

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局



(10) 国际公布号

WO 2021/184974 A1

(43) 国际公布日

2021 年 9 月 23 日 (23.09.2021)

(51) 国际专利分类号:

G06F 21/32 (2013.01)

G06F 21/62 (2013.01)

G06F 21/60 (2013.01)

省 杭 州 市 西 湖 区 西 溪 路 556 号 8 层 B 段
801-11, Zhejiang 310000 (CN)。

(21) 国际申请号:

PCT/CN2021/074244

(22) 国际申请日:

2021 年 1 月 28 日 (28.01.2021)

(25) 申请语言:

中文

(26) 公布语言:

中文

(30) 优先权:

202010198198.4 2020 年 3 月 19 日 (19.03.2020) CN

(72) 发明人: 王立彬(WANG, Libin); 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。 李亮(LI, Liang); 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。 郑丹丹(ZHENG, Dandan); 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。

(71) 申请人: 支付宝(杭州)信息技术有限公司 (ALIPAY (HANGZHOU) INFORMATION TECHNOLOGY CO., LTD.) [CN/CN]; 中国浙江

(74) 代理人: 北京博思佳知识产权代理有限公司 (BEIJING BESTIPR INTELLECTUAL PROPERTY LAW CORPORATION); 中国北京市海淀区上地三街 9 号嘉华大厦 B 座 409, Beijing 100085 (CN)。

(54) Title: IDENTITY AUTHENTICATION METHOD FOR PRIVACY PROTECTION, AND APPARATUS

(54) 发明名称: 保护隐私的身份认证方法及装置

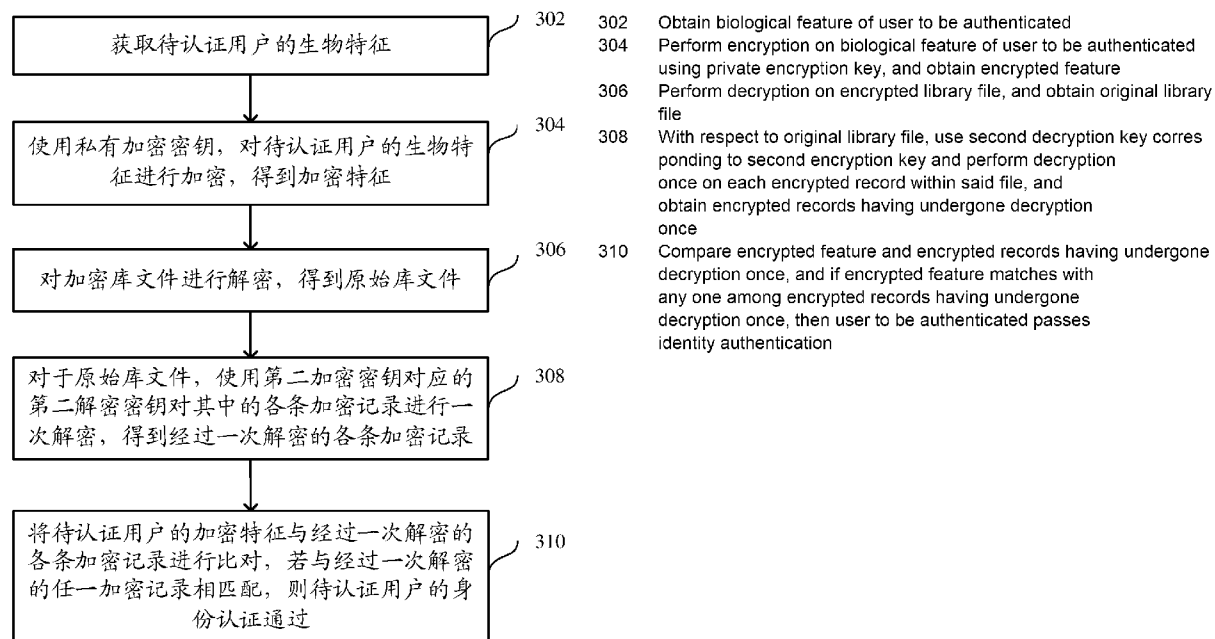


图 3

(57) Abstract: Embodiments of the present description provide an identity authentication method for privacy protection and an apparatus. In the authentication method, a biological feature of a user to be authenticated is obtained; encryption is performed on the biological feature of the user to be authenticated using a private encryption key, and an encrypted feature is obtained; decryption is performed on an encrypted library file, and an original library file is obtained; with respect to the original library file, a second decryption key corresponding to a second encryption key is used and decryption is performed once on each encrypted record within said file, and encrypted

(81) 指定国(除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

(84) 指定国(除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

records having undergone decryption once are obtained; the encrypted feature and the encrypted records having undergone decryption once are compared, and if the encrypted feature matches with any one among the encrypted records having undergone decryption once, then the user to be authenticated passes identity authentication. Thereby identity authentication can be implemented while performing privacy protection on a biological feature of a user.

(57) 摘要: 本说明书实施例提供一种保护隐私的身份认证方法及装置, 在认证方法中, 获取待认证用户的生物特征。使用私有加密密钥, 对待认证用户的生物特征进行加密, 得到加密特征。对加密库文件进行解密, 得到原始库文件。对于原始库文件, 使用第二加密密钥对应的第二解密密钥对其中的各条加密记录进行一次解密, 得到经过一次解密的各条加密记录。将加密特征与经过一次解密的各条加密记录进行比对, 若与经过一次解密的任一加密记录相匹配, 则待认证用户的身份认证通过。由此, 可实现在对用户的生物特征进行隐私保护的情况下进行身份认证。

保护隐私的身份认证方法及装置

技术领域

[01] 本说明书一个或多个实施例涉及计算机技术领域，尤其涉及一种保护隐私的身份认证方法及装置。

背景技术

[02] 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。为了避免合法用户的账号被非法用户截取，服务提供商在为用户提供各种服务之前，需要对当前用户的身份进行认证。

[03] 目前，身份认证方法可以在服务端执行，也可以直接在客户端执行。当直接在客户端执行时，其认证过程可以如下：客户端采集用户的生物特征（如，人脸特征、指纹特征或者虹膜特征等），将采集的生物特征与预先存储的生物特征进行比对，基于比对结果确定用户的身份认证是否通过。然而存储在客户端的生物特征存在被盗风险，从而现有的由客户端执行的身份认证方法不能实现用户的生物特征的隐私保护。

