(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 104469767 B
(45)授权公告日 2017.12.26

(21)申请号 201410587878.X

(22)申请日 2014.10.28

(65)同一申请的已公布的文献号
申请公布号 CN 104469767 A

(43)申请公布日 2015.03.25

(73)专利权人 杭州电子科技大学
地址 310018 浙江省杭州市下沙高教园区2号大街

(72)发明人 张程浩 吕秋云 桑永宣 王秋华 杨宝山 金都 马智超

(74)专利代理机构 杭州君度专利代理事务所(特殊普通合伙) 33240
代理人 黄前泽

(51)Int.Cl.
H04W 12/06(2009.01)
H04L 29/06(2006.01)

(56)对比文件
US 2004215971 A1,2004.10.28,
CN 103297398 A,2013.09.11,
CN 101394284 A,2009.03.25,
CN 102819918 A,2012.12.12,
CN 103761600 A,2014.04.30,
CN 104023085 A,2014.09.03,
马帅.等级保护设计要求下的移动业务系统安全防御体系.《保密科学技术》.2012,(第1期),第24-28页.
刘铮等.移动办公在发电企业中的研究和应用.《电信科学》.2013,(第11期),第115-121页.

审查员 郑丹丹

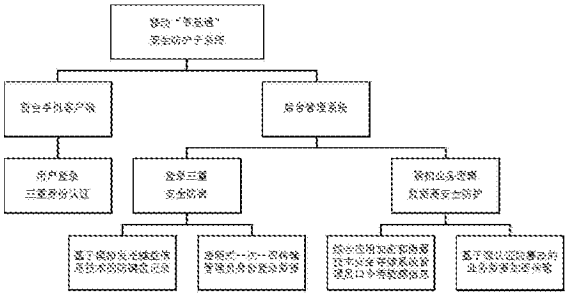
权利要求书3页 说明书7页 附图6页

(54)发明名称

一套移动办公系统中集成式安全防护子系统的实现方法

(57)摘要

本发明公开了一套移动办公系统中集成式安全防护子系统的实现方法。本发明包括手机客户端三重身份认证、后台管理系统登陆的三重安全防御、紧扣业务逻辑数据安全防护;手机客户端三重身份认证包括口令认证、人脸识别认证、图案密码认证;后台管理系统登陆的三重安全防御设计有:基于模拟发送键盘信息技术的防键盘记录、基于RSA的透明式一次一密的管理员登录身份信息加密传输方式、基于云推送的动态口令与静态用户名/口令相结合的双因素认证方式。本发明在透明地应用多种保密技术,提高数据安全性的同时,实现多重身份认证安全防御,强化访问控制能力,集成式的信息安全防护子系统,使企业通知发布和新闻浏览安全、高效。



CN 104469767 B

1.一套移动办公系统中集成式安全防护子系统的实现方法，其特征在于包括手机客户端三重身份认证、后台管理系统登陆的三重安全防御、紧扣业务逻辑的数据安全防护；

步骤1.智能手机端用户登录的三重身份认证

用户登录的三重身份认证包括口令认证、人脸识别认证、图案密码认证；

1-1.口令认证

当用户访问系统时，采用基于固定口令的认证方法，要求用户输入口令，系统收到口令后，将收到口令与系统中存储的用户口令进行比较，若口令匹配，则确认用户为合法访问者；否则提示“口令错误，请重新输入”；

所述的系统中存储的用户口令是经MD5Hash计算后保存在数据库中；

1-2.人脸识别认证

选择Face++作为第三方人脸识别云服务平台；人脸识别认证具体如下：

若用户为首次访问，则需进行注册，注册步骤如下：

①用户拍照上传包含有人脸信息的图片，并创建用户账户；

②系统通过Face++第三方人脸识别云服务平台检测提交的包含人脸信息的图片，并将检测到的人脸信息保存在云服务平台，以便后续人脸识别服务；若检测没有人脸信息，客户端提示要求用户重新上传包含人脸信息的图片；

③提取步骤②人脸信息，并通过调用云服务平台提供的API接口训练人脸模型，第三方云服务平台自动记录人脸特征值相关信息；

④重复执行三次步骤①-③，完成用户的注册，并进入用户正常使用时人脸识别认证步骤；

若用户为正常使用，则其人脸认证步骤如下：

①人脸定位检测：用户拍照上传包含有人脸信息的图片，Face++第三方人脸识别云服务平台检测提交的包含人脸信息的图片，由第三方人脸识别云服务平台检测返回人脸特征值；

②特征对比：将步骤①由第三方人脸识别云服务平台检测返回的人脸特征值与用户首次访问时建立的人脸模型中的人脸特征值进行匹配，若匹配成功，则人脸识别认证成功，用户能够解除锁定，否则提示匹配错误；

1-3.图案密码认证

用户访问时，在九宫格图案锁上输入一条带方向的路径，若该路径经过SHA-1算法后能与文件中的密文相匹配，则表示图案密码认证成功，否则提示匹配错误；若访问五次均为匹配错误，则系统将在30秒内冻结图案锁解锁，做连续3次冻结，系统则会要求用户重新输入口令，并进行人脸识别；

所述的图案密码认证通过九宫格图案锁实现，九宫格图案锁设置有9个点，分别用代码11,12,13,21,22,23,31,32,33来表示；用户在初始化设置时，设置一条带方向的路径，该路径能够以九宫格图案锁上的一串代码表示，然后将该串代码通过SHA-1算法进行计算，计算后得到密文存储在数据库中；

步骤2.后台管理系统登陆的三重安全防御

采取多因素认证方式实施三重防御；在登录接口，设计有基于模拟发送键盘信息技术的防键盘记录木马病毒攻击的功能；同时，为对抗数据流分析攻击，引入了基于RSA的透明

式一次一密的管理员登录身份信息加密传输方式;最后,专门设计有基于云推送的动态口令与静态用户名/口令相结合的双因素认证方式,进一步提高安全强度;

2-1基于模拟发送键盘信息技术的防键盘记录

基于模拟发送键盘信息技术的防键盘记录的实现通过在登录界面的HTML中插入ActiveX控件完成;

