

(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 4 月 6 日 (06.04.2017)



(10) 国际公布号
WO 2017/054480 A1

- (51) 国际专利分类号:
H04N 21/2347 (2011.01)
- (21) 国际申请号: PCT/CN2016/083713
- (22) 国际申请日: 2016 年 5 月 27 日 (27.05.2016)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201510641989.9 2015 年 9 月 30 日 (30.09.2015) CN
- (71) 申请人: 北京奇虎科技有限公司 (BEIJING QIHOO TECHNOLOGY COMPANY LIMITED) [CN/CN]; 中国北京市西城区新街口外大街 28 号 D 座 112 室 (德胜园区), Beijing 100088 (CN)。奇智软件 (北京) 有限公司 (QIZHI SOFTWARE (BEIJING) COMPANY LIMITED) [CN/CN]; 中国北京市朝阳区酒仙桥路 6 号院 2 号楼 B 座 2 层、3 层 301-306 室, Beijing 100015 (CN)。
- (72) 发明人: 赵化强 (ZHAO, Huaqiang); 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。章勋 (ZHANG, Xun); 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。田晓川 (TIAN, Xiaochuan); 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。
- (74) 代理人: 北京智汇东方知识产权代理事务所 (普通合伙) (WISEAST INTELLECTUAL PROPERTY LAW FIRM); 中国北京市海淀区花园路 13 号 5 幢 320 房间, Beijing 100088 (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,

[见续页]

(54) Title: MULTIMEDIA DATA ENCRYPTION METHOD AND APPARATUS

(54) 发明名称: 多媒体数据加密方法和装置

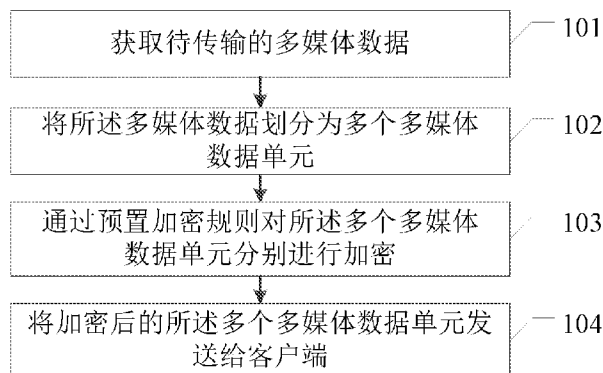


图 1

- 101 Acquiring multimedia data to be transmitted
- 102 Dividing the multimedia data into a plurality of multimedia data units
- 103 Respectively encrypting the plurality of multimedia data units through pre-set encryption rules
- 104 Sending the encrypted plurality of multimedia data units to a client

(57) Abstract: The present invention relates to the technical field of information, and disclosed are a multimedia data encryption method and apparatus. The method comprises: firstly acquiring multimedia data to be transmitted; then dividing the multimedia data into a plurality of multimedia data units; then respectively encrypting the plurality of multimedia data units through pre-set encryption rules; and finally sending the encrypted plurality of multimedia data units to a client. According to the above-mentioned method and apparatus, the transmission security of the multimedia data can be guaranteed, and network system resources occupied by the encrypted multimedia data in the transmission process can be reduced.

(57) 摘要: 本发明涉及信息技术领域, 公开了一种多媒体数据加密方法及装置。所述方法包括: 首先获取待传输的多媒体数据; 然后将所述多媒体数据划分为多个多媒体数据单元; 再通过预置加密规则对所述多个多媒体数据单元分别进行加密; 最后将加密后的所述多个多媒体数据单元发送给客户端。上述方法及装置能够保证多媒体数据的传输安全并减少加密多媒体数据在传输过程中占用的网络系统资源。

WO 2017/054480 A1



SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ,
VC, VN, ZA, ZM, ZW。

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)。

- (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,

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

多媒体数据加密方法和装置

技术领域

本发明涉及信息技术领域，尤其涉及一种多媒体数据加密方法和装置。

5

背景技术

随着信息技术的不断发展，网络摄像机随之出现，并且越来越受欢迎。其中，网络摄像机是一种结合传统摄像机与网络技术产生的新一代摄像机，它可以将记录的多媒体数据通过网络传输到服务器，然后再通过网络服务器传输到客户端上。网络摄像机可以用于监控儿童、独居老人、自己的住宅等。为了防止多媒体数据在传输过程中被黑客攻击泄露用户隐私，保证多媒体数据的安全性，通常需要对多媒体数据进行加密。

