(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 104715242 A
(43)申请公布日 2015.06.17

(21)申请号 201510136683.8

(22)申请日 2015.03.27

(71)申请人 刘学明
地址 610071 四川省成都市青羊区金凤路19号14-2-402

(72)发明人 刘学明

(51)Int.Cl.
G06K 9/00(2006.01)
G06Q 20/32(2012.01)
G06Q 20/40(2012.01)

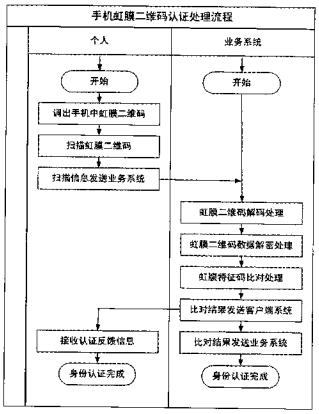
权利要求书3页 说明书4页 附图4页

(54)发明名称

基于虹膜二维码的身份认证系统及方法

(57)摘要

本发明公开一种基于虹膜二维码的身份认证系统及方法，该系统由前端系统和后端系统构成；前端系统由虹膜采集单元、终端机构成，后端系统由虹膜认证服务器和虹膜数据库构成；前端系统和后端系统通过互联网进行连接；其运行模式分为集中模式、分散模式、混合模式；本发明采用“你拥有什么”+“你是谁”的双唯一性绑定技术，利用独一无二的身体特征一虹膜特征码作为身份认证的凭据，认证中无需密码，仅需一次虹膜二维码的单向传输，具有较强的防拦截、防伪造、防仿冒、防敏感数据泄露、防个人终端遗失能力，实现了使用唯一的虹膜二维码在不同应用系统间的畅行通用。



CN 104715242 A

1. 基于虹膜二维码的身份认证系统及方法，其特征在于系统由前端系统和后端系统构成；前端系统由虹膜采集单元、终端机构成，后端系统由虹膜认证服务器和虹膜数据库构成；前端系统和后端系统通过网络进行连接；

所述前端系统的虹膜采集单元采集虹膜图像，直接传送到终端机；

所述前端系统的终端机分为个人终端机和专用终端机；个人终端机包括移动终端如智能手机、固定终端如 PC 机，均安装有专用的虹膜二维码客户端软件，个人终端机完成虹膜图像采集控制、虹膜图像预处理及发送、虹膜二维码管理及虹膜二维码认证功能；专用终端机为虹膜注册 / 认证终端机，是含有虹膜采集单元的终端机，完成虹膜图像采集控制、虹膜图像预处理及发送、虹膜认证功能；

所述后端系统的虹膜认证服务器完成虹膜图像的虹膜特征码提取、虹膜二维码生成、虹膜二维码比对认证及虹膜二维码管理功能；

所述后端系统的虹膜数据库存储虹膜图像、虹膜二维码信息。

2. 根据权利要求 1 所述的基于虹膜二维码的身份认证系统及方法，特征在于其系统运行模式分为集中模式、分散模式、混合模式三种；

所述集中模式，即集中服务模式，各应用系统的虹膜认证业务由虹膜认证服务器集中处理；此模式下，所有个人的虹膜图像及虹膜二维码信息均存储于统一的虹膜数据库中；

所述分散模式，即分散服务模式，各应用系统的虹膜认证业务由本系统的虹膜认证服务器处理；跨系统的处理需求由各应用系统的虹膜认证服务器之间的协作机构相互协同完成；此模式下，各应用系统的虹膜数据库中只存储有和本系统业务相关的注册个人的虹膜图像及虹膜二维码信息；

所述混合模式，即混合服务模式，各应用系统的虹膜认证业务由本系统的虹膜认证服务器处理；跨系统的处理需求由中心虹膜认证服务器统一协调；此模式下，各应用系统的虹膜数据库只存储有和本系统业务相关的注册个人的虹膜图像及虹膜二维码信息，中心虹膜认证服务器的虹膜数据库则存储有所有应用系统的个人的虹膜图像及虹膜二维码信息的集合。

3. 根据权利要求 1 所述的基于虹膜二维码的身份认证系统及方法，特征在于其虹膜注册，是首次用虹膜注册身份必须采用的方式，个人选择何应用系统完成虹膜注册根据其需求而定，一旦选定某一应用系统向其注册，该应用系统即成为该个人虹膜二维码的注册系统；首次虹膜注册时可选择移动终端、固定终端、虹膜注册 / 认证终端机三种方式之一；