具体的:在输入框获得焦点时,触发事件调用ActiveX控件的相关函数向系统不断模拟发送干扰的按键信息,产生随机字符;直到用户光标离开密码输入框,ActiveX控件才停止发送虚假字符;

2-2透明式一次一密传输管理员身份登录数据

隐式地从服务器获取本次会话密钥,并利用此密钥对管理员身份登录数据进行RSA公钥体制加密后传输;

当后台管理员在浏览器请求Web登录页面时,服务器自动生成一对公私钥对,并把公钥通过HTTP协议传送到浏览器,私钥存储在服务器端的Session中;当前台浏览器向服务器提交表单进行身份验证时,浏览器调用公钥加密表单数据后通过HTTP协议传送到服务器,服务器用已经生成并存储在Session中的私钥解密;

透明式一次一密传输管理员身份登录数据主要涉及的过程包括:RSA密钥的产生、RSA公钥加密数据、RSA 私钥解密数据;同时为了方便加密的二进制数据传输,所以在网络中传输的加密数据均使用Base64编码;

使用RSA非对称加密方式实现身份登录数据的保密通信,服务器端首先产生密钥对,并将公钥发送到浏览器端;浏览器使用公钥加密表单数据,并传送到服务器端;服务器端使用私钥解密收到的数据;

步骤3.紧密结合业务逻辑的数据信息的高安全防护

3-1综合应用加密和隐藏技术安全存储系统管理员敏感信息

系统对所有用户的密码口令进行MD5加密处理成密文信息,并且运用信息隐藏技术,利用LSB算法将密文信息化整为零,嵌入到载体BMP位图信息的每个字节的最低位;

所述的LSB算法选用最低位平面来嵌入密文信息,同时通过冗余嵌入的方式能够增强稳健性;即在一个区域中嵌入相同信息,提取时根据该区域中的所有像素判断;

将密文信息嵌入到载体BMP位图信息每个字节最低位的具体步骤如下:

①读入载体图像,通过读取载体图像大小,判断载体可隐藏的信息量;

②确定载体图像的LSB;

③对载体图像做预处理,将其LSB设置为0;

④将密文信息以ASCII码的形式读入;

⑤在每一个像素的第LSB位上,存储密文信息的一个bit;

⑥生成并存储嵌入密文信息的图像;

读取密文信息的具体步骤:

①读入含有密文信息的图像;

②得到每一个像素点的LSB位;

③由每8个LSB位组成一个ASCII还原密文信息;

3-2基于源认证防篡改的业务数据加密传输

基于源认证防篡改的数据加密传输是对所有传输的业务数据进行基于数字签名的完整性和可认证性检验;客户端在每次请求数据时需要预先生成一对公私密钥对,并且将公钥随HTTP请求一同发至服务器端,服务器端将需要返回的数据生成hash值后,用服务器端的私钥进行数字签名,用收到的公钥采用RSA加密所有数据,再通过HTTP响应返回需要传输的数据;手机客户端收到返回的数据后,用手机客户端的私钥进行RSA解密,将密文生成hash值,再用本次会话来自服务器的公钥验证数字签名。

一套移动办公系统中集成式安全防护子系统的实现方法

技术领域

[0001] 本发明属于信息安全及移动办公系统的技术领域，特别涉及一套移动办公系统中集成式安全防护子系统的实现方法。

背景技术

[0002] 移动“信息通”办公系统主要为企业通知与新闻的快速发布和交流，提供一个快速高效的内部办公平台，其由前台手机客户端和后台信息管理系统两个子系统组成。前台手机客户端主要功能包括：新闻与通知的接收、消息推送接收、评论、阅读回复。后台管理系统主要功能包括：信息内容的发布、审核、管理，用户管理与身份验证，部门分组管理等。

[0003] 对于没有安全防护子系统的移动“信息通”，其移动终端APP及后台管理系统普遍存在的安全问题并无有效的解决方案或有意忽略，致使企事业单位的内部办公数据甚至是内部的机密信息处于极大的安全隐患之中。在当前技术及使用环境下，移动“信息通”面临的主要安全问题如下：

[0004] 第一，手机客户端身份验证方式单一甚至缺漏，内部机密信息传播范围无法控制，给企事业单位内部的信息安全造成威胁；

[0005] 第二，手机客户端APP可以被反编译，代码可被任意修改，服务器的获取数据接口容易被暴露而恶意利用，手机软件安全漏洞甚至威胁导致整个后台服务器安全。

[0006] 第三，后台管理系统身份认证方式单一，安全措施薄弱，容易被攻击者绕过验证，是系统最严重的安全威胁；

[0007] 第四，网络中的应用数据大多以明文传输，攻击者通过嗅探分析即可获得办公系统中内部数据或机密信息，数据安全无保障。

[0008] 由此可见，上述四大安全问题无法继续依赖于防火墙、杀毒软件、入侵检测系统、VPN等完全解决。

发明内容

[0009] 本发明的目的就是针对现有移动办公系统中存在的安全的问题，从系统的登录到信息数据的生成、传输、使用、存储等每个环节入手，通过紧密结合具体业务功能逻辑，提出了移动办公系统中集成式安全防护子系统的实现方法，使企业通知发布和新闻浏览安全、高效。

[0010] 为了实现上述目的，本发明是通过如下的技术方案来实现：

[0011] 一套移动办公系统中集成式安全防护子系统的实现方法，包括手机客户端三重身份认证、后台管理系统登陆的三重安全防御、紧扣业务逻辑数据安全防护；

[0012] 步骤1.智能手机端用户登录的三重身份认证

[0013] 用户登录的三重身份认证包括口令认证、人脸识别认证、图案密码认证；

[0014] 1-1.口令认证

[0015] 当用户访问系统时，采用基于固定口令的认证方法，要求用户输入口令，系统收到

口令后，将收到口令与系统中存储的用户口令进行比较，若口令匹配，则确认用户为合法访问者；否则提示“口令错误，请重新输入”；

[0016] 所述的系统中存储的用户口令是经MD5Hash计算后保存在数据库中；

[0017] 1-2.人脸识别认证

[0018] 选择Face++作为第三方人脸识别云服务平台；人脸识别认证具体如下：

[0019] 若用户为首次访问，则需进行注册，注册步骤如下：

[0020] ①用户拍照上传包含有人脸信息的图片，并创建用户账户；

[0021] ②系统通过Face++第三方人脸识别云服务平台检测提交的包含人脸信息的图片，并将检测到的人脸信息保存在云服务平台，以便后续人脸识别服务；若检测没有人脸信息，客户端提示要求用户重新上传包含人脸信息的图片；

