

一种身份认证方法及装置

技术领域

本申请涉及网络通信技术领域，尤其涉及一种身份认证方法及装置。

5 背景技术

随着互联网技术的不断发展，越来越多的用户选择在网页上操作，并获取服务提供商提供的各种服务。例如，用户可通过在网页上对账号进行操作，获取服务提供商提供的诸如账号注册、账号登录、账号激活、账号注销等服务。

在实际应用中，为了避免合法用户的账号被非法用户截取，服务提供商在
10 为用户提供各种服务之前，需要通过服务器对当前用户的身份进行认证，当该用户的身份认证通过时，为该用户提供相应的服务，否则，拒绝为该用户提供相应的服务。

在现有技术中，服务器主要通过验证用户的证件信息（如个人身份证号），来认证该用户的身份。

15 具体的，假设用户在注册某一账号时，服务器通过终端向用户展示认证页面，当服务器接收到用户在该认证页面上输入的证件信息后，可通过第三方系统验证该证件信息是否合法，如果是，则确认身份认证通过，否则，确认身份认证不通过。

但是，通过现有技术提供的上述身份认证方法，只能确定用户的证件信息
20 是否合法，而无法确定输入证件信息的用户是否是该证件的合法持有者本人。因此，通过现有技术提供的身份认证方法，得到的身份认证结果的可信度较低。

发明内容

本申请实施例提供一种身份认证方法及装置，用以提高对用户身份认证的
25 可信度。

本申请实施例提供的一种身份认证方法，包括：

获取终端采集的待认证生物特征信息和所述终端发送的证件信息；

获取与所述证件信息对应的预存生物特征信息；

判断所述待认证生物特征信息与所述预存生物特征信息是否匹配，若是，

5 确定身份认证通过，否则，确定所述身份认证不通过。

本申请实施例提供的一种身份认证装置，包括：

第一获取模块，用于获取终端采集的待认证生物特征信息；

第二获取模块，用于获取所述终端发送的证件信息；

第三获取模块，用于获取与所述证件信息对应的预存生物特征信息；

10 身份认证模块，用于判断所述待认证生物特征信息与所述预存生物特征信息是否匹配，若是，确定身份认证通过，否则，确定所述身份认证不通过。

本申请实施例提供的身份认证方法，获取终端采集的待认证生物特征信息和该终端发送的证件信息，获取与该证件信息对应的预存生物特征信息。判断该待认证生物特征信息与预存生物特征信息是否匹配，若是，确定身份认证通
15 过，否则，确定身份认证不通过，从而可有效提高对用户身份认证的可信度。

附图说明

此处所说明的附图用来提供对本申请的进一步理解，构成本申请的一部分，本申请的示意性实施例及其说明用于解释本申请，并不构成对本申请的不
20 当限定。在附图中：

图 1 为本申请实施例提供的身份认证方法流程示意图之一；

图 2 为本申请实施例提供的身份认证方法流程示意图之二；

图 3 为本申请实施例提供的身份认证装置结构示意图。

25 具体实施方式

在现有技术中，服务器是通过验证用户的证件信息对该用户的身份进行认

证的，由于对该证件信息的验证得到的验证结果，无法确定输入证件信息的用户是否是该证件的合法持有者本人。考虑到在实际应用场景中，用户的生物特征信息与证件信息都能够证明该用户的合法身份，且生物特征信息与证件信息的对应关系是唯一的，因此，本申请通过获取当前用户提供的待认证生物特征信息
5 信息和证件信息，以及获取该证件信息对应的预存生物特征信息，判断该待认证生物特征信息与预存生物特征信息之间是否匹配，若是，说明提供证件信息的当前用户为该证件信息的合法持有者本人，否则，说明提供证件信息的当前用户为该证件信息的非法持有者，从而可有效提高对用户身份认证的可信度。

为使本申请的目的、技术方案和优点更加清楚，以下将结合本申请具体实施例及相应的附图对本申请技术方案进行清楚、完整地描述。显然，所描述的实施例仅是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，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，都属于本申请保护的范围。
10

