta_i) = \frac{1}{N}$,其中N为数据库中说话人人数;

那么辨认的目标函数为 $i^* = \arg \max_i P(x|\theta_i)$;

i^* 表示识别出的说话人, θ_i 为说话人对应的模型参数;

$P(x|\theta)$ 的对数形式为 $\ln P(x|\theta) = \sum_{i=1}^s \ln P(x_i|\theta)$;

C. 识别出的说话人与用户当前登录的用户名进行验证对比

如果语音识别出的说话人与当前用户名一致,则验证通过,服务端反馈成功的信息给客户端,否则反馈失败的信息给客户端。

2. 根据权利要求1所述的基于C/S架构和说话人识别技术的文件加密解密系统,其特征
在于,新用户注册模块能够:

A. 用户输入用户名和密码进行注册

使得用户使用账户密码登录方式登录到系统;

B. 用户浏览录音例句

界面上提示的例句作为提示用户录制语音,

C. 用户点击录制语音按钮

用户点击录制语音按钮后会出现当前录音时间提示,超过11秒将自动停止录音,客户端程序也根据内置阈值自动停止录音,或当用户停止说话时,声波能量低于内置阈值,录音自动停止;当例句录音完毕后,用户注册成功;

D. 发送录制语音到服务端

当用户把例句录音完毕后,客户端自动把录制的语音发送到服务端,服务端进行模型的训练,当服务端提示训练完成时,用户注册成功。

3. 根据权利要求1所述的基于C/S架构和说话人识别技术的文件加密解密系统,其特征
在于,所述老用户登录模块能够:

A. 用户点击声纹识别快速登录按钮

当用户点击按钮之后,系统提示用户录制语音,此时用户使用麦克风说话,系统登录界面会有例句提示;

B. 停止语音录制

系统自动判断用户是否已经停止说话,当采集的声波能量低于系统内置的阈值时,系统自动停止录音,或者如果用户说话超过11秒,系统也会自动停止;

C. 用户身份的验证

用户语音录制完毕之后,系统立即将语音发送到服务端进行身份验证,如果用户的身

份验证成功,由服务端反馈信息,用户即可登录进入系统,如果验证失败,则提示可能原因;

D.在不方便使用语音登录的情况下,点击使用密码登录按钮,用户输入完毕后,点击登录,经过系统验证成功后,用户可以登录进入系统。

4.根据权利要求1所述的基于C/S架构和说话人识别技术的文件加密解密系统,其特征在于,所述文件加密和解密模块能够:

A.用户直接选择文件

用户通过对话框选中文件后,系统读取文件内容,并且进行判断该文件是否是已加密文件或者是普通文件;

B.加密处理

系统判断是普通文件,则提示用户是否进行加密,用户选择加密时,首先进行用户的身份验证,用户录制一段语音后发送到服务端,服务端验证当前登录用户和当前说话人是同一人时,服务端使用RSA算法产生公钥和私钥,并将公钥反馈给客户端;

C.客户端使用公钥对文件进行加密

根据RSA算法,客户端使用服务端反馈回来的公钥对文件进行加密,同时改变加密文件的名称,追加已加密的文字,提示用户该文件是已加密的文件,同时客户端在文件头部加入特定的加密标志符;

D.解密处理

系统判断是已加密文件,则提示用户是否进行解密,用户选择解密时,首先进行用户的身份验证,用户录制一段语音后发送到服务端,服务端验证当前登录用户和当前说话人是同一人时,服务端从数据库中查找到解密文件的密钥并发送给客户端;

E.客户端使用私钥对文件进行解密

客户端首先去除特定的加密标志,然后通过RSA算法使用私钥对文件进行解密,并且把文件的名称恢复正常,去除已加密的提示文字。

5.根据权利要求4所述的基于C/S架构和说话人识别技术的文件加密解密系统,其特征在于,所述RSA算法设计如下:

A.首先找到两个大素数 p 、 q ,并设置为1024位;

B.计算 $n=p*q$, $\varphi(n)=(p-1)*(q-1)$,其中 n 表示两个互质的整数之积, $\varphi(n)$ 表示的是 n 的欧拉函数值;

C.任意选择一个满足要求的证书 e ,满足 $1 < e < \varphi(n)$,并且 $\gcd(\varphi(n),e)=1$,其中 $\gcd()$ 表示求最大公约数;

D.计算 d ,满足 $(d*e)\% \varphi(n) == 1$,即 d 是 e 在模 $\varphi(n)$ 下的乘法逆元;

