

(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
2020 年 8 月 20 日 (20.08.2020)



(10) 国际公布号
WO 2020/164211 A1

(51) 国际专利分类号:
G06F 21/60 (2013.01) **H04L 29/06** (2006.01)

(21) 国际申请号: PCT/CN2019/091503

(22) 国际申请日: 2019 年 6 月 17 日 (17.06.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910111103.8 2019 年 2 月 12 日 (12.02.2019) CN

(71) 申请人: 平安科技(深圳)有限公司(PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) [CN/CN]; 中国广东省深圳市福田区福田街道福安社区益田路 5033 号平安金融中心 23 楼, Guangdong 518000 (CN)。

(72) 发明人: 黄锦伦(HUANG, Jinlun); 中国广东省深圳市福田区福田街道福安社区益田路 5033 号平安金融中心 23 楼, Guangdong 518000 (CN)。
杨益(YANG, Yi); 中国广东省深圳市福田区福田街道福安社区益田路 5033 号平安金融中心 23 楼, Guangdong 518000 (CN)。

(74) 代理人: 深圳中一联合知识产权代理有限公司(SHENZHEN ZHONGYI UNION INTELLECTUAL PROPERTY AGENCY CO., LTD.); 中国广东省深圳市福田区园岭街道深南中路 1014 号报春大厦 9 楼(5 号信箱), Guangdong 518028 (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: DATA TRANSMISSION METHOD AND APPARATUS, TERMINAL DEVICE AND MEDIUM

(54) 发明名称: 一种数据传输方法、装置、终端设备及介质

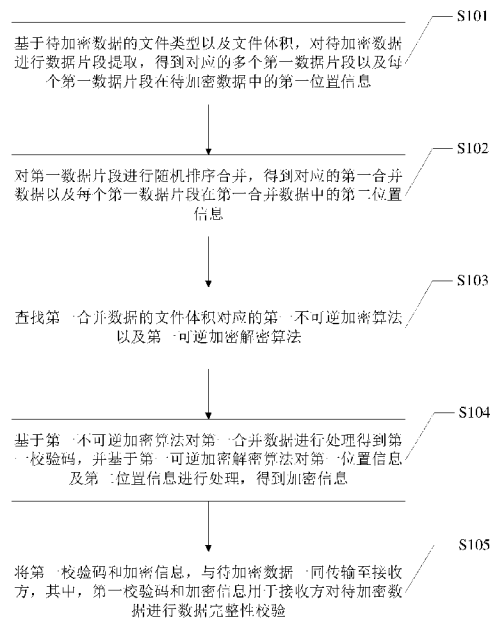


图 1

S101 Perform fragment extraction according to the file type and file size of data to be encrypted to obtain multiple corresponding first data fragments and first position information of each first data fragment in the data to be encrypted

S102 Randomly sort and combine the first fragments to obtain corresponding first combined data as well as second position information of each first data fragment in the first combined data

S103 Search for an irreversible encryption algorithm and reversible encryption algorithm corresponding to the file size of the combined data

S104 Process the first combined data according to the first irreversible encryption algorithm to obtain a first check code, and process the first position information and the second position information according to the first reversible encryption algorithm to obtain encryption information

S105 Transmit the first check code and encryption information together with the data to be encrypted to a receiver, the first check code and encryption information being used by the receiver for verifying the data integrity of the data to be encrypted

(57) Abstract: The present application is applicable in the technical field of data processing, and provided thereby are a data transmission method and apparatus, a terminal device and a medium, the method comprising: performing fragment extraction according to the file type and file size of data to be encrypted to obtain multiple data fragments and position information; randomly sorting and combining the data fragments to obtain combined data as well as position information of each data fragment in the combined data; searching for an irreversible encryption algorithm and reversible encryption algorithm corresponding to the file size of the combined data; processing the

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, 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))。

combined data on the basis of the irreversible encryption algorithm to obtain a check code, and processing the position information on the basis of the reversible encryption algorithm to obtain encryption information; and performing data transmission on the check code and encryption information together with the data to be encrypted. Compared to a fixed single processing algorithm, the embodiment of the present application increases the cracking difficulty index thereof so that criminals cannot predict possibly used algorithms and possible results, thus it is more difficult to crack a corresponding process.

(57) 摘要: 本申请提供了一种数据传输方法、装置、终端设备及介质, 适用于数据处理技术领域, 该方法包括: 基于待加密数据的文件类型和文件体积进行片段提取, 得到多个数据片段以及位置信息; 对数据片段进行随机排序合并, 得到合并数据以及每个数据片段在合并数据中的位置信息; 查找合并数据的文件体积对应的不可逆加密算法以及可逆加密解密算法; 基于不可逆加密算法对合并数据进行处理得到校验码, 并基于可逆加密解密算法对位置信息进行处理, 得到加密信息; 将校验码和加密信息, 与待加密数据一同进行数据传输。本申请实施例相对固定单一的处理算法其破解难度指数上升, 使得不法分子无法预知可能使用的算法以及可能得到的结果, 更难以破解对应的过程。

一种数据传输方法、装置、终端设备及介质

[0001] 本申请要求于2019年2月12日提交中国专利局、申请号为201910111103.8、发明名称为“一种数据传输方法、装置、终端设备及介质”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。

技术领域

[0002] 本申请属于数据处理技术领域，尤其涉及数据传输方法及终端设备。

背景技术

[0003] 在数据传输过程中，数据极其容易受到网络故障或者不法分子攻击而出错，为了保证数据传输的安全可靠，现有技术中都是采用选取的固定加密算法直接对数据进行校验码计算，再在接收端利用校验码进行验证判断数据是否完整，但由于现有技术采用的加密算法往往固定且单一，不法分子很容易针对性地进行破解。因此，为了保证数据传输的安全完整，需要一种安全性和可靠性更高的数据传输校验方法。

发明概述

技术问题

[0004] 有鉴于此，本申请实施例提供了一种数据传输方法及终端设备，以解决现有技术中数据传输过程中，数据加密校验安全性和可靠性较低的问题。

问题的解决方案

技术解决方案

[0005] 本申请实施例的第一方面提供了一种数据传输方法，包括：

[0006] 基于待加密数据的文件类型以及文件体积，对所述待加密数据进行数据片段提取，得到对应的多个第一数据片段以及每个所述第一数据片段在所述待加密数据中的第一位置信息；

[0007] 对所述第一数据片段进行随机排序合并，得到对应的第一合并数据以及每个所述第一数据片段在所述第一合并数据中的第二位置信息；

[0008] 查找所述第一合并数据的文件体积对应的第一不可逆加密算法以及第一可逆加

密解密算法；

[0009] 基于所述第一不可逆加密算法对所述第一合并数据进行处理得到第一校验码，并基于所述第一可逆加密解密算法对所述第一位置信息及所述第二位置信息进行处理，得到加密信息；

[0010] 将所述第一校验码和所述加密信息，与所述待加密数据一同传输至接收方，其中，所述第一校验码和所述加密信息用于所述接收方对所述待加密数据进行数据完整性校验。

[0011] 本申请实施例的第二方面提供了一种数据校验方法，包括：

[0012] 获取如权利要求1所述数据传输方法传输的所述待加密数据、所述第一校验码以及所述加密信息；

[0013] 基于所述待加密数据的文件类型以及文件体积，对所述待加密数据进行数据片段提取，得到对应的多个第二数据片段以及每个所述第二数据片段在所述待加密数据中的第三位置信息；

[0014] 查找所述第二数据片段的文件体积和对应的第二不可逆加密算法以及第二可逆加密解密算法，并基于所述第二可逆加密解密算法对所述加密信息进行处理，得到所述第一位置信息和所述第二位置信息；

[0015] 基于所述第三位置信息、所述第一位置信息和所述第二位置信息，对所述第二数据片段进行排序合并，得到对应的第二合并数据；

[0016] 基于所述第二不可逆加密算法对所述第二合并数据进行处理得到第二校验码，并判断所述第二校验码与所述第一校验码是否相同；

[0017] 若所述第二校验码与所述第一校验码相同，判定所述待加密数据校验完整。

[0018] 本申请实施例的第三方面提供了一种数据传输装置，包括：

[0019] 第一片段提取模块，用于基于待加密数据的文件类型以及文件体积，对所述待加密数据进行数据片段提取，得到对应的多个第一数据片段以及每个所述第一数据片段在所述待加密数据中的第一位置信息；

[0020] 片段排序模块，用于对所述第一数据片段进行随机排序合并，得到对应的第一合并数据以及每个所述第一数据片段在所述第一合并数据中的第二位置信息；

[0021] 第一算法匹配模块，用于查找所述第一合并数据的文件体积对应的第一不可逆

加密算法以及第一可逆加密解密算法；

[0022] 双重加密模块，用于基于所述第一不可逆加密算法对所述第一合并数据进行处理得到第一校验码，并基于所述第一可逆加密解密算法对所述第一位置信息及所述第二位置信息进行处理，得到加密信息；

[0023] 数据传输模块，用于将所述第一校验码和所述加密信息，与所述待加密数据一同传输至接收方，其中，所述第一校验码和所述加密信息用于所述接收方对所述待加密数据进行数据完整性校验。

[0024] 本申请实施例的第三方面提供了一种数据传输装置，包括：

[0025] 第一片段提取模块，用于基于待加密数据的文件类型以及文件体积，对所述待加密数据进行数据片段提取，得到对应的多个第一数据片段以及每个所述第一数据片段在所述待加密数据中的第一位置信息；

[0026] 片段排序模块，用于对所述第一数据片段进行随机排序合并，得到对应的第一合并数据以及每个所述第一数据片段在所述第一合并数据中的第二位置信息；

[0027] 第一算法匹配模块，用于查找所述第一合并数据的文件体积对应的第一不可逆加密算法以及第一可逆加密解密算法；

[0028] 双重加密模块，用于基于所述第一不可逆加密算法对所述第一合并数据进行处理得到第一校验码，并基于所述第一可逆加密解密算法对所述第一位置信息及所述第二位置信息进行处理，得到加密信息；

[0029] 数据传输模块，用于将所述第一校验码和所述加密信息，与所述待加密数据一同传输至接收方，其中，所述第一校验码和所述加密信息用于所述接收方对所述待加密数据进行数据完整性校验。