以下将具体说明本申请实施例提供的身份认证方法。

参见图 1，为本申请实施例提供的身份认证方法的流程示意图，该方法包括：
15

S101、获取终端采集的待认证生物特征信息和该终端发送的证件信息。

本申请实施例所述的待认证生物特征信息，可以是用户的人脸特征信息、指纹特征信息、掌纹特征信息等生理特征信息，也可以是用户的步态特征信息、声音特征信息等行为特征信息。
20

服务器在获取终端采集的待认证生物特征信息时，具体可获取终端采集的人脸图像、指纹图像、掌纹图像、步态图像或音频数据等，并识别人脸图像、指纹图像、掌纹图像、步态图像或音频数据中的待认证生物特征信息（如，人脸特征信息、指纹特征信息、掌纹特征信息、步态特征信息或声音特征信息）。

本申请实施例所述的证件信息可以是：居民身份证、护照、军官证、工作证、学生证、学位证、毕业证、银行卡、会员卡等证件上的用户信息。
25

服务器在获取终端发送的证件信息时，具体的，服务器可获取用户在终端展示的页面上输入的证件信息。

下面以待认证生物特征信息为指纹特征信息，证件信息为身份证号码为例说明。

5 用户在获取服务提供商提供的某一服务之前，服务器可通过终端向用户展示认证页面，并通过该认证页面提示用户采集该用户的指纹特征信息（生物特征信息）。用户根据认证页面的提示，启动终端上的指纹采集装置并采集指纹图像。终端识别该指纹图像中的指纹特征信息，并将该指纹特征信息作为待认证指纹特征信息发送给服务器，则服务器获取该终端采集的待认证指纹特征信息。
10 息。

服务器还可通过该认证页面提示用户输入身份证号码（证件信息）。用户根据认证页面的提示，在该页面上输入身份证号码。终端将用户输入的身份证号码发送给服务器，服务器则可获取终端发送的身份证号码。

S102、获取与证件信息对应的预存生物特征信息。

15 在实际应用过程中，第三方系统中会预先存储有与用户的证件信息对应的生物特征信息。例如用户在申请身份证时，作为第三方系统的身份证管理系统（比如公安部的身份证管理系统）会为该用户创建一个与该用户唯一对应的身份证号码，同时至少采集一种与该用户唯一对应的生物特征信息（如指纹特征信息）。该用户的身份证号码和生物特征信息的对应关系预先存储在该身份证
20 管理系统中。

沿用上例，服务器通过步骤 S101 获取到用户的身份证号码（证件信息）之后，可从身份证管理系统中查找与该身份证号码对应的指纹特征信息（生物特征信息），将该指纹特征信息作为预存指纹特征信息。

当然，用户的身份证号码和指纹特征信息的对应关系，不限于保存在第三
25 方系统中，例如，也可以预先保存在服务器的信息库中，以供服务器根据获取的身份证号码查找对应的指纹特征信息。

S103、判断该待认证生物特征信息与该预存生物特征信息是否匹配，若是，执行步骤 S104，否则，执行步骤 S105。

继续沿用上例，当服务器通过步骤 S101 获取到终端采集的待认证指纹特征信息（待认证生物特征信息），且通过步骤 S102 获取到预存指纹特征信息（预存生物特征信息）之后，判断待认证指纹特征信息和预存指纹特征信息是否匹配。具体的，服务器可判断该待认证指纹特征信息和预存指纹特征信息之间的相似度是否大于预设阈值，若是，确定待认证指纹特征信息和预存指纹特征信息匹配，并执行步骤 S104，否则，不匹配，执行步骤 S105。

