

(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
2017 年 1 月 5 日 (05.01.2017)



(10) 国际公布号
WO 2017/000606 A1

- (51) 国际专利分类号:
G06F 21/31 (2013.01) *H04L 29/06* (2006.01)
- (21) 国际申请号: PCT/CN2016/077974
- (22) 国际申请日: 2016 年 3 月 31 日 (31.03.2016)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201510375714.5 2015 年 6 月 30 日 (30.06.2015) 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: 邓海丰 (DENG, Haifeng); 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: 北京友联知识产权代理事务所(普通合
伙) (YOU LINK INTELLECTUAL PROPERTY
LAW FIRM); 中国北京市海淀区学清路 8 号科技财
富中心 A 座 506 室尚志峰, Beijing 100192 (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, IR, IS,
JP, KE, KG, KN, KP, KR, 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,

[见续页]

(54) Title: SECURE COMMUNICATION METHOD, APPARATUS AND TERMINAL

(54) 发明名称: 安全通信方法、装置和终端

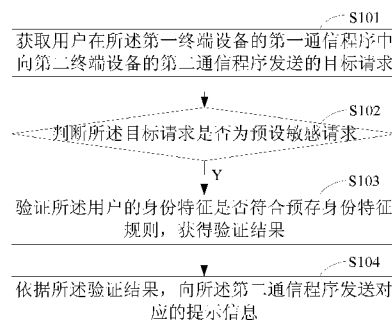


图 1

S101 A TARGET REQUEST SENT BY A USER IN A FIRST COMMUNICATION PROGRAM OF
THE FIRST TERMINAL DEVICE TO A SECOND COMMUNICATION PROGRAM OF A
SECOND TERMINAL DEVICE IS OBTAINED
S102 WHETHER THE TARGET REQUEST IS A PRESET SENSITIVE REQUEST IS DETERMINED
S103 WHETHER THE IDENTITY FEATURE OF THE USER CONFORMS TO A PRESET IDENTITY
FEATURE RULE IS VERIFIED, SO AS TO OBTAIN A VERIFICATION RESULT
S104 ACCORDING TO THE VERIFICATION RESULT, THE CORRESPONDING PROMPT
INFORMATION IS SENT TO THE SECOND COMMUNICATION PROGRAM

(57) Abstract: The present application provides an embodiment of a secure communication method applied to a first terminal device. According to the embodiment, at first, a target request sent by a user in a first communication program of the first terminal device to a second communication program is obtained, and whether the target request is a preset sensitive request is determined; if the determined result indicates that the target request is the preset sensitive request, whether the identity feature of the user conforms to a preset identity feature rule needs to verify; prompt information is sent to the second communication program according to the verification result, so that a second terminal device where the second communication program is located outputs the prompt information and thus the user of the second terminal device can execute subsequent operations according to the prompt information. Apparently, this embodiment enables verification for the identity of a particular user when the user sends the sensitive request to an opposite user, thus ensuring the communication security. The present application also provides a secure communication method applied to a verification server, a secure communication apparatus applied to the first terminal device and applied to the verification server, and a terminal using the secure communication device.

(57) 摘要:

[见续页]



WO 2017/000606 A1

RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, **本国际公布:**
CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, — 包括国际检索报告(条约第 21 条(3))。
TG)。

本申请提供了一种应用在第一终端设备上的安全通信方法实施例，本实施例首先获取用户在第一终端设备的第一通信程序中、向第二通信程序发送的目标请求，并判断该目标请求是否为预设敏感请求，若判断结果为是，则需要验证该用户的身份特征是否符合预设身份特征规则，并根据验证结果，向第二通信程序发送提示信息，以使第二通信程序所在的第二终端设备输出该提示信息，从而，第二终端设备的用户可以根据提示信息执行后续操作。可见，本实施例可以在某位用户向对方用户发送敏感请求时，对该用户的身份进行验证，保证了通信的安全。本申请还提供了应用在验证服务器上的安全通信方法、应用在第一终端设备及应用在验证服务器上的安全通信装置以及使用该安全通信装置的终端。

说明书

安全通信方法、装置和终端

技术领域

本申请涉及通信技术领域，更具体地，是安全通信方法、装置和终端。

背景技术

随着互联网技术的发展，互联网通信已经被广泛应用。人们已经越来越习惯于使用通信工具进行交流，获得了较大的便利，也因此可能会泄露个人。例如，某个用户使用手机中的QQ聊天工具，与对方用户进行通信。双方不用互相见面，便可实现交流，非常方便。但是，若用户为非法用户，使用某合法用户的QQ工具向对方用户请求隐私数据，则可能导致对方用户隐私的泄露，通信过程安全性较低。

发明内容

有鉴于此，本申请提供了应用在第一终端设备上的安全通信方法，用来解决现有的通信方式导致对方用户隐私的泄露，通信过程安全性较低的技术问题。本申请还提供了应用在验证服务器上的安全通信方法。

