

(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
2019 年 1 月 31 日 (31.01.2019)



(10) 国际公布号
WO 2019/019936 A1

(51) 国际专利分类号:
H04L 12/58 (2006.01) **H04L 29/08** (2006.01)

(21) 国际申请号: PCT/CN2018/095873

(22) 国际申请日: 2018 年 7 月 17 日 (17.07.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201710628723.X 2017 年 7 月 28 日 (28.07.2017) CN

(71) 申请人: 阿里巴巴集团控股有限公司 (ALIBABA GROUP HOLDING LIMITED) [—/CN]; 开曼群岛大开曼资本大厦一座四层 847 号邮箱, Grand Cayman (KY)。

(72) 发明人: 史明江 (SHI, Mingjiang); 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。

(74) 代理人: 北京三友知识产权代理有限公司 (BEIJING SANYOU INTELLECTUAL PROPERTY AGENCY LTD.); 中国北京市金

融街 35 号国际企业大厦 A 座 16 层, Beijing 100033 (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, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, 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, 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,

(54) Title: FILE TRANSMISSION METHOD, APPARATUS, DEVICE AND STORAGE MEDIUM

(54) 发明名称: 一种文件传输方法、装置、设备和存储介质

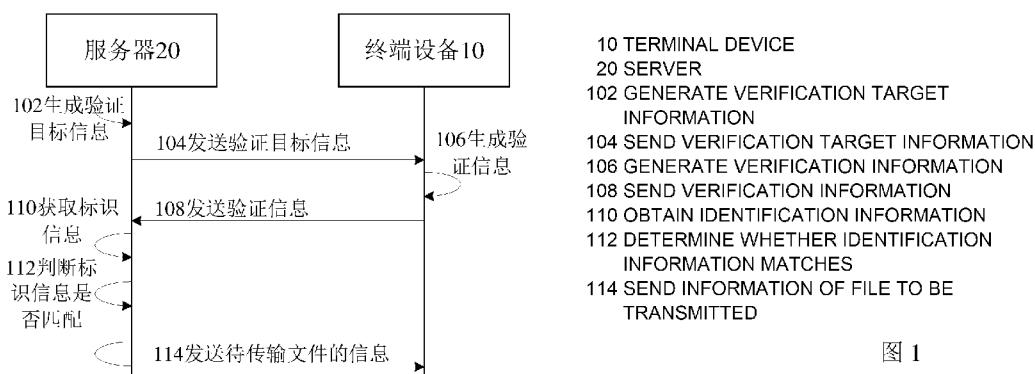


图 1

(57) Abstract: Provided are a file transmission method, an apparatus, a device and a storage medium, thereby improving the data security. The method comprises: determining verification target information of a file to be transmitted according to a saved file, and sending the verification target information, wherein the file to be transmitted matches the saved file; obtaining at least one piece of identification information in the file to be transmitted from the received verification information, wherein the identification information is determined according to the verification target information; determining whether the identification information of the file to be transmitted matches the identification information of the corresponding saved file; and after confirming that the identification information matches, sending the information of the file to be transmitted. The verification information ensures the presence of a file in both the server and the client, thereby preventing the problem of forging information to steal files and ensuring information security.

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))。

(57) 摘要：本申请实施例提供了一种文件传输方法、装置、设备和存储介质，以提高数据的安全性。所述的方法包括：依据已存文件确定待传输文件的验证目标信息，并发送所述验证目标信息，其中，所述待传输文件与已存文件匹配；从接收的验证信息中获取所述待传输文件中的至少一个标识信息，所述标识信息依据所述验证目标信息确定；判断所述待传输文件的标识信息，与对应已存文件的标识信息是否匹配；在确认标识信息匹配后，发送所述待传输文件的信息。通过验证信息保证文件在服务器和客户端均存在，防止伪造信息窃取文件的问题，保证信息的安全。

一种文件传输方法、装置、设备和存储介质

本申请要求 2017 年 07 月 28 日递交的申请号为 201710628723.X、发明名称为“一种文件传输方法、装置、设备和存储介质”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。

5

技术领域

本申请涉及计算机技术领域，特别是涉及一种文件传输方法、一种文件传输装置、一种终端设备、一种服务器、一种存储介质和一种用于终端设备的操作系统。

10 背景技术

秒传是一种“忽略式”上传方式，它使得不同用户的相同文件只需存储一份，这不但避免了不必要的文件上传，而且降低了服务端的带宽和存储成本，同时提升了用户体验。因此，在云存储系统中，秒传是必不可少的功能。

一种秒传方式如下：服务器预先计算出已存文件的 md5 值，从而存储已存文件、其 md5 值和文件标识的对应关系。客户端在上传文件前计算待传输文件的 md5 值，然后发送携带 md5 值的数据请求给服务器。服务器检测该 md5 值与已存的 md5 值是否相同，若相同则新建一文件标识，将该新建的文件标识和 md5 值、对应已存文件建立对应关系，并返回新建的文件标识给客户端，表征该文件已上传，从而实现了文件的快速上传。

但是，md5 值是 32 个字符的字符串，理论上，攻击者可以枚举所有的 md5 值，然后模拟客户端发起秒传请求，从而攻击者在不拥有文件的情况下也能秒传出文件，并且能够基于服务器回复的文件标识等获取到对应文件，导致数据泄露，影响数据安全。

发明内容

本申请实施例所要解决的技术问题是提供一种文件传输方法，以提高数据的安全性。相应的，本申请实施例还提供了一种文件传输装置、一种终端设备、一种服务器、一种存储介质和一种操作系统，用以保证上述方法的实现及应用。

为了解决上述问题，本申请实施例公开了一种文件传输方法，包括：依据已存文件确定待传输文件的验证目标信息，并发送所述验证目标信息，其中，所述待传输文件与已存文件匹配；从接收的验证信息中获取所述待传输文件中的至少一个标识信息，所述标识信息依据所述验证目标信息确定；判断所述待传输文件的标识信息，与对应已存文

件的标识信息是否匹配；在确认标识信息匹配后，发送所述待传输文件的信息。

本申请实施例还公开了一种文件传输方法，包括：接收验证目标信息，其中，所述验证目标信息是依据与待传输文件匹配的已存文件生成的；依据所述验证目标信息确定所述待传输文件的至少一个标识信息，依据所述标识信息生成验证信息；发送所述验证信息；接收所述待传输文件的信息。

本申请实施例还公开了一种文件传输装置，包括：目标发送模块，用于依据已存文件确定待传输文件的验证目标信息，并发送所述验证目标信息，其中，所述待传输文件与已存文件匹配；获取模块，用于从接收的验证信息中获取所述待传输文件中的至少一个标识信息，所述标识信息依据所述验证目标信息确定；判断模块，用于判断所述待传输文件的标识信息，与对应已存文件的标识信息是否匹配；存储发送模块，用于在确认标识信息匹配后，发送所述待传输文件的信息。

本申请实施例还公开了一种文件传输装置，包括：接收模块，用于接收验证目标信息，其中，所述验证目标信息是依据与待传输文件匹配的已存文件生成的；以及，接收所述待传输文件的信息；验证信息确定模块，用于依据所述验证目标信息确定所述待传输文件的至少一个标识信息，依据所述标识信息生成验证信息；发送模块，用于发送所述验证信息。

本申请实施例还公开了一种服务器，包括：一个或多个处理器；和其上存储有指令的一个或多个机器可读介质，当由所述一个或多个处理器执行时，使得所述服务器执行如本申请实施例中一个或多个所述的方法。

本申请实施例还公开了一个或多个机器可读介质，其上存储有指令，当由一个或多个处理器执行时，使得服务器执行如本申请实施例中一个或多个所述的方法。

本申请实施例还公开了一种终端设备，包括：一个或多个处理器；和其上存储有指令的一个或多个机器可读介质，当由所述一个或多个处理器执行时，使得所述终端设备执行如本申请实施例中一个或多个所述的方法。

本申请实施例还公开了一个或多个机器可读介质，其上存储有指令，当由一个或多个处理器执行时，使得终端设备执行如本申请实施例中一个或多个所述的方法。

本申请实施例还公开了一种用于终端设备的操作系统，包括：接收单元，接收验证目标信息，其中，所述验证目标信息是依据与待传输文件匹配的已存文件生成的；及接收所述待传输文件的信息；验证单元，依据所述验证目标信息确定所述待传输文件的至少一个标识信息，依据所述标识信息生成验证信息；通信单元，发送所述验证信息。

与现有技术相比，本申请实施例包括以下优点：

在本申请实施例中，服务器确认待传输文件与已存文件匹配后，可依据已存文件确定待传输文件的验证目标信息，从而终端设备可基于验证目标信息计算，待传输文件中至少一个目标数据的标识信息，服务器再判断所述待传输文件的标识信息，与对应已存文件的标识信息是否匹配，在确认标识信息匹配后确认终端设备中存储有该待传输文件，因此可发送所述待传输文件的信息，从而通过验证信息保证文件在服务器和客户端均存在，防止伪造信息窃取文件的问题，保证信息的安全。