[0022] ③提取步骤②人脸信息，并通过调用云服务平台提供的API接口训练人脸模型，第三方云服务平台自动记录人脸特征值相关信息；

[0023] ④重复执行三次步骤①-③，完成用户的注册，并进入用户正常使用时人脸识别认证步骤；

[0024] 若用户为正常使用，则其人脸认证步骤如下：

[0025] ①人脸定位检测：用户拍照上传包含有人脸信息的图片，Face++第三方人脸识别云服务平台检测提交的包含人脸信息的图片，提取出人脸特征值；

[0026] ②特征对比：将步骤①提取出人脸特征值与用户首次访问时建立的人脸模型中的人脸特征值进行匹配，若匹配成功，则人脸识别认证成功，用户能够解除锁定，否则提示匹配错误；

[0027] 1-3.图案密码认证

[0028] 用户访问时，在九宫格图案锁上输入一条带方向的路径，若该路径经过SHA-1算法后能与文件中的密文相匹配，则表示图案密码认证成功，否则提示匹配错误；若访问五次均为匹配错误，则系统将在30秒内冻结图案锁解锁，做连续3次冻结，系统则会要求用户重新输入口令，并进行人脸识别；

[0029] 所述的图案密码认证通过九宫格图案锁实现，九宫格图案锁设置有9个点，分别用代码11,12,13,21,22,23,31,32,33来表示；用户在初始化设置时，设置一条带方向的路径，该路径能够以九宫格图案锁上的一串代码表示，然后将该串代码通过SHA-1算法进行计算，计算后得到密文存储在数据库中；

[0030] 步骤2.后台管理系统登陆的三重安全防御

[0031] 采取多因素认证方式实施三重防御；在登录接口，设计有基于模拟发送键盘信息技术的防键盘记录木马病毒攻击的功能；同时，为对抗数据流分析攻击，引入了基于RSA的透明式一次一密的管理员登录身份信息加密传输方式；最后，专门设计有基于云推送的动态口令与静态用户名/口令相结合的双因素认证方式，进一步提高安全强度；

[0032] 2-1基于模拟发送键盘信息技术的防键盘记录

[0033] 基于模拟发送键盘信息技术的防键盘记录的实现通过在登录界面的HTML中插入ActiveX控件完成；

[0034] 具体的：在输入框获得焦点时，触发事件调用ActiveX控件的相关函数向系统不断模拟发送干扰的按键信息，产生随机字符；直到用户光标离开密码输入框，ActiveX控件才

停止发送虚假字符；

[0035] 2-2透明式一次一密传输管理员身份登录数据

[0036] 隐式地从服务器获取本次会话密钥，并对利用此密钥对管理员身份登录数据进行RSA公钥体制加密后传输；

[0037] 当后台管理员在浏览器请求Web登录页面时，服务器自动生成一对公私钥对，并把公钥通过HTTP协议传送到浏览器，私钥存储在服务器端的Session中；当前台浏览器向服务器提交表单进行身份验证时，浏览器调用公钥加密表单数据后通过HTTP协议传送到服务器，服务器用当前会话的已经生成的存储在Session中私钥解密；

[0038] 透明式一次一密传输管理员身份登录数据主要涉及的过程包括：RSA密钥的产生、RSA公钥加密数据、RAS私钥解密数据；同时为了方便加密的二进制数据传输，所以在网络中传输的加密数据均使用Base64编码；

[0039] 使用RSA非对称加密方式实现身份登录数据的保密通信，服务器端首先产生密钥对，并将公钥发送到浏览器端；浏览器使用公钥加密表单数据，并传送到服务器端；服务器端使用私钥解密收到的数据；

[0040] 步骤3.紧密结合业务逻辑的数据信息的高安全防护

[0041] 3-1综合应用加密和隐藏技术安全存储系统管理员敏感信息

[0042] 系统对所有用户的密码口令进行MD5加密处理成密文信息，并且运用信息隐藏技术，利用LSB算法将密文信息化整为零，嵌入到载体BMP位图信息的每个字节的最低位；

[0043] 所述的LSB算法选用最低位平面来嵌入密文信息，同时通过冗余嵌入的方式能够增强稳健性；即在一个区域中嵌入相同信息，提取时根据该区域中的所有像素判断；

[0044] 将密文信息嵌入到载体BMP位图信息每个字节最低位的具体步骤如下：

[0045] ①读入载体图像，通过读取载体图像大小，判断载体可隐藏的信息量；

[0046] ②确定载体图像的LSB；

[0047] ③对载体图像做预处理，将其LSB设置为0；

[0048] ④将密文信息以ACILL码的形式读入；

[0049] ⑤在每一个象素的第LSB位上，存储密文信息的一个bit；

[0050] ⑥生成并存储嵌入密文信息的图像；

[0051] 读取密文信息的具体步骤：

[0052] ①读入含有密文信息的图像；

[0053] ②得到每一个象素点的LSB位；

[0054] ③由每8个LSB位组成一个ASILL还原密文信息；

[0055] 3-2基于源认证防篡改的业务数据加密传输

[0056] 基于源认证防篡改的数据加密传输是对所有传输的业务数据进行基于数字签名的完整性和可认证性检验；客户端在每次请求数据时需要预先生成一对公私密钥对，并且将公钥随HTTP请求一同发至服务器端，服务器端将需要返回的数据生成hash值后，用私钥进行数字签名，用收到的公钥采用RSA加密所有数据，再通过HTTP响应返回需要传输的数据；手机客户端收到返回的数据后，用私钥进行RSA解密，将密文生成hash值，再用本次会话的公钥验证数字签名。

[0057] 本发明有益效果如下：

[0058] 本发明以移动“信息通”为移动办公系统的代表，研究分析了目前移动办公系统中身份鉴定和无线数据传输等目前最突出的安全问题，提出了业务系统与安全功能紧密结合的集成式保护设计思想：在透明地应用多种保密技术，提高数据安全性的同时，实现多重身份认证安全防御，强化访问控制能力。

