(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
2014 年 2 月 20 日 (20.02.2014)

WIPO | PCT

(10) 国际公布号
WO 2014/026442 A1

(51) 国际专利分类号:
H04L 9/32 (2006.01) *G06K 9/00* (2006.01)

(21) 国际申请号: PCT/CN2012/084421

(22) 国际申请日: 2012 年 11 月 10 日 (10.11.2012)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201210285035.5 2012 年 8 月 13 日 (13.08.2012) CN

(71) 申请人 (对除美国外的所有指定国): **鹤山世达光电科技有限公司 (WWTT TECHNOLOGY CHINA)** [CN/CN]; 中国广东省江门市鹤山市共和镇新材料基地鹤山市世逸电子科技有限公司 H 座, Guangdong 529728 (CN)。

(72) 发明人; 及

(71) 申请人 (仅对美国): **王国芳 (WONG, Kwokfong)** [CN/CN]; 中国广东省江门市鹤山市共和镇新材料基地鹤山市世逸电子科技有限公司 H 座, Guangdong 529728 (CN)。 **程佩仪 (CHING, Puiyi)** [CN/CN]; 中国广东省江门市鹤山市共和镇新材料基地鹤山市世逸电子科技有限公司 H 座, Guangdong 529728 (CN)。

(74) 代理人: **佛山东平知识产权事务所（普通合伙） (FOSHAN DONG PING INTELLECTUAL PROPERTY FIRM (GENERAL PARTNERSHIP))**; 中国广东省佛山市禅城区岭南大道北 123 号一座 1508 室, Guangdong 528000 (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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, 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, 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, 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, ML, MR, NE, SN, TD, TG)。

[见续页]

(54) **Title**: IDENTITY AUTHENTICATION DEVICE AND METHOD THEREOF

(54) **发明名称** : 身份认证装置及其方法

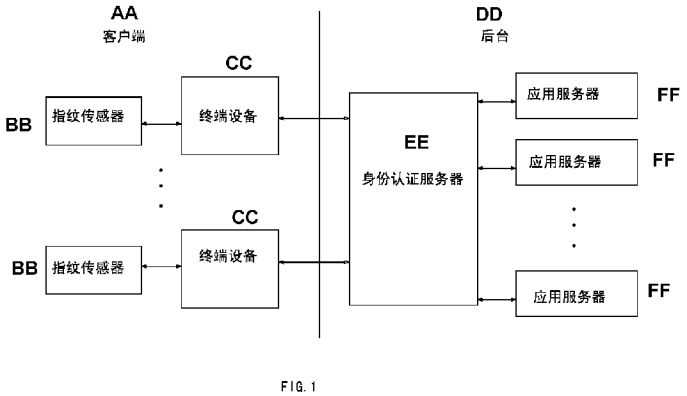

FIG. 1

AA Client
BB Fingerprint sensor
CC Terminal device
DD Background
EE Identity authentication server
FF Application server

(57) **Abstract**: An identity authentication device comprises a client and a background. The client comprises a plurality of terminal devices and fingerprint sensors interactively connected with each terminal device. Each fingerprint sensor comprises a collection recognition device used for collecting fingerprint information and a storage used for storing information including fingerprint information and user information of users corresponding to the fingerprint information. The background comprises an identity authentication server interactively connected with the terminal devices and a plurality of application servers interactively connected with the identity authentication server. The terminal devices are used for registering or determining the fingerprint information received by the finger sensor to recognize a user identity and transferring a registering or determining result to the identity authentication server at the background, and the identity authentication server determines the authority on the plurality of application servers of users according to the result.