[0030] 本申请实施例的第四方面提供了一种数据校验装置，包括：

[0031] 数据获取模块，用于获取如上述数据传输装置传输的所述待加密数据、所述第一校验码以及所述加密信息；

[0032] 第二片段提取模块，用于基于所述待加密数据的文件类型以及文件体积，对所述待加密数据进行数据片段提取，得到对应的多个第二数据片段以及每个所述第二数据片段在所述待加密数据中的第三位置信息；

[0033] 第二算法匹配模块，用于查找所述第二数据片段的文件体积和对应的第二不可

逆加密算法以及第二可逆加密解密算法，并基于所述第二可逆加密解密算法对所述加密信息进行处理，得到所述第一位置信息和所述第二位置信息；

[0034] 片段合并模块，用于基于所述第三位置信息、所述第一位置信息和所述第二位置信息，对所述第二数据片段进行排序合并，得到对应的第二合并数据；

[0035] 数据校验模块，用于基于所述第二不可逆加密算法对所述第二合并数据进行处理得到第二校验码，并判断所述第二校验码与所述第一校验码是否相同；

[0036] 判定模块，用于若所述第二校验码与所述第一校验码相同，判定所述待加密数据校验完整。

[0037] 本申请实施例的第五方面提供了一种终端设备，所述终端设备包括存储器、处理器，所述存储器上存储有可在所述处理器上运行的计算机可读指令，所述处理器执行所述计算机可读指令时实现如上所述的数据传输方法的步骤。

[0038] 本申请实施例的第六方面提供了一种终端设备，所述终端设备包括存储器、处理器，所述存储器上存储有可在所述处理器上运行的计算机可读指令，所述处理器执行所述计算机可读指令时实现如上所述的数据校验方法的步骤。

[0039] 本申请实施例的第七方面提供了一种计算机可读存储介质，包括：存储有计算机可读指令，其特征在于，所述计算机可读指令被处理器执行时实现如上所述的数据传输方法的步骤。

发明的有益效果

有益效果

[0040] 本申请实施例与现有技术相比存在的有益效果是：在加密过程中，根据待加密数据的实际文件类型和体积情况来选取对应的数据片段提取方法，并进行数据片段的提取，再对提取得到的数据片段进行随机的排序合并，同时根据数据片段的实际总体积来选取一个不可逆加密算法和可逆加密解密算法，最后再基于不可逆加密算法和可逆加密解密算法分别对合并得到的合并数据，以及数据片段在待加密数据和合并数据中的两个位置信息进行处理，得到对应的校验码以及加密信息，用以后续的校验。由于数据片段提取和及数据片段的加密均是由实际所需传输的数据决定的，同时对数据片段的排序也是每次完全随机的，从而使得每次数据传输过程的三个步骤均具有极大的随机性和唯一性，而三个随

机相乘理论上可以产生大量不同处理方式的组合，相对固定单一的处理算法其破解难度指数上升，使得不法分子无法预知可能使用的算法以及可能得到的结果，更难以破解对应的过程。

对附图的简要说明

附图说明

[0041] 为了更清楚地说明本申请实施例中的技术方案，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一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[0042] 图1是本申请实施例一提供的数据传输方法的实现流程示意图；

[0043] 图2是本申请实施例二提供的数据传输方法的实现流程示意图；

[0044] 图3是本申请实施例三提供的数据传输方法的实现流程示意图；

[0045] 图4是本申请实施例四提供的数据传输方法的实现流程示意图；

[0046] 图5是本申请实施例五提供的数据传输方法的实现流程示意图；

[0047] 图6是本申请实施例四提供的数据校验方法的实现流程示意图；

[0048] 图7是本申请实施例六提供的数据传输装置的结构示意图；

[0049] 图8是本申请实施例六提供的数据校验装置的结构示意图；

[0050] 图9是本申请实施例七提供的终端设备的示意图。

发明实施例

本发明的实施方式

[0051] 以下描述中，为了说明而不是为了限定，提出了诸如特定系统结构、技术之类的具体细节，以便透彻理解本申请实施例。然而，本领域的技术人员应当清楚，在没有这些具体细节的其它实施例中也可以实现本申请。在其它情况中，省略对众所周知的系统、装置、电路以及方法的详细说明，以免不必要的细节妨碍本申请的描述。

[0052] 为了说明本申请所述的技术方案，下面通过具体实施例来进行说明。

[0053] 图1示出了本申请实施例一提供的数据传输方法的实现流程图，详述如下：

[0054] S101，基于待加密数据的文件类型以及文件体积，对待加密数据进行数据片段

提取，得到对应的多个第一数据片段以及每个第一数据片段在待加密数据中的第一位置信息。

[0055] 其中具体可处理的文件类型可由技术人员根据实际需求设定，包括但不限于如图像、音频、视频和文本。考虑到不同文件类型的数据其特点不同，且对于每种加密算法对不同文件体积大小的加密效率也有所差异，因此，为了保证提取出的数据片段具有代表性，以保障后续加密的有效性，同时保证加密的效率以及对后续加密的随机性以提高加密校验的安全性，本申请实施例中会针对不同文件类型和不同文件体积的数据设置不同的片段提取方法，具体而言，可参考本申请实施例二至五，也可由技术人员根据实际需求自行设定。在提取出所需的第一数据片段的同时，本申请实施例还会记录第一数据片段在待加密数据中的实际第一位置信息，如当待加密数据为音频数据时，记录提取出的每个音频数据段在待加密数据中的起始时间和终止时间，从而得到其在待加密数据中的第一位置信息。

[0056] S102，对第一数据片段进行随机排序合并，得到对应的第一合并数据以及每个第一数据片段在第一合并数据中的第二位置信息。

[0057] 在得到待加密数据中提取的多个第一数据片段之后，本申请实施例会对其进行随机的排序并合并，同时记录排序后的第二位置信息，这个位置信息既可以是在第一合并数据中的绝对位置，如上述的当待加密数据为音频数据时，记录提取出的每个音频数据段在待加密数据中的起始时间和终止时间，也可以是在第一合并数据中的相对位置，如排序后的序号，具体由技术人员自行选取。

[0058] S103，查找第一合并数据的文件体积对应的第一不可逆加密算法以及第一可逆加密解密算法。

[0059] S104，基于第一不可逆加密算法对第一合并数据进行处理得到第一校验码，并基于第一可逆加密解密算法对第一位置信息及第二位置信息进行处理，得到加密信息。

[0060] 为了保证数据传输加密验证的可靠性，本申请实施例中会对不同文件体积的合并数据设置不同的不可逆加密算法和可逆加密解密算法，由于上述合并数据是第一数据片段的提取是具有一定随机性的（与每次具体传输数据的类型和体积

相关），从而使得得到的第一合并数据的体积也是具有对应的随机性的，在此基础上为不同体积的合并数据设置对应的不可逆加密算法和可逆加密解密算法，使得本申请实施例中对采用的具体加密算法也是具有一定随机性的，同时，由于第一数据片段是随机排序合并的，因此加密所得到的校验码和加密信息也都是具有极强的随机性的，因此在本申请实施例中，数据片段提取方法、数据片段排序以及合并数据加密算法，均存在随机性，其会随着具体所需传输的数据的变化而变化，且即使是对同一数据重复进行传输校验，其最终得到的校验码和加密信息也是具有随机性的，从而使得本申请实施例中每次的传输校验过程具有唯一性，而因为三个随机相乘，理论上可以产生大量不同的处理算法组合，较一般的单算法处理其破解难度指数上升，破解难度极大，使得不法分子无法预知可能使用的算法以及可能得到的结果，更无法破解对应的过程。

[0061] 其中，具体每种文件体积对应的不可逆加密算法和可逆加密解密算法，可由技术人员根据实际需求设定，包括但不限于如：不可逆的MD5算法和sha1算法，可逆的3DES算法和IDEA算法等等，但需保证所采用的不可逆加密算法和可逆加密解密算法的算法种类都大于1。

[0062] S105，将第一校验码和加密信息，与待加密数据一同传输至接收方，其中，第一校验码和加密信息用于接收方对待加密数据进行数据完整性校验。

[0063] 在生成待加密数据对应的第一校验码和加密信息之后，本申请实施例会将第一校验码和加密信息与待加密数据一同发送至接收方，以使得接收方可以对接收到的待加密数据进行完整性校验。

[0064] 在本申请实施例中，在加密过程中，根据待加密数据的实际文件类型和体积情况来选取对应的数据片段提取方法，并进行数据片段的提取，再对提取得到的数据片段进行随机的排序合并，同时根据数据片段的实际总体积来选取一个不可逆加密算法和可逆加密解密算法，最后再基于不可逆加密算法和可逆加密解密算法分别对合并得到的合并数据，以及数据片段在待加密数据和合并数据中的两个位置信息进行处理，得到对应的校验码以及加密信息，用以后续的校验。由于数据片段提取和及数据片段的加密均是由实际所需传输的数据决定的，同时对数据片段的排序也是每次完全随机的，从而使得每次数据传输过程的三

个步骤均具有极大的随机性和唯一性，而三个随机相乘理论上可以产生大量不同处理方式的组合，相对固定单一的处理算法其破解难度指数上升，使得不法分子无法预知可能使用的算法以及可能得到的结果，更难以破解对应的过程。

[0065] 作为本申请实施例一中对待加密数据进行第一数据片段提取的一种具体实现方式，如图2所示，本申请实施例二，包括：

[0066] S201，若待加密数据的文件类型为图像且文件体积小于预设体积阈值，提取待加密数据的图像特征点，并基于图像特征点中的边缘特征点进行连线，绘制对应的多边形。

[0067] S202，对多边形内的图像内容进行分割，得到与第一数据片段一一对应的多个图像区域，并获取每个图像区域在待加密数据中的第一位置信息。

[0068] 当待加密数据为图像且文件体积较小时，为了保证提取出的第一数据片段的有效性，本申请实施例针对图像的特点，以对图像进行特征点提取并绘制包含所有图像特征点的多边形的方式，将图像所有的特征点保留下来，再对多边形内的图像内容进行分割，得到多个图像内容，即为本申请实施例所需的多个第一数据片段。其中，体积阈值的具体大小可由技术人员自行设定。