选择移动终端进行虹膜注册时，需先填写相关的注册申请信息，然后使用虹膜采集单元采集虹膜图像，该图像直接传输给移动终端，移动终端对虹膜图像进行定位、一体化处理及增强处理后，经网络传输到后端系统；后端系统的虹膜认证服务器对虹膜图像进行虹膜特征码提取处理后，生成虹膜二维码图码文件，一份留存比对使用，一份发送给移动终端认证使用；

选择固定终端进行虹膜注册时，需先填写相关的注册申请信息，然后使用虹膜采集单元采集虹膜图像，该图像直接传输给固定终端，固定终端对虹膜图像进行定位、一体化处理及增强处理后，经网络传输到后端系统；后端系统的虹膜认证服务器对虹膜图像进行虹膜特征码提取处理后，生成虹膜二维码图码文件，一份留存比对使用，一份发送给固定终端认证使用；

选择虹膜注册 / 认证终端机进行虹膜注册时，需先填写相关的注册申请信息以及虹膜二维码捆绑的移动终端号码，其后，虹膜注册 / 认证终端机直接采集虹膜图像，并对虹膜图像进行定位、一体化处理及增强处理后，经网络传输到后端系统；后端系统的虹膜认证服务器对虹膜图像进行虹膜特征码提取处理后，生成虹膜二维码图码文件，一份留存比对使用，一份发送给所绑定的个人终端认证使用；

首次虹膜注册完成后，可以将虹膜注册信息复制到移动终端及固定终端上。

4. 根据权利要求 1 所述的基于虹膜二维码的身份认证系统及方法，特征在于其引用注册，是个人引用已有的虹膜二维码向其他应用系统注册的方式；在完成首次虹膜注册后，个人可以直接使用所拥有的虹膜二维码向其他应用系统进行注册；引用注册时可以选择移动终端或固定终端；其他应用系统用虹膜二维码向其注册系统核实后即可生效。

5. 根据权利要求 1 所述的基于虹膜二维码的身份认证系统及方法，特征在于其信息加密，虹膜二维码在其生成过程中选取虹膜特征码、个人姓名、公共识别号等敏感信息实施加密处理，这些敏感信息只在后端系统虹膜二维码比对计算时才予以解密还原。

6. 根据权利要求 1 所述的基于虹膜二维码的身份认证系统及方法，特征在于其绑定及迁移，根据使用需要个人可以将虹膜二维码和指定设备和指定账户实施绑定，也可以对原绑定的设备进行迁移及绑定账户进行更换；

①绑定设备：经个人申请注册系统可以将其虹膜二维码与移动终端、固定终端等设备实施绑定，经该个人授权的相关应用系统可通过技术手段获取该设备绑定信息；设备绑定信息在引用注册时自动告知相关的应用系统；

②绑定账户：经个人申请注册系统或其他应用系统可以将其虹膜二维码与指定的个人账户实施绑定；

③设备迁移：经个人申请注册系统可以将原有的虹膜二维码与移动终端、固定终端等设备的绑定关系予以迁移，注册系统更新绑定关系；迁移完成后相关应用系统可通过技术手段获取新的设备绑定信息，并据此更新本系统的绑定关系；

④账户更换：经个人申请相关业务系统可以将原有的虹膜二维码与特定的个人账户的绑定关系予以更换。

7. 根据权利要求 1 所述的基于虹膜二维码的身份认证系统及方法，其特征在于设备挂失，个人终端遗失后启动客户端系统的设备挂失，该设备挂失信息将逐一通报相关的应用系统，相关应用系统对挂失设备的虹膜二维码予以冻结，直至个人解除挂失或完成设备迁移。

8. 根据权利要求 1 所述的基于虹膜二维码的身份认证系统及方法，其特征在于个人可以选择虹膜认证和虹膜二维码认证这两种方式进行身份认证；

所述虹膜认证方式，即现场采集虹膜图像以此为认证凭据向相关应用系统进行身份认证的方式；其过程为：现场采集虹膜图像，该图像直接传输给个人终端或专用终端机，个人终端或专用终端机对虹膜图像进行定位、一体化处理及增强处理后，经网络传输到相应的后端系统；后端系统的虹膜认证服务器对虹膜图像进行虹膜特征码提取处理后，与数据库中该个人的虹膜特征码进行查找比对，产生认证结果，并将认证结果发往相关的业务系统；