[04] 因此，需要提供一种身份认证方法，以提高用户的生物特征的安全性。

发明内容

[05] 本说明书一个或多个实施例描述了一种保护隐私的身份认证方法及装置，可以提高用户的生物特征的安全性。

[06] 第一方面，提供了一种保护隐私的身份认证方法，包括：获取待认证用户的生物特征；使用所述私有加密密钥，对所述待认证用户的生物特征进行加密，得到加密特征；对所述加密库文件进行解密，得到所述原始库文件；对于所述原始库文件，使用所述第二加密密钥对应的第二解密密钥对其中的各条加密记录进行一次解密，得到经过一次解密的各条加密记录；将所述加密特征与经过一次解密的各条加密记录进行比对，若与经过一次解密的任一加密记录相匹配，则所述待认证用户的身份认证通过。

[07] 第二方面，提供了一种保护隐私的身份认证方法，包括：获取当前用户的生物特征；使用私有加密密钥，对所述生物特征进行加密，得到当前用户的加密特征；使用第二加密密钥，对当前用户的加密特征进行二次加密，得到当前用户的加密记录；将当前

用户的加密记录输出至对应的原始库文件中；在所述原始库文件中加密记录的个数达到阈值时，对所述原始库文件进行加密，得到加密库文件；向客户端发送所述加密库文件，以使得所述客户端在对所述加密库文件进行解密后通过将其中的经过一次解密的各条加密记录与待认证用户的加密特征进行比对实现所述待认证用户的身份认证。

[08] 第三方面，提供了一种保护隐私的身份认证装置，包括：获取单元，用于获取待认证用户的生物特征；加密单元，用于使用所述私有加密密钥，对所述获取单元获取的所述待认证用户的生物特征进行加密，得到加密特征；解密单元，用于对所述加密库文件进行解密，得到所述原始库文件；所述解密单元，还用于对于所述原始库文件，使用所述第二加密密钥对应的第二解密密钥对其中的各条加密记录进行一次解密，得到经过一次解密的各条加密记录；比对单元，用于将所述加密单元得到的所述加密特征与所述解密单元得到的经过一次解密的各条加密记录进行比对，若与经过一次解密的任一加密记录相匹配，则所述待认证用户的身份认证通过。

[09] 第四方面，提供了一种保护隐私的身份认证装置，包括：获取单元，用于获取当前用户的生物特征；加密单元，用于使用私有加密密钥，对所述获取单元获取的所述生物特征进行加密，得到当前用户的加密特征；所述加密单元，还用于使用第二加密密钥，对当前用户的加密特征进行二次加密，得到当前用户的加密记录；输出单元，用于将所述加密单元得到的当前用户的加密记录输出至对应的原始库文件中；所述加密单元，还用于在所述原始库文件中加密记录的个数达到阈值时，对所述原始库文件进行加密，得到加密库文件；发送单元，用于向客户端发送所述加密单元得到的所述加密库文件，以使得所述客户端在对所述加密库文件进行解密后通过将其中的经过一次解密的各条加密记录与待认证用户的加密特征进行比对实现所述待认证用户的身份认证。

[10] 第五方面，提供了一种计算机存储介质，其上存储有计算机程序，当所述计算机程序在计算机中执行时，令计算机执行第一方面的方法或第二方面的方法。

[11] 第六方面，提供了一种计算设备，包括存储器和处理器，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现第一方面的方法或第二方面的方法。

[12] 本说明书一个或多个实施例提供的保护隐私的身份认证方法及装置，在对待认证用户的身份进行认证时，先使用私有加密密钥，对待认证用户的生物特征进行加密，得到加密特征。之后，对客户端预先存储的加密库文件进行解密，并对原始库文件中的各条加密记录进行一次解密，得到仅使用私有加密密钥加密后的各用户的生物特征。将加密特征与仅使用私有加密密钥加密后的各用户的生物特征进行比对，并基于比对结果，

确定待认证用户的身份认证是否通过。由于本方案在对用户的身份进行认证时采用加密域数据的比对方法，由此可以有效提高用户的生物特征的安全性。另外，即使用户的生物特征被盗取，可以通过变更私有加密密钥，而迫使预先存储的用户的生物特征失效，由此可以有效避免欺诈行为，进而可以提升用户体验。

附图说明

[13] 为了更清楚地说明本说明书实施例的技术方案，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说明书的一些实施例，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它的附图。

[14] 图 1 为本说明书提供的保护隐私的身份认证方法的应用场景示意图；

[15] 图 2 为本说明书一个实施例提供的保护隐私的身份认证方法流程图；

[16] 图 3 为本说明书另一个实施例提供的保护隐私的身份认证方法流程图；

[17] 图 4 为本说明书一个实施例提供的保护隐私的身份认证装置示意图；

[18] 图 5 为本说明书另一个实施例提供的保护隐私的身份认证装置示意图。

具体实施方式

[19] 下面结合附图，对本说明书提供的方案进行描述。

[20] 在描述本说明书提供的方案之前，先对本方案的发明构思作以下说明。

[21] 如前所述，现有的由客户端执行的身份认证方法存在用户的生物特征被盗的风险。为了提高用户的生物特征的安全性，本申请的申请人考虑在对用户的身份进行认证时，用加密域数据的比对替换原始数据的直接比对。具体实现方式如下：

[22] 首先，服务端生成加密库文件，并将加密库文件下发至客户端。这里的加密库文件通过对原始库文件进行加密得到。该原始库文件中记录有多条加密记录，其中的每条加密记录至少通过对一个用户的生物特征先使用私有加密密钥进行一次加密，再使用第二加密密钥进行二次加密得到。

[23] 之后，在对待认证用户的身份进行认证的过程中，客户端先获取待认证用户的生物特征。使用上述私有加密密钥，对待认证用户的生物特征进行加密，得到加密特征。

再对加密库文件进行解密，得到原始库文件。对于原始库文件，使用第二加密密钥对应的第二解密密钥对其中的各条加密记录进行一次解密，得到经过一次解密的各条加密记录。将加密特征与经过一次解密的各条加密记录进行比对，若与经过一次解密的任一加密记录相匹配，则待认证用户的身份认证通过。

[24] 以上就是本说明书提供的发明构思，基于该发明构思就可以得到本方案，以下对本方案进行详细阐述。

[25] 图 1 为本说明书提供的保护隐私的身份认证方法的应用场景示意图。图 1 中，服务端可以获取用户的生物特征，并对获取的生物特征依次执行加密、编码以及二次加密等处理，得到加密记录。之后，服务端可以将加密记录输出至原始库文件中。在原始库文件中加密记录的个数达到阈值时，服务端可以对原始库文件进行加密，并且可以将加密库文件下发至客户端。客户端接收到加密库文件之后，可以对加密库文件进行解密，并对解密后的原始库文件中的各条加密记录进行一次解密。之后，通过将其中的经过一次解密的各条加密记录与待认证用户的加密特征进行比对实现待认证用户的身份认证。