[0069] 其中，具体的分割方法可由技术人员自行设定，包括但不限于如按照预设图像区域大小进行分割，如按照10像素×10像素的大小进行分割。第一位置信息，既可以是图像区域再待处理数据中的绝对位置，该绝对位置可以以图像区域各个边缘点的坐标构成，此时每个图像区域的第一位置信息可用一组数组记录，也可以是图像区域所有像素点坐标和均值得到的虚拟中心像素坐标位置来作为第一位置信息，此时每个图像区域的第一位置信息仅为一个像素点坐标，具体可由技术人员自行设定。

[0070] 作为本申请实施例一中对待加密数据进行第一数据片段提取的另一种具体实现方式，如图3所示，本申请实施例三，包括：

[0071] S301，若待加密数据的文件类型为文本且文件体积小于预设体积阈值，对待加密数据进行关键字符查找，筛选出文本中与第一数据片段一一对应的多个关键字符，并获取每个关键字符在待加密数据中的第一位置信息。

[0072] 当待加密数据为文本数据且文件体积较小时，为了保证提取出的数据片段的有效

效性，本申请实施例会对待加密数据进行关键字符查找，其中可以由技术人员预先设置好关键字符表，并根据关键字符表内包含的关键字符内容来对待加密数据进行字符匹配，以实现对待加密数据的查找。考虑到不同用户传输数据的需求不同，即对不同用户而言其关键字的内容也会存在差异，因此在本申请实施例中，具体的关键字符表内容可由技术人员根据用户的实际需求决定。其中，体积阈值的具体大小可由技术人员自行设定。

[0073] 作为本申请实施例进行关键字符查找的一种优选实施方式，考虑到实际应用中对于不同的数据而言，其关键字符的具体内容可能无法确定，例如，假设所需传输的待加密数据为保险订单数据，此时其中的订单号、投保人、受益人以及保险金额等均是关键字符，但这些关键字符的内容在每张保险订单中都不相同，因此若关键字符表中仅包含固定的一些关键字符，可能无法满足不同用户的实际需求。

[0074] 为了满足不同用户的实际需求，本申请实施例中，关键字符表中包含的不仅包含一些具体关键字符，同时还包含一些关键字符规则，在进行关键字符查找时，只要满足关键字符表中包含的具体关键字符或者关键字符规则，都可以被判定为关键字符，例如，对于上述保险订单数据而言，其可以设置关键字符规则为：“订单号”后的 n 位字符为关键字符， n 由技术人员根据实际情况设定，此时在进行关键字符查找时，“订单号”后面的 n 位数字即会被判定为关键字符。

[0075] 作为本申请实施例一中对待加密数据进行第一数据片段提取的另一种具体实现方式，如图4所示，本申请实施例四，包括：

[0076] S401，若待加密数据的文件类型为音频且文件体积小于预设体积阈值，对待加密数据进行语音识别，判断待加密数据是否为语音数据。

[0077] S402，若待加密数据为语音数据，对语音识别得到的文字内容进行关键词查找，得到待加密数据对应的关键词。

[0078] S403，从待加密数据提取出与关键词一一对应的第一数据片段，并获取每个第一数据片段在待加密数据中的第一位置信息。

[0079] 当待加密数据为音频数据且文件体积较小时，本申请实施例会对音频数据进行语音识别，以判断其是否为语音数据，若语音识别出包含文字内容，则说明其

为语音数据。其中，体积阈值的具体大小可由技术人员自行设定。

[0080] 为了保证提取出的数据片段的有效性，本申请实施例会对语音识别得到的文字内容进行关键词查找，其中具体的查找方法此处不予限定，可由技术人员自行设定或者参考本申请实施例三中对关键字符的查找方法（本申请实施例中的关键词相当于本申请实施例三中的关键字符）。在确定出其中包含的关键词之后，本申请实施例会进一步地从待处理数据中查找出这些关键词对应的音频片段，从而得到本申请实施例所需的第一数据片段，由于关键词中包含了文字内容的关键数据，因此其具有一定的代表性，从而保证了后续提取出的第一数据片段的有效性。在本申请实施例中，第一位置信息包含第一数据片段在待加密数据中的起始时间和终止时间。

[0081] 作为本申请实施例一中对待加密数据进行第一数据片段提取的另一种具体实现方式，如图5所示，本申请实施例五，包括：

[0082] S501，若待加密数据为任意文件类型，且文件体积大于或等于预设体积阈值，以预设数据间隔对待加密数据进行数据段提取，得到多个第一数据片段以及每个第一数据片段在待加密数据中的第一位置信息。

[0083] 当文件体积较大时，无论是何种文件类型在进行数据片段提取时其提取的工作量都比较大，会直接导致数据传输的效率较低，因此，在待加密数据的文件体积较大时，无论其为何种文件类型，本申请实施例都会统一采用根据预设数据间隔的形式进行数据片段的提取，以得到所需的多个第一数据片段，其中具体的数据间隔可由技术人员根据实际需求自行设定，其既可以是一个绝对数值，例如可以设置为将待加密数据转换为二进制数据，并每隔一个具体数据间隔长度提取一个设定长度的数据片段，如每隔200位二进制数，提取一个500位二进制长的数据片段，从而得到所需的第一数据片段，也可以是一个相对数值，例如可以设置为将待加密数据转换为二进制数据，并每隔n%待加密数据总长度的提取一个长度为m%待加密数据总长度的数据片段，如每隔5%待加密数据总长度提取一个长度为15%待加密数据总长度的数据片段。其中，体积阈值的具体大小可由技术人员自行设定。

[0084] 应当说明地，上述本申请实施例二至五均是对待加密数据的数据片段提取方法

，但每个实施例针对的是不同文件类型或文件体积大小的情况，因此本申请实施例二至五之间并不会存在实施时的冲突，本领域的普通技术人员可以从中选取任意数量的实施例与本申请实施例一进行结合应用实施，均应包含在本申请的保护范围之内。

[0085] 在本申请实施例二至五中，针对不同文件类型的待加密数据的特点，分别设置对应的数据片段提取方法，从而保证了提取出的数据片段的有效性。

[0086] 作为本申请实施例六，对应于本申请实施例一，本申请实施例中提出了一种利用本申请实施例一传输的第一校验码和加密信息对待加密数据进行数据完整性校验的方法，图6示出了本申请实施例六提供的的数据校验方法的实现流程图，详述如下：

[0087] S601，获取如本申请实施例一数据传输方法传输的待加密数据、第一校验码以及加密信息。

[0088] S602，基于待加密数据的文件类型以及文件体积，对待加密数据进行数据片段提取，得到对应的多个第二数据片段以及每个第二数据片段在待加密数据中的第三位置信息。

[0089] 本申请实施例中的数据片段提取方法可由技术人员自行设定，但应保证与本申请实施例一所使用的数据片段提取方法相同，即对于文件类型和文件体积相同的数据而言，本申请实施例和本申请实施例一所选取的数据片段提取方法应当保持一致，以保证后续的正常校验，具体可以参考上述本申请实施例一至五，此处不予赘述。

[0090] S603，查找第二数据片段的文件体积和对应的第二不可逆加密算法以及第二可逆加密解密算法，并基于第二可逆加密解密算法对加密信息进行处理，得到第一位置信息和第二位置信息。

[0091] 本申请实施例中第二数据片段的文件体积和与不可逆加密算法和可逆加密解密算法的对应规则可由技术人员自行设定，但应保证与本申请实施例一中第一合并数据的文件体积与不可逆加密算法和可逆加密解密算法的对应规则相同，即当第二数据片段的文件体积和与第一合并数据的文件体积相同时，本申请实施例和本申请实施例一所选取的不可逆加密算法和可逆加密解密算法应当保持一

致，以保证后续的正常校验，具体可以参考上述本申请实施例一，此处不予赘述。

[0092] S604，基于第三位置信息、第一位置信息和第二位置信息，对第二数据片段进行排序合并，得到对应的第二合并数据。

[0093] 当接收到的待加密数据与本申请实施例一中发送的待加密数据完全相同时，理论上S602中提取的第二数据片段是和本申请实施例一中的第一数据片段的数据内容和位置应当是完全一致的，同时选取出的不可逆加密算法和可逆加密解密算法也应当是完全一致的，因此，当接收到的待加密数据与本申请实施例一中发送的待加密数据完全相同时，第三位置信息与第一位置信息是完全相同的，此时根据第一位置信息与第二位置信息的对应关系即可实现对第二数据片段的排序，并保证与第一数据片段随机排序的结果完全一致。

[0094] S605，基于第二不可逆加密算法对第二合并数据进行处理得到第二校验码，并判断第二校验码与第一校验码是否相同。

[0095] S606，若第二校验码与第一校验码相同，判定待加密数据校验完整。

[0096] 当接收到的待加密数据与本申请实施例一中发送的待加密数据不完全相同时，即存在网络故障或者不法分子攻击等原因而出错，直接导致待加密数据的数据内容和/或文件体积发生变化时，会导致本申请实施例中对数据片段的提取、合并加密解密过程产生变化，由于提取、合并加密解密根据待加密数据的具体数据类型和内容不同而具有极强的随机性，会导致解密出的第一位置信息和第二位置信息出现误差，同时得到的第三位置信息也会存在错误，从而使得本申请实施例S604中第三位置信息难以和第一位置信息对应起来，使得无法正常得到第二合并数据，从而使得后续的加密过程无法正常进行，即使退一步第三位置信息和第一位置信息对应起来，由于后续的第二不可逆加密算法选取时已经随着第二数据片段的变化而变化，且第二合并数据的数据内容也随着待加密数据的变化而变化，从而使得得到的第二校验码必然与第一校验码存在差异，因此本申请实施例中只有接收到的待加密数据与本申请实施例一中发送的待加密数据完全一致时，才会得到最终的第二校验码与第一校验码的结果，从而实现了数据传输的安全完整校验。

