(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 107992728 B
(45)授权公告日 2022.05.20

(21)申请号 201610952328.2

(22)申请日 2016.10.27

(65)同一申请的已公布的文献号
申请公布号 CN 107992728 A

(43)申请公布日 2018.05.04

(73)专利权人 腾讯科技(深圳)有限公司
地址 518000 广东省深圳市福田区振兴路赛格科技园2栋东403室

(72)发明人 陈泳君

(74)专利代理机构 广州三环专利商标代理有限公司 44202
专利代理师 郝传鑫 贾允

(51)Int.Cl.
G06F 21/32(2013.01)

(56)对比文件
CN 105790948 A,2016.07.20
CN 103914748 A,2014.07.09
CN 104540032 A,2015.04.22
WO 2014143070 A1,2014.09.18

审查员 张琳

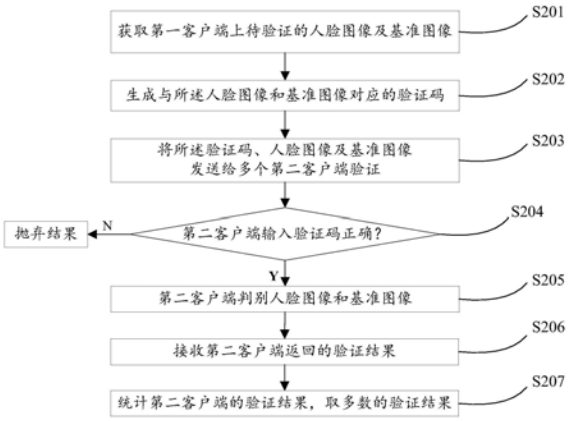
权利要求书2页 说明书13页 附图4页

(54)发明名称

人脸验证方法及装置

(57)摘要

本发明公开了一种人脸验证方法及装置，属于安全验证领域。所述人脸验证方法包括：获取待验证的人脸图像及基准图像；生成与所述人脸图像和基准图像对应的验证码；将所述验证码、人脸图像及基准图像发送给多个第二客户端验证；接收客户端返回的验证结果。本发明通过将数据库内注册的人脸图像和当前验证图像组合，作为图像验证码和普通的字符验证码一同下发给用户进行验证，无需训练样本，适用于各种应用场景，快速提升人脸验证系统的识别准确率。本方案可独立使用，也可作为现有人脸识别验证算法的技术补充。



CN 107992728 B

1.一种人脸验证方法，其特征在于，应用于人脸装置中，所述人脸装置设置于人脸用户终端，且所述人脸装置内设有数据库，所述数据库用于存储所述人脸装置验证过程中所需的数据；所述方法包括：

获取第一客户端上待验证的人脸图像及基准图像；

生成与所述人脸图像和基准图像对应的验证码；

将所述验证码、人脸图像及基准图像发送给第二客户端验证；

若所述第二客户端输入的所述验证码正确，且第二客户端在预设时间阈值内返回验证结果，则接收所述第二客户端返回的验证结果；所述第二客户端为正在进行登录、支付或者验证的客户端；

所述获取待验证的人脸图像及基准图像之前还包括：

获取与待验证的人脸图像相对应的登录账号；

所述获取待验证的人脸图像及基准图像包括：

预先为所述登录账号设置关联的基准图像，通过获取的登录账号获取相关联的基准图像；所述基准图像为注册时采集的人脸图像或者注册时提交的人脸图像；

所述将所述验证码、人脸图像及基准图像发送给第二客户端验证之后，还包括：

若所述第二客户端输入的所述验证码错误，且第二客户端在预设时间阈值内返回验证结果，则删除所述第二客户端返回的验证结果；若删除第二客户端作出的判别结果，则所述第二客户端返回的验证结果为验证失败。

2.根据权利要求1所述的方法，其特征在于，所述第二客户端作出的判别结果包括：

第二客户端判别人脸图像与基准图像是否为同一人，若判别结果为相同，则所述第二客户端返回的验证结果为验证成功；若判别结果为不同，则所述第二客户端返回的验证结果为验证失败。

3.根据权利要求1所述的方法，其特征在于，将所述验证码、人脸图像及基准图像发送给多个第二客户端验证，每个第二客户端返回一个验证结果，所述验证结果分为验证成功和验证失败，对多个第二客户端返回的验证结果进行汇总，取数量较多的验证结果。

4.根据权利要求3所述的方法，其特征在于，还包括：

删除所述第二客户端超出时间阈值范围所返回的验证结果。

5.根据权利要求4所述的方法，其特征在于，若在所述时间阈值内，第二客户端返回的验证结果数量为0，则启用人脸验证算法，包括：

对待验证的人脸图像进行预处理，并进行特征提取，以将所述人脸图像与基准图像进行比对验证。

6.根据权利要求4所述的方法，其特征在于，若在所述时间阈值内，第二客户端返回的验证结果数量为0，则启用密码登录，包括：

预先注册登录账号及对应的登录密码；

接收待验证的输入密码，比较所述输入密码与注册的登录密码是否相同，若相同，则登录成功；否则登录失败。

7.根据权利要求1所述的方法，其特征在于，所述获取待验证的人脸图像包括：

接收由摄像头采集到的待验证的人脸图像。

8.一种人脸验证装置，其特征在于，所述人脸验证装置设置于人脸用户终端，且所述人

脸装置内设有数据库，所述数据库用于存储所述人脸装置验证过程中所需的数据；包括：

存储模块，用于存储第一客户端上注册的登录账号以及与所述登录账号相关联的基准图像；所述基准图像为注册时采集的人脸图像或者注册时提交的人脸图像；

录入模块，用于获取第一客户端上的登录账号及待验证的人脸图像；

验证码模块，用于生成验证码；

发送模块，用于将所述验证码、人脸图像及基准图像发送给第二客户端；

验证模块，用于验证码的验证，及人脸图像与基准图像的判别，产生验证结果；所述第二客户端为正在进行登录、支付或者验证的客户端；

接收模块，用于若所述第二客户端输入的所述验证码正确，且第二客户端在预设时间阈值内返回验证结果，则接收验证模块的验证结果，若所述第二客户端输入的所述验证码错误，且第二客户端在预设时间阈值内返回验证结果，则删除所述第二客户端返回的验证结果，若删除第二客户端作出的判别结果，则所述第二客户端返回的验证结果为验证失败。

9.根据权利要求8所述的装置，其特征在于，还包括：

图像采集模块，用于采集基准图像和待验证的人脸图像。

10.根据权利要求8所述的装置，其特征在于，还包括：

统计模块，用于统计并比较多个第二客户端返回的验证结果，若第二客户端输入的验证码正确，且判别人脸图像与基准图像为同一人，则所述验证结果为验证成功，否则验证结果为验证失败，取数量较多的验证结果。

11.根据权利要求8所述的装置，其特征在于，还包括：

时间阈值模块，用于删除所述第二客户端超出时间阈值范围所返回的验证结果。

12.根据权利要求8所述的装置，其特征在于，还包括：

人脸验证算法模块：用于对待验证的人脸图像进行预处理，并进行特征提取，以将所述人脸图像与基准图像进行比对验证。

13.根据权利要求8所述的装置，其特征在于，还包括：

密码登录模块：用于预先注册登录账号及对应的登录密码；接收待验证的输入密码，比较所述输入密码与注册的登录密码是否相同，若相同，则登录成功；否则登录失败。

人脸验证方法及装置

技术领域

[0001] 本发明涉及安全验证领域，特别涉及一种人脸验证方法及装置。

背景技术

[0002] 生物特征识别技术是目前最为方便、安全的身份识别技术，生物特征识别技术识别的是人本身，不需要人身之外的标识物。生物特征识别技术利用人的生理特征和行为特征进行身份识别，主要有指纹识别、人脸识别、虹膜识别、步态识别等。其中，人脸识别是当前生物特征识别领域的一大热点。它与目前广泛应用的指纹识别技术相比，有着直观性、方便性、非接触性、友好性、用户接受度高等显著优点。

[0003] 人脸作为常用的生物特征已广泛应用于金融支付、安防等领域。二维人脸识别是基于人脸单个平面图像的，一般通过一个摄像头采集人脸平面图像，然后进行人脸检测、人眼定位和特征提取，再与模板库进行比对，最后做出识别判别。但是实际上通过一个摄像头采集的单个人脸平面图像的识别率受到环境光线、采集角度、姿态、表情等因素的影响，因此现有人脸验证算法在开放环境下(光线变化，人脸角度变化等)识别率受到很大局限。在MegaFace数据集上，当前最好的人脸验证算法只有75％的准确率，大大低于实用标准。且当前主流人脸验证算法均采用深度网络，需要大量的人工标注训练样本，对数据收集和人力投入提出了很高要求。