(57) **摘要**:

[见续页]

WO 2014/026442 A1

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

一种身份认证装置，它包括客户端以及后台，客户端包括多个终端设备以及分别与每个终端设备相交互连接的指纹传感器，指纹传感器包括用于采集指纹信息的采集识别装置以及用于存储包括指纹信息以及该指纹信息相对应用户的用户信息的存储器，后台包括与终端设备相交互连接的身份认证服务器以及与身份认证服务器相交互连接的多个应用服务器，终端设备用于登记或确认指纹传感器接收到的指纹信息以辨别用户的身份，并将登记或确认的结果传递至后台的身份认证服务器，身份认证服务器根据该结果以决定用户在多个应用服务器上具有的权限。

发明名称: 身份认证装置及其方法

技术领域

[1] 本发明涉及一种身份认证装置和身份认证方法。

背景技术

[2] 目前的社会网络平台可以存储用户名、密码、图片、地址、身份证号码、邮件等用户信息，然而这些信息却不能反映用户的真实身份。

[3] 网络用户可以创建不限数量的网络账户，很多用户常常会因为忘记用户名或者密码而重复创建多个不同的账户，从而造成资源的浪费。

[4] 同时，这不仅仅会引发资源浪费，还可能会对公共安全造成损害。例如，一些网络使用者可能会利用不同的身份信息创建多个虚假账号以提供色情服务或者骗取财物。

对发明的公开

技术问题

[5] 本发明的目的是提供一种身份认证装置及其方法，将指纹生物信息进行归档。由于人的指纹都是唯一的，所以一个人只能在平台上创建一个具有真实身份信息的唯一账号，从而避免和排除安全以及资源浪费问题。

问题的解决方案

技术解决方案

[6] 本发明所采用的技术方案是：一种身份认证装置，它包括客户端以及后台，所述客户端包括多个终端设备以及分别与每个终端设备相交互连接的指纹传感器，所述指纹传感器包括用于采集指纹信息的采集识别装置以及用于存储包括指纹信息以及该指纹信息相对应用户的用户信息的存储器，所述后台包括与终端设备相交互连接的身份认证服务器以及与所述身份认证服务器相交互连接的多个应用服务器，所述终端设备用于登记或确认指纹传感器接收到的指纹信息以辨别用户的身份，并将登记或确认的结果传递至所述后台的身份认证服务器，所述身份认证服务器根据该结果以决定用户在多个应用服务器上具有的权限。

[7] 优选地，所述身份认证服务器包括用于辨别用户身份的用户认证单元以及用于存放注册后的用户信息的用户档案管理单元。

[8] 优选地，每个终端设备上设置有OTP口令，所述用户档案管理单元中设置有OTP种子，所述终端设备在指纹信息确认匹配后，将OTP口令发送至所述身份认证服务器，所述用户认证单元对通过所述用户档案管理单元中的OTP种子对OTP口令进行匹配。

[9] 优选地，每个指纹传感器具有唯一的传感器ID，所述用户档案管理单元中设置有传感器ID档案，在所述终端设备在指纹信息确认匹配后，所述终端设备将指纹传感器的传感器ID传送至所述身份认证服务器，所述身份认证服务器的用户认证单元通过所述用户档案管理单元的传感器ID档案对指纹传感器的传感器ID进行匹配。

[10] 优选地，所述终端设备与所述身份认证服务器、所述身份认证服务器与所述应用服务器通过网络相交互连接。

[11] 一种身份认证的方法，它包括以下步骤：

[12] A）注册阶段：

[13] A1）通过指纹传感器的采集识别装置提取用户的指纹，并生成一对相对应的公匙和私匙；

[14] A2）将私匙存储在指纹传感器的存储器内；

[15] A3）将公匙通过主机传送至身份认证服务器，并将公匙存储在身份认证服务器的同时生成一新的注册用户；

[16] B）认证阶段：

[17] B1）通过指纹传感器的采集识别装置提取用户的指纹信息，终端设备通过存储器进行比对，如果相匹配则进入下一步，如果不相匹配则拒绝进入下一步；

[18] B2）终端设备从存储器中取出私匙，并将私匙传递至身份认证服务器；

[19] B3）身份认证服务器通过公匙对私匙进行匹配以认证用户。

[20] 优选地，在步骤B1）和步骤B2）之间包括一步骤B4），终端设备上设置有OTP口令，身份认证服务器中设置有OTP种子，终端设备在确认指纹信息匹配后，将OTP口令传递至身份认证服务器，身份认证服务器对OTP口令进行匹配。

[21] 优选地，在步骤B1）和步骤B2）之间包括一步骤B5），每个指纹传感器具有唯一的传感器ID，身份认证服务器中设置有传感器ID档案，在终端设备确认指纹信息匹配后，终端设备将指纹传感器的传感器ID传送至身份认证服务器，身份认证服务器对指纹传感器的传感器ID通过传感器ID档案进行匹配。