10 附图说明

图 1 是本申请实施例的一种数据传输架构示意图；

图 2 是本申请的一种文件传输方法实施例中终端设备侧的步骤流程图；

图 3 是本申请的一种文件传输方法实施例中服务器侧的步骤流程图；

图 4 是本申请实施例的另一种数据传输架构示意图；

15 图 5 是本申请的另一种文件传输方法实施例中终端设备侧的步骤流程图；

图 6 是本申请的另一种文件传输方法实施例中服务器侧的步骤流程图；

图 7 是本申请一种文件传输装置实施例的结构框图；

图 8 是本申请另一种文件传输装置实施例的结构框图；

图 9 是本申请另一种文件传输装置可选实施例的结构框图；

20 图 10 是本申请一实施例提供的终端设备的硬件结构示意图；

图 11 是本申请另一实施例提供的终端设备的硬件结构示意图；

图 12 是本申请一实施例提供的操作系统示意图。

具体实施方式

25 为使本申请的上述目的、特征和优点能够更加明显易懂，下面结合附图和具体实施方式对本申请作进一步详细的说明。

本申请实施例中，终端设备指的是具有智能操作系统的设备，这些设备可支持音频、视频、数据等方面的功能，包括智能移动终端如智能手机、平板电脑、智能穿戴设备，也可以是智能电视、个人计算机等设备。智能操作系统如 YunOS、IOS、Android 等。

30 参照图 1，示出了本申请实施例的一种数据传输交互示意图。

该数据传输系统包括：终端设备 10 和服务器 20。用户可在终端设备中通过客户端等应用与服务器交互，执行文件上传等操作。

其中，服务器 20 对于存储的文件，可记录该文件的标识信息，该标识信息可唯一表征一个数据内容，即不同数据的标识信息不同，相匹配数据的标识信息相匹配，该相匹配包括相同。因此对于文件可通过文件标识信息表征其数据内容，文件标识信息也是一种标识信息，不同文件的文件标识信息不同，相匹配文件的文件标识信息相匹配。其中，标识信息可通过多种算法计算得到，每一种算法对应一种类型的标识信息，同种算法得到的标识信息之间可互相比对，不同算法得到的标识信息之间不具有可比性，即本申请实施例中所执行的匹配是针对同一种算法得到标识信息之间，以及文件标识信息之间的匹配。标识信息包括：消息摘要，文件标识信息包括：消息摘要，该消息摘要（Message Digest）是唯一对应一个数据（文件）的固定长度的值，是通过一定的算法计算数据文件得到的，一旦数据文件发生变更，则消息摘要也会发生变更，因此也可看作是数据文件的数字指纹，可用于唯一标识一个数据文件。

因此当不同用户向服务器上传系统文件时，服务器只存储一份文件即可，后续上传该文件的用户即可基于秒传功能实现快速上传。但是为了防止攻击者通过伪造标识信息（如消息摘要）的方式窃取文件，本实施例在确认服务器端已存储该文件的基础上，可通过文件数据的验证来确保终端设备本地存在文件，并在此的基础上提供秒传功能，告知对应终端设备文件上传成功。因此在服务器确认存储与待传输文件相匹配的文件基础上，文件传输验证可通过如下交互过程实现：

102、服务器确认待传输文件与已存文件匹配后，依据已存文件确定待传输文件的验证目标信息。对于需要上传的待传输文件，服务器确认该待传输文件与已存文件匹配（如存在与待传输文件数据内容相同的文件，即待传输文件与已存文件相同后），可依据该已存文件确定待传输文件的验证目标信息，该验证目标信息用于告知终端设备需要验证的目标，如目标区域的数据、需要使用的算法等。

104、服务器发送所述验证目标信息。

106、终端设备依据所述验证目标信息确定所述待传输文件的至少一个标识信息，依据所述标识信息生成验证信息。终端设备依据所述验证目标信息确定需要验证的目标，因此可依据待传输文件计算至少一个标识信息，该标识信息可依据待传输文件中的部分数据如目标区域的数据计算得到，然后依据标识信息生成验证信息。

108、终端设备发送所述验证信息。

110、服务器从验证信息中获取所述待传输文件中的至少一个标识信息。

112、服务器判断所述待传输文件的标识信息，与对应已存文件的标识信息是否匹配。验证目标信息依据已存文件的标识信息确定，从而便于待传输文件的标识信息和已存文件的标识信息之间的匹配。

5 114、服务器在确认标识信息匹配后，发送所述待传输文件的信息。该信息包括存储信息，此外，若服务器验证不通过，即待传输文件不可信，也忽略该对该文件的上传，也可反馈传输失败的响应信息，此后终端设备可发送给文件给服务器，以上传文件。

从而在确认待传输文件与已存文件匹配的情况下，基于已存文件确定待传输文件中需要验证的目标，从而获取待传输文件中的至少一个标识信息，再判断所述待传输文件的标识信息，与对应已存文件的标识信息是否匹配，确认标识信息匹配即终端设备中存
10 在该待传输文件，则无需终端设备发送该待传输文件，即可发送所述待传输文件的信息，告知文件传输成功，从而基于标识信息有效的防止伪造文件的问题，保证数据的安全。

参照图 2、示出了本申请的一种文件传输方法实施例中服务器侧的步骤流程图。

步骤 202，依据已存文件确定待传输文件的验证目标信息，并发送所述验证目标信
15 息。

步骤 204，从接收的验证信息中获取所述待传输文件中的至少一个标识信息。

步骤 206，判断所述待传输文件的标识信息，与对应已存文件的标识信息是否匹配。若是，执行步骤 208；若否，结束该流程。

步骤 208，在确认标识信息匹配后，发送所述待传输文件的信息。

20 服务器确认该待传输文件与已存文件匹配（如存在与待传输文件数据内容相同的文件，即待传输文件与已存文件相同后），可依据该已存文件确定待传输文件的验证目标信息。该验证目标信息用于告知终端设备需要验证的目标，如目标区域的数据、需要使用的算法等，其中，终端设备依据验证目标信息计算待传输文件的标识信息，该验证目标信息是依据对应相匹配已存文件的标识信息确定的。因此终端设备可依据标识信息计
25 算待传输文件中的至少一个标识信息，构成验证信息后返回给服务器。

服务器对应可接收验证信息，并从验证信息中获取所述待传输文件中的至少一个标识信息，然后将每个标识信息分别与已存文件的对应标识信息进行匹配，若各标识信息均匹配，则确认终端设备中存在该待传输文件，可为其提供秒传功能，因此可所述待传输文件的信息，例如基于已存文件的存储记录生成待传输文件的存储信息，例如将已存
30 文件的存储记录中的存储地址，作为待传输文件的存储地址等，然后将存储信息反馈给

终端设备，以告知终端设备文件上传成功，依据该文件在服务器中的存储信息等。

参照图 3、示出了本申请的一种文件传输方法实施例中终端设备侧的步骤流程图。

步骤 302，接收验证目标信息。

5 步骤 304，依据所述验证目标信息确定所述待传输文件的至少一个标识信息，依据所述标识信息生成验证信息。

步骤 306，发送所述验证信息。

步骤 308，接收所述待传输文件的信息。

服务器确认该待传输文件与已存文件匹配（如存在与待传输文件数据内容相同的文件，即待传输文件与已存文件相同后），可依据该已存文件确定待传输文件的验证目标信息。终端设备接收验证目标信息后，可所述验证目标信息确定所述待传输文件的至少一个标识信息，即依据验证信息确定所述待传输文件中需要验证的至少一个目标数据，然后分别计算各目标数据的标识信息，采用得到的至少一个标识信息生成验证信息，再发送验证信息给服务器。服务器依据验证信息检验文件的可信度，即依据标识信息确定与预存文件的标识信息是否匹配，以此来验证终端设备中是否真实存储了该待传输文件，再确认标识信息匹配后认为真实存储了该待传输文件，因此可发送所述待传输文件的信息，终端接收该待传输文件的信息后确认文件上传成功，后续需要该文件时，可依据所述待传输文件的信息从服务器获取该文件。

综上所述，服务器确认待传输文件与已存文件匹配后，可依据已存文件确定待传输文件的验证目标信息，从而终端设备可基于验证目标信息计算，待传输文件中至少一个目标数据的标识信息，服务器再判断所述待传输文件的标识信息，与对应已存文件的标识信息是否匹配，在确认标识信息匹配后确认终端设备中存储有该待传输文件，因此可发送所述待传输文件的信息，从而通过验证信息保证文件在服务器和客户端均存在，防止伪造信息窃取文件的问题，保证信息的安全。

为了提高秒传功能的安全性，本实施例对于文件传输可包含两个阶段，一个阶段是查询阶段，用于查询待传输文件是否是服务器中已存文件，若为已存文件，则可执行秒传功能，进入第二个阶段即秒传阶段，为了保证文件的安全，可验证终端设备本地是否真实存储该文件，对于真实存在文件的终端设备提供秒传功能，通知其上传成功。

参照图 4，示出了本申请实施例的另一种数据传输交互示意图。

402、终端设备依据待传输文件生成文件信息。

30 所述文件信息用于确定与所述待传输文件匹配的已存文件，所述文件信息包括所述

待传输文件的文件标识信息。

404、终端设备发送待传输文件的文件信息给服务器。

406、服务器从所述文件信息中获取至少一个文件标识信息。

408、服务器判断所述待传输文件的文件标识信息，与已存文件的文件标识信息是否匹配。

410a、若文件标识信息不匹配，服务器发送响应信息告知终端设备上传文件；在 412a、终端设备上传文件给服务器。

410b、若文件标识信息匹配，服务器依据已存文件确定待传输文件的验证目标信息，并发送所述验证目标信息。

412b、终端设备依据所述验证目标信息确定所述待传输文件的至少一个标识信息，依据所述标识信息生成验证信息。终端设备发送所述验证信息。

414、服务器从验证信息中获取所述待传输文件中的至少一个标识信息。

416、服务器判断所述待传输文件的标识信息，与对应已存文件的标识信息是否匹配。验证目标信息依据已存文件的标识信息确定，从而便于待传输文件的标识信息和已存文件的标识信息之间的匹配。