S104、确定身份认证通过。

当待认证指纹特征信息和预存指纹特征信息匹配时，这说明当前输入身份证号码的用户为该身份证号码的合法持有者，从而确定该用户的身份认证通过。

S105、确定身份认证不通过。

当待认证指纹特征信息和预存指纹特征信息不匹配时，这说明当前输入身份证号码的用户为该身份证号码的非法持有者，从而确定该用户的身份认证不通过。

本申请图 1 所示的方法，服务器通过获取终端发送的当前用户的待认证生物特征信息，以及获取当前用户提供的证件信息对应的预存生物特征信息，由于用户的生物特征信息与证件信息都能够证明该用户的合法身份，且生物特征信息与证件信息的对应关系是唯一的，因此，只要判断待认证生物特征信息和预存生物特征信息是否匹配，就可以确定当前提供证件信息的用户是否为该证件信息的合法持有者本人，从而可有效提高对用户身份认证的可信度。

在本申请实施例中，相比于通过用户在页面上输入证件信息的方式，终端通过采集证件图像，并从该证件图像中识别证件信息的方式来获取证件信息，可提高用户输入证件信息的便利性。因此，本申请终端可采集证件图像，并识别该证件图像中的证件信息，以供服务器获取终端采集的证件信息。

例如，终端可通过图像采集装置（如摄像头或扫描仪）采集身份证图像，并识别身份证号码，将该识别出的身份证号码发送给服务器，服务器则可获取终端采集的身份证号码。

当然，终端采集到身份证图像后，也可将该图像发送给服务器，由服务器
5 识别该图像中的身份证号码。

需要说明的是，终端或服务器可通过光学字符识别（Optical Character Recognition, OCR）技术识别图像中的文字（如汉字和数字），以获取图像中的身份证号码。

在本申请实施例中，当服务器需要获取该掌纹图像或指纹图像时，需要在
10 终端上设置掌纹采集仪或指纹采集仪，这样不但会提高身份认证的成本，而且用户的操作便利性也较低。当服务器将终端采集的步态特征信息或声音特征信息作为待认证生物特征信息时，由于不同的步态特征信息（或声音特征信息）之间的区分度较低，对用户身份认证的可信度较低。

考虑到在实际应用中，几乎每个终端上均设置有图像采集装置（如摄像
15 头），这样，终端可通过自身配置的摄像头随时采集人脸图像，并识别人脸特征信息，服务器就可获取到终端采集的人脸特征信息。

因此，下面将以服务器获取到的待认证生物特征信息为终端采集的待认证人脸特征信息为例，详细说明本申请提供的身份认证方法，如图 2 所示。

图 2 为本申请实施例提供的服务器根据待认证人脸特征信息认证用户身份
20 的方法，具体包括以下步骤：

S201、获取终端采集的待认证人脸特征信息和该终端发送的证件信息。

例如，服务器可获取终端通过摄像头采集的人脸图像，并识别该人脸图像中的人脸特征信息。服务器将识别出的人脸特征信息作为待认证人脸特征信息。

25 具体的，服务器获取终端采集的图像后，可根据预设人脸特征首先确定该图像中存在人脸图形，然后在确定的人脸图形中识别人脸的五官轮廓的大小、

位置和距离等待认证人脸特征信息。进一步的，当服务器在确定该图像中不存在人脸图形时，可向终端返回提示信息，以提示终端当前采集的图像不符合要求。

当然，服务器也可直接获取终端发送的人脸特征信息，该人脸特征信息可以是终端根据采集的人脸图像识别出的人脸特征信息。

在获取证件信息时，服务器可获取终端发送的身份证号码，该身份证号码可以是终端获取的用户输入的身份证号码，也可以是终端从采集的身份证图像中识别出的身份证号码。

S202、获取与身份证号码对应的预存人脸特征信息。

在实际应用场景中，用户在申请身份证时，身份证管理系统（第三方系统，比如公安部的身份证管理系统。）还会采集用户的人脸图像，并保存该人脸图像与身份证号码的对应关系，或者保存该人脸图像中的人脸特征信息与身份证号码的对应关系。其中，身份证管理系统保存的人脸特征信息至少包括五官轮廓的大小、位置和距离等人脸特征信息。