[26] 以下结合图 2 对图 1 中服务端生成加密库文件的过程进行详细说明。

[27] 图 2 为本说明书一个实施例提供的保护隐私的身份认证方法流程图。所述方法的执行主体可以为图 1 中的服务端。如图 2 所示，所述方法可以包括步骤 202~步骤 212。

[28] 步骤 202，获取当前用户的生物特征。

[29] 如，可以是在用户注册会员时，获取当前用户的生物特征。这里的生物特征可以包括生理特征和行为特征。其中，生理特征可以包括以下至少一种：人脸特征、指纹特征和虹膜特征等。行为特征可以包括声音特征和步态特征等。

[30] 以生物特征为人脸特征为例来说，该获取过程可以为：服务端接收客户端通过采集模块（如，摄像头）所采集的人脸图像。之后，可以将该人脸图像输入特征提取模型，得到人脸特征。这里的特征提取模型设置于服务端，其可以包括但不限于 SURF、SIFT、ORB、FAST 以及 Harris 等特征点检测算法。

[31] 应理解，上述只是针对人脸特征的获取过程的说明，在生物特征为指纹特征时，上述采集模块可以为指纹感应器。其相应的指纹特征的获取过程可以为：服务端接收客户端通过指纹感应器所采集的初始指纹信息。之后，可以对采集到的初始指纹信息进行预定运算（如，求平均），得到指纹特征。

[32] 步骤 204，使用私有加密密钥，对获取的生物特征进行加密，得到当前用户的加密

特征。

[33] 需要说明的是，这里服务端在进行加密时所使用的加密算法，可以为预定义的加密算法，如，将被加密数据扩展至指定位数等。也可以为任一公开加密算法，如 elgamal 算法等。前提是该加密算法需由服务端和客户端预先协商得到。此外，服务端在进行加密时，可以针对该加密算法生成对应的参数（即私有加密密钥），从而服务端通过使用协商的加密算法以及对应的私有加密密钥进行加密。本说明书中，之所以将上述参数称为私有加密密钥，是因为该私有加密密钥不存在对应的解密密钥。

[34] 可以理解的是，服务端针对上述加密算法所生成的私有加密密钥是保密的，不对外公开。

[35] 可选地，对于上述加密特征，服务端可以采用编码算法，对该加密特征进行编码，得到编码结果。在一个例子中，该编码算法可以为 base64 算法等。可以理解的是，通过执行该编码的步骤，可以节约加密特征所占用的存储空间。

[36] 步骤 206，使用第二加密密钥，对当前用户的加密特征进行二次加密，得到当前用户的加密记录。

[37] 对于上述加密特征，或者加密特征的编码结果，服务端可以对其进行二次加密，得到用户的加密记录。这里服务端进行二次加密时所使用的加密算法可以为任一公开加密算法，如 elgamal 算法等。这里二次加密时所使用的加密算法也可以由服务端和客户端预先协商得到。同样地，服务端在进行二次加密时，也可以针对加密算法生成对应的参数（即第二加密密钥），从而服务端通过使用协商的加密算法以及对应的第二加密密钥进行二次加密。需要说明的是，这里的第二加密密钥与第二解密密钥相对应。

[38] 步骤 208，将当前用户的加密记录输出至对应的原始库文件中。

[39] 步骤 210，在原始库文件中加密记录的个数达到阈值时，对原始库文件进行加密，得到加密库文件。

[40] 在得到用户的加密记录之后，服务端可以将用户的加密记录输出至对应的原始库文件中。该原始库文件可以由服务端预先生成。之后，可以判断原始库文件中的加密记录的个数是否达到阈值，若是，则可以对原始库文件进行加密，得到加密库文件。

[41] 需要说明的是，这里对原始库文件加密所使用的加密算法也可以为由服务端和客户端预先协商得到的任一公开加密算法。此外，服务端在对原始库文件进行加密时，也可以针对加密算法生成对应的参数（以下称数据库加密密钥），从而服务端通过使用协

商的加密算法以及数据库加密密钥，对原始库文件进行加密。该数据库加密密钥与数据库解密密钥相对应。

[42] 还需要说明的是，在实际应用中，所生成的加密库文件的个数可以为多个。

[43] 步骤 212，向客户端发送加密库文件，以使得客户端在对加密库文件进行解密后通过将其中的经过一次解密的各条加密记录与待认证用户的加密特征进行比对实现待认证用户的身份认证。

[44] 由上可以看出，本说明书实施例中，服务端下发至客户端的用户的生物特征是经过多层加密的，从而本方案可以有效提高用户的生物特征的安全性。

[45] 以下对客户端基于服务端下发的加密库文件，对用户的身份认证过程进行说明。

[46] 图 3 为本说明书另一个实施例提供的保护隐私的身份认证方法流程图。所述方法的执行主体可以为图 1 中的客户端。如图 3 所示，所述方法可以包括步骤 302~步骤 310。

[47] 步骤 302，获取待认证用户的生物特征。

[48] 如，可以是在待认证用户向客户端请求某种服务（如，支付服务）时，获取待认证用户的生物特征。这里的生物特征可以包括生理特征和行为特征。其中，生理特征可以包括以下至少一种：人脸特征、指纹特征和虹膜特征等。行为特征可以包括声音特征和步态特征等。

[49] 以生物特征为人脸特征为例来说，该获取过程可以为：客户端通过采集模块（如，摄像头）采集待认证用户的人脸图像。之后，可以将该人脸图像输入特征提取模型，得到人脸特征。这里的特征提取模型设置于客户端，其可以包括但不限于 SURF、SIFT、ORB、FAST 以及 Harris 等特征点检测算法。

[50] 应理解，上述只是针对人脸特征的获取过程的说明，在生物特征为指纹特征时，上述采集模块可以为指纹感应器。其相应的指纹特征的获取过程可以为：客户端通过指纹感应器采集待认证用户的初始指纹信息。之后，可以对采集到的初始指纹信息进行预定运算（如，求平均），得到指纹特征。