418、服务器在确认标识信息匹配后，生成所述待传输文件的存储信息，并发送所述存储信息。此外，若服务器验证不通过，即待传输文件不可信，也忽略该对该文件的上传，也可反馈传输失败的响应信息，此后终端设备可发送给文件给服务器，以上传文件。

参照图 5，示出了本申请的另一种文件传输方法实施例中终端设备侧的步骤流程图。

步骤 502，计算所述待传输文件的至少一个文件标识信息，将所述待传输文件的至少一种文件标识信息作为文件信息。

步骤 504，发送待传输文件的文件信息。

其中，可计算所述待传输文件的至少一种文件标识信息，如文件标识信息为消息摘要，则可计算待传输文件的（Message-Digest Algorithm 5，消息摘要算法第五版）值、SHA（Secure Hash Algorithm，安全哈希算法）值、base64 值中的至少一种，将所述待传输文件的至少一种文件标识信息作为文件信息。还可获取待传输文件的文件大小，在所述文件信息中添加所述待传输文件的文件大小。即文件信息包括待传输文件的文件标识信息和文件大小，该文件标识信息可为消息摘要，消息摘要包括 md5 值、SHA 值、base64 值等。还可在文件信息中携带终端信息如 MAC 地址、用户信息如用户标识等。然后将文件信息发送给服务器，以使服务器基于文件的文件标识信息和文件大小验证是否以存

储了相匹配的文件。

步骤 506，接收验证目标信息。

若服务器判断待传输文件与已存文件不匹配，则可发送上传文件的响应信息，终端设备在接收到指示上传文件的传输响应信息后，发送待传输文件给服务器。若服务器判断待传输文件与已存文件匹配，则生成验证目标信息并发送给终端设备。本申请实施例以服务器判断待传输文件与已存文件匹配为例。

步骤 508，依据所述验证目标信息，确定所述待传输文件对应至少一个目标区域。

步骤 510，计算所述目标区域对应数据的标识信息，依据所述标识信息生成验证信息。

10 步骤 512，发送所述验证信息给服务器。

本实施例以服务器中已存文件与待传输文件匹配为例，该验证目标信息用于确定终端设备提高的验证数据，如确定提取目标数据的目标区域来计算标识信息。因此在接收到验证目标信息后，可依据该验证目标信息确定至少一个目标区域，从所述待传输文件的各目标区域中分别提取目标数据，计算各目标数据对应的标识信息如消息摘要。因此
15 计算待传输文件中一个或多个部分的标识信息，例如每隔 1024KB 提取 20KB 的数据计算消息摘要。该计算标识信息的区域是服务器中对应相匹配的已存文件也计算了标识信息的区域，从而便于服务器的匹配判断。本申请实施例中，验证信息可包括多于一个消息摘要，则多于一个消息摘要可依据所述待传输文件中非连续的目标区域对应数据计算得到。即从待传输文件中确定多于一个目标区域时，各目标区域为非连续的，从而得到的
20 消息摘要是待传输文件中非连续数据的消息摘要。

其中，一个可选实施例中，依据所述验证目标信息，确定所述待传输文件对应至少一个目标区域，包括：从验证目标信息中获取至少一个数据长度和至少一个偏移量；依据所述偏移量和数据长度，从所述待传输文件中确定目标区域。即可从验证目标信息中获取至少一个数据长度和至少一个偏移量，数据长度为需要计算消息摘要目标区域的数据长度，依据数据长度的不同可确定不同大小的目标区域，偏移量用于确定目标区域的起始位置，则可基于偏移量确定目标区域的起始位置，基于数据长度区域该起始位置对应的终止位置，从而确定出目标区域，再从该目标区域中提取数据进行标识信息的计算。其中，当数据长度和偏移量均多于一个时，验证目标信息中还可记录数据长度和偏移量之间的匹配关系，从而能够准确的确定目标区域。

30 本申请实施例中，在确定出目标区域后，还可确定计算标识信息的算法，不同标识

信息依据不同算法确定，其中，标识信息包括消息摘要，消息摘要包括以下至少一种：md5 值、SHA 值、base64 值。其中，SHA 值包括 sha1, sha125, sha256, sha512 等 SHA 家族的消息摘要。因此对于上述各种消息摘要可采取相应的算法计算得到，相同类型的消息摘要之间进行匹配判断。

5 本申请一个可选实施例中，所述验证目标信息包括：通道标识，该通道标识为服务器和终端设备通信对应通道的标识，例如在服务器和终端设备间建立会话 session，则通道标识为 sessionId，可将该 sessionId 设置为一个长度为 48 位的字符串。从通道标识可以解析出该传输通道的创建时间和过期时间。此外，通道标识中还包括签名数据来保证传输通道标识的不可伪造性，例如签名数据为经用户密钥签名的 auth_md5。则可依据所述通道标识判断对应的传输通道是否有效；在判断传输通道有效后，执行发送所述验证信息的步骤。即依据该通道标识判断对应的传输通道是否有效，例如依据创建时间、过期时间判断是否在有效时间内，又如依据签名数据判断是否是正确的等。若传输通道无效则可忽略该消息或告知服务器重新传输；若传输通道有效则可进行后续的步骤。其中，可在计算目标数据的消息摘要前判断传输通道的有效性，或者在发送所述验证信息前判断传输通道的有效性。

10

15

步骤 514，接收存储信息。

服务器判断验证信息通过校验后，即待传输文件的标识信息和已存文件中对应标识信息匹配后，服务器可生成该待传输文件的文件标识，并确定相应的存储地址等存储信息，将该存储信息反馈给中观设备，来标识该待传输文件传输成功，终端设备依据该存储信息确定对应文件的文件标识、存储地址等信息，便于后续获取。

20

参照图 6、示出了本申请的另一种文件传输方法实施例中服务器侧的步骤流程图。

步骤 602，接收所述待传输文件的文件信息，从所述文件信息中获取至少一个文件标识信息。

25 服务器可接收终端设备发送的文件信息，该文件信息可告知终端设备要上传的文件，因此可从该文件信息中获取所述待传输文件的文件标识信息，该文件标识信息可表征待传输文件的数据内容，并可从文件信息中获取所述待传输文件的文件大小。

步骤 604，判断所述待传输文件的文件标识信息，与已存文件的文件标识信息是否匹配。

30 然后可采用该待传输文件的文件标识信息与服务器中已存文件的文件标识信息进行

匹配。若是，即待传输文件的文件标识信息与已存文件的文件标识信息匹配，执行步骤 608；若否，即待传输文件的文件标识信息与已存文件的文件标识信息不匹配，执行步骤 606。其中，若待传输文件的文件标识信息和已存文件的文件标识信息相同，则可确认待传输文件和该已存文件为相同文件，即具有相同的数据内容。

5 步骤 606，生成并发送响应信息告知终端设备上传文件。

步骤 608，判断所述待传输文件的文件大小，与对应匹配的已存文件的文件大小是否相匹配。

判断待传输文件的文件标识信息与已存文件的文件标识信息相匹配后，还可判断该文件标识信息相匹配的已存文件的文件大小和待传输文件的文件大小是否相匹配。若是，
10 执行步骤 610；若否，执行步骤 606。

步骤 610，依据所述已存文件对应的标识信息，采用至少一个标识信息对应目标区域确定验证目标信息。

从而终端设备可获取已存文件的存储记录或存储信息，依据该存储信息确定该已存文件对应的标识信息，该标识信息依据已存文件中目标区域对应的数据计算得到，因此
15 计算标识信息的目标区域确定待传输文件中需要计算标识信息的至少一个目标区域，基于该至少一个目标区域得到验证目标信息。并且可获取传输通道的通道标识，如服务器和终端设备之间采用会话（session）通信，则通道标识为 sessionId，在验证目标信息中添加该通道标识。

其中，已存文件的存储记录或存储信息中存储有文件的各种信息，如文件的存储地址、至少一种算法得到的文件标识信息、文件大小、文件中至少一个目标区域对应数据的标识信息等，此外，由于文件标识信息可唯一表征一个文件的数据内容，因此在不同用户存储有相同文件（即相同数据内容的文件）时，为每个用户可分配一个文件标识，当然所有用户也可共享该文件标识，因此在存储记录或存储信息中还可记录文件标识，也可记录与文件标识对应的各用户标识。或者，在服务器中将文件存储信息和用户数据
25 分离，即文件的存储信息中存储文件的信息，如文件标识信息、文件大小、文件中至少一个目标区域对应数据的标识信息，在用户数据中存储：文件标识、用户标识、上传时间等，将该用户数据和文件的存储信息建立映射关系，从而基于文件标识可查找到该文件，基于文件标识信息也可查找到对应的用户。

本申请一个可选实施例中，采用至少一个标识信息对应目标区域确定验证目标信息，
30 包括：依据所述至少一个标识信息对应目标区域，确定偏移量和数据长度；采用所述偏

移量和数据长度生成验证目标信息。即可依据与待传输文件相匹配的已存文件，确定其计算有标识信息的各目标区域，从而中选取至少一个目标区域计算偏移量 and 数据长度，然后可采用偏移量和数据长度生成验证目标信息。

步骤 612，发送所述验证目标信息。

5 可发送验证目标信息给服务器。

步骤 614，接收验证信息。

终端设备依据验证目标信息生成验证信息，并返回验证信息给服务器。其中，验证信息包括通道标识和至少一个目标区域对应数据的标识信息。

步骤 616，从所述验证信息中获取目标区域对应数据的标识信息。

10 步骤 618，判断所述待传输文件的标识信息，与对应已存文件的标识信息是否匹配。

从所述验证信息中获取通道标识和目标区域对应数据的标识信息，然后采用依据所述传输通道标识和所述目标区域对应数据的消息摘要进行待传输文件可信度的检验，若两者均通过校验确认可信，否则不可信。