另外，本申请还提供了应用在第一终端设备上的安全通信装置、及应用在验证服务器上的安全通信装置，用以分别保证上述方法在实际中的应用及实现。

为实现所述目的，本申请提供的技术方案如下：

一种安全通信方法，应用于第一终端设备，该方法包括：

获取用户在所述第一终端设备的第一通信程序中向第二终端设备的第二通信程序发送的目标请求；

判断所述目标请求是否为预设敏感请求；

若是，验证所述用户的身份特征是否符合预存身份特征规则，获得验证结果；

依据所述验证结果，向所述第二通信程序发送对应的提示信息；其中，所述提示信息由所述第二终端设备进行输出。

可选地，上述应用在第一通信终端的安全通信方法中，所述目标请求中包含目标文字；

相应地，所述判断所述目标请求是否为预设敏感请求，包括：

判断所述目标文字中是否包含预设敏感关键字；其中，所述预设敏感关键字存储在预设数据库中。

可选地，上述应用在第一通信终端的安全通信方法中，所述判断所述目标请求是否为预设敏感请求，包括：

判断所述目标请求是否为单向视讯请求。

可选地，上述应用在第一通信终端的安全通信方法中，所述验证所述用户的身份特征是否符合预存身份特征规则，获得验证结果，以及所述依据所述验证结果，向所述第二通信程序发送对应的提示信息，包括：

将所述用户的身份特征发送至验证服务器；其中，所述身份特征以供所述验证服务器对所述身份特征进行验证获得验证结果、以及依据所述验证结果，向所述第二通信程序发送对应的提示信息。

可选地，上述应用在第一通信终端的安全通信方法中，所述验证所述用户的身份特征是否符合预存身份特征规则，获得验证结果，包括：

验证所述用户的虹膜特征是否为预存的虹膜特征，获得验证结果。

本申请还提供了一种安全通信方法，应用于验证服务器，该方法包括：

接收第一通信终端发送的用户身份特征；其中，所述身份特征为：所述第一通信终端获取用户在第一通信程序中向第二终端设备的第二通信程序发送的目标请求后，判断所述目标请求是否为预设敏感请求，在判断结果为是的情况下，向所述验证服务器发送的用户身份特征；

验证所述用户身份特征是否符合预存身份特征规则，获得验证结果；

依据所述验证结果，向所述第二通信程序发送对应的提示信息；其中，所述提示信息由所述第二终端设备进行输出。

可选地，上述应用在验证服务器的安全通信方法还包括：

向所述第一通信程序发送所述提示信息；其中，所述提示信息由所述第一终端设备进行输出。

可选地，上述应用在验证服务器的安全通信方法还包括：

响应于接收到的所述用户身份信息，向所述第二终端设备发送等待提示信息；其中，所述等待提示信息用于提示正在进行身份验证。

本申请还提供了一种安全通信装置，应用于第一终端设备，该装置包括：

目标请求获取模块，用于获取用户在所述第一终端设备的第一通信程序中向第二终端设备的第二通信程序发送的目标请求；

目标请求判断模块，用于判断所述目标请求是否为预设敏感请求；若是，触发身份特征验证模块；

第一身份特征验证模块，用于验证所述用户的身份特征是否符合预存身份特征规则，获得验证结果；

第一提示信息发送模块，用于依据所述验证结果，向所述第二通信程序发送对应的提示信息；其中，所述提示信息由所述第二终端设备进行输出。

本申请还提供了一种安全通信装置，应用于验证服务器，该装置包括：

身份特征接收模块，用于接收第一通信终端发送的用户身份特征；其中，所述身份特征为：所述第一通信终端获取用户在第一通信程序中向第二终端设备的第二通信程序发送的目标请求后，判断所述目标请求是否为预设敏感请求，在判断结果为是的情况下，向所述验证服务器发送的用户身份特征；

第二身份特征验证模块，用于验证所述用户身份特征是否符合预存身份特征规则，获得验证结果；

第二提示信息发送模块，用于依据所述验证结果，向所述第二通信程序发送对应的提示信息；其中，所述提示信息由所述第二终端设备进行输出。

由以上可知，本申请提供的应用在第一终端设备上的安全通信方法实施例，首先获取用户在第一终端设备的第一通信程序中、向第二通信程序发送的目标请求，并判断该目标请求是否为预设敏感请求，若判断结果为是，则需要验证该用户的身份特征是否符合预设身份特征规则，并根据验证结果，向第二通信程序发送提示信息，以使第二通信程序所在的第二终端设备输出该提示信息，从而，第二终端设备的用户可以根据提示信息执行后续操作。可见，本实施例可以在某位用户向对方用户发送敏感请求时，对该用户的身份进行验证，保证了通信的安全。

本申请还提供了一种终端，包括如上述任一技术方案所述的安全通信装

置。

当然，实施本申请的任一产品并不一定需要同时达到以上所述的所有优点。

附图说明

为了更清楚地说明本申请实施例或现有技术中的技术方案，下面将对实施例或现有技术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申请的实施例，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，还可以根据提供的附图获得其他的附图。