[51] 步骤 304，使用私有加密密钥，对待认证用户的生物特征进行加密，得到加密特征。

[52] 这里的私有加密密钥即为服务端在对用户的生物特征进行一次加密时所使用的私有加密密钥，此外，这里所使用的加密算法也为服务端在一次加密时所使用的预定义的加密算法或者任一公开加密算法。也就是说，该步骤中所使用的加密算法和私有加密密

钥与步骤 204 相同。

[53] 步骤 306, 对加密库文件进行解密, 得到原始库文件。

[54] 应理解, 当加密库文件的个数为多个时, 这里可以是依次将每个加密库文件读取到内存并解密。之后, 针对解密后得到的每个原始库文件执行步骤 308-步骤 310。

[55] 步骤 306 中, 对加密库文件进行解密所使用的密钥即为上述数据库解密密钥, 其可以由服务端在针对原始库文件的加密算法, 生成对应的数据库加密密钥时生成。以加密算法为 elgamal 算法为例来说, 由于其相应的解密算法为 elgamal 算法, 因此, 在生成数据库加密密钥时, 可以同时生成数据库加密密钥对应的数据库解密密钥。

[56] 步骤 308, 对于原始库文件, 使用第二加密密钥对应的第二解密密钥对其中的各条加密记录进行一次解密, 得到经过一次解密的各条加密记录。

[57] 这里的第二解密密钥可以由服务端在针对二次加密时所使用的加密算法, 生成对应的第二加密密钥时生成。以加密算法为 elgamal 算法为例来说, 由于其相应的解密算法为 elgamal 算法, 因此, 在生成第二加密密钥时, 可以同时生成第二加密密钥对应的第二解密密钥。

[58] 需要说明的是, 当服务端未执行编码的步骤时, 经过一次解密的各条加密记录即为服务端使用私有加密密钥, 对多个用户的生物特征进行一次加密后的各用户的加密特征。而当服务端还执行编码的步骤时, 服务端在得到上述经过一次解密的各条加密记录之后, 还可以基于编码算法对应的解码算法, 对其进行解码, 从而得到解码后的各条加密记录。进而解码后的各条加密记录即为服务端使用私有加密密钥, 对多个用户的生物特征进行一次加密后的各用户的加密特征。

[59] 需要说明的是, 在实际应用中, 上述步骤 302-步骤 304 与步骤 306-步骤 308 的执行顺序也可以互换, 或者也可以并行执行, 本说明书对此不作限定。

[60] 步骤 310, 将待认证用户的加密特征与经过一次解密的各条加密记录进行比对, 若与经过一次解密的任一加密记录相匹配, 则待认证用户的身份认证通过。

[61] 在一个示例中, 上述比对的步骤具体可以包括: 依次计算待认证用户的加密特征与经过一次解密的各条加密记录之间的相似度。这里的相似度可以包括但不限于余弦相似度、欧氏距离、曼哈顿距离以及皮尔逊相关系数等等。若与经过一次解密的任一加密记录之间的相似度大于阈值, 则可以认为待认证用户的加密特征与该经过一次解密的加密记录相匹配, 从而待认证用户的身份认证通过。

[62] 由上可以得出，本说明书实施例在对待认证用户的身份进行认证时，采用加密域数据的比对方法，由此可以避免在客户端存储用户的原始生物特征，从而可以有效提高用户的生物特征的安全性。此外，由于本方案采用加密域数据的比对方法，从而在用户的生物特征被盗取时，可以通过变更私有加密密钥，迫使预先存储的用户的生物特征失效。在预先存储的用户的生物特征失效的情况下，比对过程就会失败，这可以有效避免欺诈行为，进而可以提升用户体验。

[63] 与上述保护隐私的身份认证方法对应地，本说明书一个实施例还提供的一种保护隐私的身份认证装置，该装置设置于客户端。这里的客户端维护有加密库文件，该加密库文件通过对原始库文件进行加密得到。原始库文件中记录有多条加密记录，其中的每条加密记录至少通过对一个用户的生物特征先使用私有加密密钥进行一次加密，再使用第二加密密钥进行二次加密得到。如图 4 所示，该装置可以包括以下单元。

[64] 获取单元 402，用于获取待认证用户的生物特征。

[65] 这里的生物特征可以包括生理特征和行为特征。其中，生理特征可以包括以下至少一种：人脸特征、指纹特征和虹膜特征等。行为特征可以包括声音特征和步态特征等。

[66] 加密单元 404，用于使用私有加密密钥，对获取单元 402 获取的待认证用户的生物特征进行加密，得到加密特征。

[67] 解密单元 406，用于对加密库文件进行解密，得到原始库文件。

[68] 解密单元 406，还用于对于原始库文件，使用第二加密密钥对应的第二解密密钥对其中的各条加密记录进行一次解密，得到经过一次解密的各条加密记录。

[69] 比对单元 408，用于将加密单元 404 得到的加密特征与解密单元 406 得到的经过一次解密的各条加密记录进行比对，若与经过一次解密的任一加密记录相匹配，则待认证用户的身份认证通过。

[70] 本说明书上述实施例装置的各功能模块的功能，可以通过上述方法实施例的各步骤来实现，因此，本说明书一个实施例提供的装置的具体工作过程，在此不复赘述。

[71] 本说明书一个实施例提供的保护隐私的身份认证装置，可以有效提高用户的生物特征的安全性。

[72] 与上述保护隐私的身份认证方法对应地，本说明书一个实施例还提供的一种保护隐私的身份认证装置，该装置设置于服务端。如图 5 所示，该装置可以包括以下单元。

[73] 获取单元 502, 用于获取当前用户的生物特征。

[74] 这里的生物特征可以包括生理特征和行为特征。其中, 生理特征可以包括以下至少一种: 人脸特征、指纹特征和虹膜特征等。行为特征可以包括声音特征和步态特征等。

[75] 加密单元 504, 用于使用私有加密密钥, 对获取单元 502 获取的生物特征进行加密, 得到当前用户的加密特征。

[76] 加密单元 504, 还用于使用第二加密密钥, 对当前用户的加密特征进行二次加密, 得到当前用户的加密记录。

[77] 输出单元 506, 用于将加密单元 504 得到的当前用户的加密记录输出至对应的原始库文件中。

[78] 加密单元 504, 还用于在原始库文件中加密记录的个数达到阈值时, 对原始库文件进行加密, 得到加密库文件。

[79] 发送单元 508, 用于向客户端发送加密单元 504 得到的加密库文件, 以使得客户端在对加密库文件进行解密后通过将其中的经过一次解密的各条加密记录与待认证用户的加密特征进行比对实现待认证用户的身份认证。