- [0097] 对应于上文实施例的数据传输方法，图7示出了本申请实施例七提供的数据传输装置的结构框图，为了便于说明，仅示出了与本申请实施例相关的部分。图7示例的数据传输装置可以是前述实施例一提供的数据传输方法的执行主体。
- [0098] 参照图7，该数据传输装置包括：
- [0099] 第一片段提取模块71，用于基于待加密数据的文件类型以及文件体积，对所述待加密数据进行数据片段提取，得到对应的多个第一数据片段以及每个所述第一数据片段在所述待加密数据中的第一位置信息。
- [0100] 片段排序模块72，用于对所述第一数据片段进行随机排序合并，得到对应的第一合并数据以及每个所述第一数据片段在所述第一合并数据中的第二位置信息。
- [0101] 第一算法匹配模块73，用于查找所述第一合并数据的文件体积对应的第一不可逆加密算法以及第一可逆加密解密算法。
- [0102] 双重加密模块74，用于基于所述第一不可逆加密算法对所述第一合并数据进行处理得到第一校验码，并基于所述第一可逆加密解密算法对所述第一位置信息及所述第二位置信息进行处理，得到加密信息。
- [0103] 数据传输模块75，用于将所述第一校验码和所述加密信息，与所述待加密数据一同传输至接收方，其中，所述第一校验码和所述加密信息用于所述接收方对所述待加密数据进行数据完整性校验。
- [0104] 进一步地，第一片段提取模块71，包括：
- [0105] 若所述待加密数据的文件类型为图像且文件体积小于预设体积阈值，提取所述待加密数据的图像特征点，并基于所述图像特征点中的边缘特征点进行连线，绘制对应的多边形。
- [0106] 对所述多边形内的图像内容进行分割，得到与所述第一数据片段一一对应的多个图像区域，并获取每个所述图像区域在所述待加密数据中的所述第一位置信息。
- [0107] 进一步地，第一片段提取模块71，包括：
- [0108] 若所述待加密数据的文件类型为文本且文件体积小于预设体积阈值，对所述待加密数据进行关键字符查找，筛选出所述文本中与所述第一数据片段一一对应

的多个关键字符，并获取每个关键字符在所述待加密数据中的所述第一位置信息。

[0109] 进一步地，第一片段提取模块71，包括：

[0110] 若所述待加密数据的文件类型为音频且文件体积小于预设体积阈值，对所述待加密数据进行语音识别，判断所述待加密数据是否为语音数据。

[0111] 若所述待加密数据为语音数据，对语音识别得到的文字内容进行关键词查找，得到所述待加密数据对应的关键词。

[0112] 从所述待加密数据提取出与所述关键词一一对应的所述第一数据片段，并获取每个所述第一数据片段在所述待加密数据中的所述第一位置信息。

[0113] 进一步地，第一片段提取模块71，包括：

[0114] 若所述待加密数据为任意文件类型，且文件体积大于或等于预设体积阈值，以预设数据间隔对所述待加密数据进行数据段提取，得到多个所述第一数据片段以及每个所述第一数据片段在所述待加密数据中的所述第一位置信息。

[0115] 本申请实施例提供的数据传输装置中各模块实现各自功能的过程，具体可参考前述图1所示实施例一的描述，此处不再赘述。

[0116] 对应于上文实施例的数据校验方法，图8示出了本申请实施例提供的数据校验装置的结构框图，为了便于说明，仅示出了与本申请实施例相关的部分。图8示例的数据校验装置可以是前述实施例六提供的数据校验方法的执行主体。

[0117] 数据获取模块81，用于获取如本申请实施例七所述数据传输装置传输的所述待加密数据、所述第一校验码以及所述加密信息。

[0118] 第二片段提取模块82，用于基于所述待加密数据的文件类型以及文件体积，对所述待加密数据进行数据片段提取，得到对应的多个第二数据片段以及每个所述第二数据片段在所述待加密数据中的第三位置信息。

[0119] 第二算法匹配模块83，用于查找所述第二数据片段的文件体积和对应的第二不可逆加密算法以及第二可逆加密解密算法，并基于所述第二可逆加密解密算法对所述加密信息进行处理，得到所述第一位置信息和所述第二位置信息。

[0120] 片段合并模块84，用于基于所述第三位置信息、所述第一位置信息和所述第二位置信息，对所述第二数据片段进行排序合并，得到对应的第二合并数据。

- [0121] 数据校验模块85，用于基于所述第二不可逆加密算法对所述第二合并数据进行处理得到第二校验码，并判断所述第二校验码与所述第一校验码是否相同。
- [0122] 判定模块86，用于若所述第二校验码与所述第一校验码相同，判定所述待加密数据校验完整。
- [0123] 本申请实施例提供的的数据校验装置中各模块实现各自功能的过程，具体可参考前述图6所示实施例六的描述，此处不再赘述。
- [0124] 应理解，上述实施例中各步骤的序号的大小并不意味着执行顺序的先后，各过程的执行顺序应以其功能和内在逻辑确定，而不对本申请实施例的实施过程构成任何限定。
- [0125] 还应理解的是，虽然术语“第一”、“第二”等在文本中在一些本申请实施例中用来描述各种元素，但是这些元素不应该受到这些术语的限制。这些术语只是用来将一个元素与另一元素区分开。例如，第一表格可以被命名为第二表格，并且类似地，第二表格可以被命名为第一表格，而不背离各种所描述的实施例的范围。第一表格和第二表格都是表格，但是它们不是同一表格。
- [0126] 图9是本申请一实施例提供的终端设备的示意图。如图9所示，该实施例的终端设备9包括：处理器90、存储器91，所述存储器91中存储有可在所述处理器90上运行的计算机可读指令92。所述处理器90执行所述计算机可读指令92时实现上述各个数据传输方法实施例中的步骤，例如图1所示的步骤101至105。或者，所述处理器90执行所述计算机可读指令92时实现上述各装置实施例中各模块/单元的功能，例如图7所示模块71至75的功能。
- [0127] 所述终端设备9可以是桌上型计算机、笔记本、掌上电脑及云端服务器等计算设备。所述终端设备可包括，但不仅限于，处理器90、存储器91。本领域技术人员可以理解，图9仅仅是终端设备9的示例，并不构成对终端设备9的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件，例如所述终端设备还可以包括输入发送设备、网络接入设备、总线等。
- [0128] 所称处理器90可以是中央处理单元（Central Processing Unit，CPU），还可以是其他通用处理器、数字信号处理器（Digital Signal Processor，DSP）、专用集成电路（Application Specific Integrated

Circuit, ASIC)、现成可编程门阵列(Field-Programmable Gate Array, FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。

[0129] 所述存储器91可以是所述终端设备9的内部存储单元,例如终端设备9的硬盘或内存。所述存储器91也可以是所述终端设备9的外部存储设备,例如所述终端设备9上配备的插接式硬盘,智能存储卡(Smart Media Card, SMC),安全数字(Secure Digital, SD)卡,闪存卡(Flash Card)等。进一步地,所述存储器91还可以既包括所述终端设备9的内部存储单元也包括外部存储设备。所述存储器91用于存储所述计算机可读指令以及所述终端设备所需的其他程序和数据。所述存储器91还可以用于暂时地存储已经发送或者将要发送的数据。

[0130] 另外,在本申请各个实施例中的各功能单元可以集成在一个处理单元中,也可以是各个单元单独物理存在,也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现,也可以采用软件功能单元的形式实现。

[0131] 所述集成的模块/单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时,可以存储在一个计算机可读取存储介质中。基于这样的理解,本申请实现上述实施例方法中的全部或部分流程,也可以通过计算机可读指令来指令相关的硬件来完成,所述的计算机可读指令可存储于一计算机可读存储介质中,该计算机可读指令在被处理器执行时,可实现上述各个方法实施例的步骤。其中,所述计算机可读指令包括计算机可读指令代码,所述计算机可读指令代码可以为源代码形式、对象代码形式、可执行文件或某些中间形式等。所述计算机可读介质可以包括:能够携带所述计算机可读指令代码的任何实体或装置、记录介质、U盘、移动硬盘、磁碟、光盘、计算机存储器、只读存储器(Read-Only Memory, ROM)、随机存取存储器(Random Access Memory, RAM)、电载波信号、电信信号以及软件分发介质等。

[0132] 以上所述实施例仅用以说明本申请的技术方案,而非对其限制;尽管参照前述实施例对本申请进行了详细的说明,本领域的普通技术人员应当理解:其依然可以对前述各实施例所记载的技术方案进行修改,或者对其中部分技术特征进

行等同替换；而这些修改或者替换，并不使对应技术方案的本质脱离本申请各实施例技术方案的精神和范围，均应包含在本申请的保护范围之内。

权利要求书

- [权利要求 1] 一种数据传输方法，其特征在于，包括：
- 基于待加密数据的文件类型以及文件体积，对所述待加密数据进行数据片段提取，得到对应的多个第一数据片段以及每个所述第一数据片段在所述待加密数据中的第一位置信息；
- 对所述第一数据片段进行随机排序合并，得到对应的第一合并数据以及每个所述第一数据片段在所述第一合并数据中的第二位置信息；
- 查找所述第一合并数据的文件体积对应的第一不可逆加密算法以及第一可逆加密解密算法；
- 基于所述第一不可逆加密算法对所述第一合并数据进行处理得到第一校验码，并基于所述第一可逆加密解密算法对所述第一位置信息及所述第二位置信息进行处理，得到加密信息；
- 将所述第一校验码和所述加密信息，与所述待加密数据一同传输至接收方，其中，所述第一校验码和所述加密信息用于所述接收方对所述待加密数据进行数据完整性校验。
- [权利要求 2] 如权利要求1所述的数据传输方法，其特征在于，所述基于待加密数据的文件类型以及文件体积，对所述待加密数据进行数据片段提取，得到对应的多个第一数据片段以及每个所述第一数据片段在所述待加密数据中的第一位置信息，包括：
- 若所述待加密数据的文件类型为图像且文件体积小于预设体积阈值，提取所述待加密数据的图像特征点，并基于所述图像特征点中的边缘特征点进行连线，绘制对应的多边形；
- 对所述多边形内的图像内容进行分割，得到与所述第一数据片段一一对应的多个图像区域，并获取每个所述图像区域在所述待加密数据中的所述第一位置信息。
- [权利要求 3] 如权利要求1所述的数据传输方法，其特征在于，所述基于待加密数据的文件类型以及文件体积，对所述待加密数据进行数据片段提取，得到对应的多个第一数据片段以及每个所述第一数据片段在所述待加