可判断所述待传输文件的标识信息，与对应已存文件的标识信息是否匹配；若是，
15 即标识信息匹配，执行步骤 620；若否，即标识信息不匹配，可结束该流程，或者执行步骤 606，指示终端设备上传对应文件。

一个可选实施例中，即依据所述通道标识判断对应的传输通道是否有效；在判断传输通道有效后，执行发送所述验证信息的步骤。即依据该通道标识判断对应的传输通道是否有效，例如依据创建时间、过期时间判断是否在有效时间内，又如依据签名数据判断
20 断是否是正确的等。并且还可基于通道标识判断是否出现重放攻击，从而判断传输通道的有效性，即一个有效的通道标识（如 sessionId）在被使用后，会在服务端被标记为已使用，从而再遇到相同的通道标识后，服务端会拒绝这个请求，防止由于验证信息在发送过程中被截取到而导致出现重放攻击。若传输通道无效则可忽略该消息；若传输通道有效则可进行后续的步骤。

25 步骤 620，为所述待传输文件分配文件标识，并将所述文件标识和所述已存文件对应存储记录建立关联关系。

步骤 622，采用所述存储记录中的文件地址和/或所述文件标识，生成所述待传输文件的存储信息。

步骤 624，发送所述存储信息。

30 在确认待传输文件可信，即通道标识有效，且标识信息匹配后，可依据对应相同的

已存文件生成一个新的文件标识，将该文件标识分配给所述待传输文件，并将文件标识和所述已存文件对应存储记录建立关联关系，即该存储记录对应关联了终端设备要上传文件的文件标识。从而可从所述存储记录中获取文件地址，和/或，获取该文件标识，采用文件地址和/或所述文件标识，生成所述待传输文件的存储信息返回该存储信息给终端设备，以告知终端设备文件上传成功，完成秒传功能。

本申请实施例中，消息摘要包括以下至少一种：md5 值、SHA 值、base64 值。其中，SHA 值包括 sha1, sha125, sha256, sha512 等 SHA 家族的消息摘要。

因此一个可选实施例中，在查询阶段可在文件信息中携带待传输文件计算的至少一种的消息摘要，来进行待传输文件对应存储状态的判断。即在查询阶段文件信息可为 md5 值等消息摘要和文件大小的组合，也可两种或以上的消息摘要的组合，如 md5 值和 sha1 值等散列函数的组合。并且，对于验证信息，可计算待传输文件中一个目标区域对应数据的消息摘要如 md5 值，也可以计算多个不连续的目标区域对应数据的消息摘要。

综上，本申请实施例可采用消息摘要、文件大小等多种因素来唯一确定一个文件，从而查询服务器中是否存储有对应文件。在此基础上，大大降低了攻击者伪造信息窃取文件的几率。

其次，在秒传阶段，通过文件中，目标区域的消息摘要作为判断客户端拥有该文件的判断标准之一，防止了在客户端没有文件的情况下为其提供秒传功能，即客户端在没有文件的情况下无法秒传文件，提高数据的安全性。

需要说明的是，对于方法实施例，为了简单描述，故将其都表述为一系列的动作组合，但是本领域技术人员应该知悉，本申请实施例并不受所描述的动作顺序的限制，因为依据本申请实施例，某些步骤可以采用其他顺序或者同时进行。其次，本领域技术人员也应该知悉，说明书中所描述的实施例均属于优选实施例，所涉及的动作并不一定是本申请实施例所必须的。

本申请实施例还提供了一种文件传输装置，应用于服务器。

参照图 7，示出了本申请一种文件传输装置实施例的结构框图，具体可以包括如下模块：

目标发送模块 702，用于依据已存文件确定待传输文件的验证目标信息，并发送所述验证目标信息，其中，所述待传输文件与已存文件匹配。

获取模块 704，用于从接收的验证信息中获取所述待传输文件中的至少一个标识信息，所述标识信息依据所述验证目标信息确定。

判断模块 706，用于判断所述待传输文件的标识信息，与对应已存文件的标识信息是否匹配。

存储发送模块 708，用于在确认标识信息匹配后，发送所述待传输文件的信息。

综上，服务器确认待传输文件与已存文件匹配后，可依据已存文件确定待传输文件的验证目标信息，从而终端设备可基于验证目标信息计算，待传输文件中至少一个目标数据的标识信息，服务器再判断所述待传输文件的标识信息，与对应已存文件的标识信息是否匹配，在确认标识信息匹配后确认终端设备中存储有该待传输文件，因此可发送所述待传输文件的信息，从而通过验证信息保证文件在服务器和客户端均存在，防止伪造信息窃取文件的问题，保证信息的安全。

其中，所述标识信息包括：消息摘要。所述消息摘要包括以下至少一种：消息摘要算法第五版 md5 值、安全哈希算法 SHA 值、base64 值。

所述目标发送模块 702，用于依据所述已存文件对应的标识信息，采用至少一个标识信息对应目标区域确定验证目标信息。

所述目标发送模块 702，用于依据所述至少一个标识信息对应目标区域，确定偏移量和数据长度；采用所述偏移量和数据长度生成验证目标信息。

其中，所述标识信息依据所述待传输文件中目标区域的数据生成。若所述标识信息多于一个，则各标识信息依据所述待传输文件中非连续的目标区域对应数据计算确定。

所述目标发送模块 702，还用于获取传输通道的通道标识，在所述验证目标信息中添加所述传输通道的通道标识。

所述判断模块 706，还用于依据所述通道标识，判断是否所述传输通道是否有效；若所述传输通道有效，执行所述标识信息的匹配判断。

其中，所述获取模块 704，还用于接收所述待传输文件的文件信息，从所述文件信息中获取至少一个文件标识信息；所述判断模块 706，还用于判断所述待传输文件的文件标识信息，与已存文件的文件标识信息是否匹配；若文件标识信息匹配，则确认所述待传输文件和所述已存文件匹配。

所述文件信息还包括：所述待传输文件的文件大小；所述判断模块 706，还用于判断所述待传输文件的文件大小，与文件标识信息匹配的已存文件的文件大小是否相匹配；若文件大小相匹配，则确认所述待传输文件和所述已存文件匹配。

所述待传输文件的信息包括所述待传输文件的存储信息，所述存储发送模块 708，还用于为所述待传输文件分配文件标识，并将所述文件标识和所述已存文件对应存储记

录建立关联关系；采用所述存储记录中的文件地址和/或所述文件标识，生成所述待传输文件的存储信息

本申请实施例还提供了一种文件传输装置，应用于终端设备。

参照图 8，示出了本申请另一种文件传输装置实施例的结构框图，具体可以包括如下模块：

接收模块 802，用于接收验证目标信息，其中，所述验证目标信息是依据与待传输文件匹配的已存文件生成的；以及，接收所述待传输文件的信息。

验证信息确定模块 804，用于依据所述验证目标信息确定所述待传输文件的至少一个标识信息，依据所述标识信息生成验证信息。

10 发送模块 806，用于发送所述验证信息。

综上，服务器确认待传输文件与已存文件匹配后，可依据已存文件确定待传输文件的验证目标信息，从而终端设备可基于验证目标信息计算，待传输文件中至少一个目标数据的标识信息，服务器再判断所述待传输文件的标识信息，与对应已存文件的标识信息是否匹配，在确认标识信息匹配后确认终端设备中存储有该待传输文件，因此可生成
15 所述待传输文件的存储信息，从而通过验证信息保证文件在服务器和客户端均存在，防止伪造信息窃取文件的问题，保证信息的安全。

参照图 9，示出了本申请另一种文件传输装置可选实施例的结构框图。

其中，所述标识信息包括：消息摘要。所述消息摘要包括以下至少一种：消息摘要算法第五版 md5 值、安全哈希算法 SHA 值、base64 值。

20 验证信息确定模块 804，包括：区域确定子模块 8042 和计算子模块 8044。

区域确定子模块 8042，用于依据所述验证目标信息，确定所述待传输文件对应至少一个目标区域。

计算子模块 8044，用于计算所述目标区域对应数据的标识信息。

所述区域确定子模块 8044，用于从验证目标信息中获取至少一个数据长度和至少一个偏移量；依据所述偏移量和数据长度，从所述待传输文件中确定目标区域。
25

所述验证目标信息包括：通道标识；所述验证信息确定模块 804，还用于依据所述通道标识，判断对应的传输通道是否有效；在确认传输通道有效后，执行所述验证信息的发送。

其中，若所述验证信息包括多于一个标识信息，则各标识信息依据所述待传输文件中非连续的目标区域对应数据计算确定。
30

所述的装置还包括：

文件信息确定模块 808，用于生成所述待传输文件的文件信息，并发送待传输文件的文件信息，其中，所述文件信息用于确定与所述待传输文件匹配的已存文件。

所述文件信息确定模块 808，用于计算所述待传输文件的至少一个文件标识信息，
5 将所述待传输文件的至少一种文件标识信息作为文件信息。

所述文件信息确定模块 808，还用于获取所述待传输文件的文件大小，在所述文件信息中添加所述待传输文件的文件大小。

本申请实施例中，消息摘要包括以下至少一种：md5 值、SHA 值、base64 值。其中，SHA 值包括 sha1, sha125, sha256, sha512 等 SHA 家族的消息摘要。

10 因此一个可选实施例中，在查询阶段可在文件信息中携带待传输文件计算的两种或以上的消息摘要，来进行待传输文件对应存储状态的判断。即在查询阶段文件信息可为 md5 值等消息摘要和文件大小的组合，也可为两种或以上的消息摘要的组合，如 md5 值和 sha1 值其他散列函数的组合。并且，对于第二验证信息，可计算待传输文件中 1 个目标区域对应数据的消息摘要如 md5 值，也可以计算多个不连续的目标区域对应数据的消息摘要。
15