图1为本申请提供的应用在第一终端设备上的安全通信方法实施例的流程图；

图2为本申请提供的应用在验证服务器上的安全通信方法实施例1的流程图；

图3为本申请提供的应用在验证服务器上的安全通信方法实施例2的流程图；

图4为本申请提供的应用在第一终端设备上的安全通信装置实施例的结构框图；

图5为本申请提供的应用在验证服务器上的安全通信装置实施例1的结构框图；

图6为本申请提供的应用在验证服务器上的安全通信装置实施例2的结构框图；

图7是本申请提供的一种终端结构框图。

具体实施方式

下面将结合本申请实施例中的附图，对本申请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。

参照图1，其示出了应用在第一终端设备上的安全通信方法实施例的流程。如图1所示，该实施例可以具体包括步骤S101~步骤S104。

步骤 S101: 获取用户在所述第一终端设备的第一通信程序中向第二终端设备的第二通信程序发送的目标请求。

其中，第一终端设备可以是手机、平板电脑及便携式计算机等移动终端，或者，也可以是台式计算机等。第一终端设备上安装有通信程序，称为第一通信程序，第一通信程序可以是 QQ、微信等聊天程序。

用户可以在第一通信程序中发送请求，为了便于描述，将该请求称为目标请求。目标请求是向第二通信程序发送的，该第二通信程序安装在第二终端设备中。同理，第二终端设备可以是手机、平板电脑及便携式计算机等移动终端，或者，也可以是台式计算机等。例如，用户 A 在终端设备 1 中的 QQ 程序中，向终端设备 2 中的 QQ 程序发送目标请求。

步骤 S102: 判断所述目标请求是否为预设敏感请求；若是，执行步骤 S103。

在实施前，预先存储敏感请求，为了便于描述，称为预设敏感请求。预设敏感请求表明用户触发的是与用户隐私相关的请求，例如，发送银行卡号、请求身份证号、请求密码等。

预设敏感请求，可以用来验证用户发送的目标请求是否安全。具体地，判断目标请求是否为预设敏感请求。若是，表明用户正在利用第一通信程序进行与其他用户隐私相关的操作。例如，发送银行卡号，希望对方用户向该银行卡内汇钱，或者，询问身份证号码，或者询问对方用户某些账号的密码。

此种情况下，为了保证通信安全，需要对发送目标请求的用户的身分进行验证，具体验证方式如下所述。

步骤 S103: 验证所述用户的身分特征是否符合预存身分特征规则，获得验证结果。

在实施前，预先存储有身分特征规则，为了便于描述，称为预存身分特征规则。本步骤的具体实现方式为，若上述步骤 S102 判断得出目标请求为预设敏感请求，则提示用户输入身分特征，采集用户输入的身分特征，并验证该身分特征是否符合预存身分特征规则。

可选地，预存身分特征规则可以是密码规则，即预先录入的密码；或者，还可以是生物特征规则，如预先录入的指纹特征、声纹特征或虹膜特征等。

根据预存身份特征规则的类型，采集用户对应的身份特征，如采集用户输入的密码、采集用户输入的指纹、声纹或者虹膜等。

对采集身份特征进行验证后，获得验证结果。

步骤 S104：依据所述验证结果，向所述第二通信程序发送对应的提示信息；其中，所述提示信息由所述第二终端设备进行输出。

若验证结果为成功，表明用户的身份特征符合预存身份特征规则，则向第二通信程序发送成功的提示信息。相反，若验证结果为失败，表明用户的身份特征不符合预存身份特征规则，则向第二通信程序发送失败的提示信息。

可选地，提示信息可以是文字、声音或图片等形式。

第二终端设备输出提示信息后，以提示用户执行对应操作。例如，若提示信息为成功，则提示用户可以正常执行后续操作；若提示信息为失败，则提示用户可以中断与第一通信终端的通信过程。

由以上的技术方案可知，本申请提供的应用在第一终端设备上的安全通信方法实施例，首先获取用户在第一终端设备的第一通信程序中、向第二通信程序发送的目标请求，并判断该目标请求是否为预设敏感请求，若判断结果为是，则需要验证该用户的身份特征是否符合预设身份特征规则，并根据验证结果，向第二通信程序发送提示信息，以使第二通信程序所在的第二终端设备输出该提示信息，从而，第二终端设备的用户可以根据提示信息执行后续操作。可见，本实施例可以在某位用户向对方用户发送敏感请求时，对该用户的身份进行验证，保证了通信的安全。

在实际应用中，用户使用通信程序发送的目标请求可能是文字类型的请求。例如，用户A利用QQ程序与用户B聊天时，输入文字“请提供身份证号”或“这是银行卡号”。在这种场景中，上述实施例中步骤S102判断所述目标请求是否为预设敏感请求的具体实现方式包括步骤A1。

步骤A1：判断所述目标文字中是否包含预设敏感关键字；其中，所述预设敏感关键字存储在预设数据库中。

在实施前，可以预先设置有数据库，存储若干个关键字，如“身份证号”、“密码”、“银行卡号”及“汇款”等。存储的关键字可以称为预设敏感关键字，预设敏感关键字可表示用户发送的敏感请求。

为了便于描述，将目标请求中包含的文字称为目标文字。判断目标文字是否包含预设敏感关键字的方式可以是，对目标文字进行分词操作，获得若干个分词，将分词分别与预设敏感关键字进行匹配。若存在相匹配的分词，则表明目标文字中包含预设敏感关键字，若不存在相匹配的分词，则表明目标文字中并未包含预设敏感关键字。

另外，用户使用通信程序发送的目标请求还可能是请求与对方进行视讯。若该用户并不是该通信程序的合法用户，则可能想要窥探对方隐私。此种情况下，需要请求视讯请求的用户进行身份验证。进而，上述实施例中步骤S102判断所述目标请求是否为预设敏感请求的具体实现方式包括步骤B1。