[22] 优选地，在步骤B3）之后包括一步骤B6），当用户认证成功后，可在多个应用服务器上进行数据的加密或解密。

[23] 优选地，所述终端设备与所述身份认证服务器、所述身份认证服务器与所述应用服务器通过网络相交互连接。

发明的有益效果

有益效果

[24] 本发明采用以上结构或方法具有以下有益效果：

[25] 1、在这个身份认证装置上，用户的身份是唯一且真实的，必要的时候，用户的身份是可追踪的，服务器的用户档案的是不可复制的。

[26] 2、指纹信息储存在当地指纹设备上，且仅为用户自己拥有，因而具有高私密性。

[27] 3、不再单独的使用密码或者指纹进行用户的身份认证，而是采用多因素认证，例如指纹，传感器ID，一次性密码口令（OTP）均须匹配成功才能通过身份认证。

[28] 4、另外这个平台里所有数据都是通过密钥进行保护的，确保了数据的安全。因此在这样的平台上，不仅解决了网络资源的浪费问题，网络的安全性也得到了极大的保证。

对附图的简要说明

附图说明

[29] 附图1为本发明中的身份认证装置的结构示意图。

实施该发明的最佳实施例

本发明的最佳实施方式

[30] 下面结合附图对本发明的较佳实施例进行详细阐述，以使本发明的优点和特征

能更易于被本领域技术人员理解，从而对本发明的保护范围做出更为清楚明确的界定。

[31] 一种身份认证的方法，它包括以下步骤：

[32] A）注册阶段：

[33] 通过指纹传感器的采集识别装置提取用户的指纹，并生成一对相对应的公匙和私匙；

[34] 将私匙存储在指纹传感器的存储器内；

[35] 将公匙通过主机传送至身份认证服务器，并将公匙存储在身份认证服务器的同时生成一新的注册用户；

[36] 发送一个由私匙加密的确认信息；

[37] 利用公匙鉴定发送者的信息。

[38] B）认证阶段：

[39] 通过指纹传感器的采集识别装置提取用户的指纹信息，终端设备通过存储器进行比对，如果相匹配则进入下一步，如果不相匹配则拒绝进入下一步；

[40] 终端设备上设置有OTP口令，身份认证服务器中设置有OTP种子，终端设备在确认指纹信息匹配后，将OTP口令传递至身份认证服务器，身份认证服务器对OTP口令进行匹配。

[41] 每个指纹传感器具有唯一的传感器ID，身份认证服务器中设置有传感器ID档案，在终端设备确认指纹信息匹配后，终端设备将指纹传感器的传感器ID传送至身份认证服务器，身份认证服务器对指纹传感器的传感器ID通过传感器ID档案进行匹配。

[42] 终端设备从存储器中取出私匙，并将私匙传递至身份认证服务器；

[43] 身份认证服务器通过公匙对私匙进行匹配以认证用户。

[44] 当用户认证成功后，可在多个应用服务器上进行数据的加密或解密。

[45] 如附图1所示，一种身份认证装置，它包括客户端以及后台。

[46] 客户端包括多个终端设备以及分别与每个终端设备相交互连接的指纹传感器，指纹传感器包括用于采集指纹信息的采集识别装置以及用于存储包括指纹信息以及该指纹信息相对应用户的用户信息的存储器。

[47] 后台包括与终端设备相交互连接的身份认证服务器以及与所述身份认证服务器相交互连接的多个应用服务器。

[48] 终端设备用于登记或确认指纹传感器接收到的指纹信息以辨别用户的身份，并将登记或确认的结果传递至所述后台的身份认证服务器，所述身份认证服务器根据该结果以决定用户在多个应用服务器上具有的权限

[49] 身份认证服务器包括用于辨别用户身份的用户认证单元以及用于存放注册后的用户信息的用户档案管理单元。

[50] 每个终端设备上设置有OTP口令，所述用户档案管理单元中设置有OTP种子，所述终端设备在指纹信息确认匹配后，将OTP口令发送至所述身份认证服务器，所述用户认证单元对通过所述用户档案管理单元中的OTP种子对OTP口令进行匹配。