[80] 可选地, 该装置还可以包括: 编码单元 (图中未示出), 用于根据编码算法, 对当前用户的加密特征进行编码, 得到编码结果。

[81] 加密单元 504 具体可以用于: 使用第二加密密钥, 对编码结果进行二次加密, 得到当前用户的加密记录。

[82] 本说明书上述实施例装置的各功能模块的功能, 可以通过上述方法实施例的各步骤来实现, 因此, 本说明书一个实施例提供的装置的具体工作过程, 在此不复赘述。

[83] 本说明书一个实施例提供的保护隐私的身份认证装置, 可以有效提高用户的生物特征的安全性。

[84] 另一方面, 本说明书的实施例提供了一种计算机可读存储介质, 其上存储有计算机程序, 当所述计算机程序在计算机中执行时, 令计算机执行图 2 或图 3 所示的方法。

[85] 另一方面, 本说明书的实施例提供一种计算设备, 包括存储器和处理器, 所述存储器中存储有可执行代码, 所述处理器执行所述可执行代码时, 实现图 2 或图 3 所示的方法。

[86] 本说明书中的各个实施例均采用递进的方式描述, 各个实施例之间相同相似的部

分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于设备实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[87] 结合本说明书公开内容所描述的方法或者算法的步骤可以硬件的方式来实现，也可以是由处理器执行软件指令的方式来实现。软件指令可以由相应的软件模块组成，软件模块可以被存放于 RAM 存储器、闪存、ROM 存储器、EPROM 存储器、EEPROM 存储器、寄存器、硬盘、移动硬盘、CD-ROM 或者本领域熟知的任何其它形式的存储介质中。一种示例性的存储介质耦合至处理器，从而使处理器能够从该存储介质读取信息，且可向该存储介质写入信息。当然，存储介质也可以是处理器的组成部分。处理器和存储介质可以位于 ASIC 中。另外，该 ASIC 可以位于服务器中。当然，处理器和存储介质也可以作为分立组件存在于服务器中。

[88] 本领域技术人员应该可以意识到，在上述一个或多个示例中，本发明所描述的功能可以用硬件、软件、固件或它们的任意组合来实现。当使用软件实现时，可以将这些功能存储在计算机可读介质中或者作为计算机可读介质上的一个或多个指令或代码进行传输。计算机可读介质包括计算机存储介质和通信介质，其中通信介质包括便于从一个地方向另一个地方传送计算机程序的任何介质。存储介质可以是通用或专用计算机能够存取的任何可用介质。

[89] 上述对本说明书特定实施例进行了描述。其它实施例在所附权利要求书的范围内。在一些情况下，在权利要求书中记载的动作或步骤可以按照不同于实施例中的顺序来执行并且仍然可以实现期望的结果。另外，在附图中描绘的过程不一定要示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中，多任务处理和并行处理也是可以的或者可能是有利的。

[90] 以上所述的具体实施方式，对本说明书的目的、技术方案和有益效果进行了进一步详细说明，所应理解的是，以上所述仅为本说明书的具体实施方式而已，并不用于限定本说明书的保护范围，凡在本说明书的技术方案的基础之上，所做的任何修改、等同替换、改进等，均应包括在本说明书的保护范围之内。

权利要求书

1、一种保护隐私的身份认证方法，通过客户端执行；所述客户端维护有加密库文件，该加密库文件通过对原始库文件进行加密得到；所述原始库文件中记录有多条加密记录，其中的每条加密记录至少通过对一个用户的生物特征先使用私有加密密钥进行一次加密，再使用第二加密密钥进行二次加密得到；所述方法包括：

获取待认证用户的生物特征；

使用所述私有加密密钥，对所述待认证用户的生物特征进行加密，得到加密特征；

对所述加密库文件进行解密，得到所述原始库文件；

对于所述原始库文件，使用所述第二加密密钥对应的第二解密密钥对其中的各条加密记录进行一次解密，得到经过一次解密的各条加密记录；

将所述加密特征与经过一次解密的各条加密记录进行比对，若与经过一次解密的任一加密记录相匹配，则所述待认证用户的身份认证通过。

2、根据权利要求 1 所述的方法，所述生物特征包括生理特征和行为特征；所述生理特征包括以下至少一种：人脸特征、指纹特征和虹膜特征；所述行为特征包括声音特征和步态特征。

3、一种保护隐私的身份认证方法，通过服务端执行；所述方法包括：

获取当前用户的生物特征；

使用私有加密密钥，对所述生物特征进行加密，得到当前用户的加密特征；

使用第二加密密钥，对当前用户的加密特征进行二次加密，得到当前用户的加密记录；

将当前用户的加密记录输出至对应的原始库文件中；

在所述原始库文件中加密记录的个数达到阈值时，对所述原始库文件进行加密，得到加密库文件；

向客户端发送所述加密库文件，以使得所述客户端在对所述加密库文件进行解密后通过将其中的经过一次解密的各条加密记录与待认证用户的加密特征进行比对实现所述待认证用户的身份认证。

4、根据权利要求 3 所述的方法，在所述使用第二加密密钥，对当前用户的加密特征进行二次加密之前，还包括：

根据编码算法，对所述当前用户的加密特征进行编码，得到编码结果；

所述使用第二加密密钥，对当前用户的加密特征进行二次加密，包括：

使用所述第二加密密钥，对所述编码结果进行二次加密，得到当前用户的加密记录。

5、根据权利要求3或4任一项所述的方法，所述生物特征包括生理特征和行为特征；所述生理特征包括以下至少一种：人脸特征、指纹特征和虹膜特征；所述行为特征包括声音特征和步态特征。

6、一种保护隐私的身份认证装置，设置于客户端；所述客户端维护有加密库文件，该加密库文件通过对原始库文件进行加密得到；所述原始库文件中记录有多条加密记录，其中的每条加密记录至少通过对一个用户的生物特征先使用私有加密密钥进行一次加密，再使用第二加密密钥进行二次加密得到；所述装置包括：

获取单元，用于获取待认证用户的生物特征；

加密单元，用于使用所述私有加密密钥，对所述获取单元获取的所述待认证用户的生物特征进行加密，得到加密特征；

解密单元，用于对所述加密库文件进行解密，得到所述原始库文件；

所述解密单元，还用于对于所述原始库文件，使用所述第二加密密钥对应的第二解密密钥对其中的各条加密记录进行一次解密，得到经过一次解密的各条加密记录；

比对单元，用于将所述加密单元得到的所述加密特征与所述解密单元得到的经过一次解密的各条加密记录进行比对，若与经过一次解密的任一加密记录相匹配，则所述待认证用户的身份认证通过。