目前，主要是通过传统的 SSL(Secure Sockets Layer, 安全套接层)协议对多媒体数据进行加密，即需要对多媒体数据进行整体加密，由于传统的 SSL 协议对多媒体数据进行整体加密后会产生额外的数据，而额外的数据在进行传输时会占用额外的网络资源，并且传统的 SSL 协议对多媒体数据进行加密的算法较为复杂，占用较多的网络系统资源。

发明内容

鉴于上述问题，提出了本发明以便提供一种克服上述问题或者至少部分地解决上述问题的多媒体数据加密方法和装置，主要目的在于解决加密后的多媒体数据在传输过程中，占用较多的网络系统资源的问题。

依据本发明的一个方面，提供了一种多媒体数据加密方法，包括：

获取待传输的多媒体数据；

25 将所述多媒体数据划分为多个多媒体数据单元；

通过预置加密规则对所述多个多媒体数据单元分别进行加密；

将加密后的所述多个多媒体数据单元发送给客户端。

依据本发明另一个方面，提供了一种多媒体数据加密装置，包括：

获取单元，用于获取待传输的多媒体数据；

30 划分单元，用于将所述获取单元获取的多媒体数据划分为多个多媒体数据单元；
加密单元，用于通过预置加密规则对所述划分单元划分的多个多媒体数据单元分别进行加密；

发送单元，用于将加密后的所述多个多媒体数据单元发送给客户端。

依据本发明的又一方面，提供了一种计算机程序，其包括计算机可读代码，当
35 所述计算机可读代码在计算设备上运行时，导致所述计算设备执行根据上文所述的

多媒体数据加密方法。

依据本发明的再一方面，提供了一种计算机可读介质，其中存储了上述的计算机程序。

借由上述技术方案，本发明实施例提供的技术方案至少具有下列优点：

- 5 本发明实施例提供了一种多媒体数据加密方法及装置，首先获取待传输的多媒体数据；然后将所述多媒体数据划分为多个多媒体数据单元；再通过预置加密规则对所述多个多媒体数据单元分别进行加密；最后将加密后的所述多个多媒体数据单元发送给客户端。与目前通过传统的 SSL 对多媒体数据进行整体加密相比，本发明实施例首先将多媒体数据划分为多个多媒体数据单元，然后对多个多媒体数据单元
10 分别进行加密，最后输出加密后的多媒体数据单元，从而减少了网络系统资源的浪费。

上述说明仅是本发明技术方案的概述，为了能够更清楚了解本发明的技术手段，而可依照说明书的内容予以实施，并且为了让本发明的上述和其它目的、特征和优点能够更明显易懂，以下特举本发明的具体实施方式。

15

附图说明

通过阅读下文优选实施方式的详细描述，各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的，而并不认为是对本发明的限制。而且在整个附图中，用相同的参考符号表示相同的部件。在附图
20 中：

图 1 示出了本发明实施例提供的一种多媒体数据加密方法流程图；

图 2 示出了本发明实施例提供的另一种多媒体数据加密方法流程图；

图 3 示出了本发明实施例提供的一种多媒体数据加密装置结构框图；

图 4 示出了本发明实施例提供的另一种多媒体数据加密装置结构框图；

- 25 图 5 示意性地示出了用于执行根据本发明的多媒体数据加密方法的计算设备的框图；以及

图 6 示意性地示出了用于保持或者携带实现根据本发明的多媒体数据加密方法的程序代码的存储单元。

30

具体实施方式

下面结合附图和具体的实施方式对本发明作进一步的描述。

本发明实施例提供了一种多媒体数据加密方法，如图 1 所示，所述方法可以应用于中继服务器、网络摄像机等，所述方法包括：

101、获取待传输的多媒体数据。

- 35 其中，所述多媒体数据可以为视频数据，也可以为音频数据，本发明实施例不

做具体限定。所述视频数据可以为网络摄像机拍摄的需要传输给客户端的视频数据，所述视频数据可以为 AVI（Audio Video Interleaved，音频视频交错）、RM（remove，流媒体视频文件格式）、WMV（Windows Media Video，流媒体格式）、FLV（FlashVideo，流媒体格式）、DV-AVI（Digital Video Format，数字视频格式）、