综上，本申请实施例可采用消息摘要、文件大小等多种因素来唯一确定一个文件，从而查询服务器中是否存储有对应文件。在此基础上，大大降低了攻击者伪造信息窃取文件的几率。

其次，在秒传阶段，通过文件中，目标区域的消息摘要作为判断客户端拥有该文件的判断标准之一，防止了在客户端没有文件的情况下为其提供秒传功能，即客户端在没有文件的情况下无法秒传文件，提高数据的安全性。
20

本申请实施例还提供了一种非易失性可读存储介质，该存储介质中存储有一个或多个模块（programs），该一个或多个模块被应用在终端设备时，可以使得该终端设备执行本申请实施例中各方法步骤的指令（instructions）。
25

一个可选实施例中，包括：一个或多个机器可读介质，其上存储有指令，当由一个或多个处理器执行时，使得终端设备执行本申请实施例中一个或多个所述的文件传输方法。

另一个可选实施例中，包括：一个或多个机器可读介质，其上存储有指令，当由一个或多个处理器执行时，使得服务器执行本申请实施例中一个或多个所述的文件传输方法。
30

图 10 为本申请一实施例提供的设备的硬件结构示意图。该设备可包括服务器、终端设备、温度控制设备等各种设备。如图 10 所示，该终端设备可以包括输入设备 100、处理器 101、输出设备 102、存储器 103 和至少一个通信总线 104。通信总线 104 用于实现元件之间的通信连接。存储器 103 可能包含高速 RAM 存储器，也可能还包括非易失性存储 NVM，例如至少一个磁盘存储器，存储器 103 中可以存储各种程序，用于完成各种处理功能以及实现本实施例的方法步骤。

可选的，上述处理器 101 例如可以为中央处理器(Central Processing Unit, 简称 CPU)、应用专用集成电路(ASIC)、数字信号处理器(DSP)、数字信号处理设备(DSPD)、可编程逻辑器件(PLD)、现场可编程门阵列(FPGA)、控制器、微控制器、微处理器或其他电子元件实现，该处理器 101 通过有线或无线连接耦合到上述输入设备 100 和输出设备 102。

可选的，上述输入设备 100 可以包括多种输入设备，例如可以包括面向用户的用户接口、面向设备的设备接口、软件的可编程接口、摄像头、传感器中至少一种。可选的，该面向设备的设备接口可以是用于设备与设备之间进行数据传输的有线接口、还可以是用于设备与设备之间进行数据传输的硬件插入接口(例如 USB 接口、串口等)；可选的，该面向用户的用户接口例如可以是面向用户的控制按键、用于接收语音输入的语音输入设备以及用户接收用户触摸输入的触摸感知设备(例如具有触摸感应功能的触摸屏、触控板等)；可选的，上述软件的可编程接口例如可以是供用户编辑或者修改程序的入口，例如芯片的输入引脚接口或者输入接口等；可选的，上述收发信机可以是具有通信功能的射频收发芯片、基带处理芯片以及收发天线等。麦克风等音频输入设备可以接收语音数据。输出设备 102 可以包括显示器、音响等输出设备。

在本实施例中，该终端设备的处理器包括用于执行各设备中数据处理装置各模块的功能，具体功能和技术效果参照上述实施例即可，此处不再赘述。

图 11 为本申请另一实施例提供的终端设备的硬件结构示意图。图 11 是对图 10 在实现过程中的一个具体的实施例。如图 11 所示，本实施例的终端设备包括处理器 111 以及存储器 112。

处理器 111 执行存储器 112 所存放的计算机程序代码，实现上述实施例中图 1 至图 6 的文件传输方法。

存储器 112 被配置为存储各种类型的数据以支持在终端设备的操作。这些数据的示例包括用于在终端设备上操作的任何应用程序或方法的指令，例如消息，图片，视频等。

存储器 112 可能包含随机存取存储器 (random access memory, 简称 RAM), 也可能还包括非易失性存储器 (non-volatile memory), 例如至少一个磁盘存储器。

可选地, 处理器 111 设置在处理组件 110 中。该终端设备还可以包括: 通信组件 113, 电源组件 114, 多媒体组件 115, 音频组件 116, 输入/输出接口 117 和/或传感器组件 118。

5 终端设备具体所包含的组件等依据实际需求设定, 本实施例对此不作限定。

处理组件 110 通常控制终端设备的整体操作。处理组件 110 可以包括一个或多个处理器 111 来执行指令, 以完成上述图 1 至图 6 方法的全部或部分步骤。此外, 处理组件 110 可以包括一个或多个模块, 便于处理组件 110 和其他组件之间的交互。例如, 处理组件 110 可以包括多媒体模块, 以方便多媒体组件 115 和处理组件 110 之间的交互。

10 电源组件 114 为终端设备的各种组件提供电力。电源组件 114 可以包括电源管理系统, 一个或多个电源, 及其他与为终端设备生成、管理和分配电力相关联的组件。

多媒体组件 115 包括在终端设备和用户之间的提供一个输出接口的显示屏。在一些实施例中, 显示屏可以包括液晶显示器 (LCD) 和触摸面板 (TP)。如果显示屏包括触摸面板, 显示屏可以被实现为触摸屏, 以接收来自用户的输入信号。触摸面板包括一个或多个触摸传感器以感测触摸、滑动和触摸面板上的手势。所述触摸传感器可以不仅感测触摸或滑动动作的边界, 而且还检测与所述触摸或滑动操作相关的持续时间和压力。

15 音频组件 116 被配置为输出和/或输入音频信号。例如, 音频组件 116 包括一个麦克风 (MIC), 当终端设备处于操作模式, 如语音识别模式时, 麦克风被配置为接收外部音频信号。所接收的音频信号可以被进一步存储在存储器 112 或经由通信组件 113 发送。20 在一些实施例中, 音频组件 116 还包括一个扬声器, 用于输出音频信号。

输入/输出接口 117 为处理组件 110 和外围接口模块之间提供接口, 上述外围接口模块可以是点击轮, 按钮等。这些按钮可包括但不限于: 音量按钮、启动按钮和锁定按钮。

25 传感器组件 118 包括一个或多个传感器, 用于为终端设备提供各个方面的状态评估。例如, 传感器组件 118 可以检测到终端设备的打开/关闭状态, 组件的相对定位, 用户与终端设备接触的存在或不存在。传感器组件 118 可以包括接近传感器, 被配置用来在没有任何的物理接触时检测附近物体的存在, 包括检测用户与终端设备间的距离。在一些实施例中, 该传感器组件 118 还可以包括摄像头等。

通信组件 113 被配置为便于终端设备和其他设备之间有线或无线方式的通信。终端设备可以接入基于通信标准的无线网络, 如 WiFi, 2G 或 3G, 或它们的组合。在一个实
30 施例中, 该终端设备中可以包括 SIM 卡插槽, 该 SIM 卡插槽用于插入 SIM 卡, 使得终

端设备可以登录 GPRS 网络，通过互联网与服务器建立通信。

由上可知，在图 11 实施例中所涉及的通信组件 113、音频组件 116 以及输入/输出接口 117、传感器组件 118 均可以作为图 10 实施例中的输入设备的实现方式。

在本实施例的一种终端设备中，包括：一个或多个处理器；和，其上存储有指令的一个或多个机器可读介质，当由所述一个或多个处理器执行时，使得所述终端设备执行如本申请实施例中一个或多个所述的方法。

在本实施例的一种服务器中，包括：一个或多个处理器；和，其上存储有指令的一个或多个机器可读介质，当由所述一个或多个处理器执行时，使得所述服务器执行如本申请实施例中一个或多个所述的方法。

10 本申请实施例还提供一种用于终端设备的操作系统，如图 12 所示，该设备的操作系统包括：接收单元 1202、验证单元 1204 和通信单元 1206。

接收单元 1202，接收验证目标信息，其中，所述验证目标信息是依据与待传输文件匹配的已存文件生成的；及接收所述待传输文件的信息。

15 验证单元 1204，依据所述验证目标信息确定所述待传输文件的至少一个标识信息，依据所述标识信息生成验证信息。

通信单元 1006，发送所述验证信息。

对于装置实施例而言，由于其与方法实施例基本相似，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。

20 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。

本申请实施例是参照根据本申请实施例的方法、终端设备(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终端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终端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。

30 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终端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终端设备上，使得在计算机或其他可编程终端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终端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。

尽管已描述了本申请实施例的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例做出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例以及落入本申请实施例范围的所有变更和修改。

最后，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、物品或者终端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、物品或者终端设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、物品或者终端设备中还存在另外的相同要素。

以上对本申请所提供的一种文件传输方法、一种文件传输装置、一种终端设备、一种存储介质、一种操作系统，进行了详细介绍，本文中应用了具体个例对本申请的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本申请的方法及其核心思想；同时，对于本领域的一般技术人员，依据本申请的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本申请的限制。