服务器通过步骤 S201 获取到该用户的身份证号码之后，可从身份证管理系统查找与该身份证号码对应的人脸特征信息，作为预存人脸特征信息。或者可从身份证管理系统查找与该身份证号码对应的人脸图像，并识别查找到的该人脸图像中的人脸特征信息，作为预存人脸特征信息。

S203、判断该待认证人脸特征信息与该预存人脸特征信息是否匹配，若是，执行步骤 S204，否则，执行步骤 S205。

具体的，服务器获取到用户的待认证人脸特征信息和预存人脸特征信息之后，比较待认证人脸特征信息中的五官轮廓的大小、位置，或距离等待认证子特征信息，与预存人脸特征信息中对应的五官轮廓的大小、位置，或距离等预存子特征信息，确定待认证人脸特征信息和预存人脸特征信息之间的相似度。

当相似度大于预设阈值时，可确定待认证人脸特征信息与预存人脸特征信息匹配，则执行步骤 S204，否则，确定待认证人脸特征信息与预存人脸特征信

息不匹配，执行步骤 S205。

S204、确定身份认证通过。

S205、确定所述身份认证不通过。

在步骤 S201 中，服务器在获取身份证号码时，也可获取终端采集的身份
5 证图像，并从中识别身份证号码。

当服务器通过获取终端采集的图像，来识别图像中的身份证号码时，为了提高身份认证的效率，可选的，服务器可获取终端采集的同时包含人脸和身份
证的图像。也就是说，终端采集的包含待认证人脸特征信息的图像中还包含身
份证号码，则服务器获取到终端采集的图像后，可从该图像中识别待认证人脸
10 特征信息和身份证号码。

由于服务器是从整个图像中识别人脸特征信息和身份证号码的，为了减少服务器的计算量，服务器可在获取到包含待认证人脸特征信息（待认证生物特征信息）和身份证号码（证件信息）的图像之后，从该图像的第一预设区域中识别待认证人脸特征信息，从该图像的第二预设区域中识别身份证号码。

15 例如，终端在同时拍摄人脸和身份证时，可在图像采集界面上显示第一预设区域和第二预设区域，并提示用户在第一预设区域采集人脸图像，且在第二预设区域采集身份证图像。服务器获取到终端采集的该图像后，仅从第一预设区域识别人脸特征信息，且仅从第二预设区域识别身份证号码，而不是从整个图像中识别人脸特征信息和身份证号码，这样，就可有效减少服务器的计算量。

20 在实际应用场景中，可能存在非法用户将合法用户的人脸图像或人脸模型当做当前用户的实时人脸图像，则终端采集的人脸图像就不是当前用户的实时人脸图像，这样，就会导致身份认证的可信度下降。

因此，在本申请实施例中，服务器在判断所述待认证人脸特征信息与所述预存人脸特征信息是否匹配之前，可获取终端采集的至少两幅人脸图像，并判
25 断人脸图像中是否存在指定特征信息，来确定该人脸图像是否为当前用户的实时人脸图像。

具体的，在步骤 S201 中，服务器获取终端采集的图像，具体包括：获取终端采集的第一图像和第二图像。识别该图像中包含的待认证人脸特征信息，具体包括：识别所述第一图像中包含的第一待认证人脸特征信息；识别第二图像中包含的第二待认证人脸特征信息。判断该第一待认证人脸特征信息中是否包含第一指定特征信息，且判断该第二待认证人脸特征信息中是否包含第二指定特征信息；当第一待认证人脸特征信息中包含第一指定特征信息，且第二待认证人脸特征信息中包含第二指定特征信息，则可确定终端采集的图像为当前用户的实时人脸图像，通过步骤 S203 判断该待认证人脸特征信息与该预存人脸特征信息是否匹配，否则，确定该图像可能是非法用户提供的人脸图像，则
5 结束后续流程。当然，服务器确定该图像可能是非法用户提供的人脸图像后，还可向终端返回提示信息，以提示终端当前采集的图像不符合要求。