5 MPEG（Moving Pictures Experts Group/Motion Pictures Experts Group，动态图像专家组）、MOV（QuickTime，影片格式）、ASF（Advanced Streaming format，高级流格式）等格式的视频数据，本发明实施例不做具体限定。所述音频数据可以为网络摄像机录制的需要传输给客户端的音频数据，所述音频数据可以为 MP3、AVI、CD、WMA、RealAudio 等格式的音频数据，本发明实施例不做具体限定。在本发明实施
10 例中，获取待传输的多媒体数据，是为了将待传输的多媒体数据转发给客户端，以使得网络摄像机记录的多媒体数据通过网络传输给客户端。

102、将所述多媒体数据划分为多个多媒体数据单元。

其中，所述多媒体数据单元是通过对多媒体数据进行划分而得到的。在本发明实施例中，可以根据多媒体数据中的多媒体帧或多媒体播放过程中的时间点将多媒体
15 数据平均划分为多个多媒体数据单元，也可以根据多媒体数据中的多媒体帧或多媒体播放过程中的时间点将多媒体数据非平均的划分为多个多媒体数据单元，本发明实施例不做具体限定。对于本发明实施例，多媒体数据中的多媒体帧的个数或多媒体播放过程中的时间点的长短可以根据实际需求进行设置，也可以由系统默认配置，本发明实施例不做具体限定。

20 例如，待传输视频数据包含有 300 个视频帧，若要求每个视频数据单元中的视频帧的个数为 30，则可以按照每 30 帧划分一个数据单元的方式将所述待传输的视频数据平均划分成 10 个视频数据单元，每个视频数据单元中包含有 30 个视频帧；若未对每个视频数据单元中的视频帧的个数做出要求，而要求视频数据单元的个数为 10，则可将待传输视频数据平均或非平均划分成 10 个视频数据单元；若未对每个视
25 频数据单元中的视频帧的个数做出要求，也未对视频数据单元的个数做出要求，则可对所述待传输视频数据进行任意划分，最多可将待传输视频数据划分为 300 个视频数据单元，每个视频数据单元对应一个视频帧。

103、通过预置加密规则对所述多个多媒体数据单元分别进行加密。

其中，所述预置加密规则可以根据用户需求进行设置，也可以由系统默认配置，
30 本发明实施例不做具体限定。通过所述预置加密规则对多个多媒体数据单元进行加密，加密后的多媒体数据占用的存储空间和原有的多媒体数据占用的存储空间大小相同。对于本发明实施例，所述预置加密规则可以为加密算法较为简单的非对称加密规则，也可以为加密算法较为复杂的对称加密规则，对称加密规则是加密和解密的双方使用相同密钥的加解密的算法，并且对称加密规则的加密速度快，对称加密
35 规则通常适用于消息发送方需要加密大量数据时使用。所述对称加密规则具体可以

为 DES (Data Encryption Algorithm, 对称加密算法) 算法, 3DES (Triple DES, 三重数据加密算法) 算法, RC5 (分组密码算法) 算法, IDEA (IntelliJ IDEA, 数据块加密算法) 算法等, 本发明实施例不做具体限定。

对于本发明实施例, 为了满足多媒体数据加密的安全性需求, 还可以使用加密算法较为简单的非对称加密规则对所述多媒体数据进行加密, 通过加密算法简单的非对称加密规则对所述多媒体数据进行加密, 加密后的多媒体数据存储空间的

5 可以稍大于原有的多媒体数据存储空间, 从而在保证加密后的多媒体数据占用的存储空间相对较小的情况下, 进一步地提高多媒体数据加密的安全性。

104、将加密后的所述多个多媒体数据单元发送给客户端。

10 其中, 所述多个多媒体数据单元用于供所述客户端进行展示/输出, 发送加密后的所述多个多媒体数据单元是指将加密后的多个多媒体数据单元通过网络发送给网络摄像机对应的客户端设备。对于本发明实施例, 将待传输的多媒体数据划分多个多媒体数据单元, 然后根据预置加密规则对多个多媒体数据单元分别进行加密, 最后将加密后的所述多个多媒体数据单元发送给客户端。从而解决了传统 SSL 对多媒体