步骤B1：判断所述目标请求是否为单向视讯请求。

其中，若用户在通信程序中触发视讯请求操作，如点击视讯请求图标，该目标请求则为视讯请求。

在实际应用中，由于合法用户可能经常使用视讯请求，若对每个视讯请求均进行身份验证，会使合法用户的操作较为繁琐。非法用户发送视讯请求的情况，可能具有某些特征。具体地：合法用户刚刚使用终端设备进行完毕视讯，非法用户便获得终端设备，想再次发起与视讯对方的请求，该请求是单方的，即只请求对方使用摄像头但本方并不使用。此时，视讯对方可能由于刚刚进行完毕视讯，大意地接受该视讯请求，从而泄露隐私。

因此，本步骤中的该视讯请求可以是有限制条件的视讯请求，即该视讯请求是与上次视讯请求间隔预设时间段、且单向的视讯请求。其中，预设时间段为较短的时间段，如5分钟内的任意时间段。当然，该数值仅仅是一个示例，根据实际应用设置的任意较短时间段均在本申请的保护范围内。

上述实施例中步骤S103验证用户身份特征是否符合预存身份特征规则以及步骤S104依据所述验证结果向所述第二通信程序发送对应的提示信息，可以并非全部在第一终端设备中执行。具体的实现方式可以是：

将用户的身份特征发送至验证服务器，以供所述验证服务器对身份特征进行验证获得验证结果、以及依据所述验证结果，向所述第二通信程序发送对应的提示信息。

其中，设置有验证服务器，验证服务器中预存有身份特征规则。第一终

端设备将用户的身份特征发送至验证服务器，验证服务器对身份特征进行验证，进而获得验证结果，验证服务器根据验证结果，直接向第二通信程序发送提示信息。

该种实现方式中，身份验证规则预存在验证服务器中，相较于预存在第一终端设备中，安全性更高。

本申请中的预存身份特征规则可以是用户的身份特征，例如，指纹特征、声纹特征及虹膜特征。在预存身份特征规则为虹膜特征的情况下，上述实施例步骤S103验证所述用户的身份特征是否符合预存身份特征规则的具体实现方式为：

验证所述用户的虹膜特征是否为预存的虹膜特征，获得验证结果。

其中，虹膜特征作为生物特征，具有唯一性，可以利用虹膜特征辨识不同的用户。采集用户的虹膜特征，将采集的虹膜特征与预存的虹膜特征进行比对，比对方法可以是现有技术中任意一种虹膜比对方法，从而利用虹膜实现对用户身份的验证。

与上述应用在第一终端设备的安全通信方法相对应，本申请还提供了应用在验证服务器上的安全通信方法实施例。如图2所示，应用在验证服务器上的安全通信方法实施例1的具体流程可以包括步骤S201~步骤S203。

步骤 S201：接收第一通信终端发送的用户身份特征；其中，所述身份特征为：所述第一通信终端获取用户在第一通信程序中向第二终端设备的第二通信程序发送的目标请求后，判断所述目标请求是否为预设敏感请求，在判断结果为是的情况下，向所述验证服务器发送的用户身份特征。

其中，用户在第一通信终端中安装的第一通信程序中，向第二终端设备的第二通信程序发送目标请求，第一通信终端判断该目标请求是否为预设敏感请求，并在判断结果为是的情况下，采集用户的身份特征，并向验证服务器发送。进而，验证服务器接收该第一通信终端发送的用户身份特征。

步骤 S202：验证所述用户身份特征是否符合预存身份特征规则，获得验证结果。

其中，验证服务器验证用户身份特征是否符合预存身份特征规则。可选地，第一通信终端发送的用户身份特征可以是虹膜特征，验证服务器验证接收到的虹膜特征是否与预存虹膜特征匹配。

需要说明的是，预存身份特征规则是，该第一通信终端的合法用户预存的身份特征规则。验证结果为成功，表明用户为合法用户；验证结果为失败，表明用户为非法用户。

步骤S203：依据所述验证结果，向所述第二通信程序发送对应的第二提示信息；其中，所述第二提示信息由所述第二终端设备进行输出。

第二终端设备输出提示信息，以提示使用该第二终端设备的用户，接收到的该第一终端设备发送的目标请求是否为合法用户发送的请求。

由以上的技术方案可知，验证服务器可以是对第一终端设备发送的用户身份信息验证，并对第二终端设备进行提示。

验证服务器根据验证结果，生成提示信息。验证服务器除了向第二通信程序发送该提示信息外，还可以向第一通信程序发送，以提示第一通信程序验证结果。

参照图3，其示出了本申请提供的应用在验证服务器上的安全通信方法实施例2的流程。如图3所示，安全通信方法实施例2在上述图2所示的安全通信方法实施例1的基础上，还可以包括步骤S204。

步骤S204：向所述第一通信程序发送所述提示信息；其中，所述提示信息由所述第一终端设备进行输出。

若第一通信程序的用户为非法用户，则验证结果生成的提示信息为失败，合法用户查看到该提示信息后，可以知晓曾经有非法用户使用该第一通信程序进行非法操作，从而提高警惕。

用户向第二通信程序发送目标请求后，本实施对目标请求及用户身份进行验证，此时，可以向第二通信程序发送等待提示消息，以提示第二通信程序的用户正在进行身份验证，可以等待验证结果后再进行后续操作。