[0059] 同时，本发明以移动“信息通”为移动办公系统集成式安全防护子系统实施的业务平台，从系统的登录到信息数据的生成、传输、使用、存储等每个环节入手，紧密结合具体业务功能逻辑，设计实现集成式的信息安全防护子系统，使企业通知发布和新闻浏览安全、高效。本作品的安全防护子系统主要功能包括：

[0060] (1)智能手机端用户登录的三重身份认证；

[0061] (2)后台管理系统登录的三重安全防御；

[0062] (3)紧密结合业务逻辑的数据信息的高安全防护。

附图说明

[0063] 图1是本发明安全防护子系统组成结构示意图；

[0064] 图2人脸识别注册流程图

[0065] 图3人脸识别认证流程图

[0066] 图4三重身份认证流程图

[0067] 图5是防键盘记录过程

[0068] 图6是一次一密传输身份登录数据流程

[0069] 图7是安全存储系统管理员口令流程

[0070] 图8是基于源认证防篡改的业务数据安全传输模型。

具体实施方式

[0071] 为使本发明实现的技术手段、创作特征、达成目的与功效易于明白了解，下面结合附图对本发明作进一步的说明。

[0072] 如图1所示，一套移动办公系统中集成式安全防护子系统的实现方法，包括手机客户端三重身份认证、后台管理系统登陆的三重安全防御、紧扣业务逻辑数据安全防护。具体实施方式采用以下技术方案：

[0073] 步骤1.智能手机端用户登录的三重身份认证

[0074] 如图2和图3所示，为了增强手机客户端登录控制的安全性，有效验证合法用户，保证信息系统进行有效的访问控制，同时为了保护合法用户隐私安全，防止他人窃取隐私，用户登录的三重身份认证包括口令认证、人脸识别认证、图案密码认证。

[0075] 1-1.口令认证

[0076] 当用户访问系统时，采用基于固定口令的认证方法，要求用户输入口令，系统收到口令后，将收到口令与系统中存储的用户口令进行比较，若口令匹配，则确认用户为合法访问者；否则提示“口令错误，请重新输入”。

[0077] 所述的系统中存储的用户口令是经MD5Hash计算后保存在数据库中。

[0078] 1-2.人脸识别认证

[0079] 选择Face++作为第三方人脸识别云服务平台。人脸识别认证具体如下：

[0080] 若用户为首次访问，则需进行注册，如图2所示，注册步骤如下：

[0081] ①用户拍照上传包含有人脸信息的图片，并创建用户账户。

[0082] ②系统通过Face++第三方人脸识别云服务平台检测提交的包含人脸信息的图片，并将检测到的人脸信息保存在云服务平台，以便后续人脸识别服务。若检测没有人脸信息，客户端提示要求用户重新上传包含人脸信息的图片。

[0083] ③提取步骤②人脸信息，并通过调用云服务平台提供的API接口训练人脸模型，第三方云服务平台自动记录人脸特征值相关信息。

[0084] ④重复执行三次步骤①-③，完成用户的注册，并进入用户正常使用时人脸识别认证步骤。

[0085] 若用户为正常使用，则如图3所示其人脸认证步骤如下：

[0086] ②人脸定位检测：用户拍照上传包含有人脸信息的图片，Face++第三方人脸识别云服务平台检测提交的包含人脸信息的图片，提取出人脸特征值；

[0087] ②特征对比：将步骤①提取出人脸特征值与用户首次访问时建立的人脸模型中的人脸特征值进行匹配，若匹配成功，则人脸识别认证成功，用户能够解除锁定，否则提示匹配错误。

[0088] 1-3.图案密码认证

[0089] 用户访问时，在九宫格图案锁上输入一条带方向的路径，若该路径经过SHA-1算法后能与文件中的密文相匹配，则表示图案密码认证成功，否则提示匹配错误；若访问五次均为匹配错误，则系统将在30秒内冻结图案锁解锁，做连续3次冻结，系统则会要求用户重新输入口令，并进行人脸识别。

[0090] 所述的图案密码认证通过九宫格图案锁实现，九宫格图案锁设置有9个点，分别用代码11,12,13,21,22,23,31,32,33来表示；用户在初始化设置时，设置一条带方向的路径，该路径能够以九宫格图案锁上的一串代码表示，然后将该串代码通过SHA-1算法进行计算，计算后得到密文存储在数据库中。

[0091] 如图4所示，每次手机客户端开启运行使用手机客户端“信息通”应用需通过验证口令、人脸识别和图案密码锁三道防线。为了方便用户获得良好的用户体验，只有当本系统从后台运行状态切换到前台运行状态时，仅需进行图案锁解锁；否则需要通过三重身份认证才能正常使用该应用。

[0092] 步骤2.后台管理系统登陆的三重安全防御

[0093] 后台管理员的操作直接决定着整个系统的运行状况，因此，对管理员的身份验证需要从登录的接口和数据传输做特别的安全保护，同时采取多因素认证方式实施三重防御。在登录接口，设计有基于模拟发送键盘信息技术的防键盘记录木马病毒攻击的功能；同时，为对抗数据流分析攻击，引入了基于RSA的透明式一次一密的管理员登录身份信息加密传输方式；最后，专门设计了基于云推送的动态口令与静态用户名/口令相结合的双因素认证方式，进一步提高安全强度。

[0094] 2-1基于模拟发送键盘信息技术的防键盘记录

[0095] 如图5所示，基于模拟发送键盘信息技术的防键盘记录的实现通过在登录界面的HTML中插入ActiveX控件完成；

[0096] 具体的：在输入框获得焦点时，触发事件调用ActiveX控件的相关函数向系统不断

模拟发送干扰的按键信息，产生随机字符；直到用户光标离开密码输入框，ActiveX控件才停止发送虚假字符。模拟发送的按键信息能够起到干扰的作用，即使用户的计算机被注入键盘记录木马，攻击者截获的输入记录信息中含有大量的冗余掺假信息，从而使攻击者无法准确地获得真实有效的重要敏感信息，有效增强敏感信息的安全性。