其中，该第一指定特征信息和第二指定特征信息可以但不限于包括表情特征信息，该第一指定特征信息和第二指定特征信息不同。

例如，终端在采集第一图像时，提示用户采集指定表情的图像（如笑脸图像），在采集第二图像时，提示用户采集另一指定表情的图像（如哭脸图像），以获取两幅不同表情的人脸图像。这样，只有用户分别摆出笑脸的表情和哭脸的表情，终端才能成功采集到两幅不同表情的人脸图像。而当非法用户使用合法用户的人脸图像（如，合法用户的照片）充当实时人脸图像时，由于该人脸图像中人的表情是固定的，且该人脸图像中人的表情与终端指定表情不一定相符，因此，非法用户提供的人脸图像无法满足终端对图像的要求，这样其身份
15 认证就无法通过。因此，服务器就可确定提供该人脸图像的用户为非法用户，从而可有效提高身份认证的可信度。

在本申请实施例中，服务器在判断所述待认证人脸特征信息与所述预存人脸特征信息是否匹配之前，可获取终端采集的至少两幅人脸图像，并判断每幅
25 图像中的两个预设区域是否分别包含人脸图像和身份证图像，来确定该人脸图像是否为当前用户的实时人脸图像，其中，两幅图像中，两个预设区域的相对

位置不同。

具体的，在步骤 S201 中，服务器获取终端采集的图像，具体包括：获取终端采集的第一图像和第二图像。从图像的第一预设区域中识别待认证生物特征信息，具体包括：分别从该第一图像和第二图像的第一预设区域中识别待认证生物特征信息；从该图像的第二预设区域中识别证件信息，具体包括：分别从该第一图像和第二图像的第二预设区域中识别证件信息；其中，第一图像中第一预设区域和第二预设区域的相对位置，不同于第二图像中第一预设区域和第二预设区域的相对位置。

例如，终端在采集第一图像时，向用户展示第一图像采集界面，并提示用户在左上角（第一预设区域）采集人脸图像，且在右下角（第二预设区域）采集身份证图像。用户将人脸和身份证按照左上角和右下角的相对位置摆放，使得终端在第一图像采集界面的左上角成功采集到人脸图像，在右下角成功采集到身份证图像。终端在采集第二图像时，向用户展示第二图像采集界面，并提示用户在右上角（第一预设区域）采集人脸图像，且在左下角（第二预设区域）采集身份证图像。用户将人脸和身份证按照右上角和左下角的相对位置摆放，使得终端在第二图像采集界面的右上角成功采集到人脸图像，在左下角成功采集到身份证图像。

这样，终端在采集不同的图像（第一图像和第二图像）时，要求用户摆放人脸和身份证的相对位置也不相同，以保证可成功采集到符合要求的第一图像和第二图像。而当非法用户使用合法用户的人脸图像和身份证图像充当实时人脸和身份证的图像时，由于合法用户的人脸图像和身份证图像之间的相对位置是固定的，且人脸图像和身份证图像之间的相对位置不一定符合当前图像采集界面展示的第一预设区域和第二预设区域之间的相对位置，这样，非法用户就无法满足终端对图像的要求，因此，其身份认证无法通过。这样就可避免非法用户将合法用户的人脸图像或人脸模型当做当前用户的实时人脸图像，进行身份认证，从而可有效提高身份认证的可信度。

当然，从第一图像和第二图像的第二预设区域中识别出的证件信息可以不同，例如，可从第一图像的第二预设区域中识别身份证正面的证件信息，可从第二图像的第二预设区域中识别身份证反面的证件信息。这样，终端在采集不同的图像（第一图像和第二图像）时，不但要求用户摆放人脸和身份证的相对位置不相同，还要求用户摆放的身份证的正反面不同，这样可进一步避免非法用户将合法用户的人脸图像或人脸模型当做当前用户的实时人脸图像，从而可进一步提高身份认证的可信度。

在本申请实施例中，采用图 1 所示的方法的同时，可禁止终端读取该终端本地的图像，避免用户采用终端本地的图像作为当前用户的实时人脸图像，可进一步提高身份认证的可信度。