密数据中的第一位置信息，还包括：

若所述待加密数据的文件类型为文本且文件体积小于预设体积阈值，对所述待加密数据进行关键字符查找，筛选出所述文本中与所述第一数据片段一一对应的多个关键字符，并获取每个关键字符在所述待加密数据中的所述第一位置信息。

[权利要求 4]

如权利要求1所述的数据传输方法，其特征在于，所述基于待加密数据的文件类型以及文件体积，对所述待加密数据进行数据片段提取，得到对应的多个第一数据片段以及每个所述第一数据片段在所述待加密数据中的第一位置信息，还包括：

若所述待加密数据的文件类型为音频且文件体积小于预设体积阈值，对所述待加密数据进行语音识别，判断所述待加密数据是否为语音数据；

若所述待加密数据为语音数据，对语音识别得到的文字内容进行关键词查找，得到所述待加密数据对应的关键词；

从所述待加密数据提取出与所述关键词一一对应的所述第一数据片段，并获取每个所述第一数据片段在所述待加密数据中的所述第一位置信息。

[权利要求 5]

如权利要求1至4任意一项所述的数据传输方法，其特征在于，所述基于待加密数据的文件类型以及文件体积，对所述待加密数据进行数据片段提取，得到对应的多个第一数据片段以及每个所述第一数据片段在所述待加密数据中的第一位置信息，还包括：

若所述待加密数据为任意文件类型，且文件体积大于或等于预设体积阈值，以预设数据间隔对所述待加密数据进行数据段提取，得到多个所述第一数据片段以及每个所述第一数据片段在所述待加密数据中的所述第一位置信息。

[权利要求 6]

一种数据校验方法，其特征在于，包括：

获取如权利要求1所述数据传输方法传输的所述待加密数据、所述第一校验码以及所述加密信息；

基于所述待加密数据的文件类型以及文件体积，对所述待加密数据进行数据片段提取，得到对应的多个第二数据片段以及每个所述第二数据片段在所述待加密数据中的第三位置信息；

查找所述第二数据片段的文件体积和对应的第二不可逆加密算法以及第二可逆加密解密算法，并基于所述第二可逆加密解密算法对所述加密信息进行处理，得到所述第一位置信息和所述第二位置信息；

基于所述第三位置信息、所述第一位置信息和所述第二位置信息，对所述第二数据片段进行排序合并，得到对应的第二合并数据；

基于所述第二不可逆加密算法对所述第二合并数据进行处理得到第二校验码，并判断所述第二校验码与所述第一校验码是否相同；

若所述第二校验码与所述第一校验码相同，判定所述待加密数据校验完整。

[权利要求 7]

一种数据传输装置，其特征在于，包括：

第一片段提取模块，用于基于待加密数据的文件类型以及文件体积，对所述待加密数据进行数据片段提取，得到对应的多个第一数据片段以及每个所述第一数据片段在所述待加密数据中的第一位置信息；

片段排序模块，用于对所述第一数据片段进行随机排序合并，得到对应的第一合并数据以及每个所述第一数据片段在所述第一合并数据中的第二位置信息；

第一算法匹配模块，用于查找所述第一合并数据的文件体积对应的第一不可逆加密算法以及第一可逆加密解密算法；

双重加密模块，用于基于所述第一不可逆加密算法对所述第一合并数据进行处理得到第一校验码，并基于所述第一可逆加密解密算法对所述第一位置信息及所述第二位置信息进行处理，得到加密信息；

数据传输模块，用于将所述第一校验码和所述加密信息，与所述待加密数据一同传输至接收方，其中，所述第一校验码和所述加密信息用于所述接收方对所述待加密数据进行数据完整性校验。

[权利要求 8]

如权利要求7所述的数据传输装置，其特征在于，所述第一片段提取

模块，包括：

若所述待加密数据的文件类型为图像且文件体积小于预设体积阈值，提取所述待加密数据的图像特征点，并基于所述图像特征点中的边缘特征点进行连线，绘制对应的多边形。

对所述多边形内的图像内容进行分割，得到与所述第一数据片段一一对应的多个图像区域，并获取每个所述图像区域在所述待加密数据中的所述第一位置信息。

[权利要求 9]

如权利要求7所述的数据传输装置，其特征在于，所述第一片段提取模块，还包括：

若所述待加密数据的文件类型为文本且文件体积小于预设体积阈值，对所述待加密数据进行关键字符查找，筛选出所述文本中与所述第一数据片段一一对应的多个关键字符，并获取每个关键字符在所述待加密数据中的所述第一位置信息。

[权利要求 10]

如权利要求7所述的数据传输装置，其特征在于，所述第一片段提取模块，还包括：

若所述待加密数据的文件类型为音频且文件体积小于预设体积阈值，对所述待加密数据进行语音识别，判断所述待加密数据是否为语音数据。

若所述待加密数据为语音数据，对语音识别得到的文字内容进行关键词查找，得到所述待加密数据对应的关键词。

从所述待加密数据提取出与所述关键词一一对应的所述第一数据片段，并获取每个所述第一数据片段在所述待加密数据中的所述第一位置信息。

[权利要求 11]

如权利要求7所述的数据传输装置，其特征在于，所述第一片段提取模块，还包括：

若所述待加密数据为任意文件类型，且文件体积大于或等于预设体积阈值，以预设数据间隔对所述待加密数据进行数据段提取，得到多个所述第一数据片段以及每个所述第一数据片段在所述待加密数据中的

所述第一位置信息。

[权利要求 12]

一种数据校验装置，其特征在于，包括：

数据获取模块，用于获取如权利要求7所述数据传输装置传输的所述待加密数据、所述第一校验码以及所述加密信息；

第二片段提取模块，用于基于所述待加密数据的文件类型以及文件体积，对所述待加密数据进行数据片段提取，得到对应的多个第二数据片段以及每个所述第二数据片段在所述待加密数据中的第三位置信息；

第二算法匹配模块，用于查找所述第二数据片段的文件体积和对应的第二不可逆加密算法以及第二可逆加密解密算法，并基于所述第二可逆加密解密算法对所述加密信息进行处理，得到所述第一位置信息和所述第二位置信息；

片段合并模块，用于基于所述第三位置信息、所述第一位置信息和所述第二位置信息，对所述第二数据片段进行排序合并，得到对应的第二合并数据；

数据校验模块，用于基于所述第二不可逆加密算法对所述第二合并数据进行处理得到第二校验码，并判断所述第二校验码与所述第一校验码是否相同；

判定模块，用于若所述第二校验码与所述第一校验码相同，判定所述待加密数据校验完整。

[权利要求 13]

一种终端设备，其特征在于，所述终端设备包括存储器、处理器，所述存储器上存储有可在所述处理器上运行的计算机可读指令，所述处理器执行所述计算机可读指令时实现如下步骤：

基于待加密数据的文件类型以及文件体积，对所述待加密数据进行数据片段提取，得到对应的多个第一数据片段以及每个所述第一数据片段在所述待加密数据中的第一位置信息；

对所述第一数据片段进行随机排序合并，得到对应的第一合并数据以及每个所述第一数据片段在所述第一合并数据中的第二位置信息；

查找所述第一合并数据的文件体积对应的第一不可逆加密算法以及第一可逆加密解密算法；

基于所述第一不可逆加密算法对所述第一合并数据进行处理得到第一校验码，并基于所述第一可逆加密解密算法对所述第一位置信息及所述第二位置信息进行处理，得到加密信息；

将所述第一校验码和所述加密信息，与所述待加密数据一同传输至接收方，其中，所述第一校验码和所述加密信息用于所述接收方对所述待加密数据进行数据完整性校验。

[权利要求 14] 如权利要求13所述的终端设备，其特征在于，所述基于待加密数据的文件类型以及文件体积，对所述待加密数据进行数据片段提取，得到对应的多个第一数据片段以及每个所述第一数据片段在所述待加密数据中的第一位置信息，包括：

若所述待加密数据的文件类型为图像且文件体积小于预设体积阈值，提取所述待加密数据的图像特征点，并基于所述图像特征点中的边缘特征点进行连线，绘制对应的多边形；

对所述多边形内的图像内容进行分割，得到与所述第一数据片段一一对应的多个图像区域，并获取每个所述图像区域在所述待加密数据中的所述第一位置信息。

[权利要求 15] 如权利要求13所述的终端设备，其特征在于，所述基于待加密数据的文件类型以及文件体积，对所述待加密数据进行数据片段提取，得到对应的多个第一数据片段以及每个所述第一数据片段在所述待加密数据中的第一位置信息，还包括：

若所述待加密数据的文件类型为文本且文件体积小于预设体积阈值，对所述待加密数据进行关键字符查找，筛选出所述文本中与所述第一数据片段一一对应的多个关键字符，并获取每个关键字符在所述待加密数据中的所述第一位置信息。

[权利要求 16] 如权利要求13所述的终端设备，其特征在于，所述基于待加密数据的文件类型以及文件体积，对所述待加密数据进行数据片段提取，得到

对应的多个第一数据片段以及每个所述第一数据片段在所述待加密数据中的第一位置信息，还包括：

若所述待加密数据的文件类型为音频且文件体积小于预设体积阈值，对所述待加密数据进行语音识别，判断所述待加密数据是否为语音数据；

若所述待加密数据为语音数据，对语音识别得到的文字内容进行关键词查找，得到所述待加密数据对应的关键词；

从所述待加密数据提取出与所述关键词一一对应的所述第一数据片段，并获取每个所述第一数据片段在所述待加密数据中的所述第一位置信息。

[权利要求 17] 如权利要求13至16任意一项所述的终端设备，其特征在于，所述基于待加密数据的文件类型以及文件体积，对所述待加密数据进行数据片段提取，得到对应的多个第一数据片段以及每个所述第一数据片段在所述待加密数据中的第一位置信息，还包括：

若所述待加密数据为任意文件类型，且文件体积大于或等于预设体积阈值，以预设数据间隔对所述待加密数据进行数据段提取，得到多个所述第一数据片段以及每个所述第一数据片段在所述待加密数据中的所述第一位置信息。

[权利要求 18] 一种终端设备，其特征在于，所述终端设备包括存储器、处理器，所述存储器上存储有可在所述处理器上运行的计算机可读指令，所述处理器执行所述计算机可读指令时实现如下步骤：