E.以 $\{e,n\}$ 为公钥, $\{d,n\}$ 为私钥;

F.明文为 A ,则密文 $C = (A^e) \% n$ 。

6.根据权利要求1所述的基于C/S架构和说话人识别技术的文件加密解密系统,其特征在于,所述用户验证模块能够:

A.收到用户使用数字密码的验证请求

服务器监听端口当接收到用户的登录系统请求时,系统对用户输入的用户名和密码进行验证,服务器通过查询数据库进行密码验证,如果验证成功则把成功的信息反馈到用户

的客户端,从而客户端可以进行进一步操作;

B.收到用户使用声纹密码的身份验证请求

服务器监听端口当接收到用户发送的语音,系统利用语音降噪模块进行降噪处理,所述语音降噪模块采用双门限端点检测技术,去除用户语音中的静音段,把用户真正说话的语音段截取出来,然后采用维纳滤波法的语音增强算法,减少用户语音的背景噪声,突出说话人的声音,然后使用说话人模型库中的GMM模型进行模式匹配,匹配成功则返回验证成功的信息给客户端。

7.根据权利要求1所述的基于C/S架构和说话人识别技术的文件加密解密系统,其特征在于,所述模型训练模块是服务器接收到用户注册时发送来的语音,先把语音通过语音降噪模块进行预处理,然后使用高斯混合模型GMM进行训练,得到属于用户的声纹模型并且保存到数据库中,新用户就注册成功;所述数据库存储模块用于保存用户的基本信息和传统的密码信息和用户的声纹密码信息,当服务器需要时能够读写数据库。

8.根据权利要求1-7任一项所述的基于C/S架构和说话人识别技术的文件加密解密系统,其特征在于,所述系统基于服务器实现,所述服务器采用网络负载均衡服务器。

基于C/S架构和说话人识别技术的文件加密解密系统

技术领域

[0001] 本发明涉及对文件的加密与解密的技术领域,尤其涉及一种基于C/S架构和说话人识别技术的文件加密解密系统。

背景技术

[0002] 随着互联网技术的发展和智能手机的普及,越来越多的人使用电子设备来记录日常生活中的重要信息,如记账、工作安排、汇报等等,产生了文档、幻灯片等等一系列的文件形式,但网络安全的问题也在时时困扰着我们,黑客的猖獗行为严重影响了人们的日常生活,所以文件的安全问题已经无法忽视。

[0003] 根据著名的摩尔定律,计算机的计算速度将不断加快,如果使用传统的数字密码的方式进行文件加密,很有可能被高性能的计算机进行暴力破解,用户文件的安全难以得到保障,简单的增加密码的长度也是一种不可取的方法,首先不便于人们的记忆,容易增加人们的记忆负担,其次密码忘记后会给用户造成更大的不便,最后这种简单数字密码仍避免不了被暴力破解的潜在风险。

[0004] 声纹密码是人体固有的生理特征,就像人的身份证号码一样具有唯一性,并且相比于传统数字密码的优势有:可以随身携带、不需要刻意地记忆、减轻大脑记忆的负担。而说话人识别技术正是使用声纹特征对说话人进行辨认和确认的技术,利用该技术可以解决在对文件加密时,用声纹密码替换传统数字密码。

[0005] 近年来智能手机人均拥有率越来越高,并且随着4G网络的普及,甚至到5G的开始使用,使用声纹密码来对文件加密解密就变得更加方便。智能手机都有小型麦克风,所以人们可以随时随地地录制自己的语音,同时网络的发展提供了良好的传输环境,这样用户的设备只需要承担更少的硬件资源,更多的处理都交给远程服务器进行处理,这样大大方便用户的使用。

发明内容

[0006] 针对传统密码在文件加密上的不足之处,本发明提出在文件加密中,使用声纹密码来代替传统密码,以增加文件加密的安全性和用户使用的便捷性,同时使用远程服务器来执行主要功能,尽量少占用用户设备上的资源,所述的基于C/S架构和说话人识别技术的文件加密解密系统包括:

[0007] 服务端和客户端两大模块,所述客户端模块包括:用户登录界面模块、新用户注册模块、老用户登录模块、文件加密和解密模块、现场语音采集模块;

[0008] 所述用户登录界面模块提供友好的用户交互界面,让用户便于选择登录或注册;