15 数据进行整体加密后所产生的额外数据, 进而减少了网络系统资源的浪费。同时, 对多媒体数据中的多个多媒体数据单元分别进行加密并不会降低安全性。

对于本发明实施例, 可以应用的场景如下所述, 但不仅限于此, 包括: 中继服务器获取的待传输多媒体数据的多媒体帧的个数为 400, 若要求每个多媒体数据单元中的多媒体帧的个数为 100, 则可将所述待传输的多媒体数据平均划分成 4 个多媒体

20 数据单元, 每个多媒体数据单元中包含有 100 个多媒体帧。然后通过预置加密规则对所述多个多媒体数据单元分别进行加密, 所述预置加密规则可以为加密算法较为简单的非对称加密规则, 也可以为加密算法较为复杂的对称加密规则, 具体加密规则可以为 DES、DES 和 RC5 等加密算法, 再通过对称加密规则中的对应的加密密钥对多个多媒体数据单元分别进行加密, 最后将加密后的多个多媒体数据单元通过网

25 络发送给网络摄像机对应的客户端设备。在本发明实施例中, 将待传输的多媒体数据进行划分多个多媒体数据单元, 然后根据预置加密规则对多个多媒体数据单元分别进行加密, 最后将加密后的所述多个多媒体数据单元发送给客户端。从而解决了传统 SSL 对多媒体数据进行整体加密后所产生的额外数据, 进而减少了网络系统资源的浪费。

30 本发明实施例提供了一种多媒体数据加密方法, 首先获取待传输的多媒体数据; 然后将所述多媒体数据划分为多个多媒体数据单元; 再通过预置加密规则对所述多个多媒体数据单元分别进行加密; 最后将加密后的所述多个多媒体数据单元发送给客户端, 所述多个多媒体数据单元用于供所述客户端进行展示/输出。与目前通过传统的 SSL 对多媒体数据进行整体加密相比, 本发明实施例首先将多媒体数据划分为

35 多个多媒体数据单元, 然后对多个多媒体数据单元分别进行加密, 最后输出加密后

的多媒体数据单元，从而减少了网络系统资源的浪费。

本发明实施例提供了另一种多媒体数据加密方法，如图 2 所示，所述方法包括：
201、获取待传输的多媒体数据。

对于本发明实施例，所述多媒体数据为视频数据或音频数据。所述视频数据可
5 以为网络摄像机拍摄的需要传输给客户端的视频数据，所述视频数据可以为 AVI
(Audio Video Interleaved，音频视频交错)、RM (remove，流媒体视频文件格式)、
WMV (Windows Media Video，流媒体格式)、FLV (FlashVideo，流媒体格式)、
DV-AVI (Digital Video Format，数字视频格式)、MPEG (Moving Pictures Experts
Group/Motion Pictures Experts Group，动态图像专家组)、MOV (QuickTime，影片
10 格式)、ASF (Advanced Streaming format，高级流格式)等格式的视频数据，本发
明实施例不做具体限定。所述音频数据可以为网络摄像机录制的需要传输给客户端
的音频数据，所述音频数据可以为 MP3、AVI、CD、WMA、RealAudio 等格式的音
频数据，本发明实施例不做具体限定。在本发明实施例中，获取待传输的多媒体数
15 据通过网络传输给客户端。

202、按照预置规则将所述多媒体数据划分为多个多媒体帧数据。

其中，所述预置规则可以根据实际需求进行设置，也可以由系统默认配置，本
发明实施例不做具体限定。所述预置规则具体可以根据多媒体数据中的多媒体帧将
多媒体数据划分为多个多媒体帧数据，例如，可以按照每一个多媒体帧一组、每两
20 个多媒体帧一组等将多媒体数据划分为多个多媒体帧数据；或者多媒体播放过程
中的时间点将多媒体数据划分为多个多媒体帧数据。需要说明的是，预置规则中多媒
体播放过程中的时间点可以根据用户实际需求进行设置，也可以由系统默认配置，
本发明实施例不做具体限定。对于本发明实施例，预置规则中配置的多种多媒体数
据划分规则，可以根据实际需求将多媒体数据灵活的划分为多个多媒体帧数据，从
25 而提高了划分多媒体数据的效率。