权 利 要 求 书

1、一种文件传输方法，其特征在于，包括：

依据已存文件确定待传输文件的验证目标信息，并发送所述验证目标信息，其中，所述待传输文件与已存文件匹配；

5 从接收的验证信息中获取所述待传输文件中的至少一个标识信息，所述标识信息依据所述验证目标信息确定；

判断所述待传输文件的标识信息，与对应已存文件的标识信息是否匹配；

在确认标识信息匹配后，发送所述待传输文件的信息。

2、根据权利要求 1 所述的方法，其特征在于，所述标识信息包括：消息摘要。

10 3、根据权利要求 2 所述的方法，其特征在于，所述消息摘要包括以下至少一种：消息摘要算法第五版 md5 值、安全哈希算法 SHA 值、base64 值。

4、根据权利要求 1 所述的方法，其特征在于，所述依据已存文件确定待传输文件的验证目标信息，包括：

15 依据所述已存文件对应的标识信息，采用至少一个标识信息对应目标区域确定验证目标信息。

5、根据权利要求 1 所述的方法，其特征在于，采用至少一个标识信息对应目标区域确定验证目标信息，包括：

依据所述至少一个标识信息对应目标区域，确定偏移量和数据长度；

采用所述偏移量和数据长度生成验证目标信息。

20 6、根据权利要求 4 或 5 所述的方法，其特征在于，所述标识信息依据所述待传输文件中目标区域的数据生成。

7、根据权利要求 6 所述的方法，其特征在于，若所述标识信息多于一个，则各标识信息依据所述待传输文件中非连续的目标区域对应数据计算确定。

8、根据权利要求 1 所述的方法，其特征在于，还包括：

25 获取传输通道的通道标识，在所述验证目标信息中添加所述传输通道的通道标识。

9、根据权利要求 8 所述的方法，其特征在于，还包括：

依据所述通道标识，判断是否所述传输通道是否有效；

若所述传输通道有效，执行所述标识信息的匹配判断步骤。

10、根据权利要求 1 所述的方法，其特征在于，还包括：

30 接收所述待传输文件的文件信息，从所述文件信息中获取至少一个文件标识信息；

判断所述待传输文件的文件标识信息，与已存文件的文件标识信息是否匹配；

若文件标识信息匹配，则确认所述待传输文件和所述已存文件匹配。

11、根据权利要求 10 所述的方法，其特征在于，所述文件信息还包括：所述待传输文件的文件大小；所述判断文件标识信息匹配之后，还包括：

5 判断所述待传输文件的文件大小，与文件标识信息匹配的已存文件的文件大小是否相匹配；

若文件大小相匹配，则确认所述待传输文件和所述已存文件匹配。

12、根据权利要求 1 所述的方法，其特征在于，所述待传输文件的信息包括：所述待传输文件的存储信息，所述的方法还包括：

10 为所述待传输文件分配文件标识，并将所述文件标识和所述已存文件对应存储记录建立关联关系；

采用所述存储记录中的文件地址和/或所述文件标识，生成所述待传输文件的存储信息。

13、一种文件传输方法，其特征在于，包括：

15 接收验证目标信息，其中，所述验证目标信息是依据与待传输文件匹配的已存文件生成的；

依据所述验证目标信息确定所述待传输文件的至少一个标识信息，依据所述标识信息生成验证信息；

发送所述验证信息；

20 接收所述待传输文件的信息。

14、根据权利要求 13 所述的方法，其特征在于，所述标识信息包括：消息摘要。

15、根据权利要求 14 所述的方法，其特征在于，所述消息摘要包括以下至少一种：消息摘要算法第五版 md5 值、安全哈希算法 SHA 值、base64 值。

16、根据权利要求 13 所述的方法，其特征在于，所述依据所述验证目标信息确定
25 所述待传输文件的至少一个标识信息，包括：

依据所述验证目标信息，确定所述待传输文件对应至少一个目标区域；

计算所述目标区域对应数据的标识信息。

17、根据权利要求 16 所述的方法，其特征在于，依据所述验证目标信息，确定所述待传输文件对应至少一个目标区域，包括：

30 从验证目标信息中获取至少一个数据长度和至少一个偏移量；

依据所述偏移量和数据长度，从所述待传输文件中确定目标区域。

18、根据权利要求 13 所述的方法，其特征在于，所述验证目标信息包括：通道标识；所述的方法还包括：

依据所述通道标识，判断对应的传输通道是否有效；

5 在确认传输通道有效后，执行发送所述验证信息的步骤。

19、根据权利要求 16 或 17 所述的方法，其特征在于，若所述验证信息包括多于一个标识信息，则各标识信息依据所述待传输文件中非连续的目标区域对应数据计算确定。