7、根据权利要求6所述的装置，所述生物特征包括生理特征和行为特征；所述生理特征包括以下至少一种：人脸特征、指纹特征和虹膜特征；所述行为特征包括声音特征和步态特征。

8、一种保护隐私的身份认证装置，设置于服务端；所述装置包括：

获取单元，用于获取当前用户的生物特征；

加密单元，用于使用私有加密密钥，对所述获取单元获取的所述生物特征进行加密，得到当前用户的加密特征；

所述加密单元，还用于使用第二加密密钥，对当前用户的加密特征进行二次加密，得到当前用户的加密记录；

输出单元，用于将所述加密单元得到的当前用户的加密记录输出至对应的原始库文件中；

所述加密单元，还用于在所述原始库文件中加密记录的个数达到阈值时，对所述原始库文件进行加密，得到加密库文件；

发送单元，用于向客户端发送所述加密单元得到的所述加密库文件，以使得所述客户端在对所述加密库文件进行解密后通过将其中的经过一次解密的各条加密记录与待

认证用户的加密特征进行比对实现所述待认证用户的身份认证。

9、根据权利要求 8 所述的装置，还包括：

编码单元，用于根据编码算法，对所述当前用户的加密特征进行编码，得到编码结果；

所述加密单元具体用于：

使用所述第二加密密钥，对所述编码结果进行二次加密，得到当前用户的加密记录。

10、根据权利要求 8 或 9 任一项所述的装置，所述生物特征包括生理特征和行为特征；所述生理特征包括以下至少一种：人脸特征、指纹特征和虹膜特征；所述行为特征包括声音特征和步态特征。

11、一种计算机可读存储介质，其上存储有计算机程序，当所述计算机程序在计算机中执行时，令计算机执行权利要求 1-2 中任一项所述的方法或权利要求 3-5 中任一项所述的方法。

12、一种计算设备，包括存储器和处理器，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现权利要求 1-2 中任一项所述的方法或权利要求 3-5 所述的方法。