[0004] 现有技术至少存在以下缺点：

[0005] 1、需要大量人工标注的训练样本；

[0006] 2、应用与不同场景下，基本都需要重新调整训练集，重新训练；

[0007] 3、开放环境下识别率低，实用性不高；

[0008] 4、算法复杂度高，验证速度慢。

[0009] 提高现有二维人脸识别技术的识别性能是当前迫切需要解决的问题。

发明内容

[0010] 为了解决现有技术的问题，本发明提供了一种人脸验证方法及装置，将数据库内注册的人脸图像和当前验证图像组合，作为图像验证码和普通的字符验证码一同下发给用户进行验证，无需训练样本，适用于各种应用场景，快速提升人脸验证系统的识别准确率。所述技术方案如下：

[0011] 一方面，本发明提供了一种人脸验证方法，所述方法包括：

[0012] 获取第一客户端上待验证的人脸图像及基准图像；

[0013] 生成与所述人脸图像和基准图像对应的验证码；

[0014] 将所述验证码、人脸图像及基准图像发送给第二客户端验证；

[0015] 接收第二客户端返回的验证结果。

[0016] 进一步地，所述获取待验证的人脸图像及基准图像之前还包括：

[0017] 获取与待验证的人脸图像相对应的登录账号；

[0018] 所述获取待验证的人脸图像及基准图像包括：

[0019] 预先为所述登录账号设置关联的基准图像，通过获取的登录账号获取相关联的基准图像。

[0020] 可选地，所述将所述验证码、人脸图像及基准图像发送给第二客户端验证，包括：

[0021] 验证第二客户端输入的验证码是否正确，若正确，接收第二客户端作出的判别结果；否则删除第二客户端作出的判别结果；

[0022] 若删除第二客户端作出的判别结果，则所述第二客户端返回的验证结果为验证失败。

[0023] 具体地，所述第二客户端作出的判别结果包括：

[0024] 第二客户端判别人脸图像与基准图像是否为同一人，若判别结果为相同，则所述第二客户端返回的验证结果为验证成功；若判别结果为不同，则所述第二客户端返回的验证结果为验证失败。

[0025] 优选地，将所述验证码、人脸图像及基准图像发送给多个第二客户端验证，每个第二客户端返回一个验证结果，所述验证结果分为验证成功和验证失败，对多个第二客户端返回的验证结果进行汇总，取数量较多的验证结果。

[0026] 进一步地，所述方法还包括：

[0027] 设置时间阈值，删除所述第二客户端超出时间阈值范围所返回的验证结果。

[0028] 可选地，若在所述时间阈值内，第二客户端返回的验证结果数量为0，可选择以下两种备用方式进行登录：

[0029] 第一种备用方式为启用人脸验证算法，包括：

[0030] 对待验证的人脸图像进行预处理，并进行特征提取，以将所述人脸图像与基准图像进行比对验证。

[0031] 第二种备用方式为启用密码登录，包括：

[0032] 预先注册登录账号及对应的登录密码；

[0033] 接收待验证的输入密码，比较所述输入密码与注册的登录密码是否相同，若相同，则登录成功；否则登录失败。

[0034] 具体地，所述获取待验证的人脸图像包括：接收由摄像头采集到的待验证的人脸图像。

[0035] 另一方面，本发明提供了一种人脸验证装置，所述装置包括：

[0036] 存储模块，用于存储第一客户端上注册的登录账号以及与所述登录账号相关联的基准图像；

[0037] 录入模块，用于获取第一客户端的登录账号及待验证的人脸图像；

[0038] 验证码模块，用于生成验证码；

[0039] 发送模块，用于将所述验证码、人脸图像及基准图像发送给第二客户端；

[0040] 验证模块，用于验证码的验证，及人脸图像与基准图像的判别，产生验证结果；

[0041] 接收模块，用于接收验证模块的验证结果。

[0042] 进一步地，所述装置还包括：图像采集模块，用于采集基准图像和待验证的人脸图像。

[0043] 进一步地，所述装置还包括：统计模块，用于统计并比较多个第二客户端返回的验

证结果，若第二客户端输入的验证码正确，且判别人脸图像与基准图像为同一人，则所述验证结果为验证成功，否则验证结果为验证失败，取数量较多的验证结果。

[0044] 进一步地，所述装置还包括：时间阈值模块，用于删除所述第二客户端超出时间阈值范围所返回的验证结果。

[0045] 进一步地，所述装置还包括：人脸验证算法模块，用于对待验证的人脸图像进行预处理操作，并进行特征提取，以将所述人脸图像与基准图像进行比对验证。

[0046] 进一步地，所述装置还包括：密码登录模块，用于预先注册登录账号及对应的登录密码；接收待验证的输入密码，比较所述输入密码与注册的登录密码是否相同，若相同，则登录成功；否则登录失败。

[0047] 本发明提供的技术方案带来的有益效果如下：

[0048] 1)只需要人脸采集检测，其他模块无需训练样本；

[0049] 2)适用应用场景广泛，无需投入二次人力训练成本；

[0050] 3)通过验证码系统将验证图片发送给真人用户判断，在任何场景下都可达到人类的识别能力水平；

[0051] 4)验证码系统提供真人识别保障，提高人脸识别的稳定性。

附图说明

[0052] 为了更清楚地说明本发明实施例中的技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0053] 图1是本发明实施例提供的人脸验证方法及装置的实施环境示意图；

[0054] 图2是本发明实施例1提供的人脸验证方法的流程图；

[0055] 图3是本发明实施例2提供的基于多个识别客户端的人脸验证方法的流程图；

[0056] 图4是本发明实施例3提供的设定时间阈值的人脸验证方法的流程图；

[0057] 图5是本发明实施例3提供的人脸验证算法的示意图；

[0058] 图6是本发明实施例4提供的人脸验证方法的流程图；

[0059] 图7是本发明实施例提供的人脸验证装置的模块架构图；

[0060] 图8是本发明实施例提供的人脸验证装置的计算机终端的硬件结构框图。

具体实施方式

[0061] 为了使本技术领域的人员更好地理解本发明方案，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分的实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都应当属于本发明保护的范围。

[0062] 需要说明的是，本发明的说明书和权利要求书及上述附图中的术语“第一”、“第二”等是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换，以便这里描述的本发明的实施例能够以除了在这里图示或

描述的那些以外的顺序实施。此外，术语“包括”和“具有”以及他们的任何变形，意图在于覆盖不排他的包含，例如，包含了一系列步骤或单元的过程、方法、装置、产品或设备不必限于清楚地列出的那些步骤或单元，而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。

[0063] 本发明提供了一种人脸验证方法及装置，参考图1可以看出，其示出了本发明实施例提供的人脸验证方法及装置所涉及的实施环境的结构示意图。该实施环境包括配置有人脸用户终端104、真实用户终端101、人脸验证装置102和数据库103。

[0064] 其中，人脸验证装置102如下面实施例二所述，每个人脸用户终端104通过人脸验证装置102进行人脸识别验证。人脸验证装置102可以配置在人脸用户终端104中，也可以独立于人脸用户终端104而配置。实施环境中可以有一至多个人脸验证装置102，组成一个人脸验证装置的集群，当需要进行人脸验证的人脸用户终端104的个数较多时，多个人脸验证装置102可以并行执行操作，从而提高人脸验证的速度。

[0065] 数据库103中存储有人脸验证装置102在验证过程中所需的数据，如待识别的人脸图像及与之相对应的登录账号信息，以及与所述登录账号一一对应的注册信息，所述注册信息包括基准图像和注册密码信息。

[0066] 人脸用户终端104负责采集人脸图像，并将其与相应的登陆账号信息发送给人脸验证装置102，人脸验证装置102向数据库103查询相关信息，并打包发送给真实用户终端101，真实用户终端101向人脸验证装置102反馈识别结果，并由人脸验证装置102处理得到验证结果。