20、根据权利要求 13 所述的方法，其特征在于，还包括：

10 生成所述待传输文件的文件信息，并发送待传输文件的文件信息，其中，所述文件信息用于确定与所述待传输文件匹配的已存文件。

21、根据权利要求 20 所述的方法，其特征在于，所述生成所述待传输文件的文件信息，包括：

15 计算所述待传输文件的至少一个文件标识信息，将所述待传输文件的至少一种文件标识信息作为文件信息。

22、根据权利要求 21 所述的方法，其特征在于，还包括：

获取所述待传输文件的文件大小，在所述文件信息中添加所述待传输文件的文件大小。

23、一种文件传输装置，其特征在于，包括：

20 目标发送模块，用于依据已存文件确定待传输文件的验证目标信息，并发送所述验证目标信息，其中，所述待传输文件与已存文件匹配；

获取模块，用于从接收的验证信息中获取所述待传输文件中的至少一个标识信息，所述标识信息依据所述验证目标信息确定；

25 判断模块，用于判断所述待传输文件的标识信息，与对应已存文件的标识信息是否匹配；

存储发送模块，用于在确认标识信息匹配后，发送所述待传输文件的信息。

24、根据权利要求 23 所述的装置，其特征在于，所述标识信息包括：消息摘要。

25、根据权利要求 23 所述的装置，其特征在于，

30 所述获取模块，还用于接收所述待传输文件的文件信息，从所述文件信息中获取至少一个文件标识信息；

所述判断模块，还用于判断所述待传输文件的文件标识信息，与已存文件的文件标识信息是否匹配；若文件标识信息匹配，则确认所述待传输文件和所述已存文件匹配。

26、一种文件传输装置，其特征在于，包括：

接收模块，用于接收验证目标信息，其中，所述验证目标信息是依据与待传输文件匹配的已存文件生成的；以及，接收所述待传输文件的信息；

验证信息确定模块，用于依据所述验证目标信息确定所述待传输文件的至少一个标识信息，依据所述标识信息生成验证信息；

发送模块，用于发送所述验证信息。

27、根据权利要求 26 所述的装置，其特征在于，所述标识信息包括：消息摘要。

10 28、根据权利要求 26 所述的装置，其特征在于，还包括：

文件信息确定模块，用于生成所述待传输文件的文件信息，并发送待传输文件的文件信息，其中，所述文件信息用于确定与所述待传输文件匹配的已存文件。

29、一种服务器，其特征在于，包括：

一个或多个处理器；和

15 其上存储有指令的一个或多个机器可读介质，当由所述一个或多个处理器执行时，使得所述服务器执行如权利要求 1-12 中一个或多个所述的方法。

30、一个或多个机器可读介质，其上存储有指令，当由一个或多个处理器执行时，使得服务器执行如权利要求 1-12 中一个或多个所述的方法。

31、一种终端设备，其特征在于，包括：

20 一个或多个处理器；和

其上存储有指令的一个或多个机器可读介质，当由所述一个或多个处理器执行时，使得所述终端设备执行如权利要求 13-22 中一个或多个所述的方法。

32、一个或多个机器可读介质，其上存储有指令，当由一个或多个处理器执行时，使得终端设备执行如权利要求 13-22 中一个或多个所述的方法。

25 33、一种用于终端设备的操作系统，其特征在于，包括：

接收单元，接收验证目标信息，其中，所述验证目标信息是依据与待传输文件匹配的已存文件生成的；及接收所述待传输文件的信息；

验证单元，依据所述验证目标信息确定所述待传输文件的至少一个标识信息，依据所述标识信息生成验证信息；

30 通信单元，发送所述验证信息。

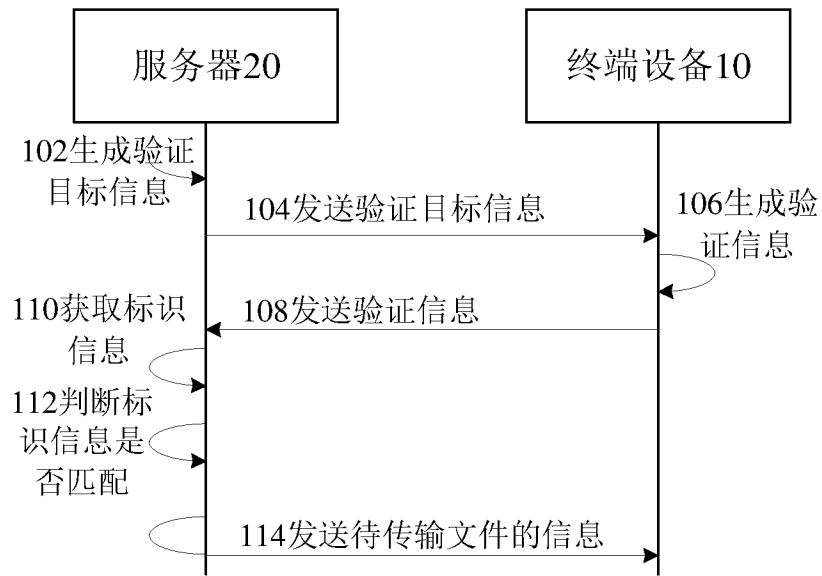


图 1

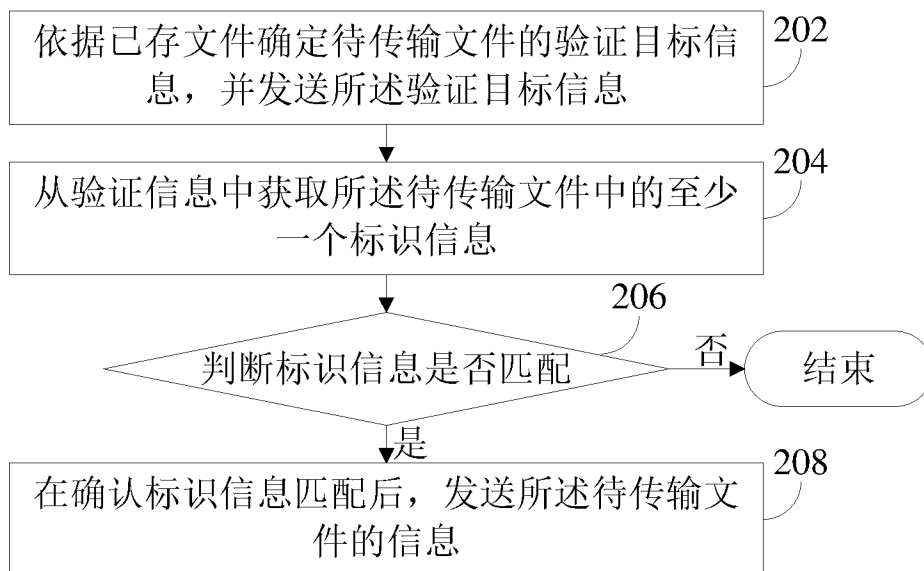


图 2

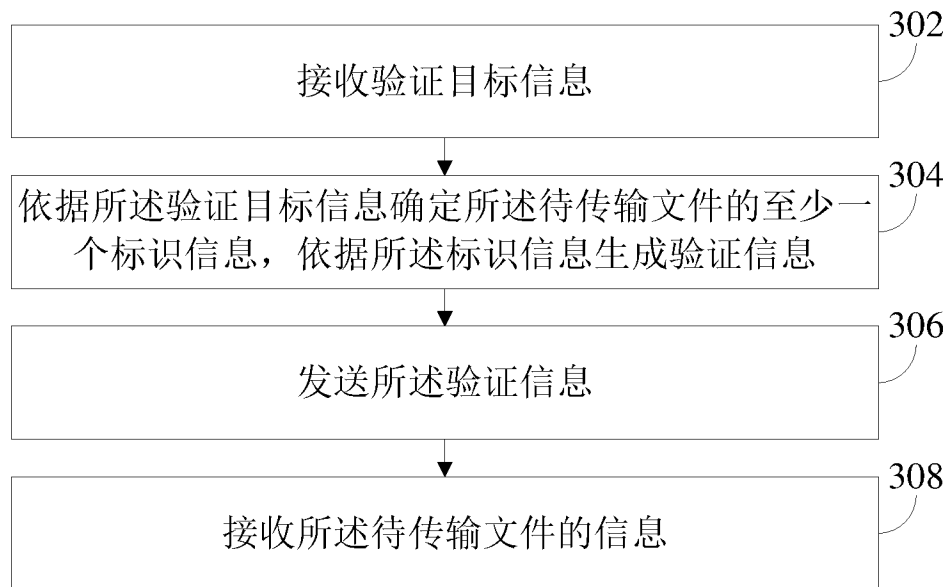


图 3

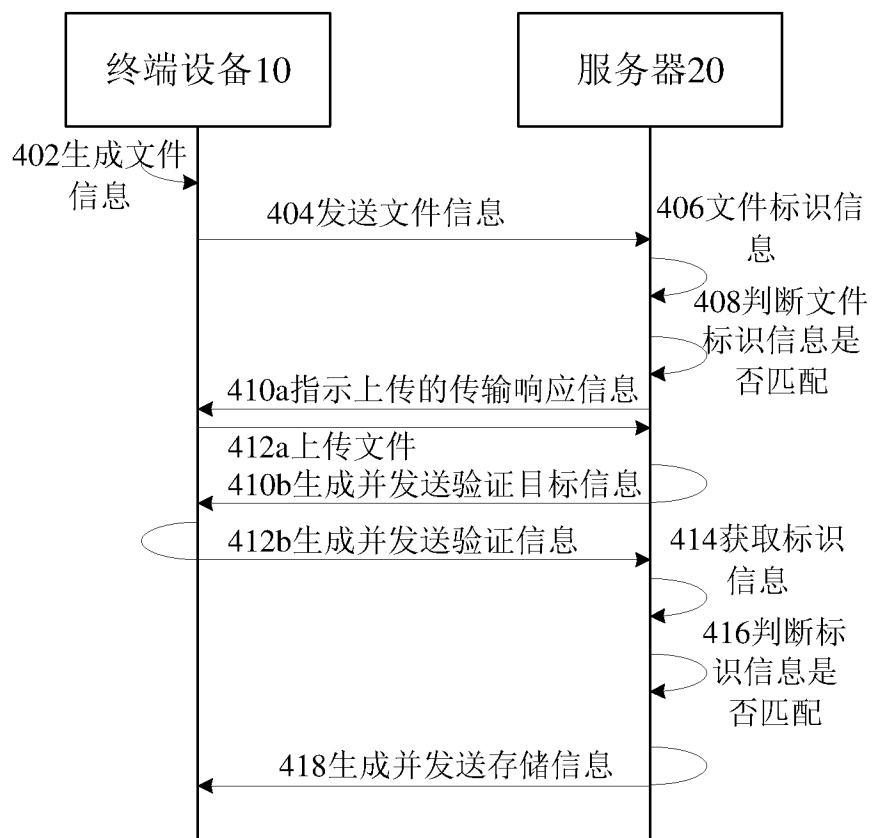


图 4

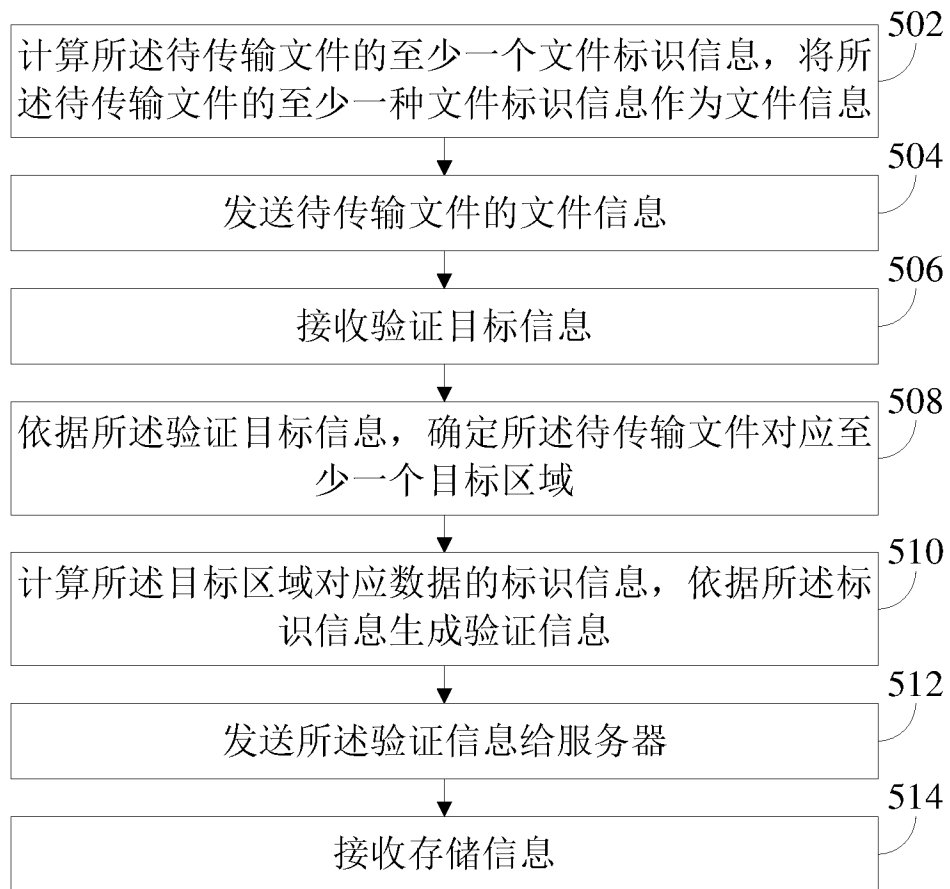


图 5

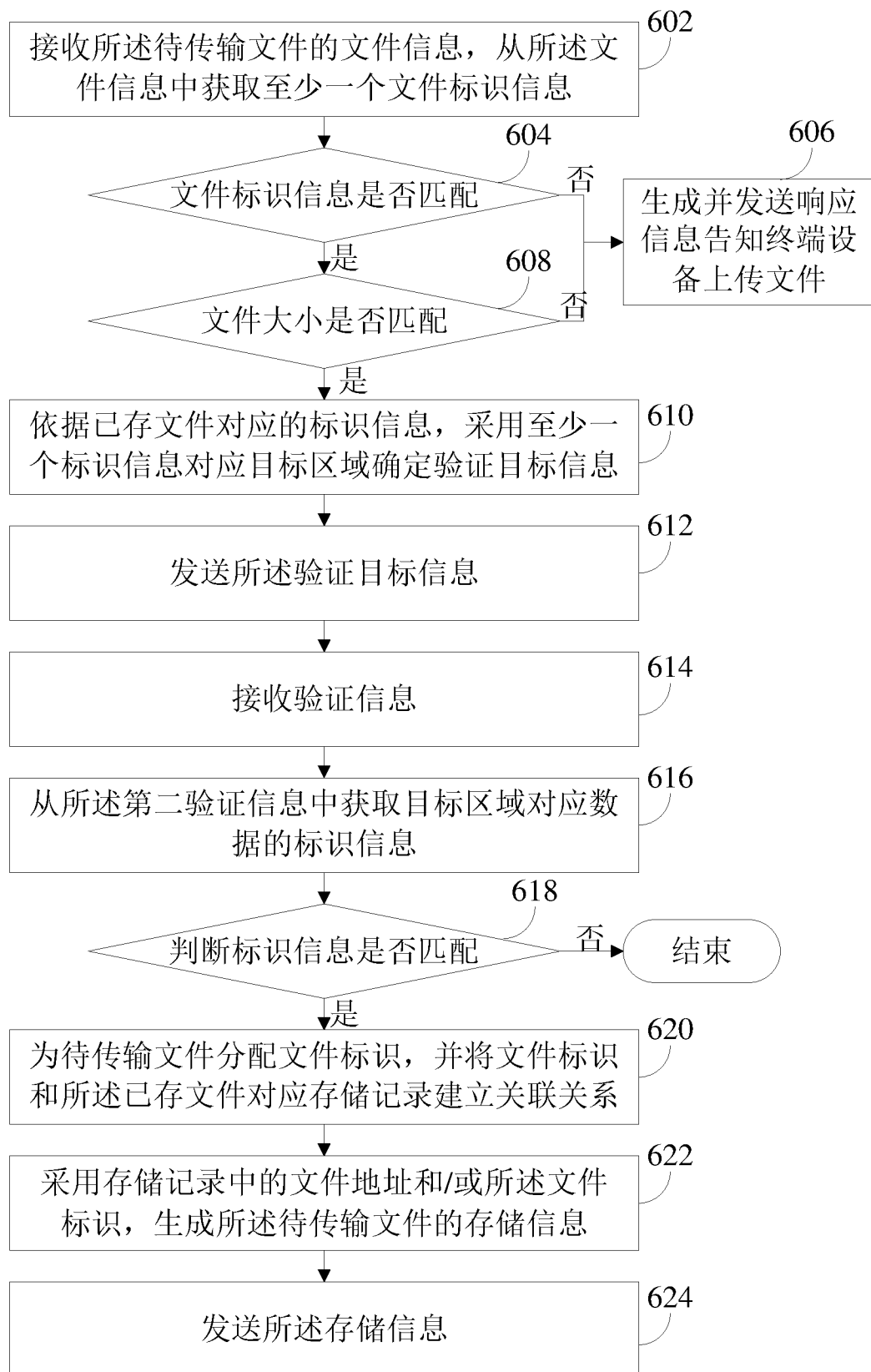


图 6



图 7



图 8



图 9

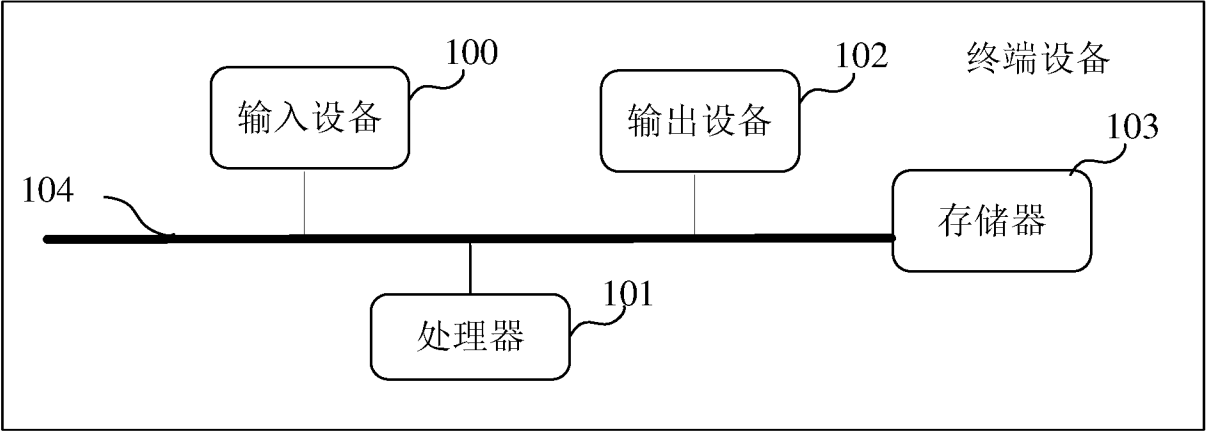


图 10

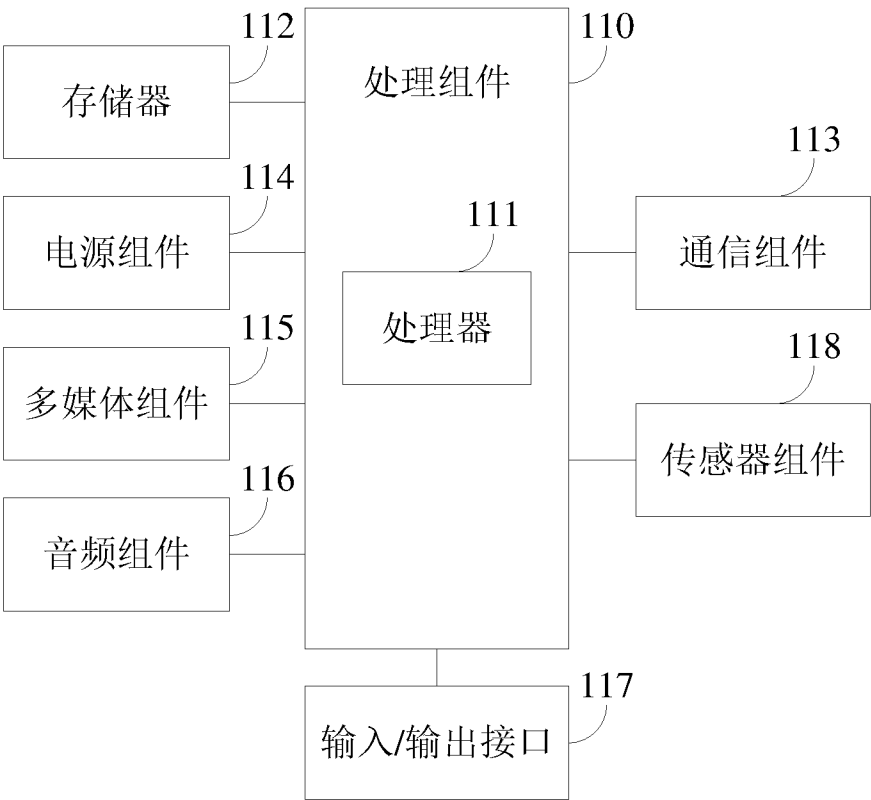


图 11



图 12

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2018/095873

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/58(2006.01)i; H04L 29/08(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, H04N, 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, WPI, EPODOC, CNKI, IEEE: 秒传, 安全, 验证, 标识, 匹配, 唯一, 摘要, 哈希, MD5, security, verify, identifier, match, digester, hash

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 104602102 A (TENCENT TECHNOLOGY (BEIJING) COMPANY LIMITED) 06 May 2015 (2015-05-06) description, paragraphs [0004]-[0009]	1-33