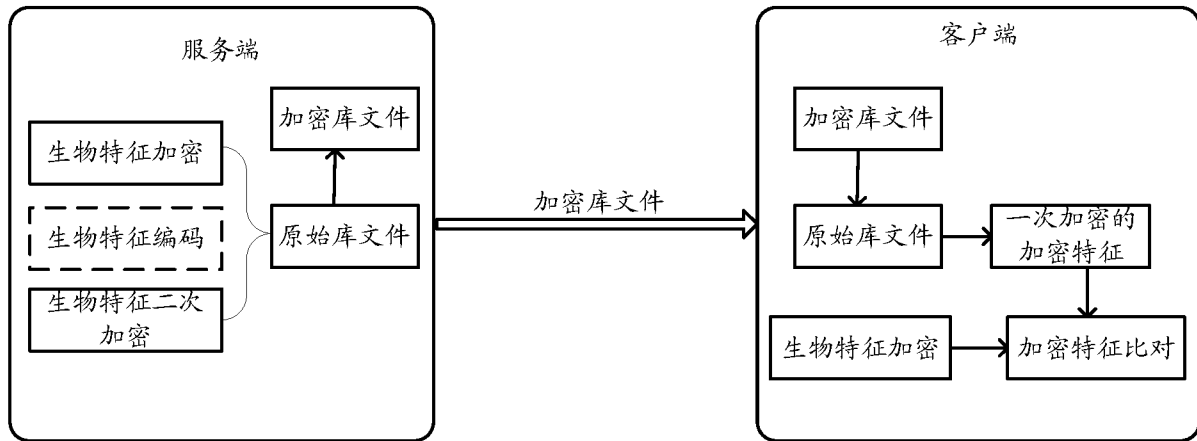


图 1

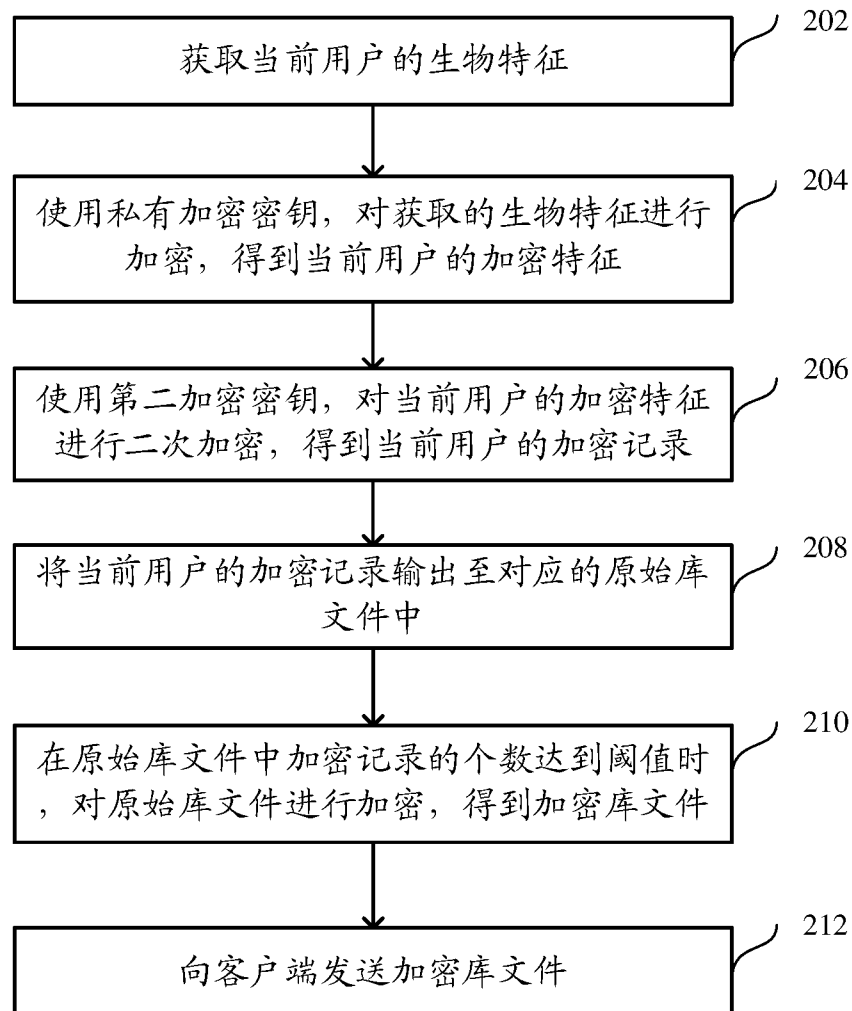


图 2

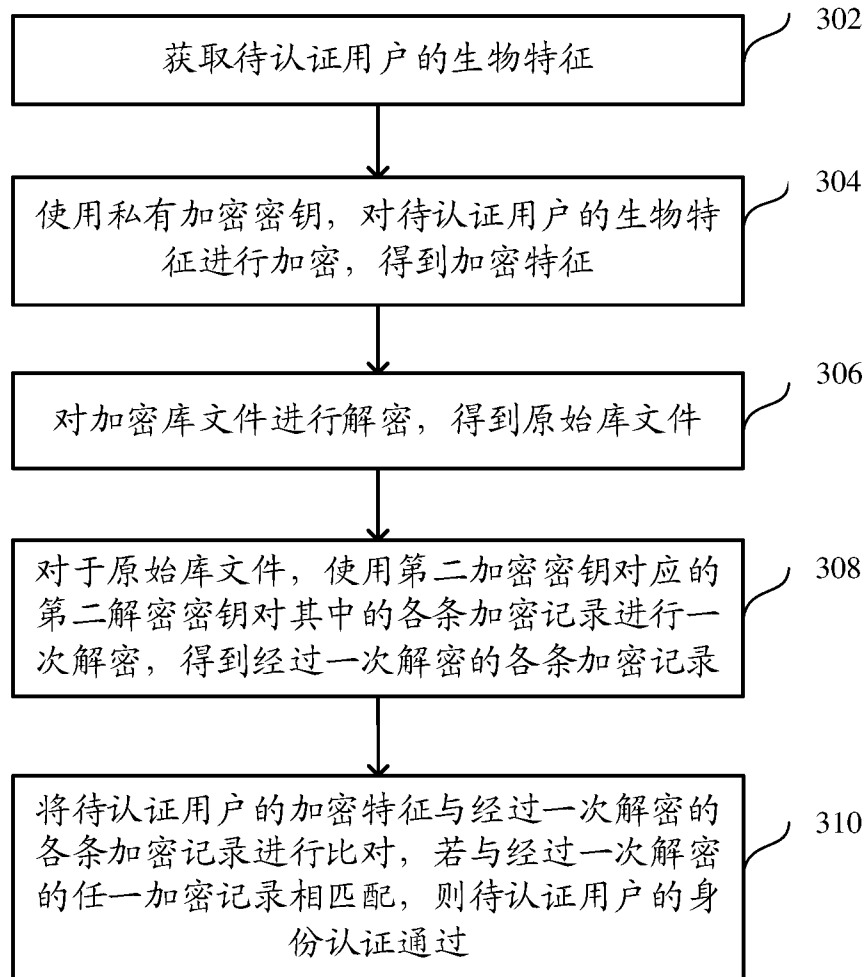


图 3

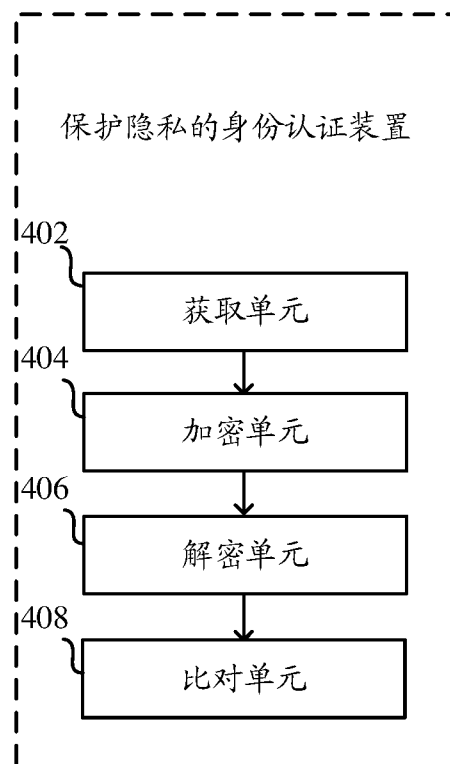


图 4

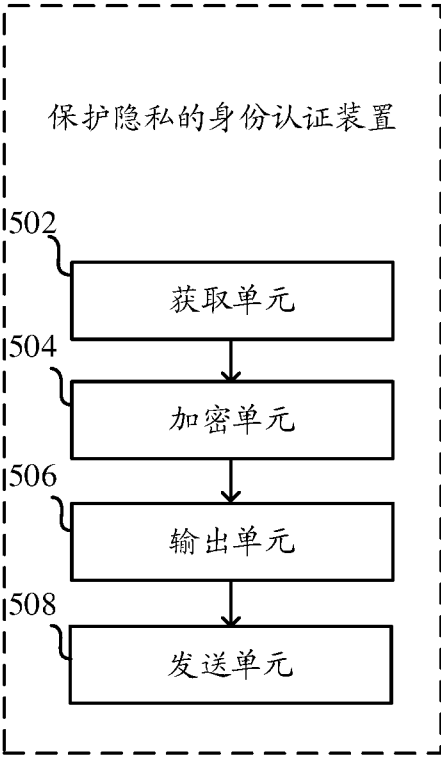


图 5

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2021/074244

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/32(2013.01)i; G06F 21/60(2013.01)i; G06F 21/62(2013.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNKI; CNABS; CNTXT; DWPI; SIPOABS; USTXT; EPTXT; WOTXT: 身份, 认证, 验证, 校验, 识别, 隐私, 生物特征, 保护, 破解, 泄漏, 泄露, 窃取, 用户端, 客户端, 手机, 终端, 两次, 双重, 加密, identity, authentication, recognise, identify, privacy, biology character, protect, leak, betray, disemboasom, divulge, filch, client, handset, terminal, second, encrypt

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 111382409 A (ALIPAY (HANGZHOU) INFORMATION TECHNOLOGY CO., LTD.) 07 July 2020 (2020-07-07) claims 1-12, description, paragraphs [0043]-[0112]	1-12
X	CN 110119608 A (ALIBABA GROUP HOLDING LIMITED) 13 August 2019 (2019-08-13) description paragraphs [0033]-[0310]	1-12
A	CN 110287670 A (BEIJING XIN'AN MICROELECTRONIC TECHNOLOGY CO., LTD.) 27 September 2019 (2019-09-27) entire document	1-12
A	CN 108965222 A (ZHAI, Hongying) 07 December 2018 (2018-12-07) entire document	1-12
A	CN 101984576 A (BEIJING UNIVERSITY OF TECHNOLOGY) 09 March 2011 (2011-03-09) entire document	1-12