[0097] 2-2透明式一次一密传输管理员身份登录数据

[0098] 为了增加数据传输保密性的安全强度，隐式地从服务器获取本次会话密钥，并对利用此密钥对管理员身份登录数据进行RSA公钥体制加密后传输，实现一个安全、高效、可靠且易于实现移动“信息通”身份验证保护。

[0099] 当后台管理员在浏览器请求Web登录页面时，服务器自动生成一对公私钥对，并把公钥通过HTTP协议传送到浏览器，私钥存储在服务器端的Session中；当前台浏览器向服务器提交表单进行身份验证时，浏览器调用公钥加密表单数据后通过HTTP协议传送到服务器，服务器用当前会话的已经生成的存储在Session中私钥解密。

[0100] 透明式一次一密传输管理员身份登录数据主要涉及的过程包括：RSA密钥的产生、RSA公钥加密数据、RAS私钥解密数据。同时为了方便加密的二进制数据传输，所以在网络中传输的加密数据均使用Base64编码。

[0101] 使用RSA非对称加密方式实现身份登录数据的保密通信如图6流程所示，服务器端首先产生密钥对，并将公钥发送到浏览器端；浏览器使用公钥加密表单数据，并传送到服务器端；服务器端使用私钥解密收到的数据。

[0102] 步骤3.紧密结合业务逻辑的数据信息的高安全防护

[0103] 3-1综合应用加密和隐藏技术安全存储系统管理员敏感信息

[0104] 图7所示，系统对所有用户的密码口令进行MD5加密处理成密文信息，并且运用信息隐藏技术，利用LSB算法将密文信息化整为零，嵌入到载体BMP位图信息的每个字节的最低位，使得系统敏感信息的隐蔽性大大提高。通过这样处理的载体图片没有明显的降质现象，而隐藏的敏感数据也无法人为地直接看见，有良好的透明性。

[0105] 所述的LSB算法选用最低位平面来嵌入密文信息。最低位平面对图像的视觉效果影响最轻微，但很容易受噪声影响和攻击，通过冗余嵌入的方式能够增强稳健性。即在一个区域(多个像素)中嵌入相同信息，提取时根据该区域中的所有像素判断。

[0106] 将密文信息嵌入到载体BMP位图信息每个字节最低位的具体步骤如下：

[0107] ②读入载体图像，通过读取载体图像大小，判断载体可隐藏的信息量；

[0108] ②确定载体图像的LSB(Least Significant Bit)；

[0109] ③对载体图像做预处理，将其LSB设置为0；

[0110] ④将密文信息以ACILL码的形式读入；

[0111] ⑤在每一个象素的第LSB位上，存储密文信息的一个bit；

[0112] ⑥生成并存储嵌入密文信息的图像。

[0113] 读取密文信息的具体步骤：

[0114] ①读入含有密文信息的图像；

[0115] ②得到每一个象素点的LSB位；

[0116] ③由每8个LSB位组成一个ASILL还原密文信息。

[0117] 3-2基于源认证防篡改的业务数据加密传输

[0118] 基于源认证防篡改的数据加密传输是对所有传输的业务数据进行基于数字签名的完整性和可认证性检验。如图8所示，为了保证数据的保密性，客户端在每次请求数据时需要预先生成一对公私密钥对，并且将公钥随HTTP请求一同发至服务器端，服务器端将需要返回的数据生成hash值后，用私钥进行数字签名，用收到的公钥采用RSA加密所有数据，再通过HTTP响应返回需要传输的数据。手机客户端收到返回的数据后，用私钥进行RSA解密，将密文生成hash值，再用本次会话的公钥验证数字签名。

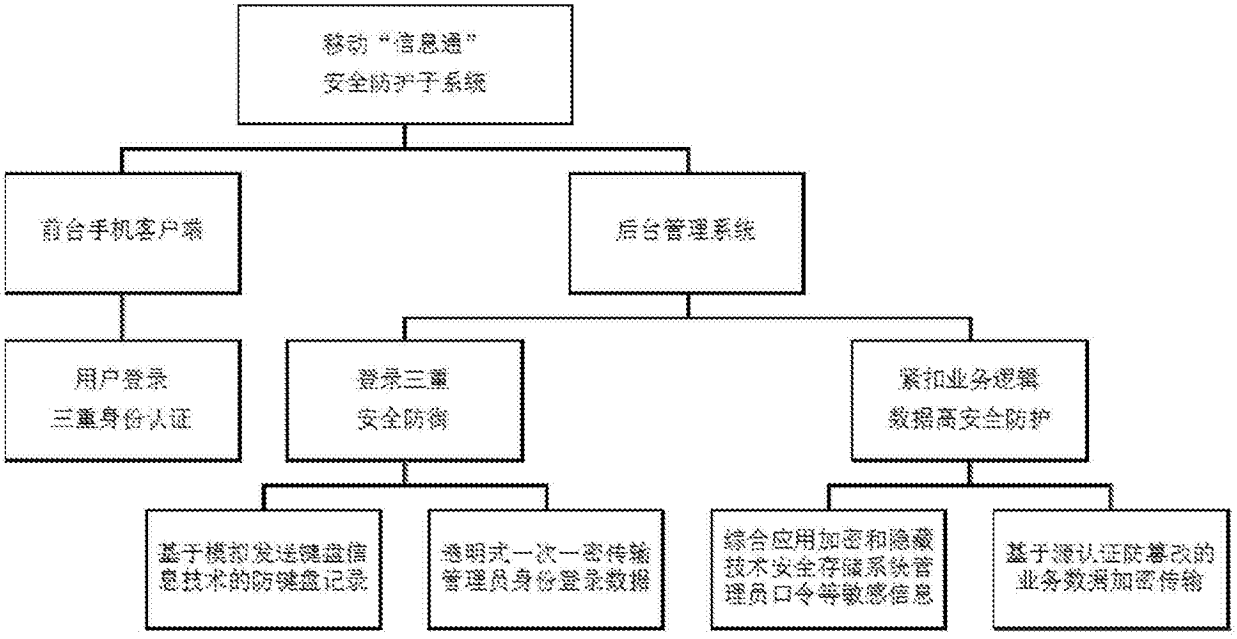

移动“信息通”
安全防护子系统
前台手机客户端
后台管理系统
用户登录
三重身份认证
登录三重
安全防御
紧扣业务逻辑
数据高安全防护
基于模拟发送键盘信息技术的防键盘记录
透明式一次一密传输管理员身份登录数据
综合应用加密和隐藏技术安全存储系统管理员口令等敏感信息
基于源认证防篡改的业务数据加密传输