[0009] 所述新用户注册模块包括用于采集用户声纹的提示性语句和发送注册信息到服务器功能,并且包括提示用户操作过程中出现的问题的可能原因;

[0010] 所述老用户登录模块包括用户选择使用传统密码或声纹密码登陆系统,登陆成功提示或登陆失败的可能原因提示;

[0011] 所述文件加密和解密模块能使用加密算法和对应的解密算法对用户的文件进行加密或解密；

[0012] 所述现场语音采集模块能调用用户设备上的麦克风进行语音录制。

[0013] 进一步的，上述的用户设备至少包含智能手机、平板电脑、笔记本电脑。

[0014] 所述服务端模块包括：用户验证模块、语音降噪模块、模型训练模块、模型识别判决模块、数据库存储模块；

[0015] 所述语音降噪模块连接到所述模型训练模块，所述语音降噪模块连接到模型识别判决模块，所述模型识别判决模块连接到所述用户验证模块；

[0016] 所述语音降噪模块是所有用户传输到服务器的语音都必经的预处理模块，用于提高用户语音的质量；

[0017] 所述模型训练模块是用于采集用户的语音进行提取用户的声纹特征并保存，所述声纹特征用于模型识别判决模块；

[0018] 所述用户验证模块包括用户输入密码登录的验证和用户用声纹密码登录的验证，以模型识别判决模块的判决结果作为验证结果；

[0019] 所述模型识别判决模块是采用说话人识别技术，把用户传输到服务器的语音进行说话人识别，同时结合用户的操作请求来进行判决，最后把判决结果反馈到客户端；

[0020] 所述数据库存储模块是存储用户的基本信息和密码信息，用于用户的验证。

[0021] 本发明的有益效果：

[0022] 1、本发明将声纹密码代替传统密码，实现用户使用轻量级的客户端和随身携带的声纹密码，轻松对文件进行加密解密，同时远程服务器对用户的操作进行严密的验证，确保用户正常加密解密专属文件和禁止非文件专属用户的非法操作，保证了用户专属文件的安全。

[0023] 2、本发明采用C/S架构，同时设置了网络均衡服务器，确保当用户访问数量增多时，选择负载较轻的服务器为用户服务，及时响应用户的访问。设置两个数据库服务器让新用户的注册与旧用户的访问独立，减小数据库服务器的负载，从而提高整个系统的鲁棒性。

附图说明

[0024] 图1是本发明所述的用户登录模块流程图。

[0025] 图2是本发明所述的用户操作模块流程图。

[0026] 图3是本发明所述的服务器应用程序执行流程图。

[0027] 图4是本发明所述的服务器架构拓扑图。

具体实施方式

[0028] 下面结合附图对本发明作进一步说明。

[0029] 一种基于C/S架构和说话人识别技术的文件加密解密系统，主要把客户端的操作简化，用户只需要简单的操作就能对文件进行加密或解密，以此来保护用户的个人文件安全和个人隐私，下面结合附图和实施例对本发明作进一步的描述。