获取如权利要求13所述终端设备传输的所述待加密数据、所述第一校验码以及所述加密信息；

基于所述待加密数据的文件类型以及文件体积，对所述待加密数据进行数据片段提取，得到对应的多个第二数据片段以及每个所述第二数据片段在所述待加密数据中的第三位置信息；

查找所述第二数据片段的文件体积和对应的第二不可逆加密算法以及第二可逆加密解密算法，并基于所述第二可逆加密解密算法对所述加

密信息进行处理，得到所述第一位置信息和所述第二位置信息；
基于所述第三位置信息、所述第一位置信息和所述第二位置信息，对所述第二数据片段进行排序合并，得到对应的第二合并数据；
基于所述第二不可逆加密算法对所述第二合并数据进行处理得到第二校验码，并判断所述第二校验码与所述第一校验码是否相同；
若所述第二校验码与所述第一校验码相同，判定所述待加密数据校验完整。

[权利要求 19]

一种计算机可读存储介质，所述计算机可读存储介质存储有计算机可读指令，其特征在于，所述计算机可读指令被至少一个处理器执行时实现如下步骤：

基于待加密数据的文件类型以及文件体积，对所述待加密数据进行数据片段提取，得到对应的多个第一数据片段以及每个所述第一数据片段在所述待加密数据中的第一位置信息；

对所述第一数据片段进行随机排序合并，得到对应的第一合并数据以及每个所述第一数据片段在所述第一合并数据中的第二位置信息；

查找所述第一合并数据的文件体积对应的第一不可逆加密算法以及第一可逆加密解密算法；

基于所述第一不可逆加密算法对所述第一合并数据进行处理得到第一校验码，并基于所述第一可逆加密解密算法对所述第一位置信息及所述第二位置信息进行处理，得到加密信息；

将所述第一校验码和所述加密信息，与所述待加密数据一同传输至接收方，其中，所述第一校验码和所述加密信息用于所述接收方对所述待加密数据进行数据完整性校验。

[权利要求 20]

如权利要求19所述的计算机可读存储介质，其特征在于，所述基于待加密数据的文件类型以及文件体积，对所述待加密数据进行数据片段提取，得到对应的多个第一数据片段以及每个所述第一数据片段在所述待加密数据中的第一位置信息，包括：