所述虹膜二维码认证方式，即个人直接使用存储于个人终端机的虹膜二维码作为认证

凭据向相关应用系统进行身份认证的方式；根据应用场景虹膜二维码使用方式有自扫描模式和被扫描模式两种可选；自扫描模式是个人终端机的二维码扫描软件扫描调取的虹膜二维码图片，发往后端系统，自扫描模式既适用于固定终端认证也可适用于移动终端认证；被扫描模式是移动终端调取虹膜二维码图片接受二维码扫描设备或扫描软件的扫描，被扫描模式适用于移动终端认证；后端系统的虹膜认证服务器在接收到虹膜二维码后首先确认虹膜二维码是从捆绑设备发出，然后解码虹膜二维码，并完成虹膜二维码解码数据的解密处理，与虹膜数据库中该个人的虹膜特征码信息进行比对，产生认证结果，并将认证结果发往相关的业务系统。

基于虹膜二维码的身份认证系统及方法

技术领域

[0001] 本发明涉及身份认证技术领域，特别是基于虹膜二维码的身份认证系统及方法。

背景技术

[0002] 账号密码＋短信验证码的短信密码认证方式，是时下银行、电子商务等业务中广泛采用的身份认证技术。由于该认证方式依赖网络往返传输密码和信息，存在被网络攻击者监听、拦截、伪造假消息，以仿冒手段达到其商业欺骗的安全漏洞，对银行、电子商务等业务是巨大的安全威胁。类似的案件陆续见诸媒体，造成客户的大量损失即可得以证明。

[0003] 《虹膜二维码》(专利申请号 201510127945.4) 发明专利提供了一种基于虹膜特征码的二维码编码方法，该发明系统地阐述了虹膜二维码的码域结构、生成及使用方法。身份认证技术可划分为三类：“你知道什么”、“你拥有什么”、“你是谁”。目前的身份认证技术大多可归类为“你知道什么”、“你拥有什么”的认证技术，目前流行的短信密码认证方式即是融合了“你知道什么”(短信验证码)和“你拥有什么”(密码＋绑定的手机、电脑等)两种技术。相比之下，“你是谁”认证技术直接根据独一无二的身体特征来证明其身份，显然更具优越性。生物认证技术即属于“你是谁”认证技术，虹膜识别因其远高于其他生物识别技术的高度精确性、防窃取和防伪造能力，成为生物认证技术中公认的佼佼者，受到一致的追捧。《虹膜二维码》发明专利解决了虹膜识别因技术复杂系统昂贵一直难于在远程认证中得到实际应用的难题，但因二维码自身特性，仍然存在保密强度不足够高被常规的扫描软件所识读后造成信息泄密等不足，如何解决，是该发明留待解决的课题之一。

发明内容

[0004] 本发明的目的在于：提供一种基于虹膜二维码的身份认证系统及方法，系统充分发挥虹膜的唯一性和安全性优势，以弥补诸如短信密码认证技术等目前主流认证技术的不足，使银行、电子商务、物流的远程认证、移动支付等认证过程更加便捷，更加安全。

[0005] 本发明基于虹膜二维码的身份认证系统及方法采用的技术方案是：

[0006] 基于虹膜二维码的身份认证系统及方法，其系统由前端系统和后端系统构成；前端系统由虹膜采集单元、终端机构成，后端系统由虹膜认证服务器和虹膜数据库构成；前端系统和后端系统通过网络进行连接。

所述前端系统的虹膜采集单元采集虹膜图像，直接传送到终端机；

所述前端系统的终端机分为个人终端机和专用终端机；个人终端机包括移动终端如智能手机、固定终端如 PC 机，均安装有专用的虹膜二维码客户端软件，个人终端机完成虹膜图像采集控制、虹膜图像预处理及发送、虹膜二维码管理及虹膜二维码认证功能；专用终端机为虹膜注册／认证终端机，是含有虹膜采集单元的终端机，完成虹膜图像采集控制、虹膜图像预处理及发送、虹膜认证功能；

所述后端系统的虹膜认证服务器完成虹膜图像的虹膜特征码提取、虹膜二维码生成、虹膜二维码比对认证及虹膜二维码管理功能；

所述后端系统的虹膜数据库存储虹膜图像、虹膜二维码信息。

[0007] 本发明提供的认证方法如下：

[0008] 系统运行模式：本发明的系统运行模式分为集中模式、分散模式、混合模式三种；

所述集中模式，即集中服务模式，各应用系统的虹膜认证业务由虹膜认证服务器集中处理；此模式下，所有个人的虹膜图像及虹膜二维码信息均存储于统一的虹膜数据库中；

所述分散模式，即分散服务模式，各应用系统的虹膜认证业务由本系统的虹膜认证服务器处理；跨系统的处理需求由各应用系统的虹膜认证服务器之间的协作机构相互协同完成；此模式下，各应用系统的虹膜数据库中只存储有和本系统业务相关的注册个人的虹膜图像及虹膜二维码信息；