图1

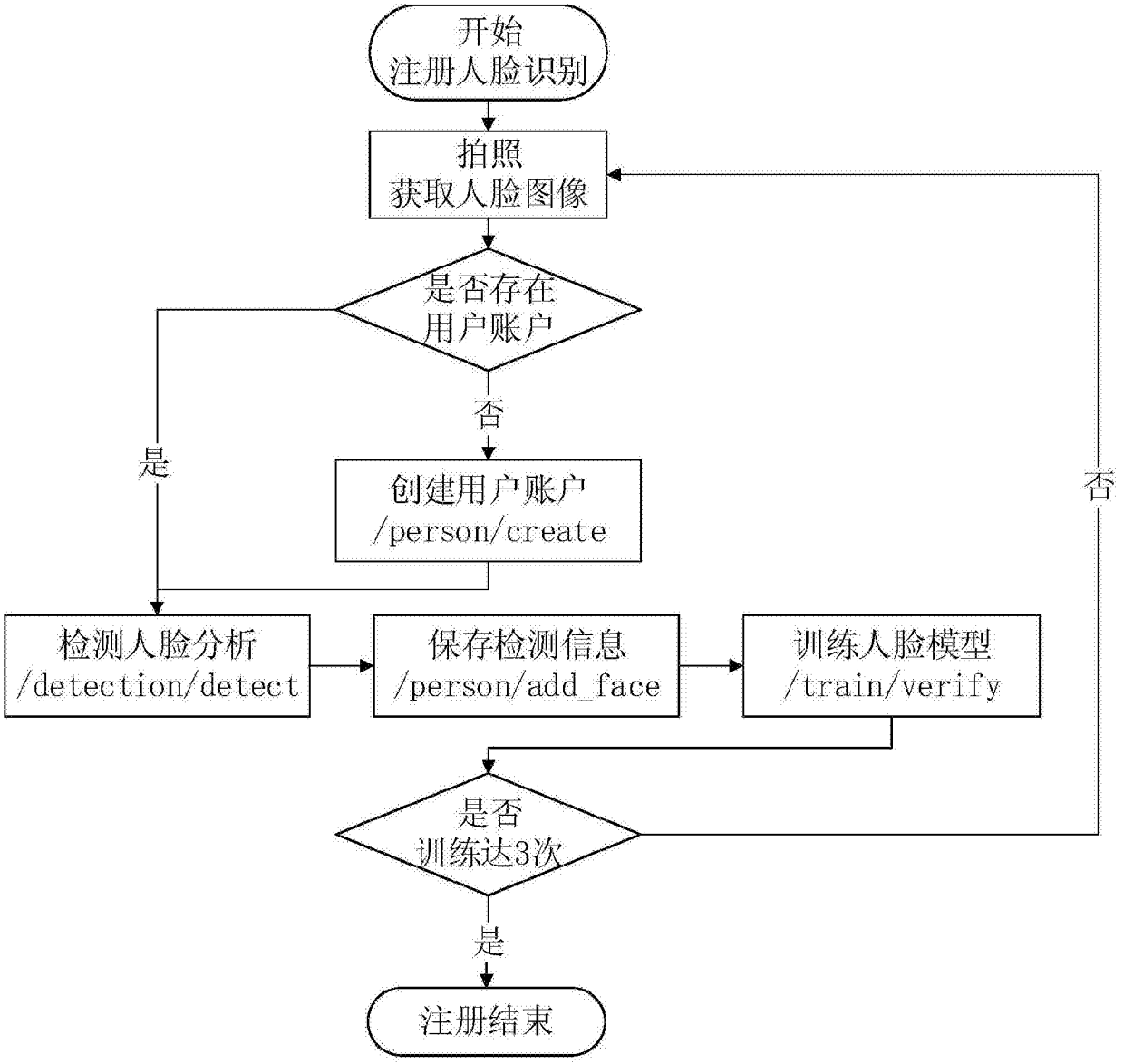

开始
注册人脸识别
拍照
获取人脸图像
是否存在
用户账户
否
是
否
创建用户账户
/person/create
检测人脸分析
/detection/detect
保存检测信息
/person/add_face
训练人脸模型
/train/verify
是否
训练达3次
是
注册结束

图2

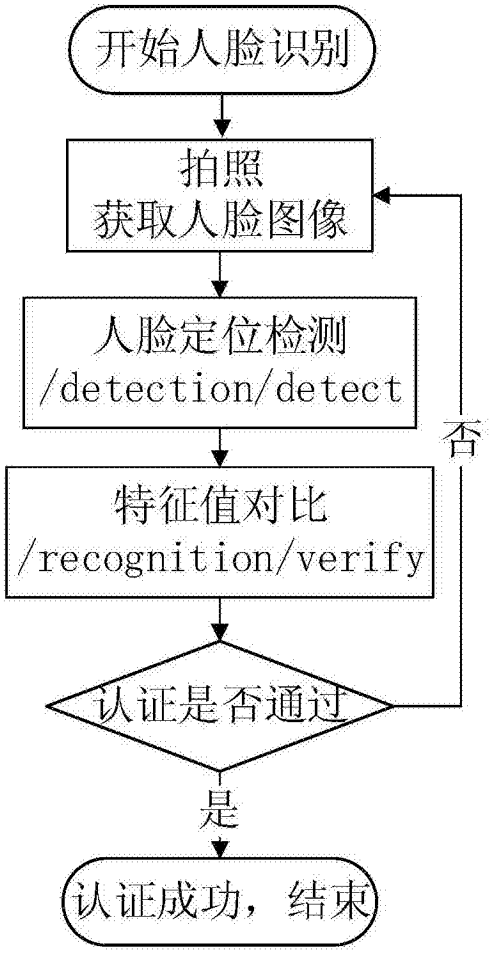

开始人脸识别
拍照
获取人脸图像
人脸定位检测
/detection/detect
特征值对比
/recognition/verify
认证是否通过
否
是
认证成功，结束