[0030] 客户端包括用户登录界面模块、新用户注册模块，老用户登录模块、文件加密和解密模块、现场语音采集模块；

- [0031] 如图1所示,用户登录界面模块提供了新用户注册通道和老用户登录的通道;
- [0032] 新用户注册模块有如下功能:
- [0033] A.用户输入用户名和密码进行注册
- [0034] 提供用户另一种登录方式,目的是方便用户在不适合使用语音登陆的场景下,使用传统的账户密码登陆方式登录到系统。
- [0035] B.用户浏览简单的录音例句
- [0036] 用户看到界面上提示的几个简单的例句作为提示用户录制语音,可以默读一下以便清晰流畅地录入语音。
- [0037] C.用户点击录制语音按钮
- [0038] 用户点击录制语音按钮后会出现当前录音时间提示,超过11秒将自动停止录音,客户端程序也根据内置阈值自动停止录音,当用户停止说话时,声波能量低于内置阈值,录音自动停止。当几个简单例句录音完毕后,用户注册成功。
- [0039] D.发送录制语音到服务端
- [0040] 当用户把几个简单例句录音完毕后,客户端自动把录制的语音发送到服务端,以便服务端进行模型的训练,当服务端提示训练完成时,用户注册成功。
- [0041] 老用户登录模块有如下功能:
- [0042] A.用户点击声纹识别快速登录按钮
- [0043] 当用户点击按钮之后,系统提示用户录制语音,此时用户可以使用麦克风说话,系统系登陆界面也会有例句提示。
- [0044] B.停止语音录制
- [0045] 系统会自动判断用户是否已经停止说话,当采集的声波能量低于系统内置的阈值时,系统自动停止录音,如果用户说话超过11秒,系统也会自动停止,避免长语音造成传输数据的不便和长静音的语音对用户声音识别的准确性。
- [0046] C.用户身份的验证
- [0047] 用户语音录制完毕之后,系统立即将语音发送到服务端进行身份验证,如果用户的身份验证成功,由系统反馈信息,用户即可登录进入系统,如果验证失败,则提示可能原因。
- [0048] D.在不方便使用语音登录的情况下,点击使用密码登录按钮
- [0049] 用户在这种场合下,可以选择使用用户名和密码登录,和常见的输入账号和密码的操作一样,用户输入完毕后,点击登录,经过系统验证成功后,用户可以登录进入系统。
- [0050] 如图2所示,文件加密和解密模块有如下的功能:
- [0051] A.用户直接选择文件
- [0052] 用户通过对话框选中文件后,系统读取文件内容,并且进行判断该文件是否是已加密文件或者是普通文件。
- [0053] B.加密
- [0054] 系统判断是普通文件,则提示用户是否进行加密,用户选择加密时,首先进行用户的身份验证,用户录制一段语音后发送到服务端,服务端验证当前登录用户和当前说话人是同一人时,服务端使用RSA算法产生公钥和私钥,并将公钥反馈给客户端。
- [0055] C.客户端使用公钥对文件进行加密

[0056] 根据RSA算法,客户端使用服务端反馈回来的公钥对文件进行加密,同时改变加密文件的名称,追加已加密的文字,可以提示用户该文件是已加密的文件,同时客户端在文件头部加入特定的加密标志符,以便系统能辨认文件的类型。

[0057] D.解密

[0058] 系统判断是已加密文件,则提示用户是否进行解密,用户选择解密时,首先进行用户的身份验证,用户录制一段语音后发送到服务端,服务端验证当前登录用户和当前说话人是同一人时,服务端从数据库中查找到解密文件的密钥并发送给客户端。

[0059] E.客户端使用私钥对文件进行解密

[0060] 客户端首先去除特定的加密标志,然后通过RSA算法使用私钥对文件进行解密,并且把文件的名称恢复正常,去除已加密的提示文字。

[0061] 使用的RSA算法流程如下:

[0062] A.首先找到两个大素数 p 、 q ,设置为1024位。

[0063] B.计算 $n=p*q$, $\varphi(n)=(p-1)*(q-1)$,其中 n 表示两个互质的整数之积, $\varphi(n)$ 表示的是 n 的欧拉函数值。

[0064] C.任意选择一个满足要求的证书 e ,满足 $1 < e < \varphi(n)$,并且 $\gcd(\varphi(n),e)=1$,其中 $\gcd()$ 表示求最大公约数。

[0065] D.计算 d ,满足 $(d*e)\% \varphi(n) == 1$,即 d 是 e 在模 $\varphi(n)$ 下的乘法逆元,因为 e 和 $\varphi(n)$ 互质,所以它的乘法逆元一定存在。

[0066] E.以 $\{e,n\}$ 为公钥, $\{d,n\}$ 为私钥。

[0067] F.明文为 A ,则密文 $C=(A^e)\%n$ 。

[0068] 服务端包括:用户验证模块、语音降噪模块、模型训练模块、模型识别判决模块、数据库存储模块;

[0069] 如图3所示,用户验证模块的功能如下:

[0070] A.收到用户使用数字密码的验证请求

[0071] 服务器监听端口当接收到用户的登录系统请求时,系统进行对用户输入的用户名和密码进行验证,服务器通过查询数据库进行密码验证,如果验证成功则把成功的信息反馈到用户的客户端,从而客户端可以进行进一步操作。

[0072] B.收到用户使用声纹密码的身份验证请求

[0073] 服务器监听端口当接收到用户发送的语音,系统的语音降噪模块进行降噪处理,采用双门限端点检测技术,去除用户语音中的静音段,把用户真正说话的语音段截取出来,然后采用维纳滤波法的语音增强算法,减少用户语音的背景噪声,突出说话人的声音,然后使用说话人模型库中的GMM模型进行模式匹配,匹配成功则返回验证成功的信息给客户端。

[0074] 模型识别判决模块的功能如下:

[0075] A.提取梅尔频率倒谱系数(MFCC)