若所述待加密数据的文件类型为图像且文件体积小于预设体积阈值，

提取所述待加密数据的图像特征点，并基于所述图像特征点中的边缘特征点进行连线，绘制对应的多边形；

对所述多边形内的图像内容进行分割，得到与所述第一数据片段一一对应的多个图像区域，并获取每个所述图像区域在所述待加密数据中的所述第一位置信息。

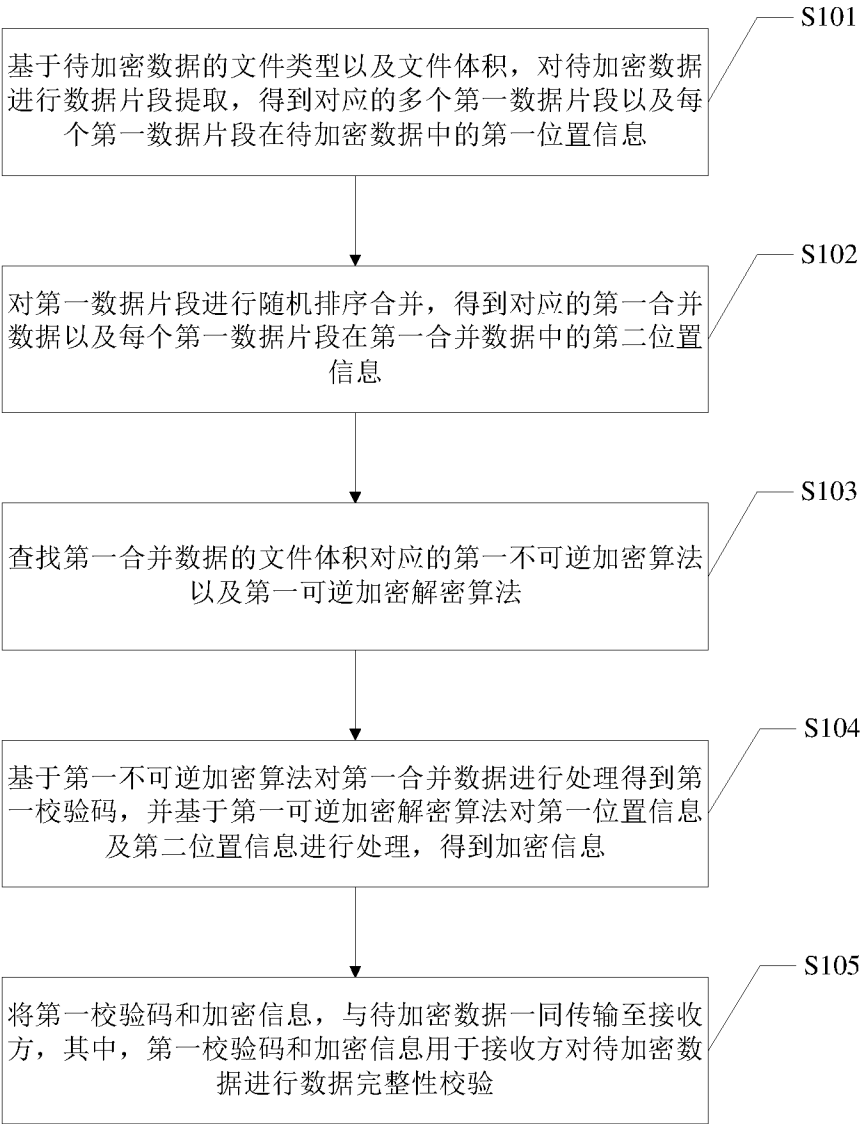


图 1

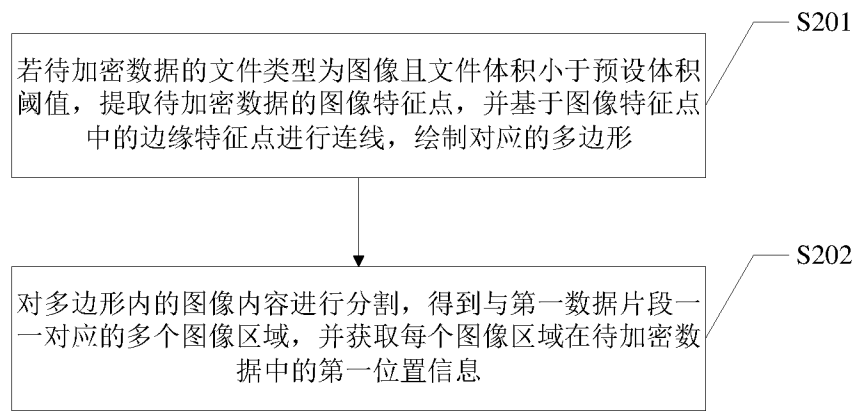


图 2

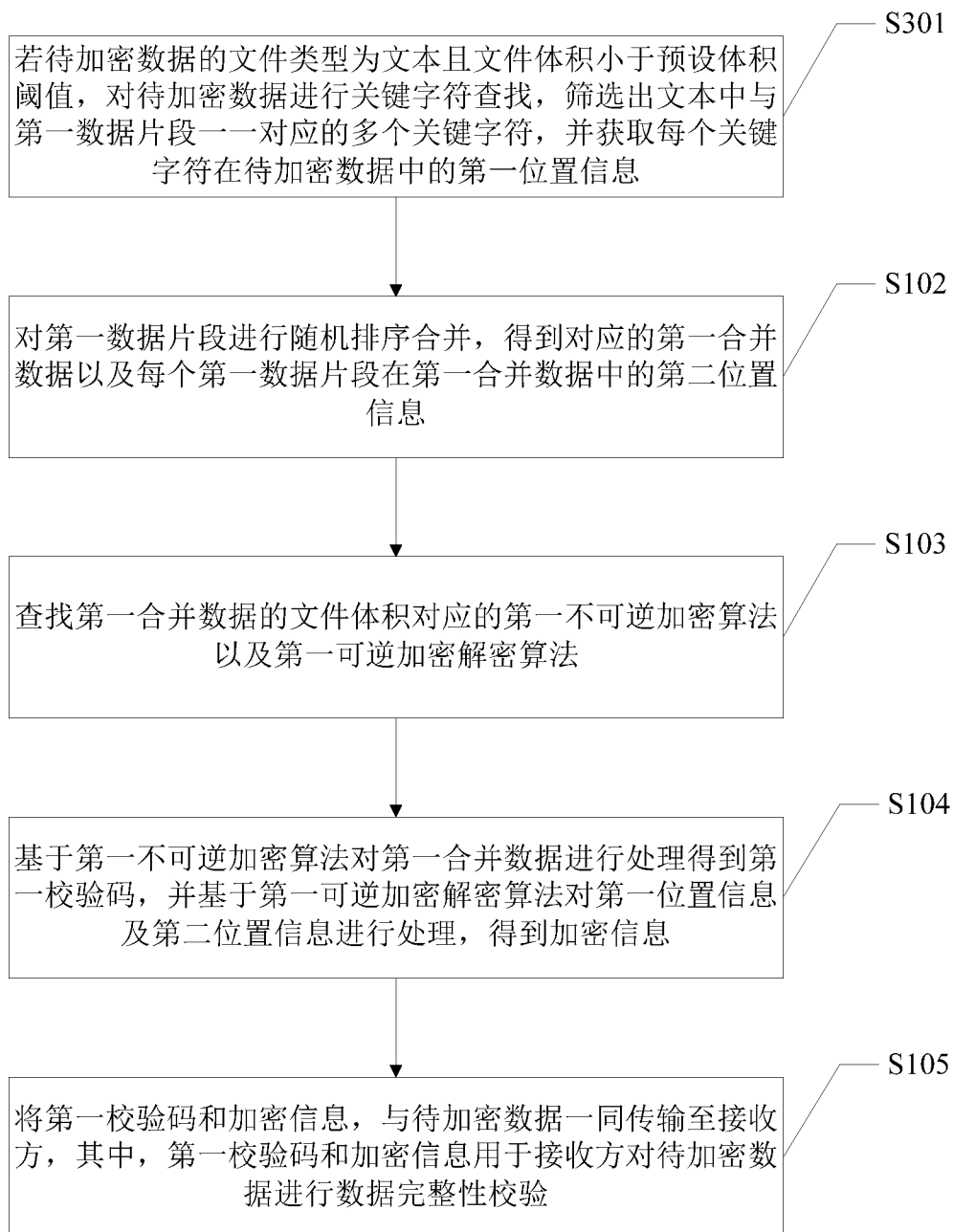


图 3

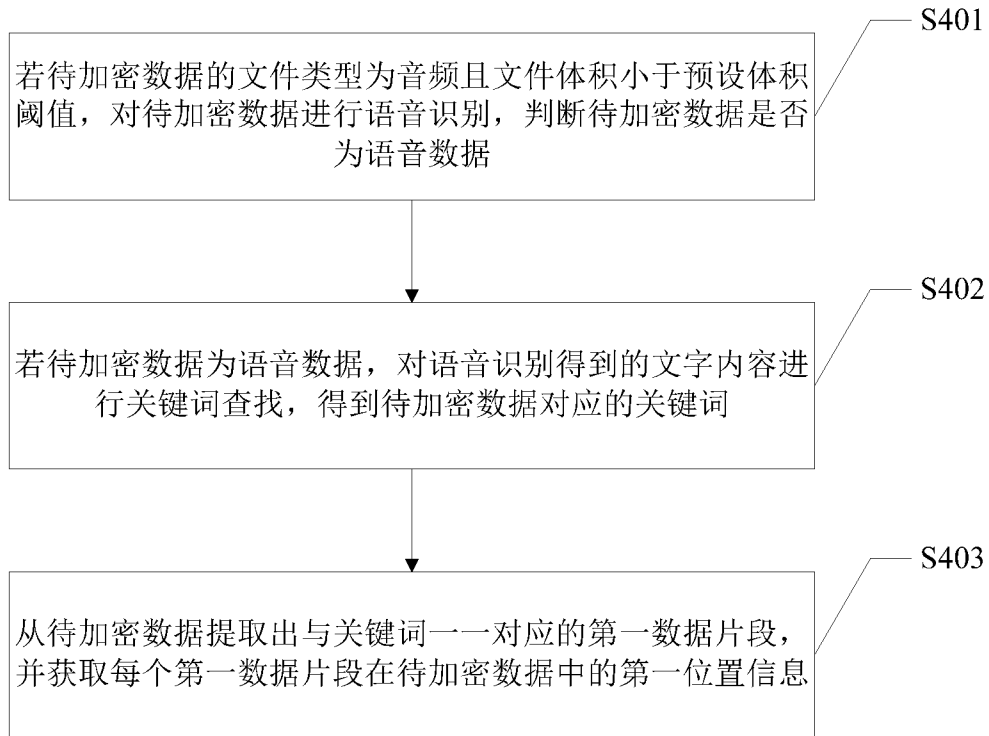


图 4

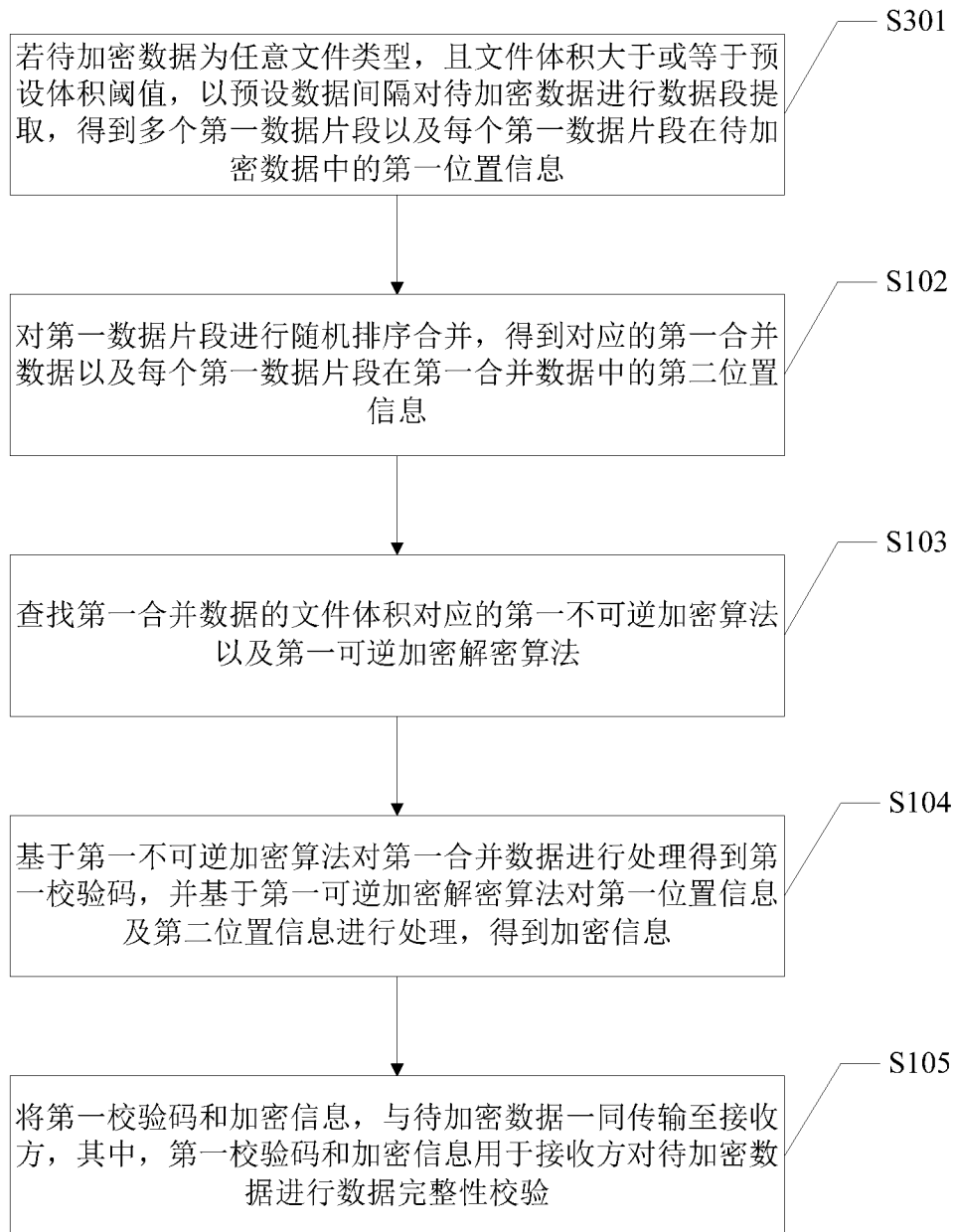


图 5

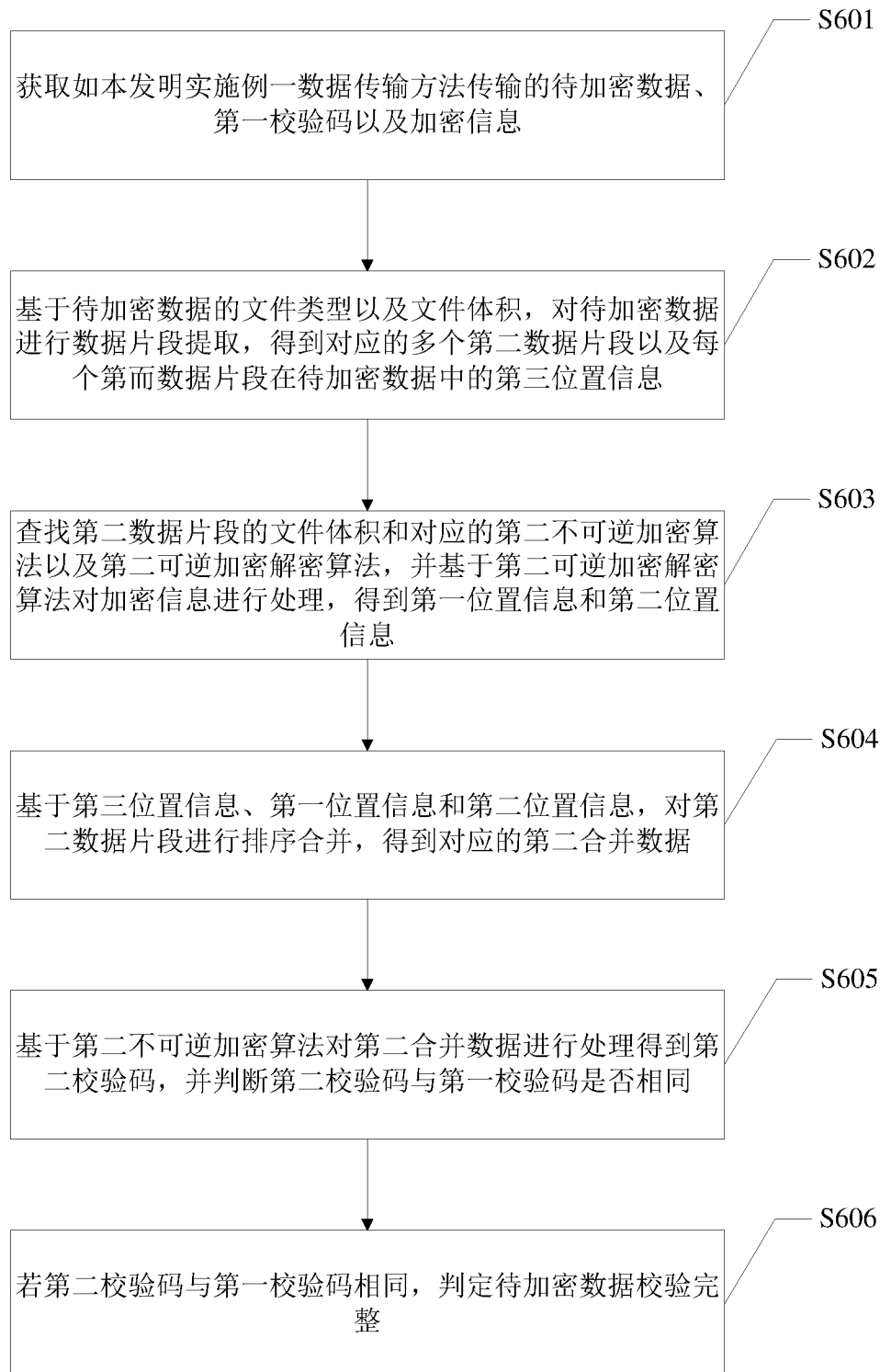


图 6

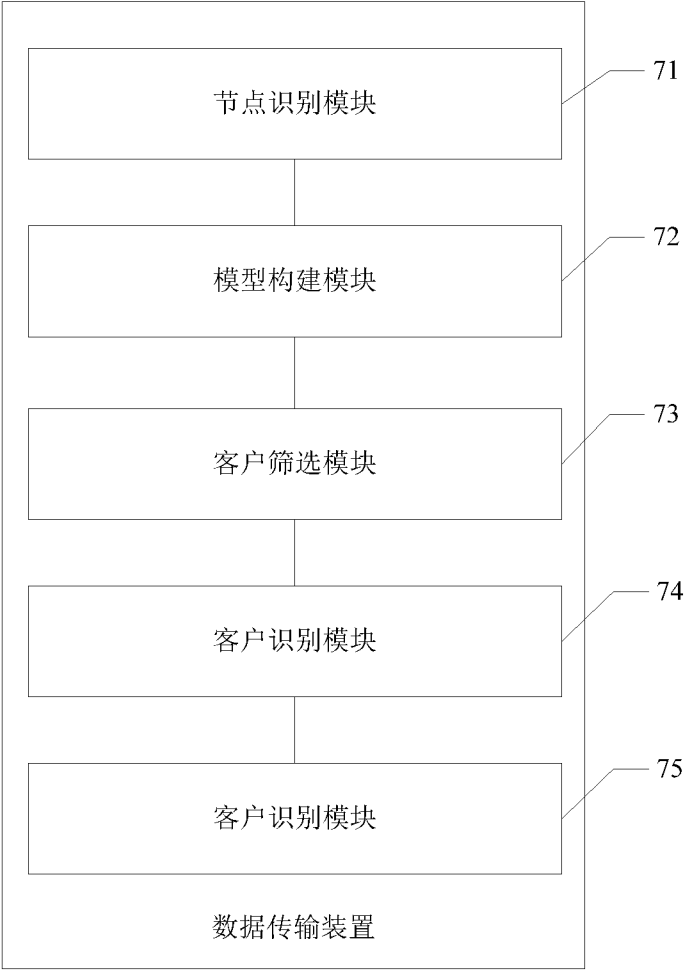


图 7

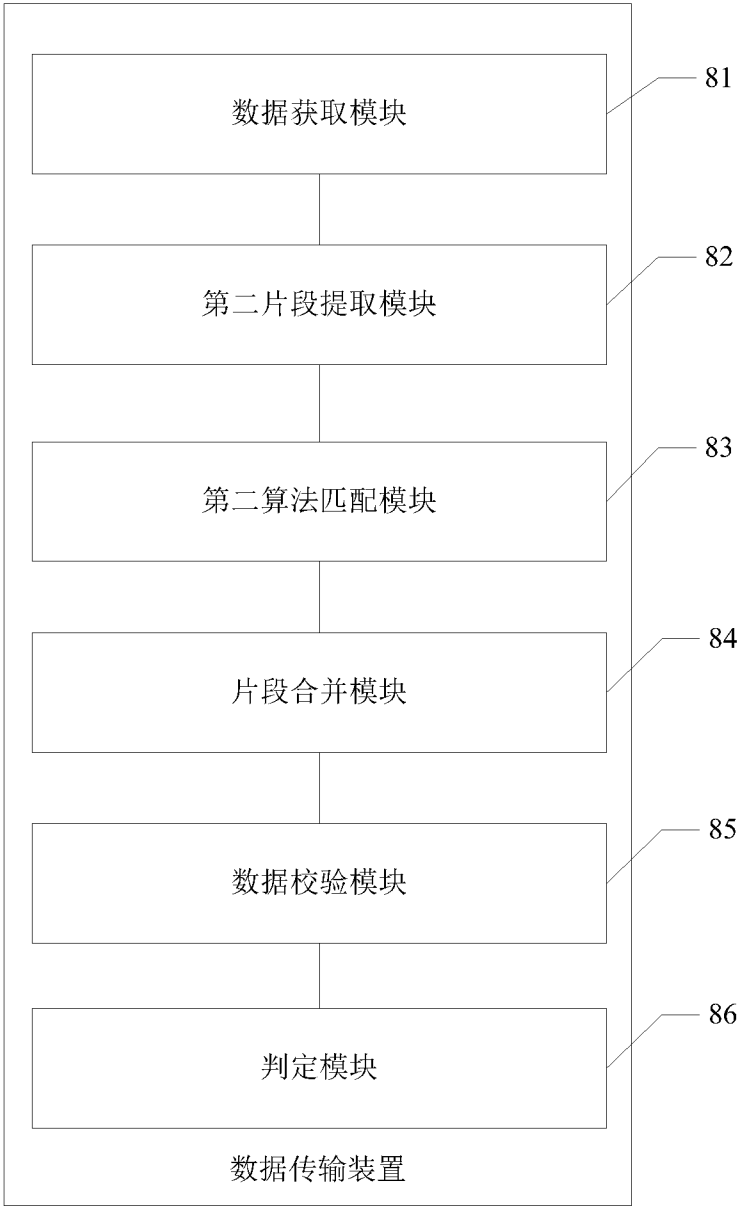


图 8

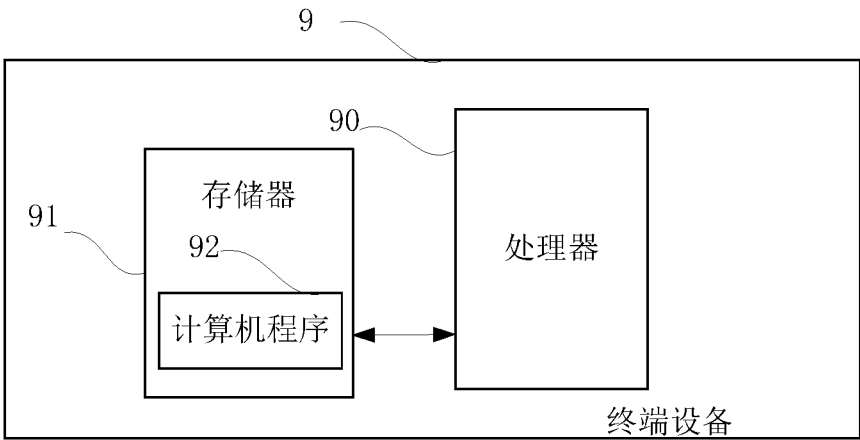


图 9

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2019/091503

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/60(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

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: 加密, 数据, 文件, 类型, 大小, 片段, 分段, 分组, 分割, 切分, 位置, 完整, 校验, 检验, 验证, encrypt, data, file, type, size, segment, piece, position, location, integrity, check, authentication

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 104091129 A (TENCENT TECHNOLOGY SHENZHEN CO., LTD.) 08 October 2014 (2014-10-08) description, paragraphs [0125]-[0163]	1-20
A	CN 102402670 A (GUANGDONG OPPO MOBILE TELECOMMUNICATIONS CORP., LTD.) 04 April 2012 (2012-04-04) entire document	1-20
A	CN 103488952 A (HUAWEI TECHNOLOGIES CO., LTD.) 01 January 2014 (2014-01-01) entire document	1-20
A	CN 109145639 A (BEIJING BEIXINYUAN INFORMATION SAFETY TECHNOLOGY CO., LTD.) 04 January 2019 (2019-01-04) entire document	1-20
A	US 2006259781 A1 (SONY CORPORATION/SONY ELECTRONICS INC.) 16 November 2006 (2006-11-16) entire document	1-20



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

10 October 2019

Date of mailing of the international search report

29 October 2019

Name and mailing address of the ISA/CN