如图3所示，安全通信方法实施例2还可以包括步骤S205。

步骤S205：响应于接收到的所述用户身份信息，向所述第二终端设备发

送等待提示信息；其中，所述等待提示信息用于提示正在进行身份验证。

其中，验证服务器接收到用户身份信息，则可以向第二终端设备发送提示信息，为了便于与上文的提示信息进行区分，将该提示信息称为等待提示信息。等待提示信息用于提示第二终端设备的用户：当前正在对第一终端设备的用户进行身份验证，可以等待身份验证结果后，再进行后续操作。

下面对本申请提供的应用在第一终端设备的安全通信装置及应用在验证服务器的安全通信装置进行介绍，需要说明的是，有关安全通信装置的说明可以参照上文的安全通信方法，以下并不赘述。

参照图4，其示出了应用在第一终端设备的安全通信装置实施例的结构。如图4所示，该安全通信装置实施例可以包括：目标请求获取模块401、目标请求判断模块402、第一身份特征验证模块403及第一提示信息发送模块404；其中：

目标请求获取模块 401，用于获取用户在所述第一终端设备的第一通信程序中向第二终端设备的第二通信程序发送的目标请求；

目标请求判断模块 402，用于判断所述目标请求是否为预设敏感请求；若是，触发身份特征验证模块；

第一身份特征验证模块 403，用于验证所述用户的身份特征是否符合预存身份特征规则，获得验证结果；

第一提示信息发送模块404，用于依据所述验证结果，向所述第二通信程序发送对应的提示信息；其中，所述提示信息由所述第二终端设备进行输出。

可选地，所述目标请求中包含目标文字；相应地，所述目标请求判断模块 402 可以包括：第一目标请求判断子模块，用于判断所述目标文字中是否包含预设敏感关键字；其中，所述预设敏感关键字存储在预设数据库中。

可选地，所述目标请求判断模块 402 可以包括：第一目标请求判断子模块，用于判断所述目标请求是否为单向视讯请求。

可选地，所述第一身份特征验证模块 403 以及所述第一提示信息发送模块 404 的具体实现方式可以是：

身份特征发送子模块，用于将所述用户的身份特征发送至验证服务器；其中，所述身份特征以供所述验证服务器对所述身份特征进行验证获得验证结果、以及依据所述验证结果，向所述第二通信程序发送对应的提示信息。

可选地，所述第一身份特征验证模块 403 可以包括：

虹膜特征验证子模块，用于验证所述用户的虹膜特征是否为预存的虹膜特征，获得验证结果。

参照图 5，其示出了应用在验证服务器的安全通信装置实施例 1 的结构。如图 5 所示，该安全通信装置实施例 1 可以包括：身份特征接收模块 501、第二身份特征验证模块 502 及第二提示信息发送模块 503；其中：

身份特征接收模块 501，用于接收第一通信终端发送的用户身份特征；其中，所述身份特征为：所述第一通信终端获取用户在第一通信程序中向第二终端设备的第二通信程序发送的目标请求后，判断所述目标请求是否为预设敏感请求，在判断结果为是的情况下，向所述验证服务器发送的用户身份特征；

第二身份特征验证模块 502，用于验证所述用户身份特征是否符合预存身份特征规则，获得验证结果；

第二提示信息发送模块 503，用于依据所述验证结果，向所述第二通信程序发送对应的提示信息；其中，所述提示信息由所述第二终端设备进行输出。

参照图 6，其示出了应用在验证服务器的安全通信装置实施例 2 的结构。如图 6 所示，安全通信装置实施例 2 在安全通信装置实施例 1 的基础上，还可以包括：第三提示信息发送模块 504 及

第三提示信息发送模块 504，用于向所述第一通信程序发送所述提示信息；其中，所述提示信息由所述第一终端设备进行输出。

等待提示信息发送模块 505，用于响应于接收到的所述用户身份信息，向所述第二终端设备发送等待提示信息；其中，所述等待提示信息用于提示正在进行身份验证。

参照图 7，其示出了一种终端的结构。本发明还提供了一种终端 600，包括如上述任一技术方案所述的安全通信装置。

需要说明的是，本说明书中的各个实施例均采用递进的方式描述，每个实施例重点说明的都是与其他实施例的不同之处，各个实施例之间相同相似的部分互相参见即可。

还需要说明的是，在本文中，诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物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、物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，并不排除在包括上述要素的过程、方法、物品或者设备中还存在另外的相同要素。

对所公开的实施例的上述说明，使本领域专业技术人员能够实现或使用本申请。对这些实施例的多种修改对本领域的专业技术人员来说将是显而易见的，本文中所定义的一般原理可以在不脱离本申请的精神或范围的情况下，在其它实施例中实现。因此，本申请将不会被限制于本文所示的这些实施例，而是要符合与本文所公开的原理和新颖特点相一致的最宽的范围。