以上为本申请实施例提供的身份认证方法，基于同样的思路，本申请实施例还提供了一种身份认证装置，如图 3 所示，包括：

第一获取模块 31，用于获取终端采集的待认证生物特征信息；

第二获取模块 32，用于获取所述终端发送的证件信息；

第三获取模块 33，用于获取与所述证件信息对应的预存生物特征信息；

身份认证模块 34，用于判断所述待认证生物特征信息与所述预存生物特征信息是否匹配，若是，确定身份认证通过，否则，确定所述身份认证不通过。

可选的，所述待认证生物特征信息包括待认证人脸特征信息，所述预存生物特征信息包括预存人脸特征信息。

可选的，第一获取模块 31 具体用于，获取终端采集的图像，识别所述图像中包含的待认证生物特征信息。

可选的，第一获取模块 31 具体用于，获取终端采集的第一图像和第二图像，识别所述第一图像中包含的第一待认证人脸特征信息，识别所述第二图像中包含的第二待认证人脸特征信息；

所述装置还包括：

指定特征信息确定模块 35，用于在判断所述待认证生物特征信息与所述预

存生物特征信息是否匹配之前，确定所述第一待认证人脸特征信息中包含第一指定特征信息，且确定所述第二待认证人脸特征信息中包含第二指定特征信息；其中，所述第一指定特征信息和第二指定特征信息包括表情特征信息，所述第一指定特征信息和第二指定特征信息不同。

5 可选的，所述图像中包含证件信息；第二获取模块 32 具体用于，从终端采集的所述图像中识别证件信息。

可选的，第一获取模块 31 具体用于，从所述图像的第一预设区域中识别待认证生物特征信息，从所述图像的第二预设区域中识别证件信息。

10 可选的，第一获取模块 31 具体用于，获取终端采集的第一图像和第二图像，分别从所述第一图像和第二图像的第一预设区域中识别待认证生物特征信息，以及分别从所述第一图像和第二图像的第二预设区域中识别证件信息；

其中，所述第一图像中所述第一预设区域和所述第二预设区域的相对位置，不同于所述第二图像中所述第一预设区域和所述第二预设区域的相对位置。

15 本申请实施例提供的身份认证方法及装置，服务器通过获取终端发送的当前用户的待认证生物特征信息，以及获取当前用户提供的证件信息对应的预存生物特征信息，由于用户的生物特征信息与证件信息都能够证明该用户的合法身份，且生物特征信息与证件信息是唯一对应的，因此，只要判断待认证生物特征信息和预存生物特征信息是否匹配，就可以确定当前提供证件信息的用户
20 是否为该证件信息的合法持有者本人，从而可有效提高对用户身份认证的可信度。

本领域内的技术人员应明白，本申请的实施例可提供为方法、系统、或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本申请可采用在一个或多个其中包含
25 有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

本申请是参照根据本申请实施例的方法、设备（系统）、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

在一个典型的配置中，计算设备包括一个或多个处理器（CPU）、输入/输出接口、网络接口和内存。

内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器（RAM）和/或非易失性内存等形式，如只读存储器（ROM）或闪存（flash RAM）。内存是计算机可读介质的示例。

计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存（PRAM）、静态随机存取存储器（SRAM）、动态随机存取存储器（DRAM）、其他类型的随机存取存储器（RAM）、只读存储器（ROM）、电可擦除可编程只读存储器（EEPROM）、快闪记忆体或其他内存技术、只读光盘只读存储器

(CD-ROM)、数字多功能光盘(DVD)或其他光学存储、磁盒式磁带, 磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质, 可用于存储可以被计算设备访问的信息。按照本文中的界定, 计算机可读介质不包括暂存电脑可读媒体(transitory media), 如调制的数据信号和载波。

5 还需要说明的是, 术语“包括”、“包含”或者其任何其他变体意在涵盖非排除性的包含, 从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素, 而且还包括没有明确列出的其他要素, 或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下, 由语句“包括一个……”限定的要素, 并不排除在包括要素的过程、方法、商品或者设备中
10 还存在另外的相同要素。

