(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

(43) 国际公布日
2018 年 4 月 5 日 (05.04.2018)

WIPO | PCT

(10) 国际公布号
WO 2018/058833 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2016/112772

(22) 国际申请日: 2016 年 12 月 28 日 (28.12.2016)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201610863809.6 2016年9月29日 (29.09.2016) CN

(71) 申请人: 宇龙计算机通信科技（深圳）有限公司 (YULONG COMPUTER TELECOMMUNICATION SCIENTIFIC (SHENZHEN) CO., LTD.) [CN/CN]; 中国广东省深圳市南山区科技园北区梦溪道2号, Guangdong 518057 (CN)。

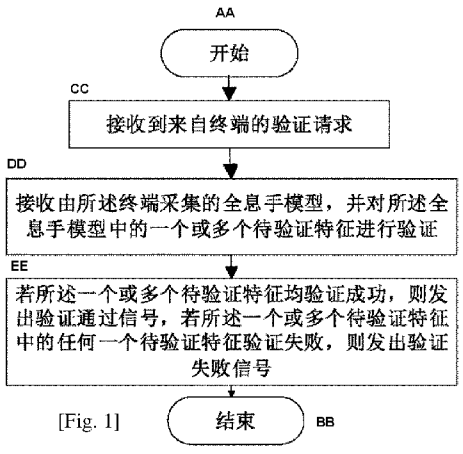
(72) 发明人: 梁文栋 (LIANG, Wendong); 中国广东省深圳市南山区科技园北区梦溪道2号, Guangdong 518057 (CN)。

(74) 代理人: 深圳市赛恩倍吉知识产权代理有限公司 (SHENZHEN SCIENBIZIP INTELLECTUAL PROPERTY AGENCY CO., LTD.); 中国广东省深圳市龙华新区龙观东路83号荣群大厦9楼, Guangdong 518109 (CN)。

(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,

(54) **Title:** VERIFICATION METHOD, VERIFICATION DEVICE, TERMINAL AND SERVER

(54) 发明名称: 验证方法、验证装置、终端和服务器



[Fig. 1]

AA Start
BB End
CC Receiving a verification request from a terminal
DD Receiving a holographic hand model collected by the terminal and verifying one or more features to be verified in the holographic hand model
EE If the one or more features to be verified are verified successfully, sending a verification success signal, and if any one of the one or more features to be verified is verified unsuccessfully, sending a verification failure signal

(57) Abstract: Provided are a verification method and verification device for a server, and a verification method and verification apparatus for a terminal. The verification method for the server comprises: receiving a verification request from a terminal; receiving a holographic hand model collected by the terminal and verifying one or more features to be verified in the holographic hand model; and if the one or more features to be verified are verified successfully, sending a verification success signal, and if any one of the one or more features to be verified is verified unsuccessfully, sending a verification failure signal. In the present invention, by means of verifying one or more features to be verified in a holographic hand model collected by a terminal, more user information is obtained, so as to not only improve the reliability of identity authentication but also restrict user rights to use of the terminal to perform an operation, thereby providing a certain security support for a user's operation and enhancing the user experience and security.

(57) 摘要: 本发明提供了一种用于服务器的验证方法和验证装置，一种用于终端的验证方法和验证装置，其中，用于服务器的验证方法包括：接收到来自终端的验证请求；接收由终端采集的全息手模型，并对全息手模型中的一个或多个待验证特征进行验证；若一个或多个待验证特征均验证成功，则发出验证通过信号，若一个或多个待验证特征中的任何一个待验证特征验证失败，则发出验证失败信号。本发明通过对终端采集到的全息手模型中一个或多个待验证特征进行验证，获得的用户信息更多，从而不仅能提高身份验证的可靠性，还限制了使用终端进行操作的用户权限，为用户的操作提供了一定的安全支持，增强了用户的体验性和安全性。

WO 2018/058833 A1

[见续页]

GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, 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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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))。

发明名称: 验证方法、验证装置、终端和服务器

[1] 本申请要求于2016年9月29日提交中国专利局，申请号为201610863809.6、发明名称为“验证方法、验证装置、终端和服务器”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

[2] 本发明涉及生物特征识别及生物特征建模领域，具体而言，涉及一种用于终端的验证方法、一种用于终端的验证装置、一种用于服务器的验证方法和一种用于服务器的验证装置。

背景技术

[3] 现代人的对信息安全的保护意识越来越强烈，近年来，随着生物特征识别技术的不断提高，生物特征技术也愈加常见地出现在日常生活中。

[4] 相关技术中，对生物特征的识别一般是静态的，通常采用对指纹等信息进行验证，因用户在验证过程中，每次验证的指纹和验证时的指纹姿势都是固定的，犯罪分子在经过一定时间了解后会比较容易窃取到指纹信息进行复制，从而对需保护的物品或信息造成侵害，从而对用户造成比较大的影响。

[5] 因此，需要能够动态地使用生物信息来进行验证的方案。

对发明的公开

发明内容

[6] 本发明旨在至少解决现有技术或相关技术中存在的技术问题之一。

[7] 为此，本发明的一个目的在于提出了一种用于服务器的验证方法。

[8] 本发明的另一个目的在于提出了一种用于终端的验证方法。

[9] 本发明的再一目的在于提出了一种用于服务器的验证装置。

[10] 本发明的第四个目的在于提出了一种用于终端的验证装置。

[11] 本发明的第五个目的在于提出了一种服务器。

[12] 本发明的第六个目的在于提出了一种终端。

[13] 为实现上述目的，根据本发明的第一方面的实施例，提出了一种验证方法，用

于服务器，包括：接收到来自终端的验证请求；接收由终端采集的全息手模型，并对全息手模型中的一个或多个待验证特征进行验证；若一个或多个待验证特征均验证成功，则发出验证通过信号，若一个或多个待验证特征中的任何一个待验证特征验证失败，则发出验证失败信号。

[14] 根据本发明的实施例的一种验证方法，服务器在接收到来自终端的验证请求后，接收全息手模型，根据接收到的全息手模型，可以寻找预留的若干特征进行验证，在验证过程中只有当所有特征的验证都通过时，才认为验证通过，如果其中有一个特征验证失败，则认为验证失败。通过这样的验证方法，因为每次选择的待验证特征可能不同，所以可以在使用过程中不易发生对验证特征的泄露，可以对用户进行较大程度的安全保护，提高用户信息的安全性。

[15] 其中，同时由于每次选择的待验证特征可能不同，所以减少了盗取者通过获取了用户手上的部分特征来通过验证的可能性。例如，盗取者如果只获取了用户的指纹，但是如果在验证过程中，指纹只是待验证特征的其中一个特征，其余抽查的特征还有手指长度，那么在指纹这一特征通过验证后，由于手指长度这一特征没有通过验证，因此盗取者对终端的操作也被拒绝。当然，本领域技术人员应该理解，所选择的特征越多，安全性越高，但是验证需要的资源和所需的时间也必然增加。