权 利 要 求 书

1、一种安全通信方法，其特征在于，应用于第一终端设备，该方法包括：
获取用户在所述第一终端设备的第一通信程序中向第二终端设备的第二通信程序发送的目标请求；

判断所述目标请求是否为预设敏感请求；

若是，验证所述用户的身份特征是否符合预存身份特征规则，获得验证结果；

依据所述验证结果，向所述第二通信程序发送对应的提示信息；其中，所述提示信息由所述第二终端设备进行输出。

2、根据权利要求1所述的安全通信方法，其特征在于，所述目标请求中包含目标文字；

相应地，所述判断所述目标请求是否为预设敏感请求，包括：

判断所述目标文字中是否包含预设敏感关键字；其中，所述预设敏感关键字存储在预设数据库中。

3、根据权利要求1所述的安全通信方法，其特征在于，所述判断所述目标请求是否为预设敏感请求，包括：

判断所述目标请求是否为单向视讯请求。

4、根据权利要求1所述的安全通信方法，其特征在于，所述验证所述用户的身份特征是否符合预存身份特征规则，获得验证结果，以及所述依据所述验证结果，向所述第二通信程序发送对应的提示信息，包括：

将所述用户的身份特征发送至验证服务器；其中，所述身份特征以供所述验证服务器对所述身份特征进行验证获得验证结果、以及依据所述验证结果，向所述第二通信程序发送对应的提示信息。

5、根据权利要求1-4任意一项所述的安全通信方法，其特征在于，所述验证所述用户的身份特征是否符合预存身份特征规则，获得验证结果，包括：

验证所述用户的虹膜特征是否为预存的虹膜特征，获得验证结果。

6、一种安全通信方法，其特征在于，应用于验证服务器，该方法包括：

接收第一通信终端发送的用户身份特征；其中，所述身份特征为：所述第一通信终端获取用户在第一通信程序中向第二终端设备的第二通信程序发

送的目标请求后,判断所述目标请求是否为预设敏感请求,在判断结果为是的情况下,向所述验证服务器发送的用户身份特征;

验证所述用户身份特征是否符合预存身份特征规则,获得验证结果;

依据所述验证结果,向所述第二通信程序发送对应的提示信息;其中,所述提示信息由所述第二终端设备进行输出。

7、根据权利要求6所述的安全通信方法,其特征在于,还包括:

向所述第一通信程序发送所述提示信息;其中,所述提示信息由所述第一终端设备进行输出。

8、根据权利要求6或7所述的安全通信方法,其特征在于,还包括:

响应于接收到的所述用户身份信息,向所述第二终端设备发送等待提示信息;其中,所述等待提示信息用于提示正在进行身份验证。

9、一种安全通信装置,其特征在于,应用于第一终端设备,该装置包括:

目标请求获取模块,用于获取用户在所述第一终端设备的第一通信程序中向第二终端设备的第二通信程序发送的目标请求;

目标请求判断模块,用于判断所述目标请求是否为预设敏感请求;若是,触发身份特征验证模块;

第一身份特征验证模块,用于验证所述用户的身份特征是否符合预存身份特征规则,获得验证结果;

第一提示信息发送模块,用于依据所述验证结果,向所述第二通信程序发送对应的提示信息;其中,所述提示信息由所述第二终端设备进行输出。

10、一种安全通信装置,其特征在于,应用于验证服务器,该装置包括:

身份特征接收模块,用于接收第一通信终端发送的用户身份特征;其中,所述身份特征为:所述第一通信终端获取用户在第一通信程序中向第二终端设备的第二通信程序发送的目标请求后,判断所述目标请求是否为预设敏感请求,在判断结果为是的情况下,向所述验证服务器发送的用户身份特征;

第二身份特征验证模块,用于验证所述用户身份特征是否符合预存身份特征规则,获得验证结果;