[51] 每个指纹传感器具有唯一的传感器ID，所述用户档案管理单元中设置有传感器ID档案，在所述终端设备在指纹信息确认匹配后，所述终端设备将指纹传感器的传感器ID传送至所述身份认证服务器，所述身份认证服务器的用户认证单元通过所述用户档案管理单元的传感器ID档案对指纹传感器的传感器ID进行匹配。

[52] 终端设备与所述身份认证服务器、所述身份认证服务器与所述应用服务器通过网络相交互连接。

[53] 指纹传感器包含存储器和采集识别装置两部分。在用户注册和认证时，该设备提取用户生物指纹数据，连同私钥以及用户的其他信息储存在存储器上。私钥以及其对应的公钥，是根据用户注册的指纹信息所生成的加密和解密的算法。私钥存储在指纹传感器的存储器上，而公钥则被上传到身份认证服务器上。一旦用户身份被服务认证通过，密钥匹配成功则可在不用的应用中进行数据加密和解密。

[54] 终端设备可以是电脑、平板电脑或者手机等。在身份注册和认证中，终端设备负责指纹的登记与确认。同时，一次性口令（OTP）也存储于终端设备中，在指纹确认之后用于身份认证。一次性口令（OTP）在不同的情形生成不同的密码。这样的话，指纹传感设备的ID、一次性口令以及其他被私钥加密的信息一并发

送至到身份认证服务器确认。一旦用户被认证，在服务器的不同应用就可以使用而且数据受加密保护。

[55] 身份认证服务器包括用户认证单元和用户档案管理单元。

[56] 用户认证单元通过匹配主机中的一次性口令、传感器ID、以及解密其他加密信息完成用户的认证。以上信息一旦匹配成功，可以鉴定用户的身份是真实的，而且允许用户使用平台的应用。

[57] 用户档案管理单元管理注册用户的档案。所有档案由系统储存及管理。这些档案包括OTP 种子、传感器ID，指纹数据信息（如注册者的指纹号码）、公钥、用户群以及用户特权等等。这些档案用于进行认证以及不同应用的服务器间的沟通。

[58] 为了使该身份认证装置具有不同的功能，需要许多不同的应用服务器。这些应用服务器可以是邮件、聊天、文件共享等等。身份认证服务器认证用户的真实身份，身份认证装置上的所有用户都是实际注册的那个人。从而注册用户与其他用户安全的交谈。邮件的发件人是被认可的。只有注册用户可以读取他们自己的邮件。此外，身份认证装置的注册用户可以根据身份认证服务器档案里的群组信息与不同的用户组成不同的群。同一群里的人可以共享他们的秘密文件，音乐文件或者视频文件，只有被认证的实际注册的用户才能访问这些文件。因此在这个身份认证装置中，所有的注册用户的身份都是被认可的。

[59] 在这个身份认证装置上，用户的身份是唯一且真实的，必要的时候，用户的身份是可追踪的，服务器的用户档案的是不可复制的。指纹信息储存在当地指纹设备上，且仅为用户自己拥有，因而具有高私密性。不再单独的使用密码或者指纹进行用户的身份认证，而是采用多因素认证，例如指纹，传感器ID，一次性密码口令（OTP）均须匹配成功才能通过身份认证。另外这个平台里所有数据都是通过密钥进行保护的，确保了数据的安全。因此在这样的平台上，不仅解决了网络资源的浪费问题，网络的安全性也得到了极大的保证。

[60] 以上对本发明的特定实施例结合图示进行了说明，很明显，在不离开本发明的范围和精神的基础上，可以对现有技术和工艺进行很多修改。在本发明的所属技术领域中，只要掌握通常知识，就可以在本发明的技术要旨范围内，进行多