[16] 根据本发明的上述实施例的验证方法，还可以具有以下技术特征：

[17] 根据本发明的一个实施例，在接收到来自终端的验证请求之后，还包括：随机建立待验证的手势姿态模型，并将手势姿态模型发送至终端；接收终端采集的用户手势姿态模型，其中用户手势姿态模型为通过采集用户按照手势姿态模型摆放的手势而建立的模型；将手势姿态模型与用户手势姿态模型进行匹配，若匹配失败，则直接发送验证失败信号，若匹配成功，发送验证成功信号，并接收由终端采集的全息手模型，其中，手势姿态模型包括：手心朝上、手心朝下、手指方向、握拳、展开、并拢一根或多根手指和蜷缩一根或多根手指中一项或任意多项组合。

[18] 在该实施例中，服务器在接收到终端有需要验证的请求后，为了加强验证的安全性，会随机建立一个需要验证的手势姿态模型，手势姿态模型发送给终端显

示，同时为了节省资源和时间，用户在对其它手上细节特征验证操作之前，按照终端显示出的手势姿态模型摆放的手势，服务器会接收终端发出的用户摆出的手势，先对手势姿态进行验证，如果手势姿态不匹配，那么直接退出，也不需要浪费系统资源去对其它细节特征进行一一的匹配，如果手势姿态匹配成功，则接收终端采集的全息手模型，并从中选取一定的特征进行匹配。

[19] 其中，由于手势姿态可以有多种，在接收到验证请求之后，在常用的手势姿态中随机选取几种进行组合，将组合后的手势姿态模型发送至终端等待验证，例如：将手心朝上、手指指向左侧、中指与无名指蜷缩以及其余三根手指展开的姿态组合建立一个手势姿态模型，使用者只有通过这种随机组成的手势姿态模型，才可以分配资源对使用者的细节进行验证。

[20] 根据本发明的一个实施例，待验证特征包括：掌纹、一个或多个手指的指纹、一个或多个手指的指宽、一个或多个手指的指长和一个或多个手指关节的位置中一项或任意多项组合。

[21] 在该实施例中，服务器选择的待验证特征并不局限于现有技术的指纹或掌纹，而是包括手的各个方向上的各个特征，采用上述手段可以减少盗取者会将用户的某些常见特征获取到，从而对用户信息的安全造成威胁的可能性。

[22] 本发明第二方面的实施例提供的一种验证方法，用于终端，包括：向服务器发出验证请求；采集用户的全息手模型，并将全息手模型发送给服务器；接收来自服务器的验证成功信号或验证失败信号。

[23] 在该实施例中，在需要对操作进行安全权限的验证时，向服务器发出验证请求，随后对用户的手进行采集，建立一个全息手模型并将此全息手模型发送给服务器，等待服务器进行验证，待验证过后，终端会接收到来自服务器的验证成功信号或验证失败信号，如果接收到验证成功信号，则将允许进行安全权限验证的操作执行，如果接收到验证失败信号，则拒绝执行操作。

[24] 根据本发明的第二方面的实施例，用于终端的验证方法还包括：接收由服务器建立的待验证的手势姿态模型；向用户显示手势姿态模型；采集用户手势姿态模型，其中用户手势姿态模型为通过采集用户按照手势姿态模型摆放的手势而建立的模型；将用户手势姿态模型发送给服务器；以及接收服务器发送的验证

失败信号或验证成功信号。

[25] 在该实施例中，终端可以接收并向用户显示服务器所建立的待验证手势姿态模型，用户按照待验证的手势姿态模型摆出相应姿势，此时终端会对此时用户的手势进行采集，并将采集到的用户手势姿态模型发送给服务器，从而进行验证，在服务器验证之后，终端会接收到相应的验证信号，若接收到验证成功信号则执行待验证的操作，若接收到验证失败信号则拒绝执行待验证的操作，提高用户在操作验证过程中的安全性及可靠性，同时由于终端并不会直接对姿态模型进行验证，也降低了用于终端的验证装置所占据的资源，可以在一定程度上减少终端的成本，提高经济性。

[26] 根据本发明的第二方面的实施例，向用户显示手势姿态模型具体包括：将手势姿态模型建立在虚拟空间中，并在虚拟空间中的预设位置显示手势姿态模型；或将手势姿态模型建立在现实空间中，并在现实空间中的预设位置显示手势姿态模型。

[27] 在该实施例中，终端可以通过VR（即Virtual Reality）技术，将从服务器接收到的手势姿态模型建立在虚拟空间中进行显示，此时用户也通过VR技术看到手势姿态模型的位置，可以避免在用户周围的人观察到需要验证的手势姿态模型，尽管每次终端操作验证，服务器发出的手势姿态模型均不相同，可以减少盗取者可以通过某些手段获得用户的指定手势模型的可能性，进一步的从根本上减少盗取者会在不经用户允许下侵犯用户财产安全和用户信息安全的可能性。

[28] 在替换实施例中，终端也可以通过AR（即Augmented Reality）技术，在接收到由服务器发出的手势姿态模型后，将手势姿态模型显示在现实空间中，此时用户可以根据现实看到的手势姿态模型进行后续操作。采用上述显示方式，不需额外配置辅助显示工具，在现实空间中预设位置，可以快速清晰的观看到所需验证的手势姿态，增强了用户的体验性。

[29] 根据本发明的第二方面的实施例，采集用户的全息手模型，具体包括：在用户的手的位置与手势姿态模型的位置重合时，通过摄像装置对用户的手的特征进行立体采集。

[30] 在该实施例中，在现实空间中或在虚拟空间中，仅需用户的手的位置与手势姿

态模型的预设位置重合时，对用户手的特征进行立体的采集，根据不同的设置对手特征的采集也可以进行不同的选择，在一些安全权限比较低的操作验证中，例如：观看加密信息，仅需采集3个特征进行验证即可；对加密信息进行删除或提取，则需要采集10个特征进行验证。对不同操作根据不同的安全级别可以灵活的设置验证等级，可以降低装置占据的使用资源，延长装置的使用期限。

[31] 本发明第三方面的实施例提供的一种用于服务器的验证装置，包括：接收单元，设置为接收验证请求；验证单元，设置为接收由终端采集的全息手模型，并对全息手模型中的一个或多个待验证特征进行验证；发送单元，若一个或多个待验证特征均验证成功，则发出验证通过信号，若一个或多个待验证特征中的任何一个待验证特征验证失败，则发出验证失败信号。

[32] 根据本发明的实施例的一种验证方法，服务器在接收到来自终端的验证请求后，接收全息手模型，根据接收到的全息手模型，可以寻找预留的若干特征进行验证，在验证过程中只有当所有特征的验证都通过时，才认为验证通过，如果其中有一个特征验证失败，则认为验证失败。通过这样的验证方法，因为每次选择的待验证特征可能不同，所以可以在使用过程中不易发生对验证特征的泄露，可以对用户进行较大程度的安全保护，提高用户信息的安全性。

[33] 其中，同时由于每次选择的待验证特征可能不同，所以减少了盗取者通过获取了用户手上的部分特征来通过验证的可能性。例如，盗取者如果只获取了用户的指纹，但是如果在验证过程中，指纹只是待验证特征的其中一个特征，其余抽查的特征还有手指长度，那么在指纹这一特征通过验证后，由于手指长度这一特征没有通过验证，因此盗取者对终端的操作也被拒绝。当然，本领域技术人员应该理解，所选择的特征越多，安全性越高，但是验证需要的资源和所需的时间也必然增加。