[0076] 提取梅尔频率倒谱系数的主要过程为预加重、分帧加窗、短时傅里叶变换(STFT)、Mel频率滤波和离散余弦变换(DCT),具体步骤:

[0077] (a)预加重:语音大部分能量集中在低频范围,通过预加重处理,提高语音信号高频段的信噪比。

[0078] (b) 分帧加窗:语音信号在一个短时间范围内,其特性基本保持不变即相对稳定,将语音信号分成若干段,每一段称为一帧,每帧的时长设置为20ms。

[0079] 为了保证帧与帧之间的平滑过渡,保持连续性,每个语音帧乘一个窗函数保证两端能平滑过渡。

[0080] (c) 短时傅里叶变换:把语音从时域变换到频域,在频域中进行分析。

[0081] (d) Mel频率滤波:把离散频谱用序列三角滤波器进行滤波得到一组系数,

[0082] (e) DCT变换:在经过一次变换,最后求得MFCC倒谱系数。

[0083] B. 使用高斯混合模型 (GMM) 进行计算概率

[0084] 上面提取的MFCC倒谱系数,可以看作为一批观察数据

[0085] $X = \{x^{(1)}, x^{(2)}, \dots, x^{(s)}\}$

[0086] 单高斯模型可以用多位高斯 (正态) 分布概率密度函数表示:

[0087]
$$N(x; \mu, \Sigma) = \frac{1}{\sqrt{(2\pi)^d |\Sigma|}} \exp\left(-\frac{1}{2}(x - \mu)^T \Sigma^{-1}(x - \mu)\right)$$

[0088] 其中 x 是维数为 d 的样本向量; μ 是模型期望; Σ 是模型方差;

[0089] 数据的概率分布函数通过概率加权函数表示

[0090]
$$P(x^{(i)}) = \sum_{j=1}^m \alpha_j N_j(x^{(i)}; \mu_j, \Sigma_j)$$

[0091] 上式为高斯混合模型,其中 α_j 表示第 j 个单高斯模型在混合模型中占的比例, $N_j(x^{(i)}; \mu_j, \Sigma_j)$ 表示第 j 个单高斯模型, μ_j 是均值向量, Σ_j 是协方差矩阵。

[0092] 通过最大后验概率来辨认语音的说话人身份,最大后验概率表示为

[0093]
$$p(\theta_i | x) = \frac{P(x | \theta_i) P(\theta_i)}{P(x)}$$

[0094] 假设数据库中说话人的可能性相等,则 $P(\theta_i) = \frac{1}{N}$,其中 N 为数据库中说话人人数量;

[0095] 那么辨认的目标函数为 $i^* = \arg \max_i P(x | \theta_i)$

[0096] i^* 表示识别出的说话人, θ_i 为说话人对应的模型参数。

[0097] $P(x | \theta)$ 的对数形式为 $\ln P(x | \theta) = \sum_{i=1}^s \ln P(x_i | \theta)$

[0098] C. 识别出的说话人与用户当前登录的用户名进行验证对比

[0099] 如果语音识别出的说话人与当前用户名一致,则验证通过,服务端反馈成功的信息给客户端,否则反馈失败的信息给客户端。

[0100] 模型训练模块是服务器接收到用户注册时发送来的语音,先把语音通过语音降噪模块进行预处理,然后使用高斯混合模型 (GMM) 进行训练,最终得到属于用户的声纹模型并且保存到数据库中,这样新用户就注册成功;数据库存储模块是保存了用户的基本信息和传统的密码信息和用户的声纹密码信息等,当服务器需要时可以读写数据库。

[0101] 一种基于C/S架构和说话人识别技术的文件加密解密系统是基于服务器来实现的,对应的服务器架构的拓扑图如图4所示,当多个用户同时进行访问服务器的时候,为了降低服务器的负担,加入网络负载均衡服务器,通过网络负载均衡服务器进行调度,把新来的用户请求分配到较为空闲的服务器;应用服务器使用多台,可以更好的分担多个用户的

同时请求;数据库服务器采用了多个,分别满足应用服务器的写操作和读操作,因为用户注册时服务器会把用户的信息写入到数据库中,而用户登陆、验证身份进行文件的加密和解密时,都是服务器对数据库进行读操作,根据用户的需求,服务器读操作比写操作多,为了降低数据库服务器的负担分为多台数据库服务器。