种多样的变更

权利要求书

[权利要求 1] 一种身份认证装置，其特征在于，它包括客户端以及后台，所述客户端包括多个终端设备以及分别与每个终端设备相交互连接的指纹传感器，所述指纹传感器包括用于采集指纹信息的采集识别装置以及用于存储包括指纹信息以及该指纹信息相对应用户的用户信息的存储器，所述后台包括与终端设备相交互连接的身份认证服务器以及与所述身份认证服务器相交互连接的多个应用服务器，所述终端设备用于登记或确认指纹传感器接收到的指纹信息以辨别用户的身份，并将登记或确认的结果传递至所述后台的身份认证服务器，所述身份认证服务器根据该结果以决定用户在多个应用服务器上具有的权限。

[权利要求 2] 根据权利要求1所述的身份认证装置，其特征在于：所述身份认证服务器包括用于辨别用户身份的用户认证单元以及用于存放注册后的用户信息的用户档案管理单元。

[权利要求 3] 根据权利要求2所述的身份认证装置，其特征在于：每个终端设备上设置有OTP口令，所述用户档案管理单元中设置有OTP种子，所述终端设备在指纹信息确认匹配后，将OTP口令发送至所述身份认证服务器，所述用户认证单元对通过所述用户档案管理单元中的OTP种子对OTP口令进行匹配。

[权利要求 4] 根据权利要求2所述的身份认证装置，其特征在于：每个指纹传感器具有唯一的传感器ID，所述用户档案管理单元中设置有传感器ID档案，在所述终端设备在指纹信息确认匹配后，所述终端设备将指纹传感器的传感器ID传送至所述身份认证服务器，所述身份认证服务器的用户认证单元通过所述用户档案管理单元的传感器ID档案对指纹传感器的传感器ID进行匹配。

[权利要求 5] 根据权利要求1所述的身份认证装置，其特征在于：所述终端设备与所述身份认证服务器、所述身份认证服务器与所述应用服务器通过网络相交互连接。

[权利要求 6] 一种身份认证的方法，其特征在于，它包括以下步骤：

A）注册阶段：

A1）通过指纹传感器的采集识别装置提取用户的指纹，并生成一对相对应的公匙和私匙；

A2）将私匙存储在指纹传感器的存储器内；

A3）将公匙通过主机传送至身份认证服务器，并将公匙存储在身份认证服务器的同时生成一新的注册用户；

B）认证阶段：

B1）通过指纹传感器的采集识别装置提取用户的指纹信息，终端设备通过存储器进行比对，如果相匹配则进入下一步，如果不相匹配则拒绝进入下一步；

B2）终端设备从存储器中取出私匙，并将私匙传递至身份认证服务器；

B3）身份认证服务器通过公匙对私匙进行匹配以认证用户。

[权利要求 7] 根据权利要求6所述的身份认证方法，其特征在于：在步骤B1）和步骤B2）之间包括一步骤B4），终端设备上设置有OTP口令，身份认证服务器中设置有OTP种子，终端设备在确认指纹信息匹配后，将OTP口令传递至身份认证服务器，身份认证服务器对OTP口令进行匹配。

[权利要求 8] 根据权利要求6所述的身份认证方法，其特征在于：在步骤B1）和步骤B2）之间包括一步骤B5），每个指纹传感器具有唯一的传感器ID，身份认证服务器中设置有传感器ID档案，在终端设备确认指纹信息匹配后，终端设备将指纹传感器的传感器ID传送至身份认证服务器，身份认证服务器对指纹传感器的传感器ID通过传感器ID档案进行匹配。