例如，中继服务器获取的待传输视频数据中包含有 80 个视频帧，则根据视频帧
可将所述视频数据划分为 80 个视频帧数据。再比如，中继服务器获取的待传输视频
数据的播放时长为 30 分钟，预置规则中配置的视频播放过程中的时间点为 3 分钟，
则根据视频播放过程中的时间点 3 分钟将视频数据数据平均划分为 10 个播放时长为
30 3 分钟的视频数据单元，每一个视频数据单元中包含有一个或多个视频帧。

对于本发明实施例，所述按照预置规则将所述多媒体数据划分为多个多媒体帧
数据之后，还包括：按照预置排序规则调整所述多个多媒体帧数据在所述多媒体数
据中所在的位置顺序。对于本发明实施例，按照预置排序规则调整所述多个多媒体
帧数据在所述多媒体数据中的位置顺序，可以进一步地提高后续多媒体帧数据加密
35 的安全性。其中，所述预置排序规则可以按照多媒体帧数据的原始序列号排序，也

可以按照多媒体帧数据的存储空间大小排序，还可以按照多媒体帧数据的播放时长排序，本发明实施例不做具体限定。

例如，将视频数据划分为 5 个视频帧数据后，若获取到这 5 个视频帧数据在原始视频数据中对应的原始序列号分别为 1、2、3、4、5，预置排序规则为根据视频帧数据的原始序列号调整视频帧数据的位置顺序，由此调整后的多个视频帧数据的对应位置的原始序列号可以为 5、4、3、2、1。对于本发明实施例，按照预置排序规则调整所述多个多媒体帧数据在所述多媒体数据中的位置顺序，可以进一步地提高后续多媒体帧数据加密的安全性。

203、通过预置对称加密规则和所述加密密钥，对所述多个多媒体帧数据分别进行加密。

对于本发明实施例，所述方法还包括：生成所述预置加密规则对应的加密密钥；或者接收外部设备发送的所述预置加密规则对应的加密密钥。其中，所述对称加密规则为单钥系统的加密方式，对称加密规则中的加密密钥可以同时作为信息的加密和解密。所述预置对称加密规则可以根据用户的实际需求进行设置，也可以由系统默认配置，本发明实施例不做具体限定。

在本发明实施例中，所述预置对称加密规则对应的加密密钥可以由数据发送方生成，即可以由网络摄像机或者网络摄像机对应的中继服务器生成；也可以将所述预置对称加密规则对应的加密密钥配置在外部设备中，每次在对多媒体数据进行传输之前，根据外部设备中的预置对称加密规则动态的产生一个加密密钥，然后将所述加密密钥以 HTTPS（Hyper Text Transfer Protocol over Secure Socket Layer，网络协议）传输方式，分别传输给数据发送端和客户端，数据发送端和客户端收到加密密钥后，进行数据传输。需要说明的是，外部设备向数据发送端和客户端传输加密密钥时，由于加密密钥是通过 HTTPS 进行传输的，因此可将加密密钥安全的传输至数据发送端和客户端，并且外部设备通过 HTTPS 仅传输加密密钥，而不是传输加密的多媒体数据本身，因此该种加密方式并不会占用较多的网络系统资源。

对于本发明实施例，通过所述预置对称加密规则对多个多媒体帧数据进行加密，加密后的多媒体数据占用的存储空间和原有的多媒体数据占用的存储空间大小相同。在本发明实施例中，所述预置对称加密规则具体可以为 DES（Data Encryption Algorithm，对称加密算法）算法，3DES（Triple DES，三重数据加密算法）算法，RC5（分组密码算法）算法，IDEA（IntelliJ IDEA，数据块加密算法）算法等，本发明实施例不做具体限定。对于本发明实施例，由于对称加密规则具有计算量小、加密速度快、加密效率高等优点，因此通过预置对称加密规则对所述多个多媒体帧数据分别进行加密，可以提高多媒体数据加密的效率。同时，对多媒体数据划分的多个多媒体帧数据分别进行加密并不会降低安全性。