图3

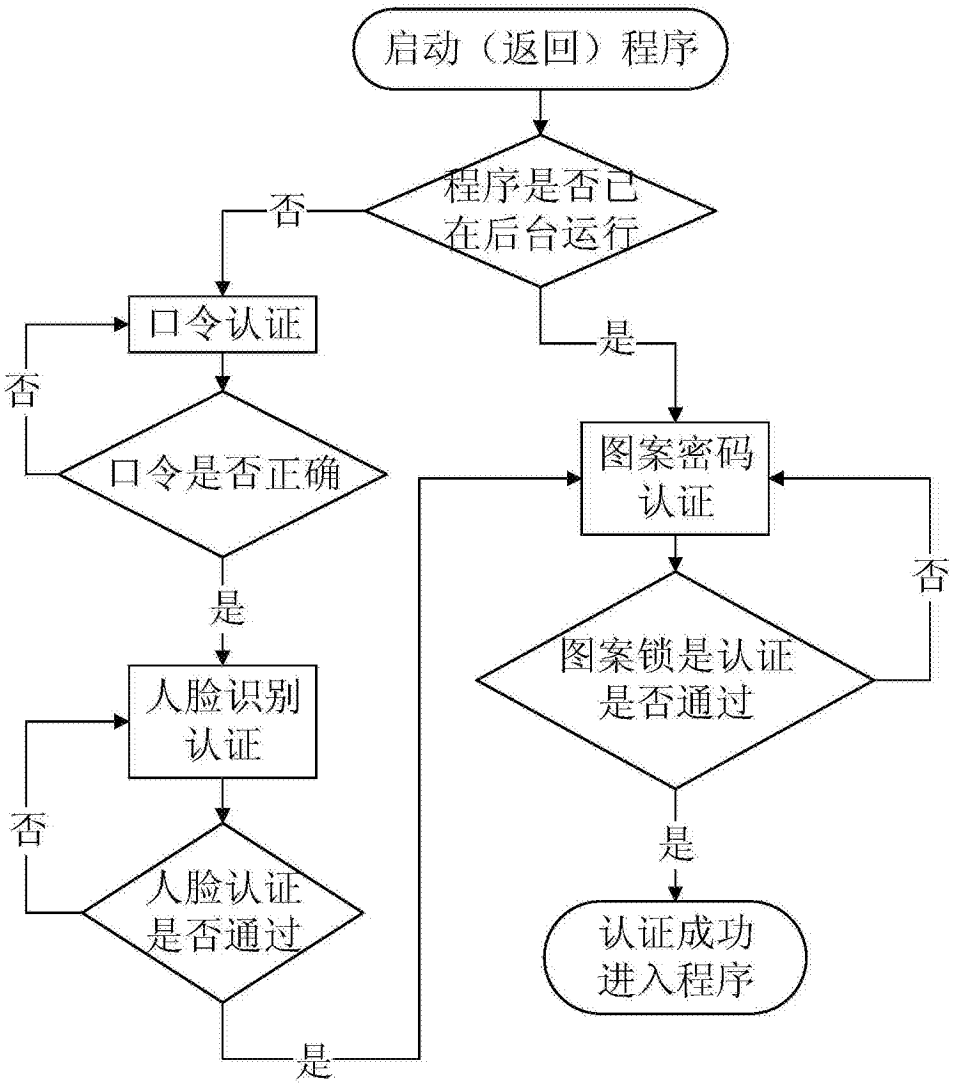

启动（返回）程序
程序是否已在后台运行
否
是
口令认证
否
口令是否正确
是
人脸识别认证
否
人脸认证是否通过
是
图案密码认证
图案锁是认证是否通过
否
是
认证成功进入程序