[0067] 数据库103除了可以独立于人脸验证装置102和人脸用户终端104配置之外，还可以配置在人脸验证装置102中，使得人脸验证装置102可以直接从自身配置的数据库中获取所需的数据，或者数据库103还可以配置在人脸用户终端104中，使得人脸验证装置102从人脸用户终端104配置的数据库中获取所需的数据，本发明实施例在此不对数据库103的配置方式进行具体限定。

[0068] 人脸用户终端104与人脸验证装置102之间通过网络进行通信，真实用户终端101与人脸验证装置102之间通过网络进行通信，人脸验证装置102与数据库103之间也通过网络进行通信，该网络可以为无线网络或有线网络。

[0069] 实施例1：本发明实施例提供了一种人脸验证方法，可应用在安全中心刷脸登录场景，参见图2，方法流程包括：

[0070] 预先注册步骤有：用户输入注册信息，所述注册信息包括登录账号和相应的基准图像，上述基准图像可以为采集注册用户在注册时的人脸图像，也可以为注册用户向注册系统提交的人脸图像，所述基准图像与登录账号一一对应，所述基准图像作为登录账号的图像密码。

[0071] S101、获取第一客户端上待验证的人脸图像及基准图像。

[0072] 用户在第一客户端输入登录账号后，第一客户端的图像采集装置对用户进行人脸图像采集，所述图像采集装置优选为摄像头；同时通过登录账号与基准图像的关联映射，可以获取对应的基准图像。

[0073] S102、生成与所述人脸图像和基准图像对应的验证码。

[0074] 由验证码系统生成传统字符串验证码，将生成的验证码与上述获取的人脸图像、

基准图像进行对应配置。

[0075] S103、将所述验证码、人脸图像及基准图像发送给第二客户端验证。

[0076] 第二客户端所处的场景为接收各种验证码的场景，比如系统登录、密码支付及实名认证等场景，第二客户端为了完成自己的登录、支付或者认证任务，须接收验证码、人脸图像和基准图像。首先，第二客户端的用户需输入传统的字符验证码，在输入验证码正确的前提下，对人脸图像和基准图像进行判别，判别内容为两个图像中的人脸是否为同一人，若是，则验证结果为验证成功，若否，则验证结果为验证失败。如果第二客户端的用户输入的字符验证码错误，则无需进一步对人脸图像和基准图像进行判别，或者抛弃删除其所作出的判别结果。

[0077] S104、接收第二客户端返回的验证结果。

[0078] 接收第二客户端返回的验证结果后，产生后续操作，若验证结果为验证成功，则第一客户端的用户成功登陆安全中心；若验证结果为验证失败，则阻止第一客户端的用户登录安全中心。

[0079] 实施例2：为避免单个用户识别错误造成验证结果的不稳定性，本发明实施例提供了一种基于多个识别客户端的人脸验证方法，可应用在实名认证场景，参见图3，本发明实施例提供的方法流程包括：

[0080] 预先注册步骤有：用户输入注册信息，所述注册信息包括认证账号和相应的基准图像，上述基准图像可以为采集注册用户在注册时的人脸图像，也可以为注册用户向注册系统提交的人脸图像，所述基准图像与认证账号一一对应，所述基准图像作为认证账号的图像认证密码。

[0081] S201、获取第一客户端上待验证的人脸图像及基准图像。

[0082] 用户在第一客户端输入认证账号后，第一客户端的图像采集装置对用户进行人脸图像采集，所述图像采集装置优选为摄像头；同时通过认证账号与基准图像的关联映射，可以获取到对应的基准图像。

[0083] S202、生成与所述人脸图像和基准图像对应的验证码。

[0084] 由验证码系统生成传统字符串验证码，将生成的验证码与上述获取的人脸图像、基准图像进行对应配置。

[0085] S203、将所述验证码、人脸图像及基准图像发送给多个第二客户端验证。

[0086] 多个第二客户端所处的场景为接收各种验证码的场景，比如系统登录、密码支付及实名认证等场景，多个第二客户端可以处于相同的场景，也可以处于不同的场景，第二客户端为了完成自己的登录、支付或者认证任务，须接收验证码、人脸图像和基准图像。

[0087] S204、判断第二客户端输入的验证码是否正确，若正确，执行S205，否则抛弃第二客户端作出的验证结果。

[0088] 验证码系统接收第二客户端输入的验证码，验证码系统将第二客户端输入的验证码与生成的传统字符串验证码进行比较是否相同，若两者相同，则验证码正确，否则验证码错误。若验证码错误，则无需进一步对人脸图像和基准图像进行判别，或者抛弃删除其所作出的判别结果。

[0089] S205、第二客户端判别人脸图像和基准图像。

[0090] 在输入验证码正确的前提下，对人脸图像和基准图像进行判别，判别内容为两个

图像中的人脸是否为同一人，若是，则验证结果为验证成功，若否，则验证结果为验证失败。

[0091] S206、接收第二客户端返回的验证结果。

[0092] 每个第二客户端返回一个验证结果，多个第二客户端返回多个验证结果，所述验证结果分为验证成功和验证失败。

[0093] S207、统计第二客户端的验证结果，取多数的验证结果。

[0094] 统计验证成功的结果数量和验证失败的结果数量，可以以取多数的规则进行选取，或者设定数量比例进行选取，本发明实施例对此不作具体限定。

[0095] 选取得到最终验证结果后，产生后续操作，若验证结果为验证成功，则第一客户端的用户认证成功；若验证结果为验证失败，则第一客户端的用户认证失败。

[0096] 实施例3：本发明的人脸验证的技术方案可以独立使用，也可作为现有验证算法(如深度学习)的技术补充。为提高识别验证过程的及时性，本发明实施例提供了一种设定时间阈值的人脸验证方法，可应用在刷脸支付场景，参见图4，本发明实施例提供的方法流程包括：

[0097] 预先注册步骤有：用户输入注册信息，所述注册信息包括支付账号和相应的基准图像，上述基准图像可以为采集注册用户在注册时的人脸图像，也可以为注册用户向注册系统提交的人脸图像，所述基准图像与支付账号一一对应，所述基准图像作为支付账号的图像认证密码。

[0098] S301、获取第一客户端上待验证的人脸图像及基准图像。

[0099] 用户在第一客户端输入支付账号后，第一客户端的图像采集装置对用户进行人脸图像采集，所述图像采集装置优选为摄像头；同时通过支付账号与基准图像的关联映射，可以获取到对应的基准图像。

[0100] S302、生成与所述人脸图像和基准图像对应的验证码。

[0101] 由验证码系统生成传统字符串验证码，将生成的验证码与上述获取的人脸图像、基准图像进行对应配置。

[0102] S303、将所述验证码、人脸图像及基准图像发送给第二客户端验证。

[0103] 多个第二客户端所处的场景为接收各种验证码的场景，比如系统登录、密码支付及实名认证等场景，第二客户端为了完成自己的登录、支付或者认证任务，须接收传统字符串验证码、人脸图像和基准图像。验证码系统接收第二客户端输入的验证码，验证码系统将第二客户端输入的验证码与生成的传统字符串验证码进行比较是否相同，若两者相同，则验证码正确，否则验证码错误。若验证码错误，则无需进一步对人脸图像和基准图像进行判别，或者抛弃删除其所作出的判别结果。第二客户端进行验证的过程如下：在输入验证码正确的前提下，对人脸图像和基准图像进行判别，判别内容为两个图像中的人脸是否为同一人，若是，则验证结果为验证成功，若否，则验证结果为验证失败。

[0104] S304、预设时间阈值，判断在所述时间阈值内，第二客户端是否返回验证结果。若是，则执行S305，否则启用人脸验证算法。

[0105] 第一客户端的刷脸支付速度取决于第二客户端的验证速度，然而第二客户端的验证速度受到环境或者应用场景等客观因素的局限，比如线上第二客户端的用户不处于接收验证码的场景，或者互联网网络不通畅的情况，也受到第二客户端上的用户主观因素的影响，比如，第二客户端的用户迟迟不递交验证结果，综上，需要设置时间阈值，保证第一客户

端刷脸支付的及时性。假如设定时间阈值为30秒，在30秒内第二客户端返回的验证结果为有效结果，超出30 秒则为无效结果，取用有效结果，抛弃无效结果。

[0106] 若在时间阈值内返回的有效验证结果数量为0，则启用人脸验证算法对第一客户端的用户进行人脸支付验证。所述人脸验证算法的流程如图5所示，主要包括预处理和特征提取两大部分，所述预处理部分包括人脸图像检测、五官定位、人脸切片和光照归一化，所述特征提取部分采用深度卷积网络实现。