第二提示信息发送模块,用于依据所述验证结果,向所述第二通信程序发送对应的提示信息;其中,所述提示信息由所述第二终端设备进行输出。

11、一种终端,其特征在于,包括如权利要求9所述的安全通信装置。

说明书附图

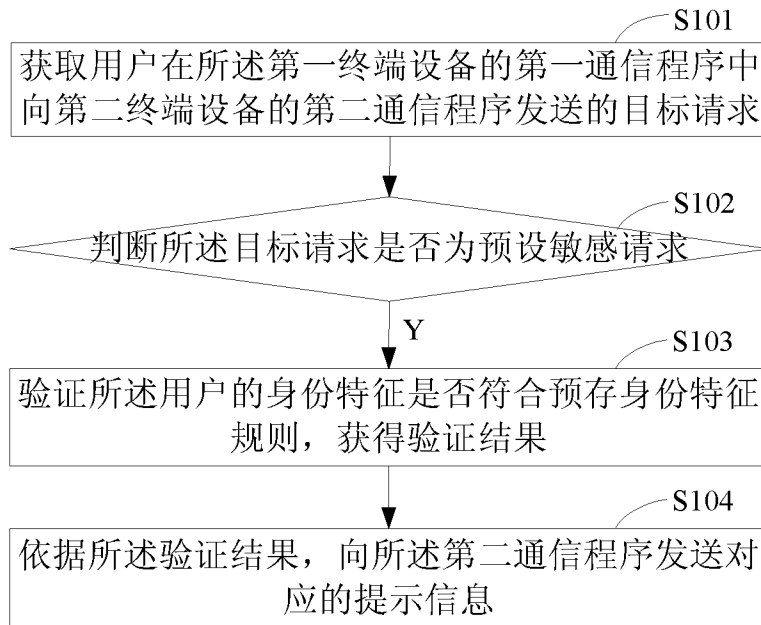


图 1

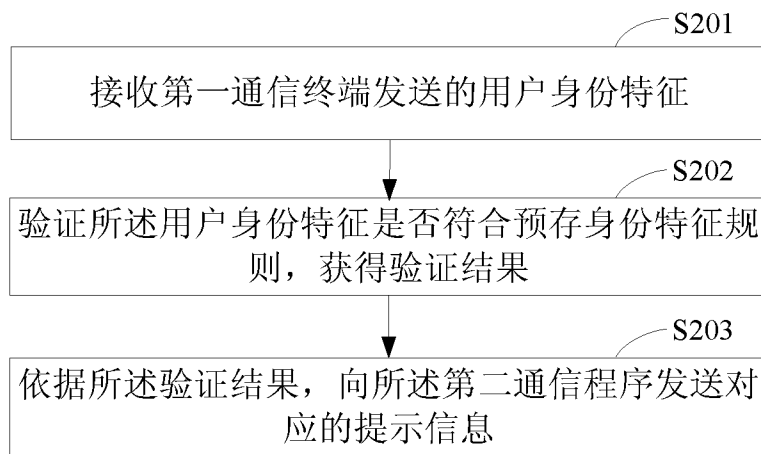


图 2

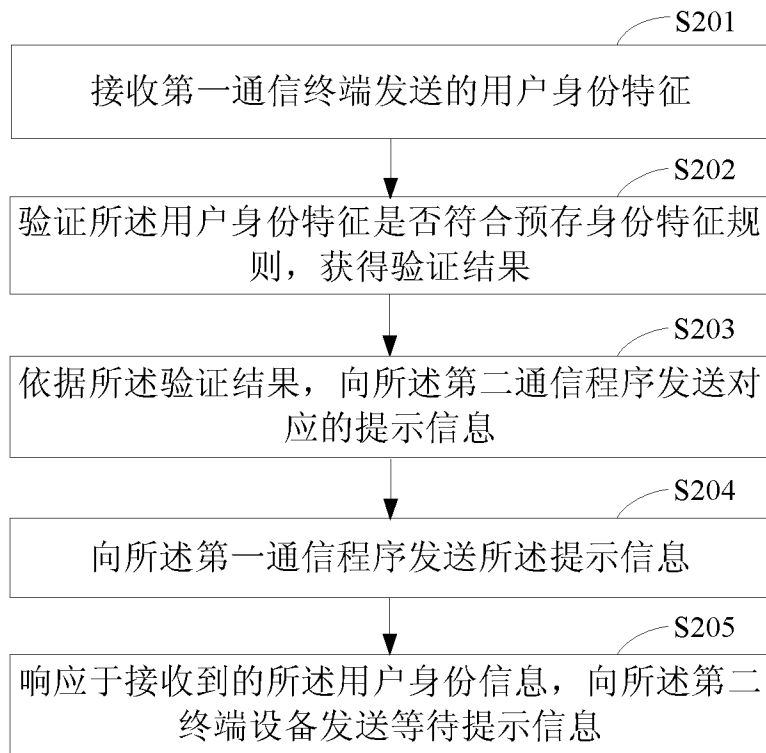


图 3

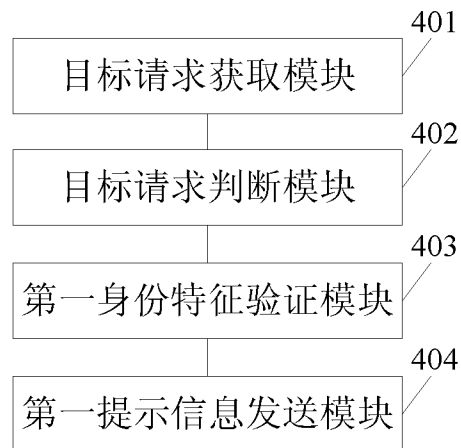


图 4

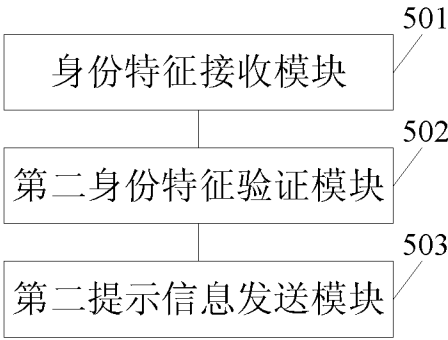


图 5

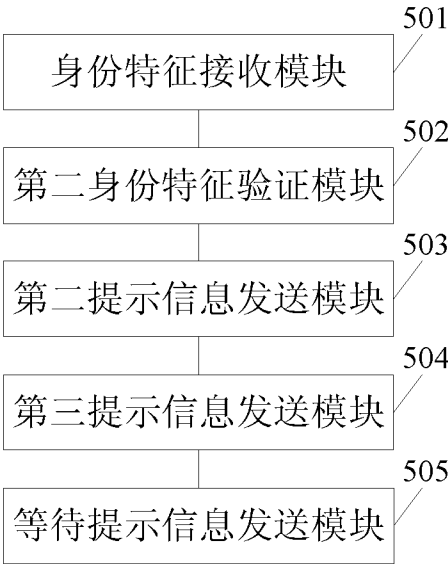


图 6

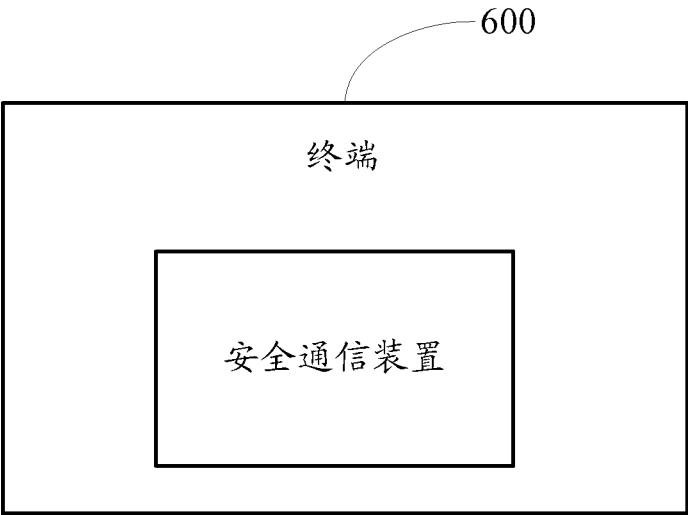


图 7

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2016/077974

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/31 (2013.01) i; 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)

G06F; H04L; H04W; H04Q

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, WPI, EPODOC, CNKI, IEEE: instant messaging, WeChat, sensitive, remittance, transfer of account, property, theft, deception, fraud, safe, biometrics, pay+, privacy, id, identi+, accout?, key, iris, fingerprint, authentication

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 103200150 A (TENCENT INC.), 10 July 2013 (10.07.2013), description, paragraph [0065]	1-11
A	CN 104574086 A (YULONG COMPUTER TELECOMMUNICATION SCIENTIFIC (SHENZHEN) CO., LTD.), 29 April 2015 (29.04.2015), the whole document	1-11
A	US 2014137191 A1 (RESERCH IN MOTION LIMITED), 15 May 2014 (15.05.2014), the whole document	1-11

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	“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
“A” document defining the general state of the art which is not considered to be of particular relevance	“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
“E” earlier application or patent but published on or after the international filing date	“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
“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)	“&” document member of the same patent family
“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	

Date of the actual completion of the international search 18 May 2016 (18.05.2016)	Date of mailing of the international search report 21 June 2016 (21.06.2016)
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 LV, Miao Telephone No.: (86-10) 010-82246954