图4

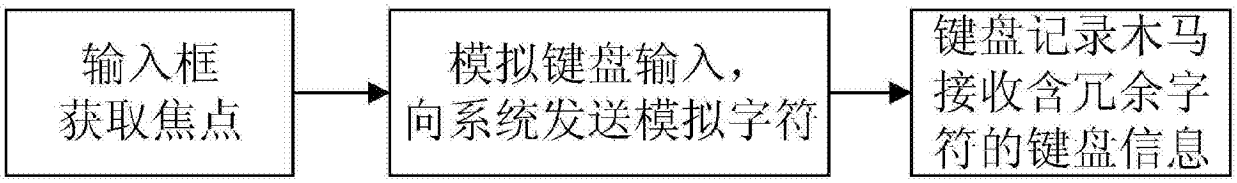

输入框获取焦点
模拟键盘输入，向系统发送模拟字符
键盘记录木马接收含冗余字符的键盘信息

图5

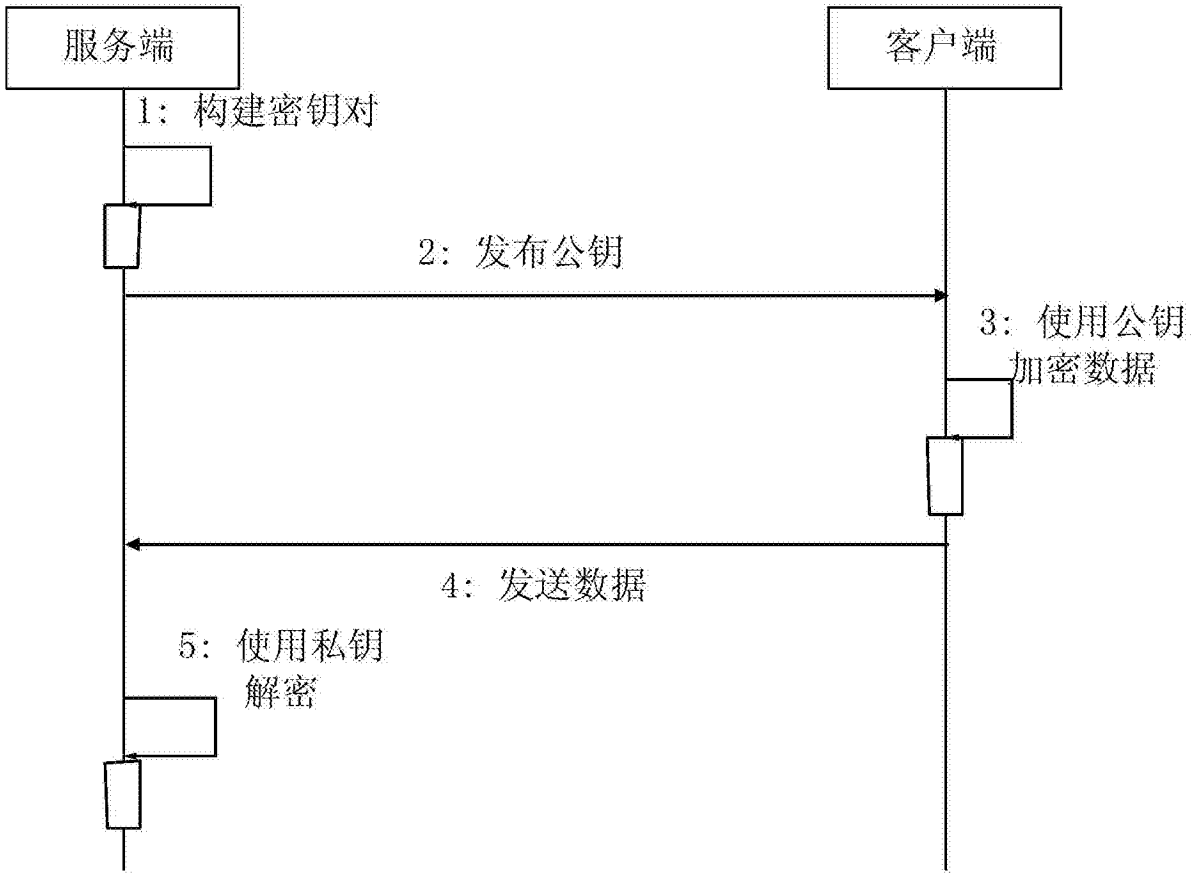

服务端
客户端
1：构建密钥对
2：发布公钥
3：使用公钥
加密数据
4：发送数据
5：使用私钥
解密

图6

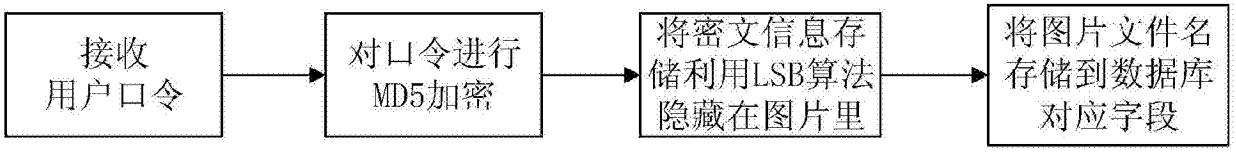

接收
用户口令
对口令进行
MD5加密
将密文信息存
储利用LSB算法
隐藏在图片里
将图片文件名
存储到数据库
对应字段

图7

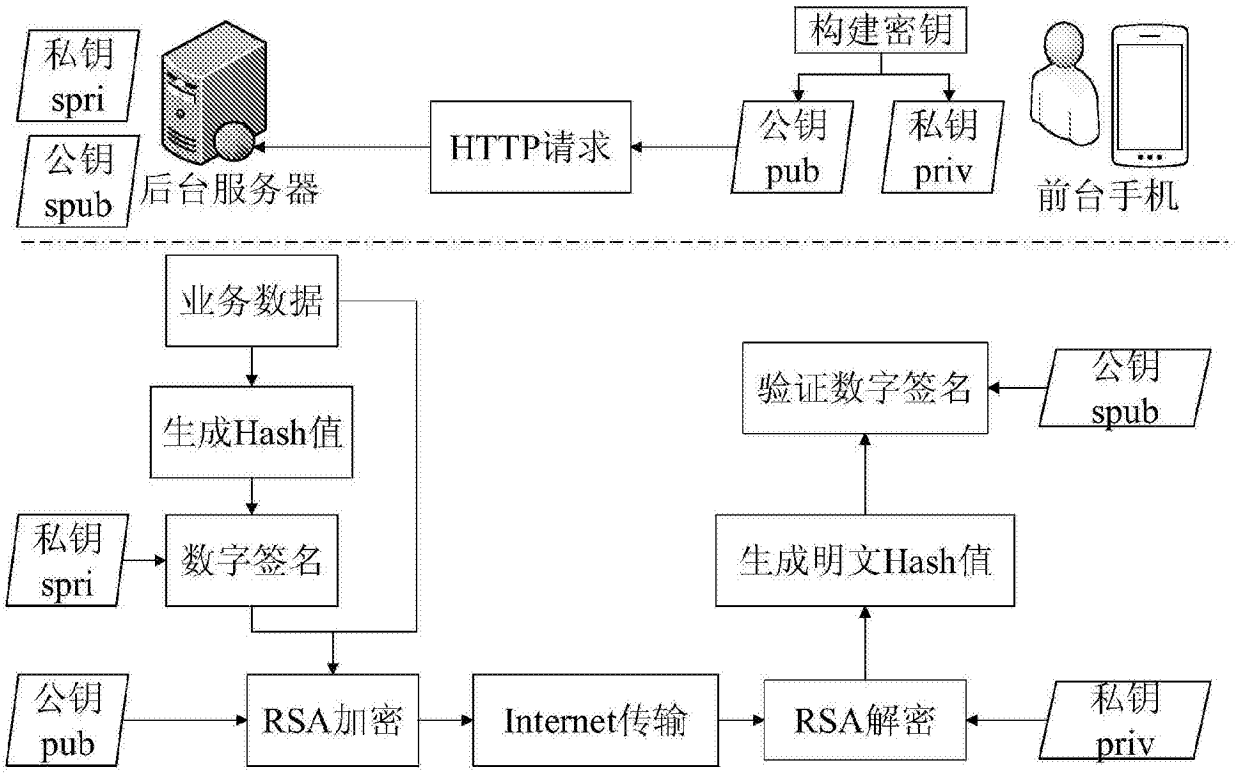

私钥
spri
公钥
spub
后台服务器
HTTP请求
构建密钥
公钥
pub
私钥
priv
前台手机
业务数据
生成Hash值
私钥
spri
数字签名
公钥
pub
RSA加密
Internet传输
RSA解密
私钥
priv
生成明文Hash值
验证数字签名
公钥
spub

图8