本领域技术人员应明白, 本申请的实施例可提供为方法、系统或计算机程序产品。因此, 本申请可采用完全硬件实施例、完全软件实施例或结合软件和硬件方面的实施例的形式。而且, 本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、
15 光学存储器等)上实施的计算机程序产品的形式。

以上仅为本申请的实施例而已, 并不用于限制本申请。对于本领域技术人员来说, 本申请可以有各种更改和变化。凡在本申请的精神和原理之内所作的任何修改、等同替换、改进等, 均应包含在本申请的权利要求范围之内。

权 利 要 求 书

1、一种身份认证方法，其特征在于，包括：

获取终端采集的待认证生物特征信息和所述终端发送的证件信息；

获取与所述证件信息对应的预存生物特征信息；

5 判断所述待认证生物特征信息与所述预存生物特征信息是否匹配，若是，
确定身份认证通过，否则，确定所述身份认证不通过。

2、如权利要求 1 所述的方法，其特征在于，所述待认证生物特征信息包括待认证人脸特征信息，所述预存生物特征信息包括预存人脸特征信息。

3、如权利要求 2 所述的方法，其特征在于，获取终端采集的待认证生物
10 特征信息，具体包括：

获取终端采集的图像；

识别所述图像中包含的待认证生物特征信息。

4、如权利要求 3 所述的方法，其特征在于，获取终端采集的图像，具体
包括：

15 获取终端采集的第一图像和第二图像；

识别所述图像中包含的待认证生物特征信息，具体包括：

识别所述第一图像中包含的第一待认证人脸特征信息；以及

识别所述第二图像中包含的第二待认证人脸特征信息；

20 判断所述待认证生物特征信息与所述预存生物特征信息是否匹配之前，所述方法还包括：

确定所述第一待认证人脸特征信息中包含第一指定特征信息，且确定所述第二待认证人脸特征信息中包含第二指定特征信息；其中，所述第一指定特征信息和第二指定特征信息包括表情特征信息，所述第一指定特征信息和第二指定特征信息不同。

25 5、如权利要求 3 所述的方法，其特征在于，所述图像中包含证件信息；
获取所述终端发送的证件信息，具体包括：

从终端采集的所述图像中识别证件信息。

6、如权利要求 5 所述的方法，其特征在于，识别所述图像中包含的待认证生物特征信息，具体包括：

从所述图像的第一预设区域中识别待认证生物特征信息；

5 从终端采集的所述图像中识别证件信息，具体包括：

从所述图像的第二预设区域中识别证件信息。

7、如权利要求 6 所述的方法，其特征在于，获取终端采集的图像，具体包括：

获取终端采集的第一图像和第二图像；

10 从所述图像的第一预设区域中识别待认证生物特征信息，具体包括：

分别从所述第一图像和第二图像的第一预设区域中识别待认证生物特征信息；

从所述图像的第二预设区域中识别证件信息，具体包括：

分别从所述第一图像和第二图像的第二预设区域中识别证件信息；

15 其中，所述第一图像中所述第一预设区域和所述第二预设区域的相对位置，不同于所述第二图像中所述第一预设区域和所述第二预设区域的相对位置。

8、如权利要求 1 所述的方法，其特征在于，所述获取与所述证件信息对应的预存生物特征信息，包括：从一第三方系统获得与所述证件信息对应的预
20 存生物特征信息。

9、如权利要求 8 所述的方法，其特征在于，所述第三方系统为公安部的身份证管理系统。

10、一种身份认证装置，其特征在于，包括：

第一获取模块，用于获取终端采集的待认证生物特征信息；

25 第二获取模块，用于获取所述终端发送的证件信息；

第三获取模块，用于获取与所述证件信息对应的预存生物特征信息；

身份认证模块，用于判断所述待认证生物特征信息与所述预存生物特征信息是否匹配，若是，确定身份认证通过，否则，确定所述身份认证不通过。