所述混合模式，即混合服务模式，各应用系统的虹膜认证业务由本系统的虹膜认证服务器处理；跨系统的处理需求由中心虹膜认证服务器统一协调；此模式下，各应用系统的虹膜数据库只存储有和本系统业务相关的注册个人的虹膜图像及虹膜二维码信息，中心虹膜认证服务器的虹膜数据库则存储有所有应用系统的个人的虹膜图像及虹膜二维码信息的集合。

[0009] 虹膜注册：是首次用虹膜注册身份必须采用的方式。个人选择何应用系统完成虹膜注册根据其需求而定，一旦选定某一应用系统向其注册，该应用系统即成为该个人虹膜二维码的注册系统；首次虹膜注册时可选择移动终端、固定终端、虹膜注册／认证终端机三种方式之一；

选择移动终端进行虹膜注册时，需先填写相关的注册申请信息，然后使用虹膜采集单元采集虹膜图像，该图像直接传输给移动终端，移动终端对虹膜图像进行定位、一体化处理及增强处理后，经网络传输到后端系统；后端系统的虹膜认证服务器对虹膜图像进行虹膜特征码提取处理后，生成虹膜二维码图码文件，一份留存比对使用，一份发送给移动终端认证使用；

选择固定终端进行虹膜注册时，需先填写相关的注册申请信息，然后使用虹膜采集单元采集虹膜图像，该图像直接传输给固定终端，固定终端对虹膜图像进行定位、一体化处理及增强处理后，经网络传输到后端系统；后端系统的虹膜认证服务器对虹膜图像进行虹膜特征码提取处理后，生成虹膜二维码图码文件，一份留存比对使用，一份发送给固定终端认证使用；

选择虹膜注册／认证终端机进行虹膜注册时，需现填写相关的注册申请信息以及虹膜二维码捆绑的移动终端号码，其后，虹膜注册／认证终端机直接采集虹膜图像，并对虹膜图像进行定位、一体化处理及增强处理后，经网络传输到后端系统；后端系统的虹膜认证服务器对虹膜图像进行虹膜特征码提取处理后，生成虹膜二维码图码文件，一份留存比对使用，一份发送给所绑定的个人终端认证使用；

首次虹膜注册完成后，可以将虹膜注册信息复制到移动终端及固定终端上。

[0010] 引用注册：是个人引用已有的虹膜二维码向其他应用系统注册的方式；在完成首次虹膜注册后，个人可以直接使用所拥有的虹膜二维码向其他应用系统进行注册；引用注册时可以选择移动终端或固定终端；其他应用系统用虹膜二维码向其注册系统核实后即可生效。

[0011] 信息加密：虹膜二维码在其生成过程中选取虹膜特征码、个人姓名、公共识别号等

敏感信息实施加密处理，这些敏感信息只在后端系统虹膜二维码比对计算时才予以解密还原。

[0012] 绑定及迁移：根据使用需要个人可以将虹膜二维码和指定设备和指定账户实施绑定，也可以对原绑定的设备进行迁移及绑定账户进行更换；

①绑定设备：经个人申请注册系统可以将其虹膜二维码与移动终端、固定终端等设备实施绑定，经该个人授权的相关应用系统可通过技术手段获取该设备绑定信息；设备绑定信息在引用注册时自动告知相关的应用系统；

②绑定账户：经个人申请注册系统或其他应用系统可以将其虹膜二维码与指定的个人账户实施绑定；

③设备迁移：经个人申请注册系统可以将原有的虹膜二维码与移动终端、固定终端等设备的绑定关系予以迁移，注册系统更新绑定关系；迁移完成后相关应用系统可通过技术手段获取新的设备绑定信息，并据此更新本系统的绑定关系；

④账户更换：经个人申请相关业务系统可以将原有的虹膜二维码与特定的个人账户的绑定关系予以更换。

[0013] 设备挂失：个人终端遗失后启动客户端系统的设备挂失，该设备挂失信息将逐一通报相关的应用系统，相关应用系统对挂失设备的虹膜二维码予以冻结，直至个人解除挂失或完成设备迁移。