[34] 根据本发明的第三方面的验证装置，还可以具有以下技术特征：

[35] 根据本发明的第三方面的实施例，验证装置还包括：模型建立单元和匹配单元，其中模型建立单元，设置为随机建立待验证的手势姿态模型，并将手势姿态模型发送至终端；接收单元还设置为：接收终端采集的用户手势姿态模型，其中用户手势姿态模型为通过采集用户按照手势姿态模型摆放的手势而建立的模

型；匹配单元，设置为将手势姿态模型与用户手势姿态模型进行匹配，若匹配失败，则直接发送验证失败信号，若匹配成功，发送验证成功信号，并接收由所述终端采集的全息手模型，其中，手势姿态模型包括：手心朝上、手心朝下、手指方向、握拳、展开、并拢一根或多根手指和蜷缩一根或多根手指中一项或任意多项组合。

[36] 在该实施例中，服务器在接收到终端有需要验证的请求后，为了加强验证的安全性，会随机建立一个需要验证的手势姿态模型，手势姿态模型发送给终端显示，同时为了节省资源和时间，用户在对其它手上细节特征验证操作之前，按照终端显示出的手势姿态模型摆放的手势，服务器会接收终端发出的用户摆出的手势，先对手势姿态进行验证，如果手势姿态不匹配，那么直接退出，也不需要浪费系统资源去对其它细节特征进行一一的匹配，如果手势姿态匹配成功，则接收终端采集的全息手模型，并从中选取一定的特征进行匹配。

[37] 其中，由于手势姿态可以有多种，在接收到验证请求之后，在常用的手势姿态中随机选取几种进行组合，将组合后的手势姿态模型发送至终端等待验证，例如：将手心朝上、手指指向左侧、中指与无名指蜷缩以及其余三根手指展开的姿态组合建立一个手势姿态模型，使用者只有通过这种随机组成的手势姿态模型，才可以分配资源对使用者的细节进行验证。

[38] 根据本发明的第三方面的实施例，待验证特征包括：掌纹、一个或多个手指的指纹、一个或多个手指的指宽、一个或多个手指的指长和一个或多个手指关节的位置中一项或任意多项组合。

[39] 在该实施例中，服务器选择的待验证特征并不局限于现有技术的指纹或掌纹，而是包括手的各个方向上的各个特征，采用上述手段可以减少盗取者会将用户的某些常见特征获取到，从而对用户信息的安全造成威胁的可能性。

[40] 本发明第四方面的实施例提供的一种验证装置，用于终端，包括：发送单元，设置为向服务器发出验证请求；采集单元，设置为采集用户的全息手模型，并将全息手模型发送给服务器；以及接收单元，设置为接收来自服务器的验证成功信号或验证失败信号。

[41] 在该实施例中，在需要对操作进行安全权限的验证时，向服务器发出验证请求

，随后对用户的手进行采集，建立一个全息手模型并将此全息手模型发送给服务器，等待服务器进行验证，待验证过后，终端会接收到 来自服务器的验证成功信号或验证失败信号，如果接收到验证成功信号，则将允许进行安全权限验证的操作执行，如果接收到验证失败信号，则拒绝执行操作。

[42] 根据本发明的第四方面的实施例，验证装置还包括：显示单元，其中，接收单元还设置为接收由服务器建立的待验证的手势姿态模型；显示单元，设置为向用户显示手势姿态模型；采集单元还设置为：采集用户手势姿态模型，其中用户手势姿态模型为通过采集用户按照手势姿态模型摆放的手势而建立的模型；发送单元还设置为：将用户手势姿态模型发送给所述服务器；以及接收单元还设置为：接收服务器发送的验证失败信号或验证成功信号。

[43] 在该实施例中，终端可以接收并向用户显示服务器所建立的待验证手势姿态模型，用户按照待验证的手势姿态模型摆出相应姿势，此时终端会对此时用户的手势进行采集，并将采集到的用户手势姿态模型发送给服务器，从而进行验证，在服务器验证之后，终端会接收到相应的验证信号，若接收到验证成功信号则执行待验证的操作，若接收到验证失败信号则拒绝执行待验证的操作，提高用户在操作验证过程中的安全性及可靠性，同时由于终端并不需要直接对姿态模型进行验证，也降低了用于终端的验证装置所占据的资源，可以在一定程度上减少终端的成本，提高经济性。

[44] 根据本发明的第四方面的实施例，显示单元包括：建立子单元，设置为将手势姿态模型建立在虚拟空间中，并在虚拟空间中的预设位置显示手势姿态模型；或设置为将手势姿态模型建立在现实空间中，并在现实空间中的预设位置显示手势姿态模型。

[45] 在该实施例中，终端可以通过VR（即Virtual Reality）技术，将从服务器接收到的手势姿态模型建立在虚拟空间中进行显示，此时用户也通过VR技术看到手势姿态模型的位置，可以避免在用户周围的人观察到需要验证的手势姿态模型，尽管每次终端操作验证，服务器发出的手势姿态模型均不相同，可以减少盗取者可以通过某些手段获得用户的指定手势模型的可能性，进一步的从根本上减少盗取者会在不经用户允许下侵犯用户财产安全和用户信息安全的可能性。

[46] 在替换实施例中，终端也可以通过AR（即Augmented Reality）技术，在接收到由服务器发出的手势姿态模型后，将手势姿态模型显示在现实空间中，此时用户可以根据现实看到的手势姿态模型进行后续操作。采用上述显示方式，不需额外配置辅助显示工具，在现实空间中预设位置，可以快速清晰的观看到所需验证的手势姿态，增强了用户的体验性。

[47] 根据本发明的第四方面的实施例，采集单元具体包括：图像获取子单元，在用户的手的位置与手势姿态模型的位置重合时，对用户的手的特征进行立体采集。

[48] 在该实施例中，在现实空间中或在虚拟空间中，仅需用户的手的位置与手势姿态模型的预设位置重合时，对用户手的特征进行立体的采集，根据不同的设置对手特征的采集也可以进行不同的选择，在一些安全权限比较低的操作验证中，例如：观看加密信息，仅需采集3个特征进行验证即可；对加密信息进行删除或提取，则需要采集10个特征进行验证。对不同操作根据不同的安全级别可以灵活的设置验证等级，可以降低装置占据的使用资源，延长装置的使用期限。

[49] 本发明第五方面的实施例提供的一种服务器，包括第三方面实施例中任一实施例的验证装置。

[50] 本发明第六方面的实施例提供的一种终端，包括第四方面实施例中任一实施例的验证装置。

[51] 本发明的附加方面和优点将在下面的描述中部分给出，部分将从下面的描述中变得明显，或通过本发明的实践了解到。

附图说明

[52] 本发明的上述和/或附加的方面和优点从结合下面附图对实施例的描述中将变得明显和容易理解，其中：

[53] 图1示出了根据本发明的第一实施例的验证方法的流程图；

[54] 图2示出了根据本发明的第二实施例的验证方法的流程图；

[55] 图3示出了根据本发明的第三实施例的验证装置的示意框图；

[56] 图4示出了根据本发明的第四实施例的验证装置的示意框图；

[57] 图5示出了根据本发明的手势姿态模型的示意图；

[58] 图6示出了根据本发明的验证装置的实体装置示意图。

具体实施方式

[59] 为了能够更清楚地理解本发明的上述目的、特征和优点，下面结合附图和具体实施方式对本发明进行进一步的详细描述。需要说明的是，在不冲突的情况下，本申请的实施例及实施例中的特征可以相互组合。