[0107] S305、接收第二客户端返回的验证结果。

[0108] 无论在时间阈值内，第二客户端是否返回有效的验证结果，第一客户端上的用户终将得到验证结果，并产生后续操作，若验证结果为验证成功，则第一客户端的用户刷脸支付成功；若验证结果为验证失败，则第一客户端的用户刷脸支付失败。

[0109] 实施例4：为提高识别验证过程的及时性，本发明实施例提供了第二种基于时间阈值的人脸验证方法，可应用在网页或者App登录场景，参见图6，本发明实施例提供的方法流程包括：

[0110] 预先注册步骤有：用户输入注册信息，所述注册信息包括登录账号和相应的注册人脸图像，并注册有登录密码，以下注册人脸图像简称基准图像，所述基准图像与登录账号一一对应，所述基准图像作为登录账号的图像认证密码，所述登录密码作为登录账号的字符认证密码。

[0111] S401、获取第一客户端上待验证的人脸图像及基准图像。

[0112] 用户在第一客户端输入登录账号后，第一客户端的图像采集装置对用户进行人脸图像采集，所述图像采集装置优选为摄像头；同时通过登录账号与基准图像的关联映射，可以获取到对应的基准图像。

[0113] S402、生成与所述人脸图像和基准图像对应的验证码。

[0114] 由验证码系统生成传统字符串验证码，将生成的验证码与上述获取的人脸图像、基准图像进行对应配置。

[0115] S403、将所述验证码、人脸图像及基准图像发送给第二客户端验证。

[0116] 多个第二客户端所处的场景为接收各种验证码的场景，比如系统登录、密码支付及实名认证等场景，第二客户端为了完成自己的登录、支付或者认证任务，须接收传统字符串验证码、人脸图像和基准图像。验证码系统接收第二客户端输入的验证码，验证码系统将第二客户端输入的验证码与生成的传统字符串验证码进行比较是否相同，若两者相同，则验证码正确，否则验证码错误。若验证码错误，则无需进一步对人脸图像和基准图像进行判别，或者抛弃删除其所作出的判别结果。第二客户端进行验证的过程如下：在输入验证码正确的前提下，对人脸图像和基准图像进行判别，判别内容为两个图像中的人脸是否为同一人，若是，则验证结果为验证成功，若否，则验证结果为验证失败。

[0117] S404、预设时间阈值，判断在所述时间阈值内，第二客户端是否返回验证结果。若是，则执行S305，否则启用人脸验证算法。

[0118] 第一客户端的刷脸支付速度取决于第二客户端的验证速度，然而第二客户端的验证速度受到环境或者应用场景等客观因素的局限，比如线上第二客户端的用户不处于接收验证码的场景，或者互联网网络不通畅的情况，也受到第二客户端上的用户主观因素的影响，比如，第二客户端的用户迟迟不递交验证结果，综上，需要设置时间阈值，保证第一客户

端刷脸支付的及时性。假如设定时间阈值为60秒，在60秒内第二客户端返回的验证结果为有效结果，超出60 秒则为无效结果，取用有效结果，抛弃无效结果。

[0119] 若在所述时间阈值内返回的有效验证结果数量为0，则启用密码验证登录。第一客户端所在系统提示待登录的用户输入登录密码，系统接收待验证的输入密码，比较所述输入密码与注册的登录密码是否相同，若相同，则登录成功；否则登录失败。

[0120] S405、接收第二客户端返回的验证结果。

[0121] 在时间阈值内，第二客户端返回了有效的验证结果，第一客户端上的用户根据接收到的验证结果，并产生后续操作，若验证结果为验证成功，则第一客户端的用户刷脸登录成功；若验证结果为验证失败，则第一客户端的用户刷脸登录失败。

[0122] 需要说明的是，对于前述的各方法实施例，为了简单描述，故将其都表述为一系列的动作组合，但是本领域技术人员应该知悉，本发明并不受所描述的动作顺序的限制，因为依据本发明，某些步骤可以采用其他顺序或者同时进行。其次，本领域技术人员也应该知悉，说明书中所描述的实施例均属于优选实施例，所涉及的动作和模块并不一定是本发明所必须的。

[0123] 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到根据上述实施例的方法可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质(如ROM/RAM、磁碟、光盘)中，包括若干指令用以使得一台终端设备(可以是手机，计算机，服务器，或者网络设备等)执行本发明各个实施例所述的方法。

[0124] 实施例5：本发明实施例还提供了一种人脸验证装置，所述装置的模块架构参见图7，所述装置包括以下模块：

[0125] 存储模块711，用于存储第一客户端上注册的登录账号以及与所述登录账号相关联的基准图像；

[0126] 录入模块712，用于获取第一客户端上的登录账号及待验证的人脸图像；

[0127] 验证码模块713，用于生成验证码；

[0128] 发送模块720，用于将所述验证码、人脸图像及基准图像发送给第二客户端；

[0129] 验证模块730，用于验证码的验证，及人脸图像与基准图像的判别，产生验证结果；

[0130] 接收模块740，用于接收验证模块的验证结果。

[0131] 所述装置还包括图像采集模块714，用于采集基准图像和待验证的人脸图像。

[0132] 作为一种可选的实施例，所述人脸验证装置发送给多个第二客户端，相应地，所述装置还包括：统计模块760，用于统计并比较多个第二客户端返回的验证结果，若第二客户端输入的验证码正确，且判别人脸图像与基准图像为同一人，则所述验证结果为验证成功，否则验证结果为验证失败，取数量较多的验证结果。

[0133] 作为另一种可选的实施例，所述人脸验证装置预设时间阈值，以限定人脸验证的速度，相应地，所述装置还包括：时间阈值模块750，用于删除所述第二客户端超出时间阈值范围所返回的验证结果。

[0134] 根据时间阈值模块750的信息反馈，若反馈结果为在所述时间阈值内，返回的验证结果数量为0，则需要通过另外的方式进行验证登录。

[0135] 第一种方式是启用人脸验证算法，及所述装置可结合现有验证算法(如深度学习)使用，即所述装置还包括人脸验证算法模块770：用于对待验证的人脸图像进行预处理，并进行特征提取，以将所述人脸图像与基准图像进行比对验证；

[0136] 第二种方式是启用密码登录，相应地，所述装置还包括密码登录模块780：用于预先注册登录账号及对应的登录密码；接收待验证的输入密码，比较所述输入密码与注册的登录密码是否相同，若相同，则登录成功；若不相同，则登录失败。

[0137] 综上所述，本发明实施例提供的人脸验证装置，通过将数据库内的注册人脸图像和当前验证图像合成图像验证码，将图像验证码结合普通字符验证码一同下发给真实用户，如果真实用户提交的字符验证码正确，则信任该真实用户对图像验证码的判别，即信任真实用户判定基准图像和当前人脸图像是否是同一个人的判别结果。为避免单个用户识别错误造成的不确定性，可通过将图像验证码和字符验证码下发给多个真实用户进行判别，最终结果由所有真实用户的验证结果取多数解。通过本发明实施例提供的装置，人脸验证结果的准确性达到了人类的识别精度，同时，可提供给传统人脸验证算法进行训练。

[0138] 需要说明的是：上述实施例提供的人脸验证装置在进行人脸验证时，仅以上述各功能模块的划分进行举例说明，实际应用中，可以根据需要而将上述功能分配由不同的功能模块完成，即将人脸验证装置的内部结构划分成不同的功能模块，以完成以上描述的全部或者部分功能。另外，本实施例提供的人脸验证装置实施例与上述实施例提供人脸验证方法属于同一构思，其具体实现过程详见方法实施例，这里不再赘述。

[0139] 实施例6：本发明实施例提供的方法实施例可以在移动终端、计算机终端或者类似的运算装置中执行。以运行在计算机终端上为例，图8是本发明实施例的人脸验证装置的计算机终端的硬件结构框图。如图8所示，终端800可以包括RF(Radio Frequency，射频)电路110、包括有一个或一个以上计算机可读存储介质的存储器120、输入单元130、显示单元140、传感器150、音频电路 160、WiFi(wireless fidelity，无线保真)模块170、包括有一个或者一个以上处理核心的处理器180、以及电源190等部件。本领域技术人员可以理解，图1中示出的终端结构并不构成对终端的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件布置。其中：