[0102] 本发明所述的基于C/S架构和说话人识别技术的文件加密解密系统使用上述的具体实施过程,为用户提供方便的文件加密和解密操作,保护了用户文件的安全。

[0103] 上文所列出的一系列的详细说明仅仅是针对本发明的可行性实施方式的具体说明,它们并非用以限制本发明的保护范围,凡未脱离本发明技艺精神所作的等效实施方式或变更均应包含在本发明的保护范围之内。

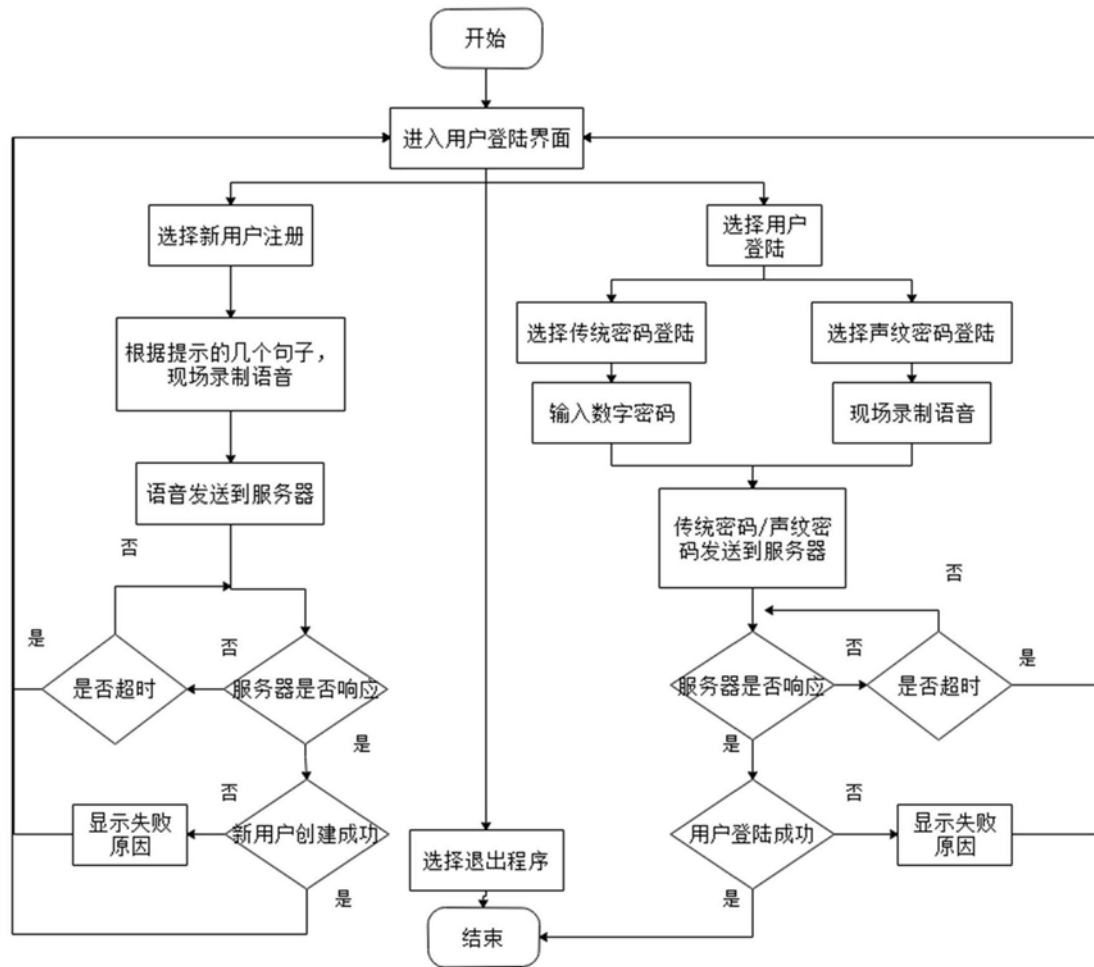


图1