[60] 在下面的描述中阐述了很多具体细节以便于充分理解本发明，但是，本发明还可以采用第三方不同于在此描述的第三方方式来实施，因此，本发明的保护范围并不受下面公开的具体实施例的限制。

[61] 下面结合图1至图4对根据本发明的实施例的终端200、服务器100、验证方法和验证装置进行具体说明。

[62] 如图1所示，根据本发明的实施例，提出了一种验证方法，用于服务器100，包括：接收到来自终端200的验证请求；接收由终端200采集的全息手模型，并对全息手模型中的一个或多个待验证特征进行验证；若一个或多个待验证特征均验证成功，则发出验证通过信号，若一个或多个待验证特征中的任何一个待验证特征验证失败，则发出验证失败信号。

[63] 根据本发明的实施例的一种验证方法，服务器100在接收到来自终端200的验证请求后，接收全息手模型，根据接收到的全息手模型，可以寻找预留的若干特征进行验证，在验证过程中只有当所有特征的验证都通过时，才认为验证通过，如果其中有一个特征验证失败，则认为验证失败。通过这样的验证方法，因为每次选择的待验证特征可能不同，所以可以在使用过程中不易发生对验证特征的泄露，可以对用户进行较大程度的安全保护，提高用户信息的安全性。

[64] 其中，同时由于每次选择的待验证特征可能不同，所以减少了盗取者通过获取了用户手上的部分特征来通过验证的可能性。例如，盗取者如果只获取了用户的指纹，但是如果在验证过程中，指纹只是待验证特征的其中一个特征，其余抽查的特征还有手指长度，那么在指纹这一特征通过验证后，由于手指长度这一特征没有通过验证，因此盗取者对终端200的操作也被拒绝。当然，本领域技术人员应该理解，所选择的特征越多，安全性越高，但是验证需要的资源和所需的时间也必然增加。

[65] 根据本发明的上述实施例的验证方法，还可以具有以下技术特征：

[66] 根据本发明的一个实施例，在所述接收到来自终端200的验证请求之后，还包括：随机建立待验证的手势姿态模型，并将手势姿态模型发送至终端200；接收终端200采集的用户手势姿态模型，其中用户手势姿态模型为通过采集用户按照手势姿态模型摆放的手势而建立的模型；将手势姿态模型与用户手势姿态模型进行匹配，若匹配失败，则直接发送验证失败信号，若匹配成功，发送验证成功信号，并接收由终端200采集的全息手模型，其中，手势姿态模型包括：手心朝上、手心朝下、手指方向、握拳、展开、并拢一根或多根手指和蜷缩一根或多根手指中一项或任意多项组合。

[67] 在该实施例中，服务器100在接收到终端200有需要验证的请求后，为了加强验证的安全性，会随机建立一个需要验证的手势姿态模型，手势姿态模型发送给终端200显示，同时为了节省资源和时间，用户在对其它手上细节特征验证操作之前，按照终端200显示出的手势姿态模型摆放的手势，服务器100会接收终端200发出的用户摆出的手势，先对手势姿态进行验证，如果手势姿态不匹配，那么直接退出，也不需要浪费系统资源去对其它细节特征进行一一的匹配，如果手势姿态匹配成功，则接收终端200采集的全息手模型，并从中选取一定的特征进行匹配。

[68] 如图5所示，其中，由于手势姿态可以有多种，在接收到验证请求之后，在常用的手势姿态中随机选取几种进行组合，将组合后的手势姿态模型发送至终端200等待验证，例如：将手心朝上、手指指向左侧、中指与无名指蜷缩以及其余三根手指展开的姿态组合建立一个手势姿态模型，使用者只有通过这种随机组成的手势姿态模型，才可以分配资源对使用者的细节进行验证。

[69] 根据本发明的一个实施例，待验证特征包括：掌纹、一个或多个手指的指纹、一个或多个手指的指宽、一个或多个手指的指长和一个或多个手指关节的位置中一项或任意多项组合。

[70] 在该实施例中，服务器100选择的待验证特征并不局限于现有技术的指纹或掌纹，而是包括手的各个方向上的各个特征，采用上述手段可以减少盗取者会将用户的某些常见特征获取到，从而对用户信息的安全造成威胁的可能性。

[71] 图2示出了根据本发明的第二实施例的验证方法的流程图

[72] 本发明第二方面的实施例提供的一种验证方法，用于终端200，包括：向服务器100发出验证请求；采集用户的全息手模型，并将全息手模型发送给服务器100；接收来自服务器100的验证成功信号或验证失败信号。

[73] 在该实施例中，在需要对操作进行安全权限的验证时，向服务器100发出验证请求，随后对用户的手进行采集，建立一个全息手模型并将此全息手模型发送给服务器100，等待服务器100进行验证，待验证过后，终端200会接收到 来自服务器100的验证成功信号或验证失败信号，如果接收到验证成功信号，则将允许进行安全权限验证的操作执行，如果接收到验证失败信号，则拒绝执行操作。

[74] 根据本发明的第二方面的实施例，用于终端200的验证方法还包括：接收由服务器100建立的待验证的手势姿态模型；向用户显示手势姿态模型；采集用户手势姿态模型，其中用户手势姿态模型为通过采集用户按照手势姿态模型摆放的手势而建立的模型；将用户手势姿态模型发送给服务器100；以及接收服务器100发送的验证失败信号或验证成功信号。

[75] 在该实施例中，终端200可以接收并向用户显示服务器100所建立的待验证手势姿态模型，用户按照待验证的手势姿态模型摆出相应姿势，此时终端200会对此时用户的手势进行采集，并将采集到的用户手势姿态模型发送给服务器100，从而进行验证，在服务器100验证之后，终端200会接收到相应的验证信号，若接收到验证成功信号则执行待验证的操作，若接收到验证失败信号则拒绝执行待验证的操作，提高用户在操作验证过程中的安全性及可靠性，同时由于终端200并不会直接对姿态模型进行验证，也降低了用于终端200的验证装置所占据的资源，可以在一定程度上减少终端200的成本，提高经济性。

[76] 根据本发明的第二方面的实施例，向用户显示手势姿态模型具体包括：将手势姿态模型建立在虚拟空间中，并在虚拟空间中的预设位置显示手势姿态模型；或将手势姿态模型建立在现实空间中，并在现实空间中的预设位置显示手势姿态模型。

[77] 在该实施例中，终端200可以通过VR（即Virtual Reality）技术，将从服务器100接收到的手势姿态模型建立在虚拟空间中进行显

示，此时用户也通过VR技术看到手势姿态模型的位置，可以避免在用户周围的人观察到需要验证的手势姿态模型，尽管每次终端200操作验证，服务器100发出的手势姿态模型均不相同，可以减少盗取者可以通过某些手段获得用户的指定手势模型的可能性，进一步的从根本上减少盗取者会在不经用户允许下侵犯用户财产安全和用户信息安全的可能性。