[0140] RF电路110可用于收发信息或通话过程中，信号的接收和发送，特别地，将基站的下行信息接收后，交由一个或者一个以上处理器180处理；另外，将涉及上行的数据发送给基站。通常，RF电路110包括但不限于天线、至少一个放大器、调谐器、一个或多个振荡器、用户身份模块(SIM)卡、收发信机、耦合器、LNA(Low Noise Amplifier，低噪声放大器)、双工器等。此外，RF电路 110还可以通过无线通信与网络和其他设备通信。所述无线通信可以使用任一通信标准或协议，包括但不限于GSM(Global System of Mobile communication，全球移动通讯系统)、GPRS(General Packet Radio Service，通用分组无线服务)、CDMA(Code Division Multiple Access，码分多址)、WCDMA(Wideband Code Division Multiple Access，宽带码分多址)、LTE(Long Term Evolution，长期演进)、电子邮件、SMS(Short Messaging Service，短消息服务)等。

[0141] 存储器120可用于存储软件程序以及模块，处理器180通过运行存储在存储器120的软件程序以及模块，从而执行各种功能应用以及数据处理。存储器120可主要包括存储程序区和存储数据区，其中，存储程序区可存储操作系统、功能所需的应用程序(比如声音播

放功能、图像播放功能等)等;存储数据区可存储根据终端800的使用所创建的数据(比如音频数据、电话本等)等。此外,存储器120可以包括高速随机存取存储器,还可以包括非易失性存储器,例如至少一个磁盘存储器件、闪存器件、或其他易失性固态存储器件。相应地,存储器120还可以包括存储器控制器,以提供处理器180和输入单元130对存储器120的访问。

[0142] 输入单元130可用于接收输入的数字或字符信息,以及产生与用户设置以及功能控制有关的键盘、鼠标、操作杆、光学或者轨迹球信号输入。具体地,输入单元130可包括触敏表面131以及其他输入设备132。触敏表面131,也称为触摸显示屏或者触控板,可收集用户在其上或附近的触摸操作(比如用户使用手指、触笔等任何适合的物体或附件在触敏表面131上或在触敏表面131附近的操作),并根据预先设定的程式驱动相应的连接装置。可选的,触敏表面131 可包括触摸检测装置和触摸控制器两个部分。其中,触摸检测装置检测用户的触摸方位,并检测触摸操作带来的信号,将信号传送给触摸控制器;触摸控制器从触摸检测装置上接收触摸信息,并将它转换成触点坐标,再送给处理器180,并能接收处理器180发来的命令并加以执行。此外,可以采用电阻式、电容式、红外线以及表面声波等多种类型实现触敏表面131。除了触敏表面131,输入单元130还可以包括其他输入设备132。具体地,其他输入设备132可以包括但不限于物理键盘、功能键(比如音量控制按键、开关按键等)、轨迹球、鼠标、操作杆等中的一种或多种。

[0143] 显示单元140可用于显示由用户输入的信息或提供给用户的信息以及终端 800的各种图形用户接口,这些图形用户接口可以由图形、文本、图标、视频和其任意组合来构成。显示单元140可包括显示面板141,可选的,可以采用 LCD(Liquid Crystal Display,液晶显示器)、OLED(Organic Light-Emitting Diode, 有机发光二极管)等形式来配置显示面板141。进一步的,触敏表面131可覆盖显示面板141,当触敏表面131检测到在其上或附近的触摸操作后,传送给处理器180以确定触摸事件的类型,随后处理器180根据触摸事件的类型在显示面板141上提供相应的视觉输出。虽然在图1中,触敏表面131与显示面板141 是作为两个独立的部件来实现输入和输入功能,但是在某些实施例中,可以将触敏表面131与显示面板141集成而实现输入和输出功能。

[0144] 终端800还可包括至少一种传感器150,比如光传感器、运动传感器以及其他传感器。具体地,光传感器可包括环境光传感器及接近传感器,其中,环境光传感器可根据环境光线的明暗来调节显示面板141的亮度,接近传感器可在终端800移动到耳边时,关闭显示面板141和/或背光。作为运动传感器的一种,重力加速度传感器可检测各个方向上(一般为三轴)加速度的大小,静止时可检测出重力的大小及方向,可用于识别终端姿态的应用(比如横竖屏切换、相关游戏、磁力计姿态校准)、振动识别相关功能(比如计步器、敲击)等;至于终端800还可配置的陀螺仪、气压计、湿度计、温度计、红外线传感器等其他传感器,在此不再赘述。

[0145] 音频电路160、扬声器161,传声器162可提供用户与终端800之间的音频接口。音频电路160可将接收到的音频数据转换后的电信号,传输到扬声器161,由扬声器161转换为声音信号输出;另一方面,传声器162将收集的声音信号转换为电信号,由音频电路160接收后转换为音频数据,再将音频数据输出处理器180处理后,经RF电路110以发送给比如另一终端,或者将音频数据输出至存储器120以便进一步处理。音频电路160还可能包括耳塞插孔,以提供外设耳机与终端800的通信。

[0146] WiFi属于短距离无线传输技术，终端800通过WiFi模块170可以帮助用户收发电子邮件、浏览网页和访问流式媒体等，它为用户提供了无线的宽带互联网访问。虽然图1示出了WiFi模块170，但是可以理解的是，其并不属于终端 800的必须构成，完全可以根据需要在不改变发明的本质的范围内而省略。

[0147] 处理器180是终端800的控制中心，利用各种接口和线路连接整个终端的各个部分，通过运行或执行存储在存储器120内的软件程序和/或模块，以及调用存储在存储器120内的数据，执行终端800的各种功能和处理数据，从而对终端进行整体监控。可选的，处理器180可包括一个或多个处理核心；优选的，处理器180可集成应用处理器和调制解调处理器，其中，应用处理器主要处理操作系统、用户界面和应用程序等，调制解调处理器主要处理无线通信。可以理解的是，上述调制解调处理器也可以不集成到处理器180中。

[0148] 终端800还包括给各个部件供电的电源190(比如电池)，优选的，电源可以通过电源管理系统与处理器180逻辑相连，从而通过电源管理系统实现管理充电、放电、以及功耗管理等功能。电源190还可以包括一个或一个以上的直流或交流电源、再充电系统、电源故障检测电路、电源转换器或者逆变器、电源状态指示器等任意组件。

[0149] 尽管未示出，终端800还可以包括摄像头、蓝牙模块等，在此不再赘述。具体在本实施例中，终端的显示单元是触摸屏显示器，终端还包括有存储器，以及一个或者一个以上的程序，其中一个或者一个以上程序存储于存储器中，且经配置以由一个或者一个以上处理器执行述一个或者一个以上程序包含用于进行以下操作的指令：

[0150] 获取待验证的人脸图像及基准图像；

[0151] 生成与所述人脸图像和基准图像对应的验证码；

[0152] 将所述验证码、人脸图像及基准图像发送给客户端验证；

[0153] 接收客户端返回的验证结果。

[0154] 具体地，终端的处理器还用于执行以下操作的指令：

[0155] 获取与待验证的人脸图像相对应的登录账号；

[0156] 所述获取待验证的人脸图像及基准图像包括：

[0157] 预先为所述登录账号设置关联的基准图像，通过获取的登录账号获取相关联的基准图像。

[0158] 可选地，所述将所述验证码、人脸图像及基准图像发送给客户端验证，包括：

[0159] 验证客户端输入的验证码是否正确，若正确，接收客户端作出的判别结果；否则删除客户端作出的判别结果；

[0160] 若删除客户端作出的判别结果，则所述客户端返回的验证结果为验证失败。

[0161] 具体地，所述客户端作出的判别结果包括：

[0162] 客户端判别人脸图像与基准图像是否为同一人，若判别结果为相同，则所述客户端返回的验证结果为验证成功；若判别结果为不同，则所述客户端返回的验证结果为验证失败。

[0163] 具体地，终端的处理器还用于执行以下操作的指令：

[0164] 将所述验证码、人脸图像及基准图像发送给多个客户端验证，每个客户端返回一个验证结果，所述验证结果分为验证成功和验证失败，对多个客户端返回的验证结果进行汇总，取数量较多的验证结果。