[0014] 身份认证：个人可以选择虹膜认证和虹膜二维码认证这两种方式进行身份认证；

所述虹膜认证方式，即现场采集虹膜图像以此为认证凭据向相关应用系统进行身份认证的方式；其过程为：现场采集虹膜图像，该图像直接传输给个人终端或专用终端机，个人终端或专用终端机对虹膜图像进行定位、一体化处理及增强处理后，经网络传输到相应的后端系统；后端系统的虹膜认证服务器对虹膜图像进行虹膜特征码提取处理后，与数据库中该个人的虹膜特征码进行查找比对，产生认证结果，并将认证结果发往相关的业务系统；

所述虹膜二维码认证方式，即个人直接使用存储于个人终端机的虹膜二维码作为认证凭据向相关应用系统进行身份认证的方式；根据应用场景虹膜二维码使用方式有自扫描模式和被扫描模式两种可选；自扫描模式是个人终端机的二维码扫描软件扫描调取的虹膜二维码图片，发往后端系统，自扫描模式既适用于固定终端认证也可适用于移动终端认证；被扫描模式是移动终端调取虹膜二维码图片接受二维码扫描设备或扫描软件的扫描，被扫描模式适用于移动终端认证；后端系统的虹膜认证服务器在接收到虹膜二维码后首先确认虹膜二维码是从捆绑设备发出，然后解码虹膜二维码，并完成虹膜二维码解码数据的解密处理，与虹膜数据库中该个人的虹膜特征码信息进行比对，产生认证结果，并将认证结果发往相关的业务系统。

[0015] 本发明的有益效果是：

1. 本发明利用独一无二的身体特征一虹膜特征码作为身份认证的凭据，认证中不使用传统的密码技术，不存在密码遗忘、密码被窃的问题；

2. 本发明的认证过程仅需一次认证凭据的单向传输，大大降低了被网络攻击者监听、拦截的几率；

3. 本发明的认证过程中传输的关键信息是虹膜二维码，其完善的校验码技术保证任何

改动都将被发现，因而无法伪造，无法仿冒；

4. 本发明对虹膜二维码中的敏感数据在虹膜二维码生成时即被加密处理，普通的二维码扫描软件只可扫描不能解码识读，化解了敏感数据的泄露风险；

5. 本发明采用个人虹膜二维码与个人终端设备绑定技术，实现“你拥有什么”+“你是谁”的双唯一性绑定技术，明显比目前主流的短信密码认证方式的“你知道什么”+“你拥有什么”关联方案的安全强度更高；

6. 本发明实现了用唯一的虹膜二维码在不同应用系统间的畅行通用，最大限度地体现了虹膜的个体特性、资源特性、价值特性和安全特性，为本发明在不同行业的广泛应用奠定了技术基础。

附图说明

[0016] 图 1 为本发明系统按集中模式运行的实例示意图。

[0017] 图 2 为本发明系统按分散模式运行的实例示意图。

[0018] 图 3 为本发明系统按混合模式运行的实例示意图。

[0019] 图 4 为本发明绑定设备迁移处理流程示意图。

[0020] 图 5 为本发明绑定账户迁移处理流程示意图。

[0021] 图 6 为本发明手机虹膜二维码认证处理流程示意图。

具体实施方式

[0022] 下面结合附图对本发明做进一步的描述。各图方案仅仅是本发明基本思想的原理说明，根据本发明的思想所能采用的具体实施方式并不仅限于此。

[0023] 实施例 1：如图 1 所示。图 1 是本发明系统按集中模式运行的实例示意图。在该实施例中，应用系统 11、应用系统 12、应用系统 13 的虹膜认证业务由虹膜认证服务器 10 集中处理。

[0024] 实施例 2：如图 2 所示。图 2 是本发明系统按分散模式运行的实例示意图。在该实施例中，应用系统 11、应用系统 12、应用系统 13 的虹膜认证业务由各系统的虹膜认证服务器系统处理；跨系统的处理需求由各应用系统的前置机 111、前置机 121、前置机 131 相互协同完成。

[0025] 实施例 3：如图 3 所示。图 3 是本发明系统按混合模式运行的实例示意图。在该实施例中，应用系统 11、应用系统 12、应用系统 13 的虹膜认证业务由本系统的虹膜认证服务器处理；跨系统的处理需求由各应用系统的前置机 111、前置机 121、前置机 131 通过虹膜认证服务器 10 统一协调处理。