[78] 在替换实施例中，终端200也可以通过AR（即Augmented Reality）技术，在接收到由服务器100发出的手势姿态模型后，将手势姿态模型显示在现实空间中，此时用户可以根据现实看到的手势姿态模型进行后续操作。采用上述显示方式，不需额外配置辅助显示工具，在现实空间中预设位置，可以快速清晰的观看到所需验证的手势姿态，增强了用户的体验性。

[79] 根据本发明的第二方面的实施例，采集用户的全息手模型，具体包括：在用户的手的位置与手势姿态模型的位置重合时，通过摄像装置对用户的手的特征进行立体采集。

[80] 在该实施例中，在现实空间中或在虚拟空间中，仅需用户的手的位置与手势姿态模型的预设位置重合时，对用户手的特征进行立体的采集，根据不同的设置对手特征的采集也可以进行不同的选择，在一些安全权限比较低的操作验证中，例如：观看加密信息，仅需采集3个特征进行验证即可；对加密信息进行删除或提取，则需要采集10个特征进行验证。对不同操作根据不同的安全级别可以灵活的设置验证等级，可以降低装置占据的使用资源，延长装置的使用期限。

[81] 图3示出了本发明第三方面实施例的示意框图。

[82] 本发明第三方面的实施例提供了一种用于服务器100的验证装置，包括：接收单元102，设置为接收验证请求；验证单元104，设置为接收由终端200采集的全息手模型，并对全息手模型中的一个或多个待验证特征进行验证；发送单元106，若一个或多个待验证特征均验证成功，则发出验证通过信号，若一个或多个待验证特征中的任何一个待验证特征验证失败，则发出验证失败信号。

[83] 根据本发明的实施例的一种验证方法，服务器100在接收到来自终端200的验证请求后，接收全息手模型，根据接收到的全息手模型，可以寻找预留的若干特征进行验证，在验证过程中只有当所有特征的验证都通过时，才认为验证通过

，如果其中有一个特征验证失败，则认为验证失败。通过这样的验证方法，因为每次选择的待验证特征可能不同，所以可以在使用过程中不易发生对验证特征的泄露，可以对用户进行较大程度的安全保护，提高用户信息的安全性。

[84] 其中，同时由于每次选择的待验证特征可能不同，所以减少了盗取者通过获取了用户手上的部分特征来通过验证的可能性。例如，盗取者如果只获取了用户的指纹，但是如果在验证过程中，指纹只是待验证特征的其中一个特征，其余抽查的特征还有手指长度，那么在指纹这一特征通过验证后，由于手指长度这一特征没有通过验证，因此盗取者对终端200的操作也被拒绝。当然，本领域技术人员应该理解，所选择的特征越多，安全性越高，但是验证需要的资源和所需的时间也必然增加。

[85] 根据本发明的第三方面的验证装置，还可以具有以下技术特征：

[86] 根据本发明的第三方面的实施例，验证装置还包括：模型建立单元108和匹配单元110，其中模型建立单元108，设置为随机建立待验证的手势姿态模型，并将手势姿态模型发送至终端200；接收单元102还设置为：接收终端200采集的用户手势姿态模型，其中用户手势姿态模型为通过采集用户按照手势姿态模型摆放的手势而建立的模型；匹配单元110，设置为将手势姿态模型与用户手势姿态模型进行匹配，若匹配失败，则直接发送验证失败信号，若匹配成功，发送验证成功信号，并接收由所述终端200采集的全息手模型，其中，手势姿态模型包括：手心朝上、手心朝下、手指方向、握拳、展开、并拢一根或多根手指和蜷缩一根或多根手指中一项或任意多项组合。

[87] 在该实施例中，服务器100在接收到终端200有需要验证的请求后，为了加强验证的安全性，会随机建立一个需要验证的手势姿态模型，手势姿态模型发送给终端200显示，同时为了节省资源和时间，用户在对其它手上细节特征验证操作之前，按照终端200显示出的手势姿态模型摆放的手势，服务器100会接收终端200发出的用户摆出的手势，先对手势姿态进行验证，如果手势姿态不匹配，那么直接退出，也不需要浪费系统资源去对其它细节特征进行一一的匹配，如果手势姿态匹配成功，则接收终端200采集的全息手模型，并从中选取一定的特征进行匹配。

[88] 如图5所示，其中，由于手势姿态可以有多种，在接收到验证请求之后，在常用的手势姿态中随机选取几种进行组合，将组合后的手势姿态模型发送至终端200等待验证，例如：将手心朝上、手指指向左侧、中指与无名指蜷缩以及其余三根手指展开的姿态组合建立一个手势姿态模型，使用者只有通过这种随机组成的手势姿态模型，才可以分配资源对使用者的细节进行验证。

[89] 根据本发明的第三方面的实施例，待验证特征包括：掌纹、一个或多个手指的指纹、一个或多个手指的指宽、一个或多个手指的指长和一个或多个手指关节的位置中一项或任意多项组合。

[90] 在该实施例中，服务器100选择的待验证特征并不局限于现有技术的指纹或掌纹，而是包括手的各个方向上的各个特征，采用上述手段可以减少盗取者会将用户的某些常见特征获取到，从而对用户信息的安全造成威胁的可能性。

[91] 图4示出了本发明第四方面实施例的示意框图。

[92] 本发明第四方面的实施例提供了一种用于终端200的验证装置，包括：发送单元202，设置为向服务器100发出验证请求；采集单元204，设置为采集用户的全息手模型，并将全息手模型发送给服务器100；以及接收单元206，设置为接收来自服务器100的验证成功信号或验证失败信号。

[93] 在该实施例中，在需要对操作进行安全权限的验证时，向服务器100发出验证请求，随后对用户的手进行采集，建立一个全息手模型并将此全息手模型发送给服务器100，等待服务器100进行验证，待验证过后，终端200会接收到 来自服务器100的验证成功信号或验证失败信号，如果接收到验证成功信号，则将允许进行安全权限验证的操作执行，如果接收到验证失败信号，则拒绝执行操作。

[94] 根据本发明的第四方面的实施例，验证装置还包括：显示单元208，其中，接收单元206还设置为接收由服务器100建立的待验证的手势姿态模型；显示单元208，设置为向用户显示手势姿态模型；采集单元204还设置为：采集用户手势姿态模型，其中用户手势姿态模型为通过采集用户按照手势姿态模型摆放的手势而建立的模型；发送单元202还设置为：将用户手势姿态模型发送给所述服务器100；以及接收单元206还设置为：接收服务器100发送的验证失败信号或验证成功信号。

[95] 在该实施例中，终端200可以接收并向用户显示服务器100所建立的待验证手势姿态模型，用户按照待验证的手势姿态模型摆出相应姿势，此时终端200会对此时用户的手势进行采集，并将采集到的用户手势姿态模型发送给服务器100，从而进行验证，在服务器100验证之后，终端200会接收到相应的验证信号，若接收到验证成功信号则执行待验证的操作，若接收到验证失败信号则拒绝执行待验证的操作，提高用户在操作验证过程中的安全性及可靠性，同时由于终端200并不会直接对姿态模型进行验证，也降低了用于终端200的验证装置所占据的资源，可以在一定程度上减少终端200的成本，提高经济性。