[0165] 具体地，终端的处理器还用于执行以下操作的指令：设置时间阈值，删除所述客户端超出时间阈值范围所返回的验证结果。

[0166] 可选地，若在所述时间阈值内，客户端返回的验证结果数量为0，终端的存储器中，还包含用于执行以下操作的指令：

[0167] 第一种为启用人脸验证算法，包括：

[0168] 对待验证的人脸图像进行预处理，并进行特征提取，以将所述人脸图像与基准图像进行比对验证。

[0169] 第二种为启用密码登录，包括：

[0170] 预先注册登录账号及对应的登录密码；

[0171] 接收待验证的输入密码，比较所述输入密码与注册的登录密码是否相同，若相同，则登录成功；否则登录失败。

[0172] 具体地，所述获取待验证的人脸图像包括：接收由摄像头采集到的待验证的人脸图像。

[0173] 通过以上实施方式的描述，本领域的技术人员可以清楚地了解到本发明提供的人脸验证技术方案可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质(如ROM/RAM、磁碟、光盘)中，包括若干指令用以使得一台终端设备(可以是手机，计算机，服务器，或者网络设备等)执行本发明各个实施例所述的方法。

[0174] 实施例7：本发明实施例提供了一种计算机可读存储介质，该计算机可读存储介质可以是上述实施例中的存储器中所包含的计算机可读存储介质；也可以是单独存在，未装配入终端中的计算机可读存储介质。计算机可读存储介质存储有一个或者一个以上程序，一个或者一个以上程序被一个或者一个以上的处理器用来执行一个人脸验证的方法，所述方法包括：

[0175] 获取第一客户端上待验证的人脸图像及基准图像；

[0176] 生成与所述人脸图像和基准图像对应的验证码；

[0177] 将所述验证码、人脸图像及基准图像发送给第二客户端验证；

[0178] 接收第二客户端返回的验证结果。

[0179] 进一步地，所述获取待验证的人脸图像及基准图像之前还包括：

[0180] 获取与待验证的人脸图像相对应的登录账号；

[0181] 所述获取待验证的人脸图像及基准图像包括：

[0182] 预先为所述登录账号设置关联的基准图像，通过获取的登录账号获取相关联的基准图像。

[0183] 可选地，所述将所述验证码、人脸图像及基准图像发送给第二客户端验证，包括：

[0184] 验证第二客户端输入的验证码是否正确，若正确，接收第二客户端作出的判别结果；否则删除第二客户端作出的判别结果；

[0185] 若删除第二客户端作出的判别结果，则所述第二客户端返回的验证结果为验证失败。

[0186] 具体地，所述第二客户端作出的判别结果包括：

[0187] 第二客户端判别人脸图像与基准图像是否为同一人，若判别结果为相同，则所述第二客户端返回的验证结果为验证成功；若判别结果为不同，则所述第二客户端返回的验证结果为验证失败。

[0188] 优选地，将所述验证码、人脸图像及基准图像发送给多个第二客户端验证，每个第二客户端返回一个验证结果，所述验证结果分为验证成功和验证失败，对多个第二客户端返回的验证结果进行汇总，取数量较多的验证结果。

[0189] 进一步地，所述方法还包括：

[0190] 设置时间阈值，删除所述第二客户端超出时间阈值范围所返回的验证结果。

[0191] 可选地，若在所述时间阈值内，第二客户端返回的验证结果数量为0，可选择以下两种备用方式进行登录：

[0192] 第一种备用方式为启用人脸验证算法，包括：

[0193] 对待验证的人脸图像进行预处理，并进行特征提取，以将所述人脸图像与基准图像进行比对验证。

[0194] 第二种备用方式为启用密码登录，包括：

[0195] 预先注册登录账号及对应的登录密码；

[0196] 接收待验证的输入密码，比较所述输入密码与注册的登录密码是否相同，若相同，则登录成功；否则登录失败。

[0197] 具体地，所述获取待验证的人脸图像包括：接收由摄像头采集到的待验证的人脸图像。

[0198] 上述本发明实施例序号仅仅为了描述，不代表实施例的优劣。

[0199] 本领域普通技术人员可以理解实现上述实施例的全部或部分步骤可以通过硬件来完成，也可以通过程序来指令相关的硬件完成，所述的程序可以存储于一种计算机可读存储介质中，上述提到的存储介质可以是只读存储器，磁盘或光盘等。

[0200] 以上所述仅为本发明的较佳实施例，并不用以限制本发明，凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

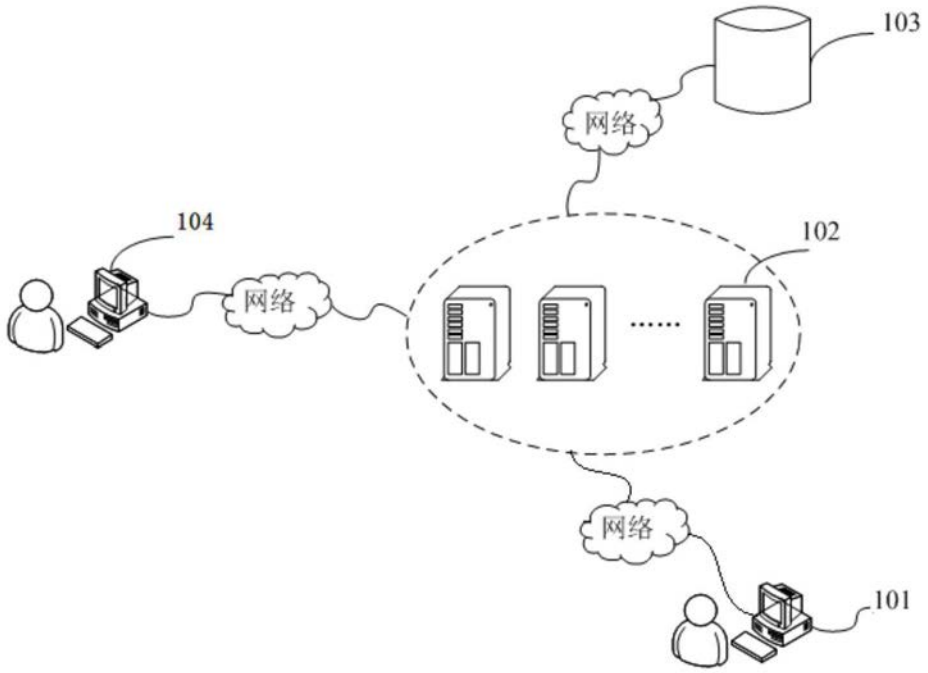

103
网络
104
网络
102
网络
101

图1

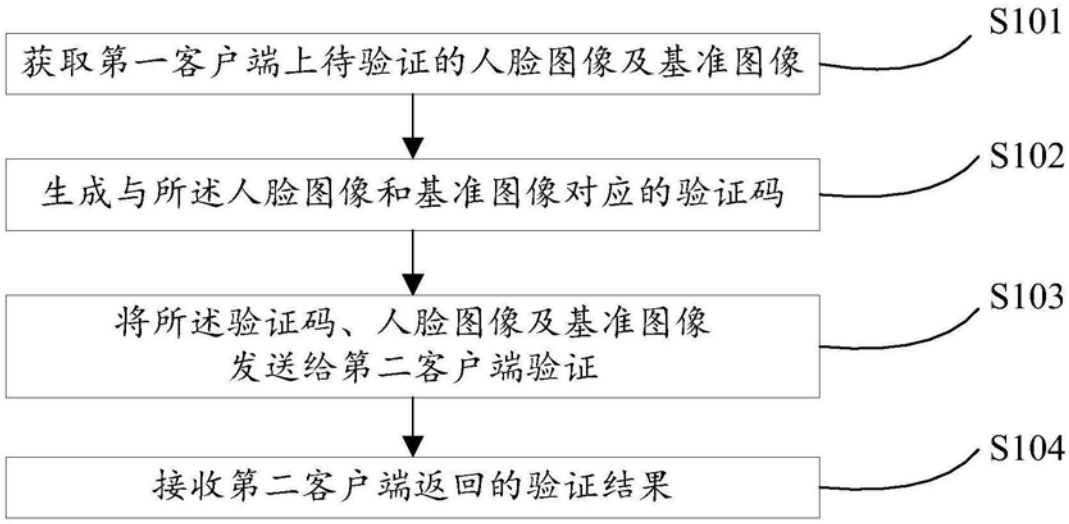

获取第一客户端上待验证的人脸图像及基准图像
S101
生成与所述人脸图像和基准图像对应的验证码
S102
将所述验证码、人脸图像及基准图像
发送给第二客户端验证
S103
接收第二客户端返回的验证结果
S104