[0026] 实施例 4：如图 4 所示。图 4 是本发明捆绑设备迁移处理流程示意图。该图给出一个分散模式下个人设备捆绑迁移过程的处理流程实施例。

[0027] 实施例 5：如图 5 所示。图 5 是本发明捆绑账户更换处理流程示意图。该图给出一个分散模式下个人捆绑账户更换过程的处理流程实施例。

[0028] 实施例 6：如图 6 所示。图 6 是本发明手机虹膜二维码认证处理流程示意图。该图给出一个分散模式下使用手机虹膜二维码进行身份认证的处理流程实施例。

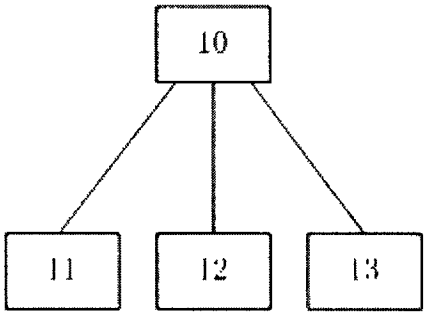


图 1

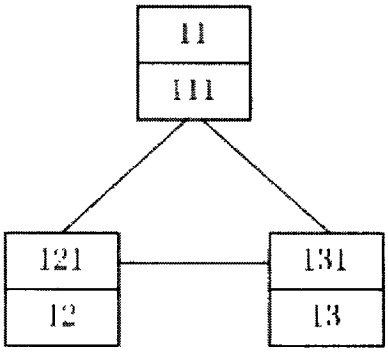


图 2

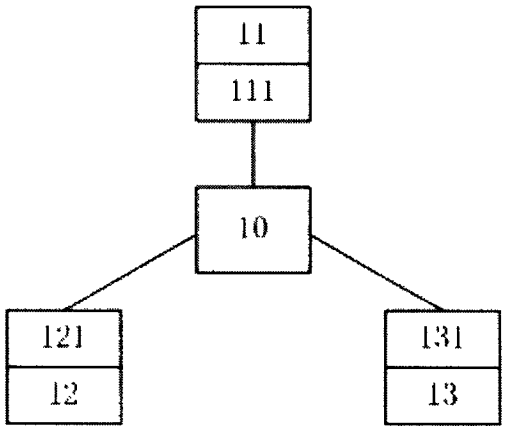