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2016/077974

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103200150 A	10 July 2013	None	
CN 104574086 A	29 April 2015	None	
US 2014137191 A1	15 May 2014	EP 2733635 A2	21 May 2014
		CA 2832675 A1	14 May 2014
		US 2016042164 A1	11 February 2016

A. 主题的分类 G06F 21/31(2013.01)i; 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) G06F; H04L; H04W; H04Q 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, WPI, EPODOC, CNKI, IEEE: 即时通讯, 微信, 隐私, 敏感, 支付, 汇款, 转账, 财产, 身份验证, 鉴权, 盗, 欺骗, 欺诈, 安全, 指纹, 虹膜, 生物特征, pay+, privacy, id, identi+, accout?, key, iris, fingerprint, authentication														
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>X</td> <td>CN 103200150 A (深圳市腾讯计算机系统有限公司) 2013年 7月 10日 (2013 - 07 - 10) 说明书第[0065]段</td> <td>1-11</td> </tr> <tr> <td>A</td> <td>CN 104574086 A (宇龙计算机通信科技深圳有限公司) 2015年 4月 29日 (2015 - 04 - 29) 全文</td> <td>1-11</td> </tr> <tr> <td>A</td> <td>US 2014137191 A1 (RESERCH IN MOTION LIMITED) 2014年 5月 15日 (2014 - 05 - 15) 全文</td> <td>1-11</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	X	CN 103200150 A (深圳市腾讯计算机系统有限公司) 2013年 7月 10日 (2013 - 07 - 10) 说明书第[0065]段	1-11	A	CN 104574086 A (宇龙计算机通信科技深圳有限公司) 2015年 4月 29日 (2015 - 04 - 29) 全文	1-11	A	US 2014137191 A1 (RESERCH IN MOTION LIMITED) 2014年 5月 15日 (2014 - 05 - 15) 全文	1-11
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求												
X	CN 103200150 A (深圳市腾讯计算机系统有限公司) 2013年 7月 10日 (2013 - 07 - 10) 说明书第[0065]段	1-11												
A	CN 104574086 A (宇龙计算机通信科技深圳有限公司) 2015年 4月 29日 (2015 - 04 - 29) 全文	1-11												
A	US 2014137191 A1 (RESERCH IN MOTION LIMITED) 2014年 5月 15日 (2014 - 05 - 15) 全文	1-11												
☐ 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 2016年 5月 18日		国际检索报告邮寄日期 2016年 6月 21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		授权官员 吕淼 电话号码 (86-10)010-82246954												

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2016/077974

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	103200150	A	2013年 7月 10日	无			
CN	104574086	A	2015年 4月 29日	无			
US	2014137191	A1	2014年 5月 15日	EP	2733635	A2	2014年 5月 21日
				CA	2832675	A1	2014年 5月 14日
				US	2016042164	A1	2016年 2月 11日