[96] 根据本发明的第四方面的实施例，显示单元208包括：建立子单元2082，设置为将手势姿态模型建立在虚拟空间中，并在虚拟空间中的预设位置显示手势姿态模型；或设置为将手势姿态模型建立在现实空间中，并在现实空间中的预设位置显示手势姿态模型。

[97] 在该实施例中，终端200可以通过VR（即Virtual Reality）技术，将从服务器100接收到的手势姿态模型建立在虚拟空间中进行显示，此时用户也通过VR技术看到手势姿态模型的位置，可以避免在用户周围的人观察到需要验证的手势姿态模型，尽管每次终端200操作验证，服务器100发出的手势姿态模型均不相同，可以减少盗取者可以通过某些手段获得用户的指定手势模型的可能性，进一步的从根本上减少盗取者会在不经用户允许下侵犯用户财产安全和用户信息安全的可能性。

[98] 在替换实施例中，终端200也可以通过AR（即Augmented Reality）技术，在接收到由服务器100发出的手势姿态模型后，将手势姿态模型显示在现实空间中，此时用户可以根据现实看到的手势姿态模型进行后续操作。采用上述显示方式，不需额外配置辅助显示工具，在现实空间中预设位置，可以快速清晰的观看到所需验证的手势姿态，增强了用户的体验性。

[99] 根据本发明的第四方面的实施例，采集单元204具体包括：图像获取子单元2042，在用户的手的位置与手势姿态模型的位置重合时，对用户的手的特征进行立体采集。

[100] 在该实施例中，在现实空间中或在虚拟空间中，仅需用户的手的位置与手势姿

态模型的预设位置重合时，对用户手的特征进行立体的采集，根据不同的设置对手特征的采集也可以进行不同的选择，在一些安全权限比较低的操作验证中，例如：观看加密信息，仅需采集3个特征进行验证即可；对加密信息进行删除或提取，则需要采集10个特征进行验证。对不同操作根据不同的安全级别可以灵活的设置验证等级，可以降低装置占据的使用资源，延长装置的使用期限。

[101] 根据本发明的实施例的一种服务器100，包括如本发明第三方面实施例中任一实施例提供的一种验证装置。

[102] 根据本发明的实施例的一种终端200，包括如本发明第四方面实施例中任一实施例提供的一种验证装置。

[103] 图5是根据本发明实施例的手势姿态模型。

[104] 如图5所示，终端200从服务器100中接收到如图5中随机一种手势姿态模型，并将此手势姿态模型显示在用户的眼前，此时用户将自己的手放置在所显示的手势姿态模型所处的位置，并摆出相同的手势，此时终端会通过摄像装置将用户手的特征进行立体采集，从而将采集到的特征发送至服务器100中，进行操作的验证。

[105] 为了便于更好地实施本发明实施例的上述用于服务器的验证方法以及用于终端的验证方法，本发明还提供了用于实施上述方法的服务器及终端

[106] 如图6所示，本实施例中的终端200包括：摄像头220、发送端口、立体成像装置222以及接收端口，服务器100包括：处理器102、接收端口以及发送端口。以上各个部件之间均可通过总线或其它方式相连，其中处理器可以是通用处理器或是配制成实施本发明实施例的一个或多个集成电路。其中，通用处理器例如：中央处理器、数字信号处理器或专用集成电路。

[107] 在该实施例中，用户在终端200上操作，当一些操作需要进行验证的时候，终端200向服务器100发送验证请求；

[108] 服务器100的处理器102在接收到验证请求后，随机建立一个待验证的手势姿态模型；

[109] 同时将这个手势姿态模型通过服务器100的发送端口发送给终端200。

[110] 终端200通过自身的立体成像装置222将手势姿态模型显示出来；

[111] 用户按照手势姿态模型显示的位置以及姿势，将用户的手以相同的姿势摆放在模型显示的位置；

[112] 此时终端的摄像头220会将用户的全息手模型进行采集；

[113] 其中，用户的全息手模型的采集参数可以但不局限于手掌宽度，手掌长度，手指类型，手指宽度，手指指纹，掌纹和各个手指的指关节参数。通过采集上述采集参数，

[114] 待采集完毕后，将采集到的全息手模型通过终端200的发送端口发送给服务器100；

[115] 服务器100中的接收端口接收到采集的全息手模型，并由服务器100中处理器102进行验证判断。

[116] 如果处理器102在验证比对过程中验证成功，则允许在终端200上进行操作，否则，则拒绝上述操作。以上结合附图详细说明了本发明的技术方案，本发明提出了一种新的用于服务器或终端的验证方法或验证装置，通过对终端采集到的全息手模型中一个或多个待验证特征进行验证，获得的用户信息更多，从而不仅能提高身份验证的可靠性，还限制了使用终端进行操作的用户权限，为用户的操作提供了一定的安全支持，增强了用户的体验性和安全性。

[117] 在本说明书的描述中，术语“第一”、“第二”仅用于描述的目的，而不能理解为指示或暗示相对重要性；术语“连接”、“安装”、“固定”等均应做广义理解，例如，“连接”可以是固定连接，也可以是可拆卸连接，或一体地连接；可以是直接相连，也可以通过中间媒介间接相连。对于本领域的普通技术人员而言，可以根据具体情况理解上述术语在本发明中的具体含义。

[118] 在本说明书的描述中，术语“一个实施例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或特点包含于本发明的至少一个实施例或示例中。在本说明书中，对上述术语的示意性表述不一定指的是相同的实施例或实例。而且，描述的具体特征、结构、材料或特点可以在任何的一个或多个实施例或示例中以合适的方式结合。

[119] 以上仅为本发明的优选实施例而已，并不用于限制本发明，对于本领域的技术人员来说，本发明可以有各种更改和变化。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。