图2

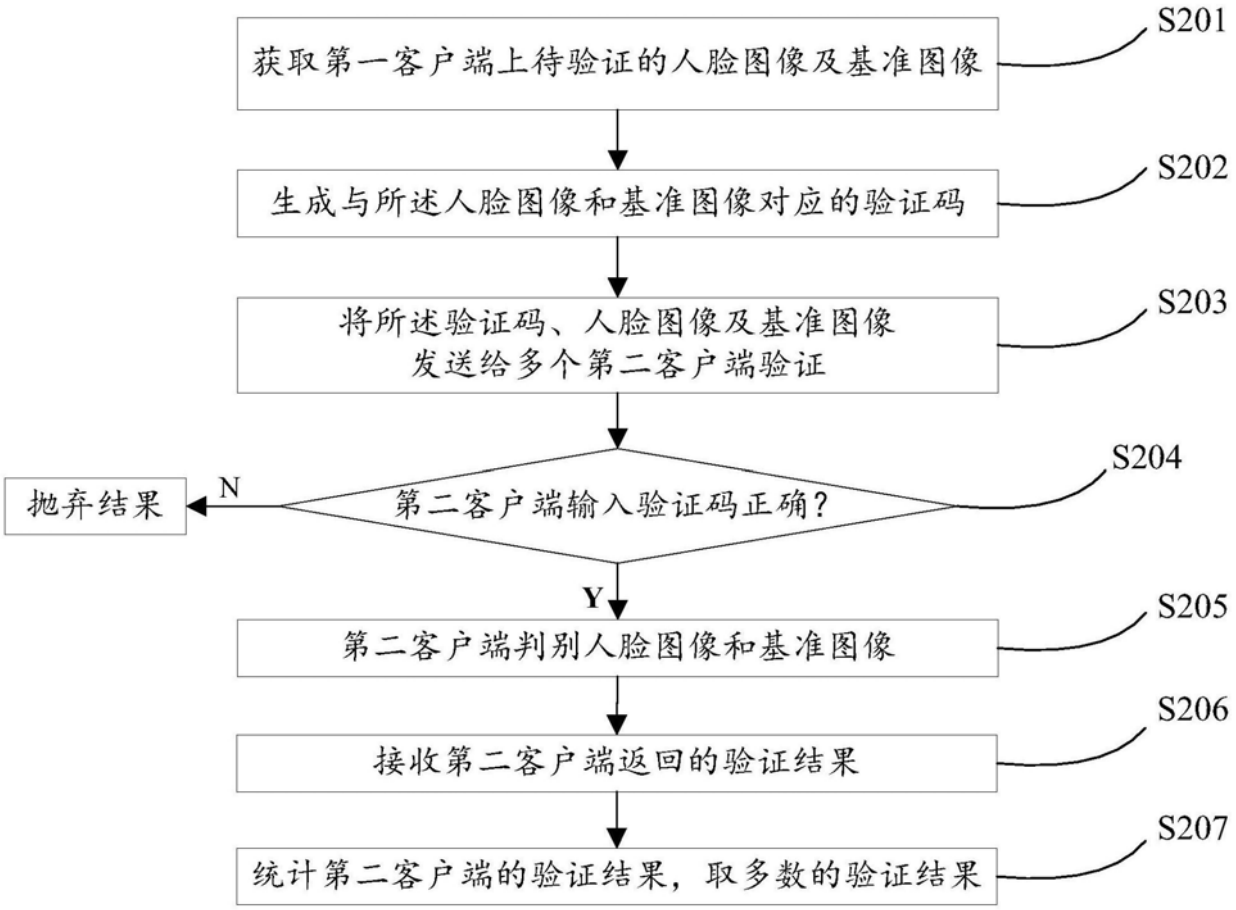

获取第一客户端上待验证的人脸图像及基准图像
S201
生成与所述人脸图像和基准图像对应的验证码
S202
将所述验证码、人脸图像及基准图像
发送给多个第二客户端验证
S203
第二客户端输入验证码正确?
S204
N
抛弃结果
Y
第二客户端判别人脸图像和基准图像
S205
接收第二客户端返回的验证结果
S206
统计第二客户端的验证结果，取多数的验证结果
S207

图3

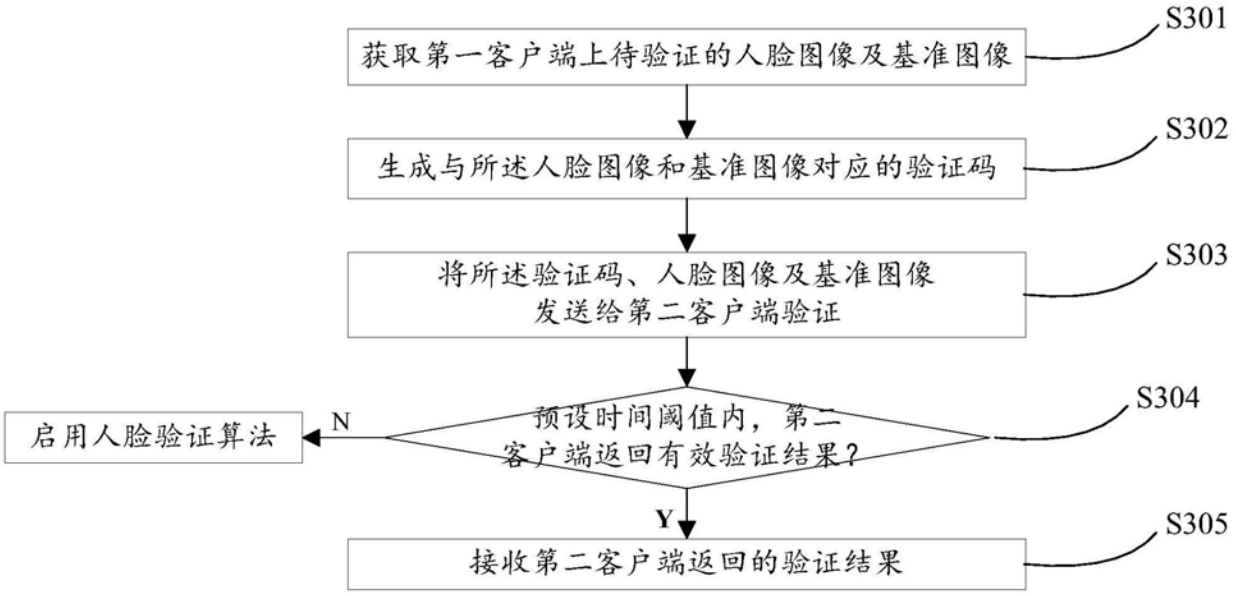

获取第一客户端上待验证的人脸图像及基准图像
S301
生成与所述人脸图像和基准图像对应的验证码
S302
将所述验证码、人脸图像及基准图像
发送给第二客户端验证
S303
预设时间阈值内，第二
客户端返回有效验证结果?
S304
N
启用人脸验证算法
Y
接收第二客户端返回的验证结果
S305