图 3

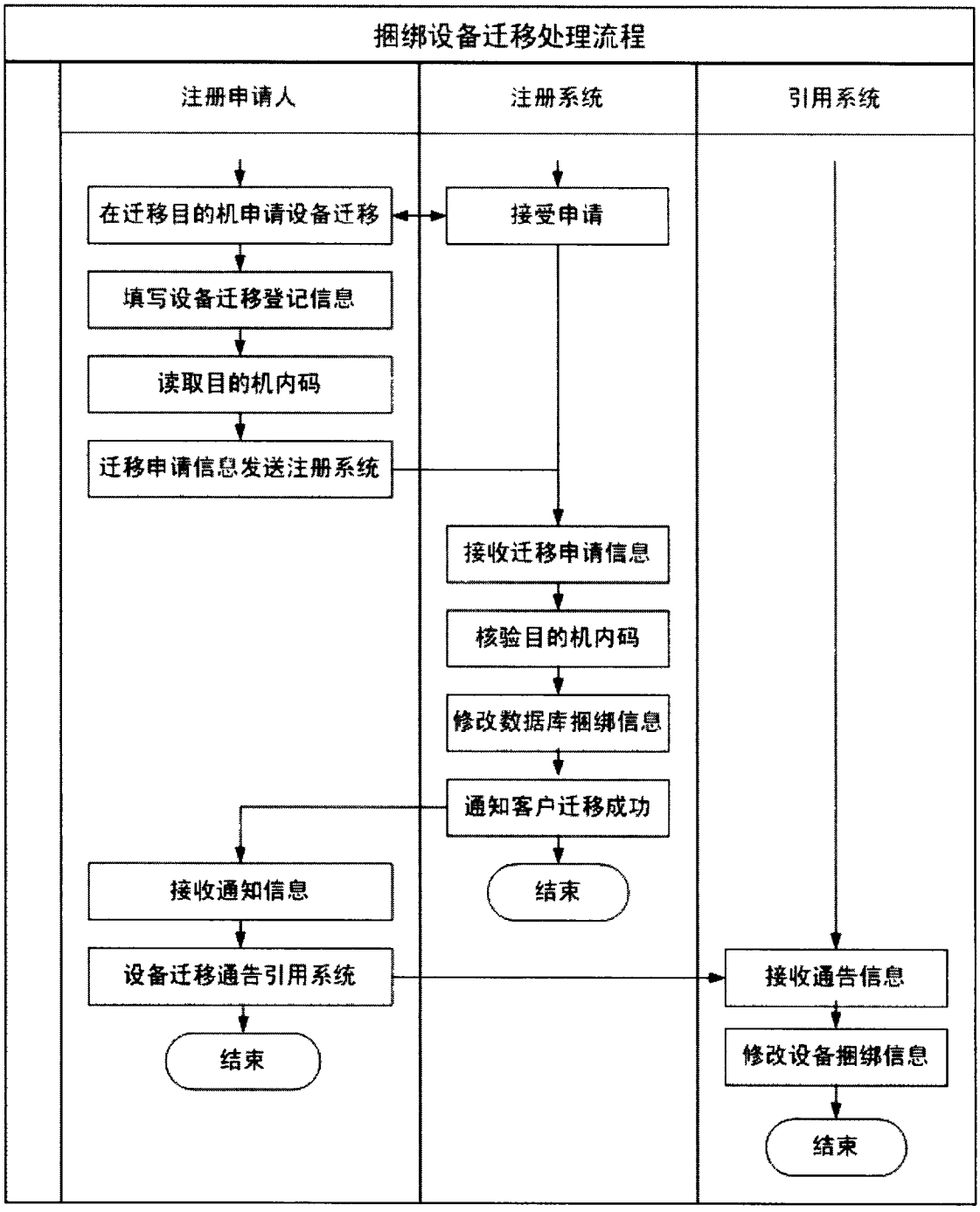

捆绑设备迁移处理流程
注册申请人
注册系统
引用系统
在迁移目的机申请设备迁移
接受申请
填写设备迁移登记信息
读取目的机内码
迁移申请信息发送注册系统
接收迁移申请信息
核验目的机内码
修改数据库捆绑信息
通知客户迁移成功
结束
接收通知信息
设备迁移通告引用系统
结束
接收通告信息
修改设备捆绑信息
结束

图 4

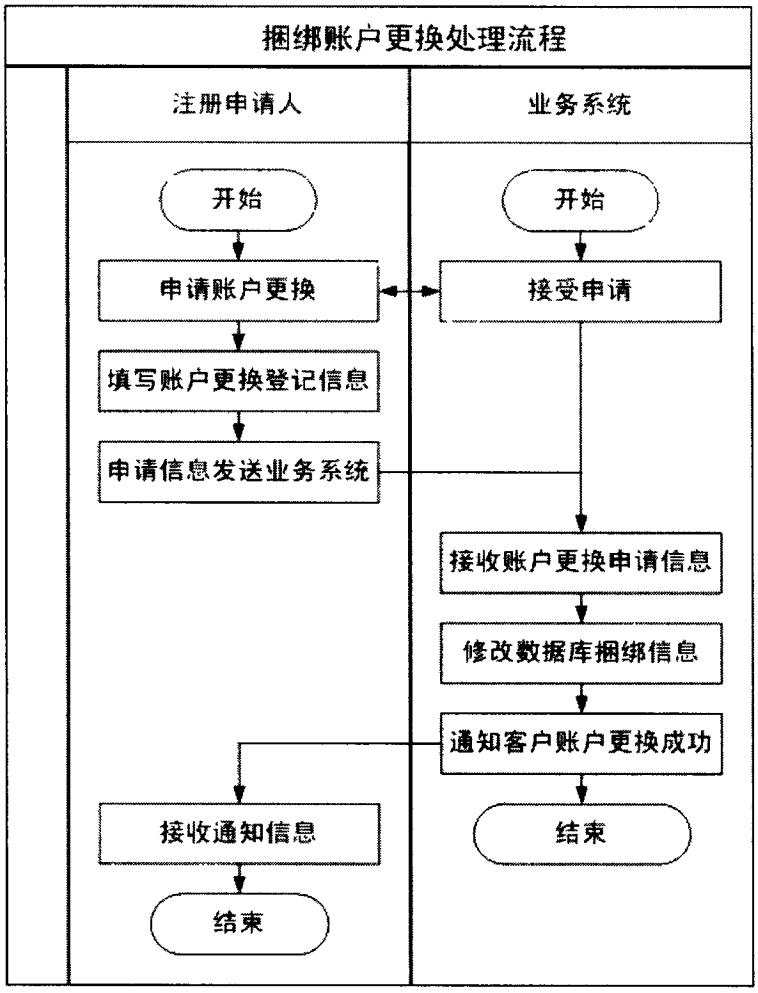

捆绑账户更换处理流程
注册申请人
业务系统
开始
开始
申请账户更换
接受申请
填写账户更换登记信息
申请信息发送业务系统
接收账户更换申请信息
修改数据库捆绑信息
通知客户账户更换成功
接收通知信息
结束
结束