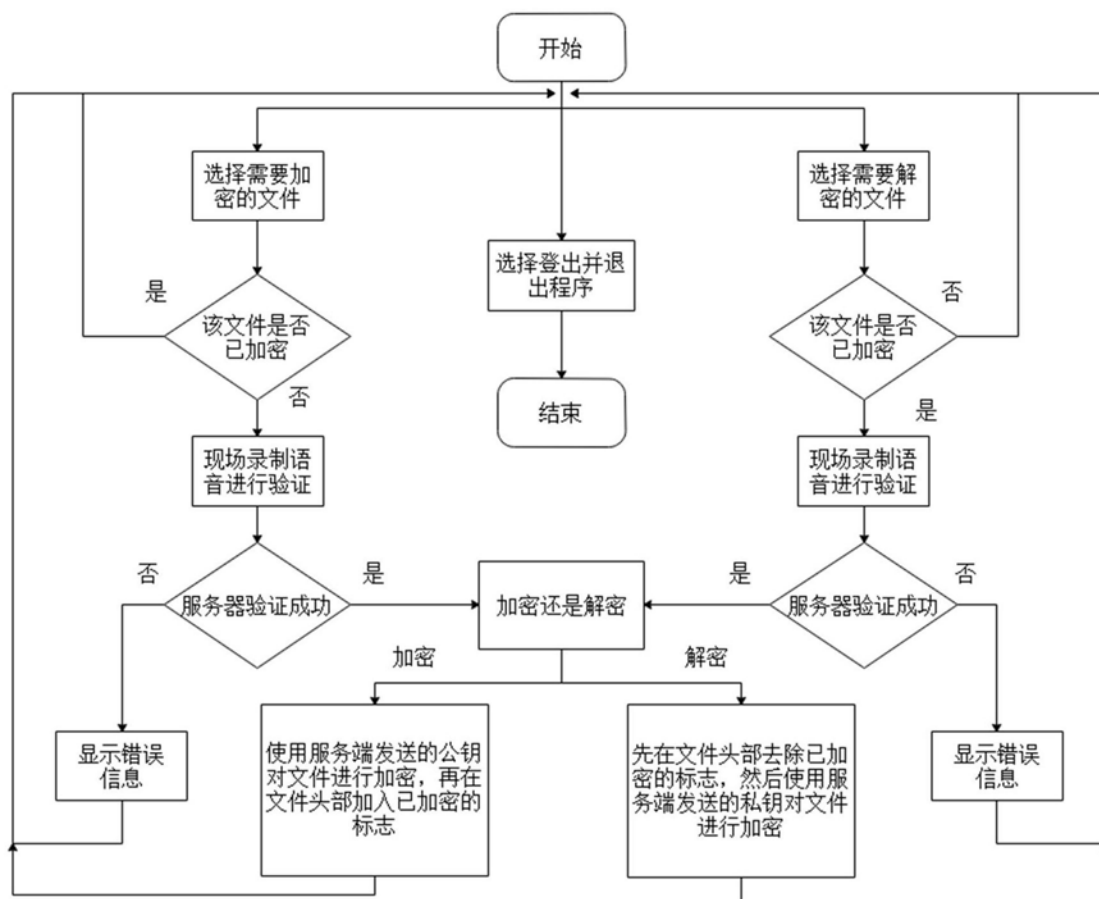


图2

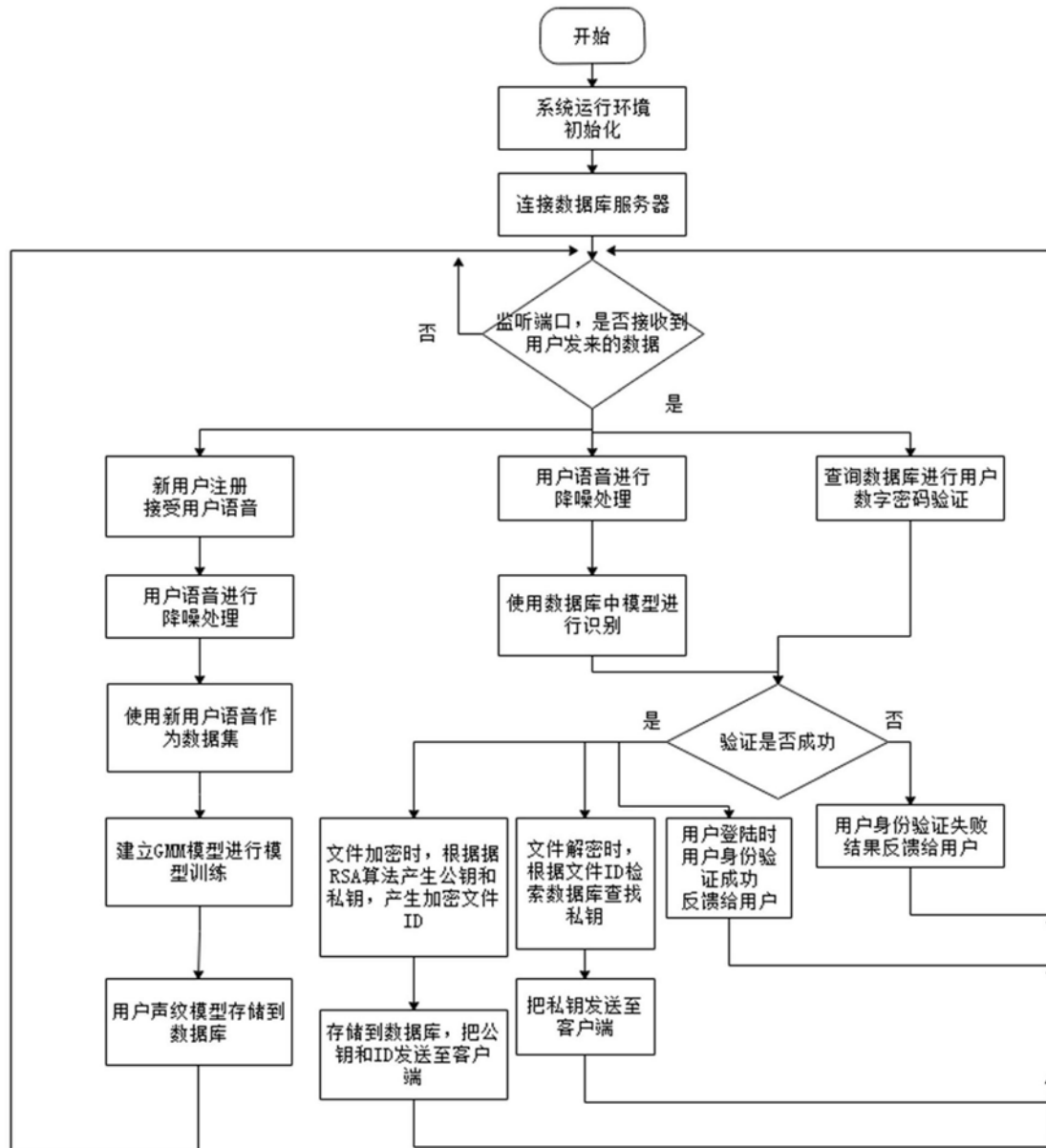


图3

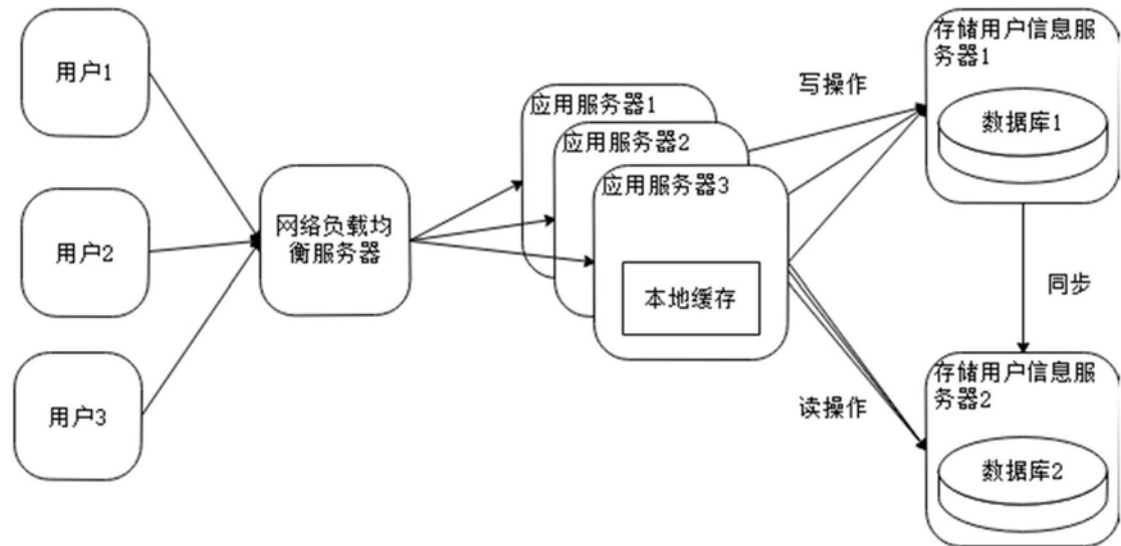


图4