权利要求书

[权利要求 1] 一种验证方法，用于服务器，其特征在于，包括：

接收到来自终端的验证请求；

接收由所述终端采集的全息手模型，并对所述全息手模型中的一个或多个待验证特征进行验证；

若所述一个或多个待验证特征均验证成功，则发出验证通过信号，若所述一个或多个待验证特征中的任何一个待验证特征验证失败，则发出验证失败信号。

[权利要求 2] 根据权利要求1所述的验证方法，其特征在于，在所述接收到来自终端的验证请求之后，还包括：

随机建立待验证的手势姿态模型，并将所述手势姿态模型发送至所述终端；

接收所述终端采集的用户手势姿态模型，其中所述用户手势姿态模型为通过采集所述用户按照所述手势姿态模型摆放的手势而建立的模型；

将所述手势姿态模型与所述用户手势姿态模型进行匹配，若匹配失败，则直接发送验证失败信号，若匹配成功，发送验证成功信号，并接收由所述终端采集的全息手模型，

其中，所述手势姿态模型包括：手心朝上、手心朝下、手指方向、握拳、展开、并拢一根或多根手指和蜷缩一根或多根手指中一项或任意多项组合。

[权利要求 3] 根据权利要求1或2所述的验证方法，其特征在于，所述待验证特征包括：

掌纹、一个或多个手指的指纹、一个或多个手指的指宽、一个或多个手指的指长和一个或多个手指关节的位置中一项或任意多项组合。

[权利要求 4] 一种验证方法，用于终端，其特征在于，包括：

向服务器发出验证请求；

采集用户的全息手模型，并将所述全息手模型发送给所述服务器；

接收来自所述服务器的验证成功信号或验证失败信号。

[权利要求 5] 根据权利要求4所述的验证方法，其特征在于，还包括：

接收由所述服务器建立的待验证的手势姿态模型；

向所述用户显示所述手势姿态模型；

采集用户手势姿态模型，其中所述用户手势姿态模型为通过采集所述用户按照所述手势姿态模型摆放的手势而建立的模型；

将所述用户手势姿态模型发送给所述服务器；以及

接收所述服务器发送的验证失败信号或验证成功信号。

[权利要求 6] 根据权利要求5所述的验证方法，其特征在于，向所述用户显示所述手势姿态模型具体包括：

将所述手势姿态模型建立在虚拟空间中，并在所述虚拟空间中的预设位置显示所述手势姿态模型；或

将所述手势姿态模型建立在现实空间中，并在现实空间中的预设位置显示所述手势姿态模型。

[权利要求 7] 根据权利要求4至6中任一项所述的验证方法，其特征在于，所述采集用户的全息手模型，具体包括：

在用户的手的位置与所述手势姿态模型的位置重合时，通过摄像装置对所述用户的手的特征进行立体采集。

[权利要求 8] 一种验证装置，用于服务器，其特征在于，包括：

接收单元，设置为接收验证请求；

验证单元，设置为接收由所述终端采集的全息手模型，并对所述全息手模型中的一个或多个待验证特征进行验证；

发送单元，若所述一个或多个待验证特征均验证成功，则发出验证通过信号，若所述一个或多个待验证特征中的任何一个待验证特征验证失败，则发出验证失败信号。

[权利要求 9] 根据权利要求8所述的验证装置，其特征在于，还包括：模型建立

单元和匹配单元，其中

所述模型建立单元，设置为随机建立待验证的手势姿态模型，并将所述手势姿态模型发送至所述终端；

所述接收单元还设置为：接收所述终端采集的用户手势姿态模型，其中所述用户手势姿态模型为通过采集所述用户按照所述手势姿态模型摆放的手势而建立的模型；

所述匹配单元，设置为将所述手势姿态模型与所述用户手势姿态模型进行匹配，若匹配失败，则直接发送验证失败信号，若匹配成功，发送验证成功信号，并接收由所述终端采集的全息手模型，

其中，所述手势姿态模型包括：手心朝上、手心朝下、手指方向、握拳、展开、并拢一根或多根手指和蜷缩一根或多根手指中一项或任意多项组合。

[权利要求 10] 根据权利要求8或9所述的验证装置，其特征在于，所述待验证特征包括：

掌纹、一个或多个手指的指纹、一个或多个手指的指宽、一个或多个手指的指长和一个或多个手指关节的位置中一项或任意多项组合。

[权利要求 11] 一种验证装置，用于终端，其特征在于，包括：

发送单元，设置为向服务器发出验证请求；

采集单元，设置为采集用户的全息手模型，并将所述全息手模型发送给所述服务器；以及

接收单元，设置为接收来自所述服务器的验证成功信号或验证失败信号。

[权利要求 12] 根据权利要求11所述的验证装置，其特征在于，还包括显示单元，其中，

所述接收单元还设置为接收由所述服务器建立的待验证的手势姿态模型；

所述显示单元，设置为向所述用户显示所述手势姿态模型；

所述采集单元还设置为：采集用户手势姿态模型，其中所述用户手势姿态模型为通过采集所述用户按照所述手势姿态模型摆放的手势而建立的模型；

所述发送单元还设置为：将所述用户手势姿态模型发送给所述服务器；以及

所述接收单元还设置为：接收所述服务器发送的验证失败信号或验证成功信号。

[权利要求 13] 根据权利要求12所述的验证装置，其特征在于，所述显示单元包括：

建立子单元，设置为将所述手势姿态模型建立在虚拟空间中，并在所述虚拟空间中的预设位置显示所述手势姿态模型；或

设置为将所述手势姿态模型建立在现实空间中，并在现实空间中的预设位置显示所述手势姿态模型。

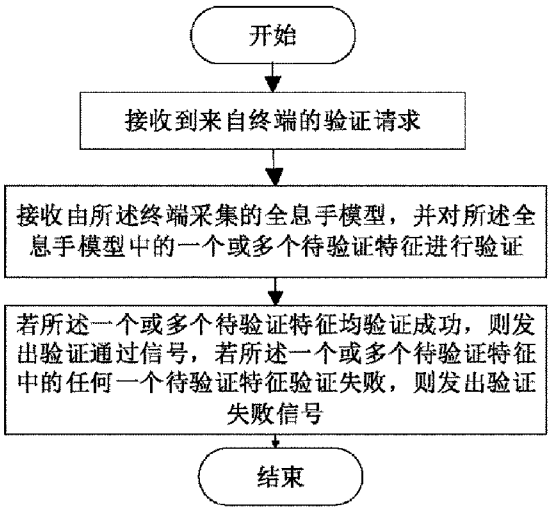
[权利要求 14] 根据权利要求11至13中任一项所述的验证装置，其特征在于，所述采集单元具体包括：

图像获取子单元，在用户的手的位置与所述手势姿态模型的位置重合时，对所述用户的手的特征进行立体采集。

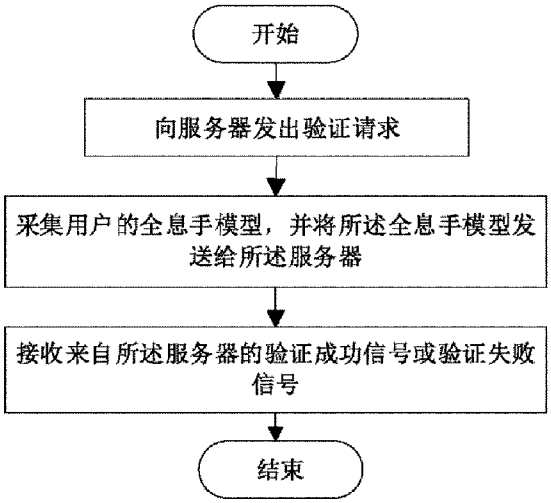
[权利要求 15] 一种服务器，其特征在于，包括根据权利要求8至10中任一项所述的验证装置。

[权利要求 16] 一种终端，其特征在于，包括根据权利要求11至14中任一项所述的验证装置。

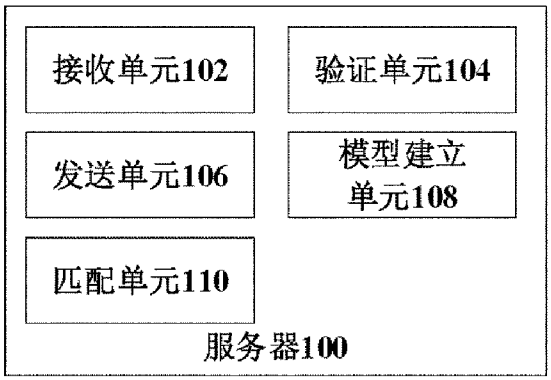
[Fig. 1]


开始
接收到来自终端的验证请求
接收由所述终端采集的全息手模型，并对所述全息手模型中的一个或多个待验证特征进行验证
若所述一个或多个待验证特征均验证成功，则发出验证通过信号，若所述一个或多个待验证特征中的任何一个待验证特征验证失败，则发出验证失败信号
结束