China National Intellectual Property Administration
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/CN2019/091503

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	104091129	A	08 October 2014	None			
CN	102402670	A	04 April 2012	None			
CN	103488952	A	01 January 2014	None			
CN	109145639	A	04 January 2019	None			
US	2006259781	A1	16 November 2006	WO	2006118896	A2	09 November 2006
				CN	101164069	A	16 April 2008
				JP	2008539525	A	13 November 2008

国际检索报告

国际申请号

PCT/CN2019/091503

A. 主题的分类

G06F 21/60 (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

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, EPDOC: 加密, 数据, 文件, 类型, 大小, 片段, 分段, 分组, 分割, 切分, 位置, 完整, 校验, 检验, 验证, encrypt, data, file, type, size, segment, piece, position, location, integrity, check, authentication

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
A	CN 104091129 A (腾讯科技深圳有限公司) 2014年 10月 8日 (2014 - 10 - 08) 说明书第[0125]-[0163]段	1-20
A	CN 102402670 A (广东欧珀移动通信有限公司) 2012年 4月 4日 (2012 - 04 - 04) 全文	1-20
A	CN 103488952 A (华为技术有限公司) 2014年 1月 1日 (2014 - 01 - 01) 全文	1-20
A	CN 109145639 A (北京北信源信息安全技术有限公司) 2019年 1月 4日 (2019 - 01 - 04) 全文	1-20
A	US 2006259781 A1 (SONY CORPORATION/SONY ELECTRONICS INC.) 2006年 11月 16日 (2006 - 11 - 16) 全文	1-20

☐ 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

2019年 10月 10日

国际检索报告邮寄日期

2019年 10月 29日

ISA/CN的名称和邮寄地址

中国国家知识产权局 (ISA/CN)

中国北京市海淀区蓟门桥西土城路6号 100088

传真号 (86-10)62019451

受权官员

冯骥

电话号码 86-(10)-53961610

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2019/091503

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	104091129	A	2014年 10月 8日	无			
CN	102402670	A	2012年 4月 4日	无			
CN	103488952	A	2014年 1月 1日	无			
CN	109145639	A	2019年 1月 4日	无			
US	2006259781	A1	2006年 11月 16日	W0	2006118896	A2	2006年 11月 9日
				CN	101164069	A	2008年 4月 16日
				JP	2008539525	A	2008年 11月 13日