[权利要求 9] 根据权利要求6所述的身份认证方法，其特征在于：在步骤B3）之后包括一步骤B6），当用户认证成功后，可在多个应用服务器上进行数据的加密或解密。

[权利要求 10] 根据权利要求6所述的身份认证方法，其特征在于：所述终端设备与所述身份认证服务器、所述身份认证服务器与所述应用服务器通过网络相交互连接。

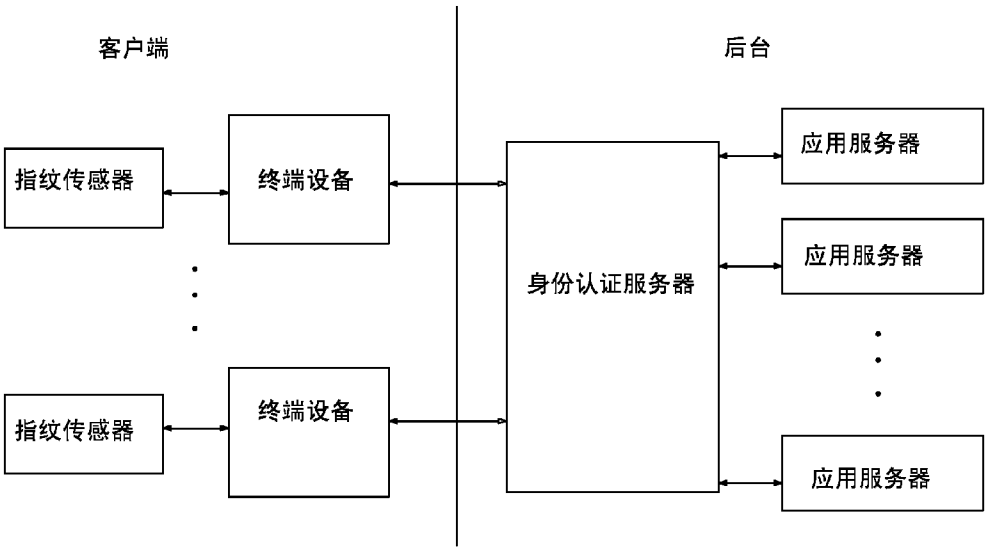

FIG. 1

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2012/084421

A. CLASSIFICATION OF SUBJECT MATTER

See the extra sheet

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)

IPC: H04L, H04W, H04Q, G06K

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)

CNABS, CNTXT, VEN, CNKI: identity authentication, authority, authenticat???, fingerprint, finger mark, collect???, gather???, user, sensor?, OTP

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 101610508 A (HU, Chengjun), 23 December 2009 (23.12.2009), description, page 1, line 21 to page 3, line 10, and figure 1	1-10
X	CN 101034981 A (SHANGHAI PINEWAVE DIGITAL TECHNOLOGY CO., LTD.), 12 September 2007 (12.09.2007), description, page 2, lines 11-37	1-10
PX	CN 102769531 A (HESHAN SHIDA OPTOELECTRONIC SCIENCE & TECHNOLOGY CO., LTD.), 07 November 2012 (07.11.2012), claims 1-10	1-10

☐ 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
28 January 2013 (28.01.2013)	**16 May 2013 (16.05.2013)**
Name and mailing address of the ISA/CN: 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 **YIN, Yue** Telephone No.: (86-10) **62411244**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2012/084421

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 101610508 A	23.12.2009	None	
CN 101034981 A	12.09.2007	None	
CN 102769531 A	07.11.2012	None	

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2012/084421

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32 (2006.01) i

G06K 9/00 (2006.01) i

国际检索报告

国际申请号
PCT/CN2012/084421

A. 主题的分类

参见附加页

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)

IPC: H04L,H04W,H04Q,G06K

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）)

CNABS,CNTXT,VEN,CNKI: 身份认证，指纹，采集，用户，权限，传感器，authenticat???, fingerprint, finger mark, collect???, gather???, user, sensor?, OTP

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
X	CN101610508A(胡承俊) 23.12 月 2009(23.12.2009) 说明书第 1 页第 21 行-第 3 页第 10 行，附图 1	1-10
X	CN101034981A(上海品伟数码科技有限公司) 12.9 月 2007(12.09.2007) 说明书第 2 页第 11-37 行	1-10
PX	CN102769531A(鹤山世达光电科技有限公司) 07.11 月 2012(07.11.2012) 权利要求 1-10	1-10

☐ 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
28.1 月 2013(28.01.2013)	**16.5 月 2013 (16.05.2013)**
ISA/CN 的名称和邮寄地址： 中华人民共和国国家知识产权局 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 殷跃 电话号码：(86-10) **62411244**

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2012/084421

检索报告中引用的专利文件	公布日期	同族专利	公布日期
CN101610508A	23.12.2009	无	
CN101034981A	12.09.2007	无	
CN102769531A	07.11.2012	无	

国际检索报告

国际申请号
PCT/CN2012/084421

A. 主题的分类

H04L9/32(2006.01)i

G06K9/00(2006.01)i