A	CN 103269302 A (BEIJING QIHOO TECHNOLOGY CO., LTD. ET AL.) 28 August 2013 (2013-08-28) entire document	1-33
A	US 2006101220 A1 (COHN, J.A.) 11 May 2006 (2006-05-11) entire document	1-33



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

14 September 2018

Date of mailing of the international search report

27 September 2018

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

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2018/095873

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	104602102	A	06 May 2015	None			
CN	103269302	A	28 August 2013	None			
US	2006101220	A1	11 May 2006	CN	1773502	A	17 May 2006

国际检索报告

国际申请号

PCT/CN2018/095873

A. 主题的分类 H04L 12/58(2006.01)i; H04L 29/08(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, H04N, 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, WPI, EPODOC, CNKI, IEEE: 秒传, 安全, 验证, 标识, 匹配, 唯一, 摘要, 哈希, MD5, security, verify, identifier, match, digester, hash														
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>A</td> <td>CN 104602102 A (腾讯科技北京有限公司) 2015年 5月 6日 (2015 - 05 - 06) 说明书第[0004]-[0009]段</td> <td>1-33</td> </tr> <tr> <td>A</td> <td>CN 103269302 A (北京奇虎科技有限公司等) 2013年 8月 28日 (2013 - 08 - 28) 全文</td> <td>1-33</td> </tr> <tr> <td>A</td> <td>US 2006101220 A1 (COHN, JEREMY A.) 2006年 5月 11日 (2006 - 05 - 11) 全文</td> <td>1-33</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	A	CN 104602102 A (腾讯科技北京有限公司) 2015年 5月 6日 (2015 - 05 - 06) 说明书第[0004]-[0009]段	1-33	A	CN 103269302 A (北京奇虎科技有限公司等) 2013年 8月 28日 (2013 - 08 - 28) 全文	1-33	A	US 2006101220 A1 (COHN, JEREMY A.) 2006年 5月 11日 (2006 - 05 - 11) 全文	1-33
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求												
A	CN 104602102 A (腾讯科技北京有限公司) 2015年 5月 6日 (2015 - 05 - 06) 说明书第[0004]-[0009]段	1-33												
A	CN 103269302 A (北京奇虎科技有限公司等) 2013年 8月 28日 (2013 - 08 - 28) 全文	1-33												
A	US 2006101220 A1 (COHN, JEREMY A.) 2006年 5月 11日 (2006 - 05 - 11) 全文	1-33												
☐ 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 2018年 9月 14日		国际检索报告邮寄日期 2018年 9月 27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)-53961742												

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2018/095873

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	104602102	A	2015年 5月 6日	无	
CN	103269302	A	2013年 8月 28日	无	
US	2006101220	A1	2006年 5月 11日	CN 1773502 A	2006年 5月 17日