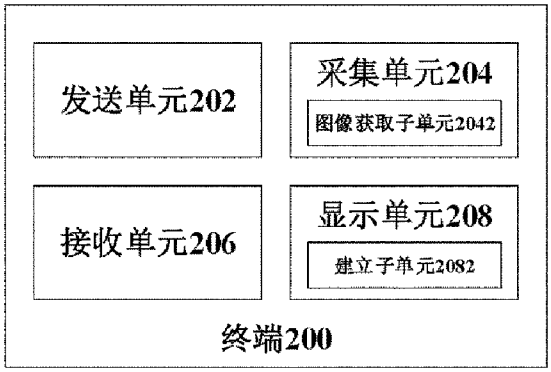
[Fig. 2]


开始
向服务器发出验证请求
采集用户的全息手模型，并将所述全息手模型发送给所述服务器
接收来自所述服务器的验证成功信号或验证失败信号
结束

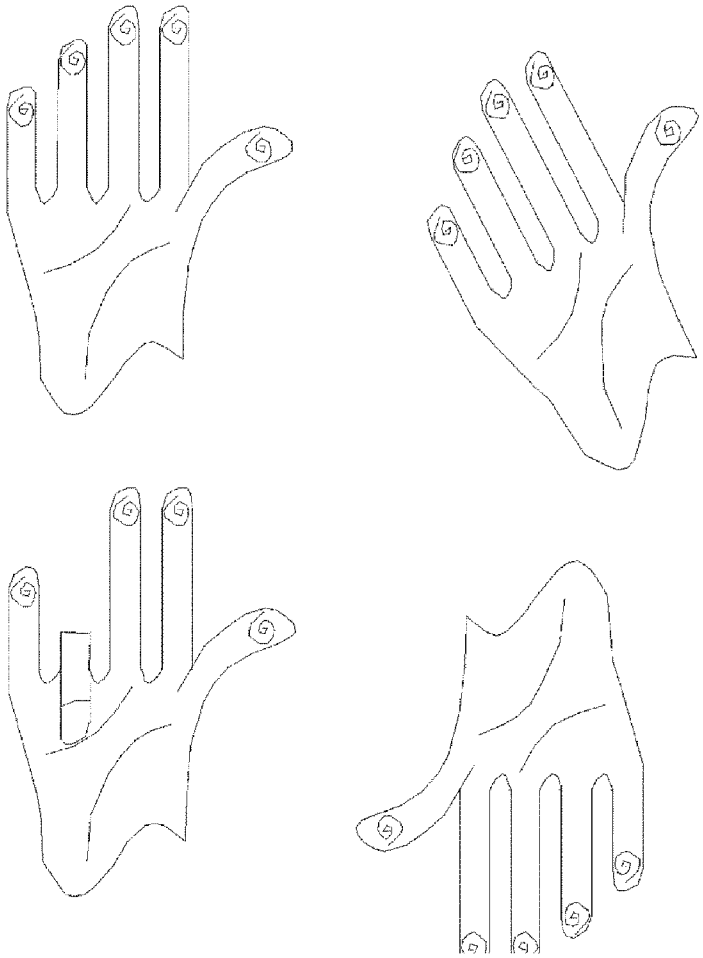
[Fig. 3]



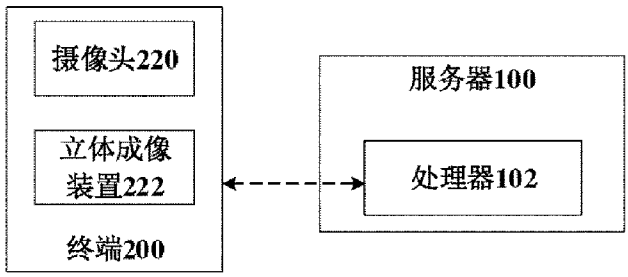
[Fig. 4]


发送单元202
采集单元204
图像获取子单元2042
接收单元206
显示单元208
建立子单元2082
终端200

[Fig. 5]



[Fig. 6]



INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/112772

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (2006.01) 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)

H04L, G06K, 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)

CNPAT; CNKI; WPI; EPODOC; IEEE: 验证, 生物, 特征, 全息, 手, 指纹, 掌纹, 匹配, 随机, 服务器, 客户端, 虚拟现实, authenticate, biometric, holographic, hand, fingerprint, palm, match, random, server, client, Virtual Reality

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 102306286 A (YULONG COMPUTER TELECOMMUNICATION SCIENTIFIC (SHENZHEN) CO., LTD.), 04 January 2012 (04.01.2012), description, paragraphs 0008-0062	1-16
Y	CN 102509387 A (XU, Guoyuan), 20 June 2012 (20.06.2012), description, paragraphs 0004-0027	1-16
Y	CN 101976358 A (XU, Guoyuan), 16 February 2011 (16.02.2011), description, paragraphs 0002-0048	1-16
A	US 2006039049 A1 (CROSS MATCH TECHNOLOGIES), 23 February 2006 (23.02.2006), entire document	1-16

☐ 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	Date of mailing of the international search report
05 April 2017	03 May 2017
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer LIU, Jingwei Telephone No. (86-10) 62413285

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/112772

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 102306286 A	04 January 2012	None	
CN 102509387 A	20 June 2012	None	
CN 101976358 A	16 February 2011	None	
US 2006039049 A1	23 February 2006	US 2006039050 A1	23 February 2006
		US 2006039588 A1	23 February 2006
		US 2006039048 A1	23 February 2006
		US 2006098551 A1	11 May 2006

国际检索报告

国际申请号
PCT/CN2016/112772

A. 主题的分类

H04L 29/06(2006.01)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)

H04L G06K 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））

CNPAT;CNKI;WPI;EPODOC;IEEE: 验证，生物，特征，全息，手，指纹，掌纹，匹配，随机，服务器，客户端，虚拟现实，authenticate, biometric, holographic, hand, fingerprint, palm, match, random, server, client, Virtual Reality

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
Y	CN 102306286 A (宇龙计算机通信科技深圳有限公司) 2012年 1月 4日 (2012-01-04) 说明书第0008-0062段	1-16
Y	CN 102509387 A (徐国元) 2012年 6月 20日 (2012-06-20) 说明书第0004-0027段	1-16
Y	CN 101976358 A (徐国元) 2011年 2月 16日 (2011-02-16) 说明书第0002-0048段	1-16
A	US 2006039049 A1 (CROSS MATCH TECHNOLOGIES) 2006年 2月 23日 (2006-02-23) 全文	1-16

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 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	国际检索报告邮寄日期
2017年 4月 5日	2017年 5月 3日
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局(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 刘静微 电话号码 (86-10)62413285

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2016/112772

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	102306286	A	2012年 1月 4日	无			
CN	102509387	A	2012年 6月 20日	无			
CN	101976358	A	2011年 2月 16日	无			
US	2006039049	A1	2006年 2月 23日	US	2006039050	A1	2006年 2月 23日
				US	2006039588	A1	2006年 2月 23日
				US	2006039048	A1	2006年 2月 23日
				US	2006098551	A1	2006年 5月 11日