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search

15 March 2021

Date of mailing of the international search report

20 April 2021

Name and mailing address of the ISA/CN

China National Intellectual Property Administration (ISA/
CN)
No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing
100088
China

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2021/074244

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN	111382409	A	07 July 2020	None	
CN	110119608	A	13 August 2019	None	
CN	110287670	A	27 September 2019	None	
CN	108965222	A	07 December 2018	None	
CN	101984576	A	09 March 2011	CN 101984576 B	04 July 2012

国际检索报告

国际申请号

PCT/CN2021/074244

A. 主题的分类 G06F 21/32(2013.01)i; G06F 21/60(2013.01)i; G06F 21/62(2013.01)i 按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类																				
B. 检索领域 检索的最低限度文献(标明分类系统和分类号) G06F 包含在检索领域中的除最低限度文献以外的检索文献 在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用)) CNKI;CNABS;CNTXT;DWPI;SIPOABS;USTXT;EPTXT;WOTXT: 身份, 认证, 验证, 校验, 识别, 隐私, 生物特征, 保护, 破解, 泄漏, 泄露, 窃取, 用户端, 客户端, 手机, 终端, 两次, 双重, 加密, identity, authentication, recognise, identify, privacy, biology character, protect, leak, betray, disemboasom, divulge, filch, client, handset, terminal, second, encrypt																				
C. 相关文件 <table border="1"> <thead> <tr> <th>类 型*</th> <th>引用文件, 必要时, 指明相关段落</th> <th>相关的权利要求</th> </tr> </thead> <tbody> <tr> <td>PX</td> <td>CN 111382409 A (支付宝杭州信息技术有限公司) 2020年 7月 7日 (2020 - 07 - 07) 权利要求第1-12项, 说明书第[0043]-[0112]段</td> <td>1-12</td> </tr> <tr> <td>X</td> <td>CN 110119608 A (阿里巴巴集团控股有限公司) 2019年 8月 13日 (2019 - 08 - 13) 说明书第[0033]-[0310]段</td> <td>1-12</td> </tr> <tr> <td>A</td> <td>CN 110287670 A (北京芯安徽电子科技有限公司) 2019年 9月 27日 (2019 - 09 - 27) 全文</td> <td>1-12</td> </tr> <tr> <td>A</td> <td>CN 108965222 A (翟红鹰) 2018年 12月 7日 (2018 - 12 - 07) 全文</td> <td>1-12</td> </tr> <tr> <td>A</td> <td>CN 101984576 A (北京工业大学) 2011年 3月 9日 (2011 - 03 - 09) 全文</td> <td>1-12</td> </tr> </tbody> </table>			类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求	PX	CN 111382409 A (支付宝杭州信息技术有限公司) 2020年 7月 7日 (2020 - 07 - 07) 权利要求第1-12项, 说明书第[0043]-[0112]段	1-12	X	CN 110119608 A (阿里巴巴集团控股有限公司) 2019年 8月 13日 (2019 - 08 - 13) 说明书第[0033]-[0310]段	1-12	A	CN 110287670 A (北京芯安徽电子科技有限公司) 2019年 9月 27日 (2019 - 09 - 27) 全文	1-12	A	CN 108965222 A (翟红鹰) 2018年 12月 7日 (2018 - 12 - 07) 全文	1-12	A	CN 101984576 A (北京工业大学) 2011年 3月 9日 (2011 - 03 - 09) 全文	1-12
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求																		
PX	CN 111382409 A (支付宝杭州信息技术有限公司) 2020年 7月 7日 (2020 - 07 - 07) 权利要求第1-12项, 说明书第[0043]-[0112]段	1-12																		
X	CN 110119608 A (阿里巴巴集团控股有限公司) 2019年 8月 13日 (2019 - 08 - 13) 说明书第[0033]-[0310]段	1-12																		
A	CN 110287670 A (北京芯安徽电子科技有限公司) 2019年 9月 27日 (2019 - 09 - 27) 全文	1-12																		
A	CN 108965222 A (翟红鹰) 2018年 12月 7日 (2018 - 12 - 07) 全文	1-12																		
A	CN 101984576 A (北京工业大学) 2011年 3月 9日 (2011 - 03 - 09) 全文	1-12																		
☐ 其余文件在C栏的续页中列出。 ☒ 见同族专利附件。																				
<table border="0"> <tr> <td> * 引用文件的具体类型: “A” 认为不特别相关的表示了现有技术一般状态的文件 “E” 在国际申请日的当天或之后公布的在先申请或专利 “L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件(如具体说明的) “O” 涉及口头公开、使用、展览或其他方式公开的文件 “P” 公布日先于国际申请日但迟于所要求的优先权日的文件 </td> <td> “T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 “X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 “Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 “&” 同族专利的文件 </td> </tr> </table>			* 引用文件的具体类型: “A” 认为不特别相关的表示了现有技术一般状态的文件 “E” 在国际申请日的当天或之后公布的在先申请或专利 “L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件(如具体说明的) “O” 涉及口头公开、使用、展览或其他方式公开的文件 “P” 公布日先于国际申请日但迟于所要求的优先权日的文件	“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 “X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 “Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 “&” 同族专利的文件																
* 引用文件的具体类型: “A” 认为不特别相关的表示了现有技术一般状态的文件 “E” 在国际申请日的当天或之后公布的在先申请或专利 “L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件(如具体说明的) “O” 涉及口头公开、使用、展览或其他方式公开的文件 “P” 公布日先于国际申请日但迟于所要求的优先权日的文件	“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 “X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 “Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 “&” 同族专利的文件																			
国际检索实际完成的日期 2021年 3月 15日		国际检索报告邮寄日期 2021年 4月 20日																		
ISA/CN的名称和邮寄地址 中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451		受权官员 邢白灵 电话号码 (86-512) 88995718																		

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2021/074244

检索报告引用的专利文件			公布日 (年/月/日)	同族专利	公布日 (年/月/日)
CN	111382409	A	2020年 7月 7日	无	
CN	110119608	A	2019年 8月 13日	无	
CN	110287670	A	2019年 9月 27日	无	
CN	108965222	A	2018年 12月 7日	无	
CN	101984576	A	2011年 3月 9日	CN 101984576 B	2012年 7月 4日