图 5

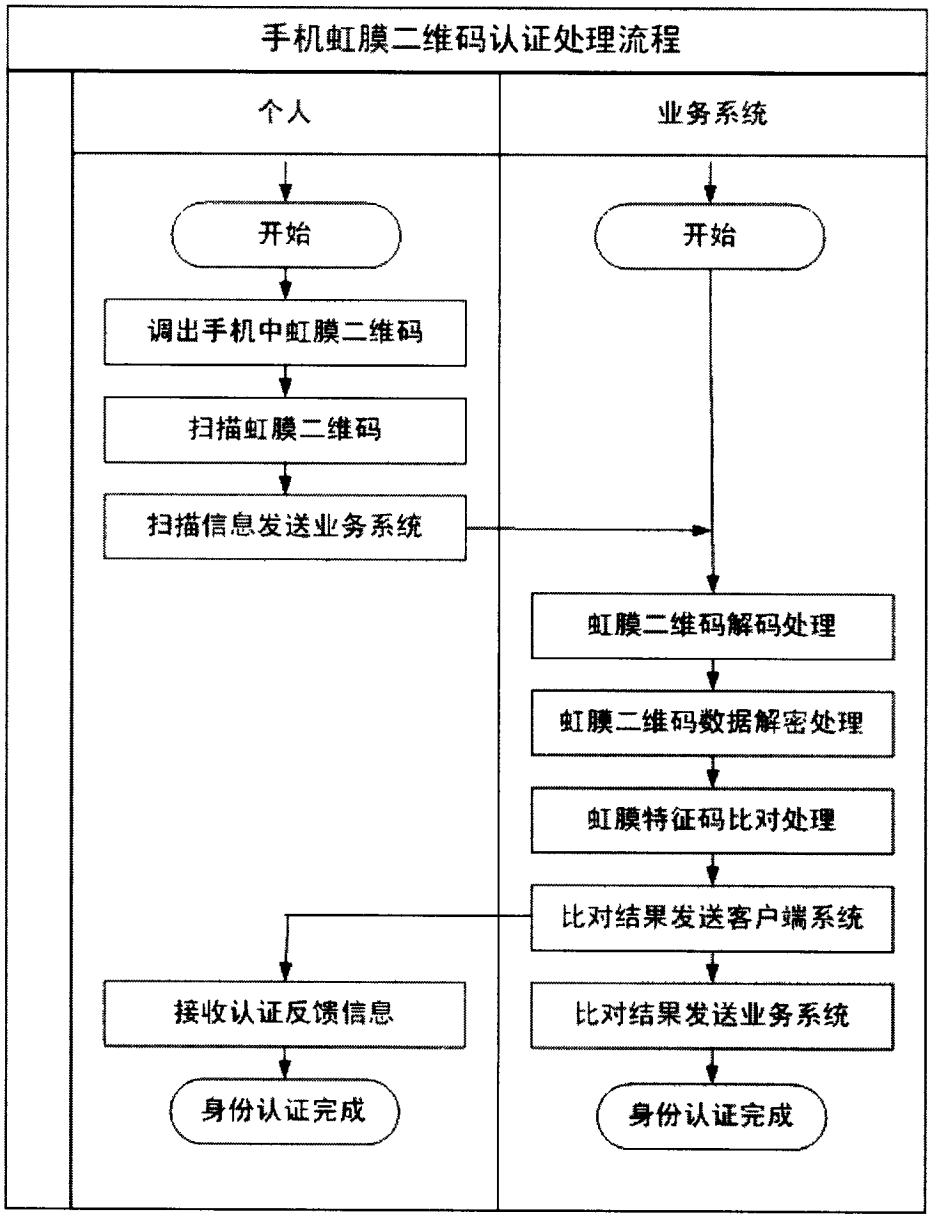

手机虹膜二维码认证处理流程
个人
业务系统
开始
开始
调出手机中虹膜二维码
扫描虹膜二维码
扫描信息发送业务系统
虹膜二维码解码处理
虹膜二维码数据解密处理
虹膜特征码比对处理
比对结果发送客户端系统
接收认证反馈信息
比对结果发送业务系统
身份认证完成
身份认证完成

图 6