图4

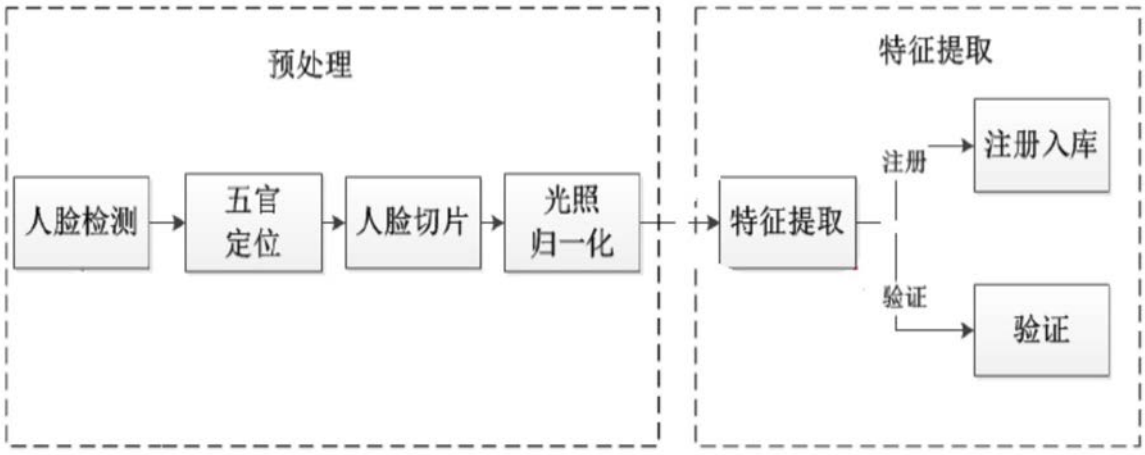

预处理
人脸检测
五官定位
人脸切片
光照归一化
特征提取
特征提取
注册
注册入库
验证
验证

图5

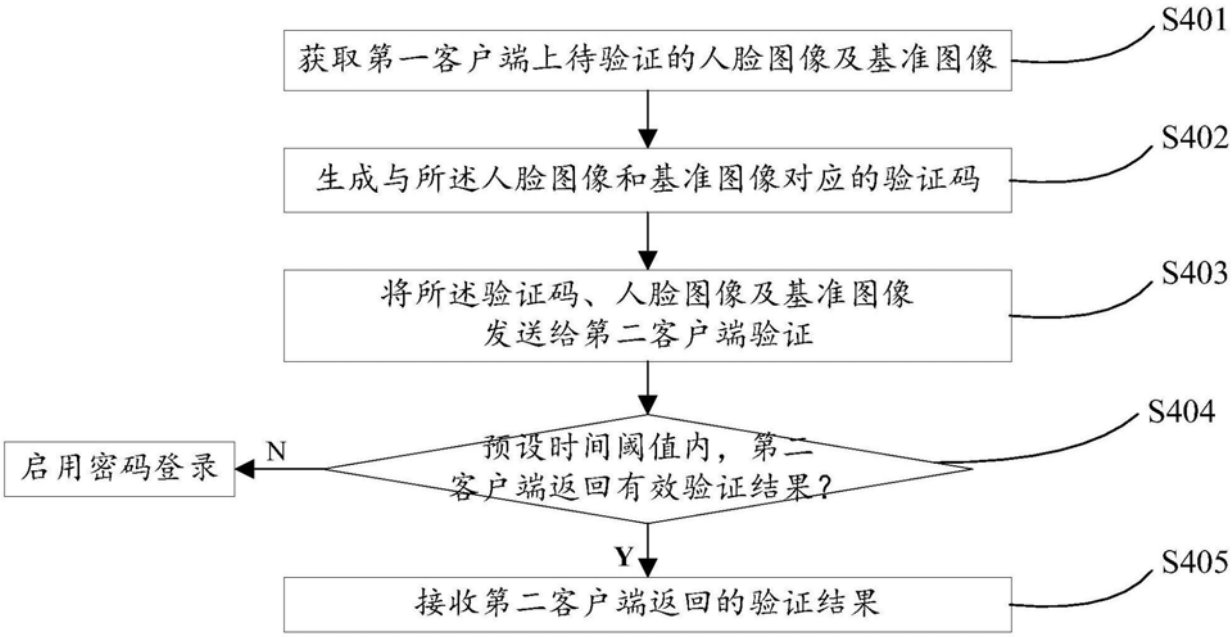

S401
获取第一客户端上待验证的人脸图像及基准图像
S402
生成与所述人脸图像和基准图像对应的验证码
S403
将所述验证码、人脸图像及基准图像发送给第二客户端验证
S404
预设时间阈值内，第二客户端返回有效验证结果？
N
启用密码登录
Y
S405
接收第二客户端返回的验证结果

图6

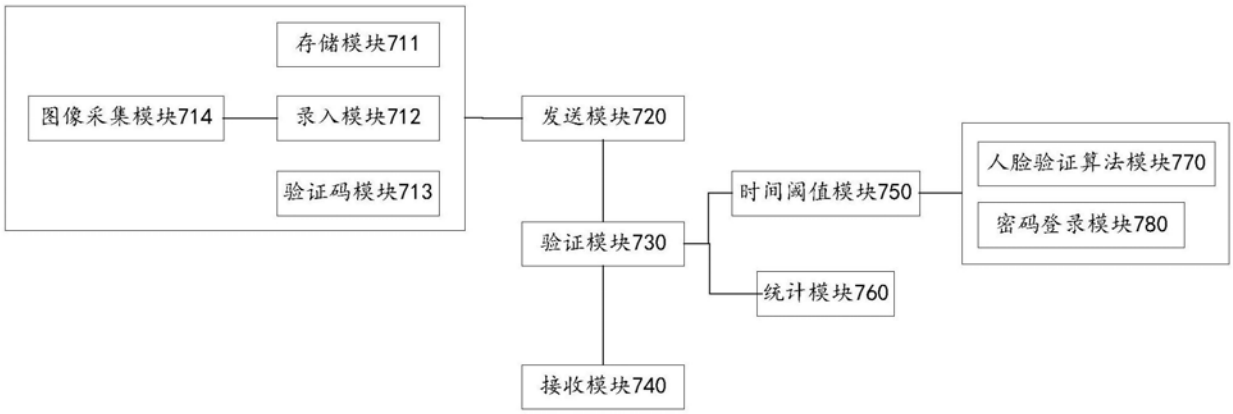

存储模块711
图像采集模块714
录入模块712
验证码模块713
发送模块720
验证模块730
时间阈值模块750
人脸验证算法模块770
密码登录模块780
统计模块760
接收模块740

图7

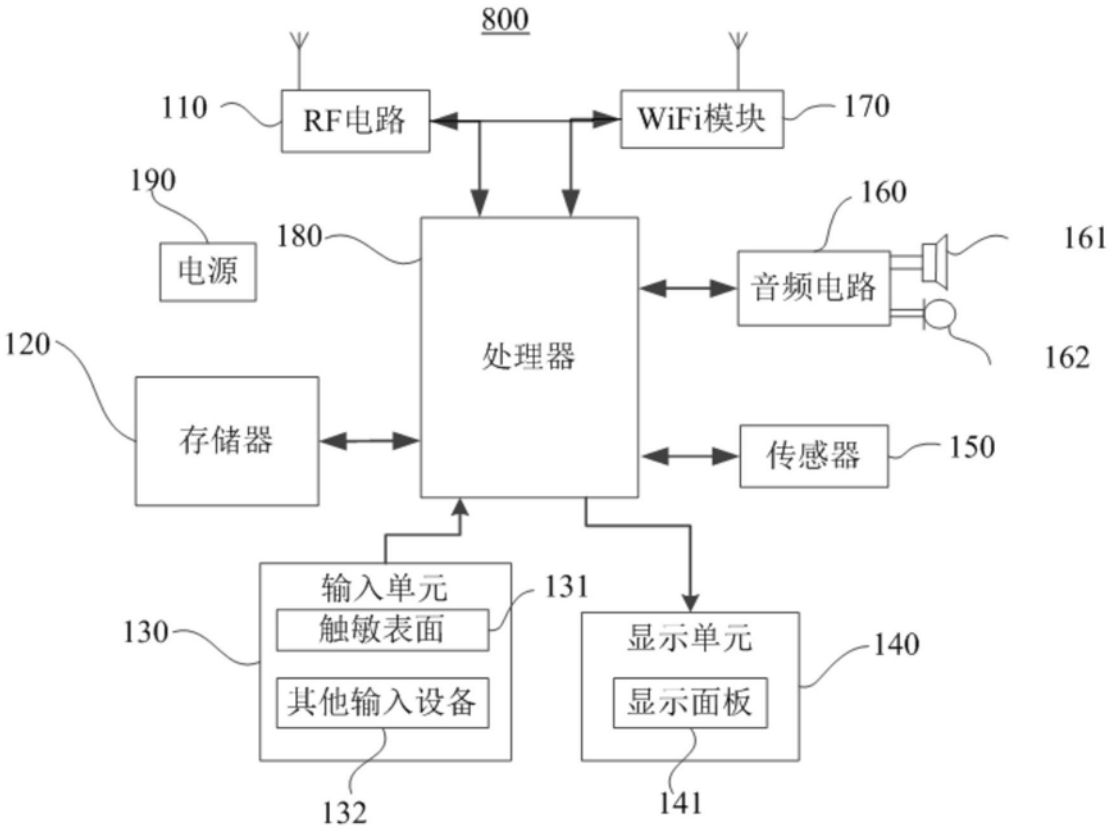

800
110
RF电路
WiFi模块
170
190
电源
180
处理器
160
音频电路
161
162
120
存储器
传感器
150
输入单元
131
130
触敏表面
其他输入设备
132
显示单元
140
显示面板
141

图8