对于本发明实施例，所述通过预置对称加密规则和所述加密密钥，对所述多个

多媒体帧数据分别进行加密之前，还包括：获取各个多媒体帧数据的原始序列号；根据所述加密密钥和所述各个多媒体帧数据的原始序列号，分别生成与所述各个多媒体帧数据分别对应的密钥。其中，多媒体帧数据的原始序列号用于表示多媒体帧数据在多媒体数据中的位置顺序，具体可以通过数据编号表示多媒体帧数据的原始序列号，所述预置对称加密规则的加密密钥可以从中继服务器中获取。例如，获取的各个多媒体帧数据的原始序列号分别为 5、4、2、1 和 3，预置对称加密规则的加密密钥为 123，则根据对称加密规则的私钥 123 和多媒体帧数据原始序列号 5，生成原始序列号为 5 的多媒体帧数据的密钥；根据对称加密规则的加密密钥 123 和多媒体帧数据原始序列号 4，生成原始序列号为 4 的多媒体帧数据的密钥；根据对称加密规则的加密密钥 123 和多媒体帧原始序列号 2，生成原始序列号为 2 的多媒体帧数据的密钥；根据对称加密规则的加密密钥 123 和多媒体帧原始序列号 1，生成原始序列号为 1 的多媒体帧数据的密钥；根据对称加密规则的加密密钥 123 和多媒体帧原始序列号 3，生成原始序列号为 3 的多媒体帧数据的密钥。在本发明实施例中，根据预置对称加密规则的加密密钥和所述各个多媒体帧数据的原始序列号生成的各个多媒体帧数据分别对应的密钥，可以进一步地提高加密密钥的复杂性，从而提高了多媒体数据加密的安全性。

对于本发明实施例，所述通过预置对称加密规则对所述多个多媒体帧数据分别进行加密包括：通过所述各个多媒体帧数据分别对应的密钥对所述多个多媒体帧数据分别进行加密。例如，原始序列号为 1 的多媒体帧数据对应的密钥为 145；原始序列号为 2 的多媒体帧数据对应的密钥为 147；原始序列号为 3 的多媒体帧数据对应的密钥为 124。则根据密钥 145 对原始序列号为 1 的多媒体帧数据进行加密；根据密钥 147 对原始序列号为 2 的多媒体帧数据进行加密；根据密钥 124 对原始序列号为 3 的多媒体帧数据进行加密。在本发明实施例中，根据所述预置所述加密密钥和所述各个多媒体帧数据的原始序列号，分别生成与所述各个多媒体帧数据分别对应的密钥，并且通过生成的密钥加密多媒体帧数据，可以进一步提高多媒体数据加密的安全性。

204、将调整顺序后的加密的所述多个多媒体帧数据发送给客户端。

其中，发送加密后的所述多个多媒体数据单元是指将加密后的多个多媒体数据单元通过网络发送给网络摄像机对应的客户端设备。对于本发明实施例，将待传输的多媒体数据划分多个多媒体数据单元，然后根据预置加密规则对多个多媒体数据单元分别进行加密，最后将调整顺序后的加密的所述多个多媒体帧数据发送给客户端。从而解决了传统 SSL 对多媒体数据进行整体加密后所产生的额外数据，进而减少了网络系统资源的浪费。同时，对多媒体数据中的多个多媒体数据单元分别进行加密并不会降低安全性。

对于本发明实施例，进一步将所述加密密钥发送给所述客户端，所述加密密钥用于供所述客户端对加密后的所述多个多媒体数据单元进行解密。其中，所述加密

密钥可以通过 HTTPS 传输方式，由网络摄像机或者网络摄像机对应的中级服务器发送给客户端。需要说明的是，网络摄像机或者网络摄像机对应的中级服务器向客户端传输加密密钥时，由于加密密钥是通过 HTTPS 进行传输的，因此可将加密密钥安全的传输至客户端。

5 对于本发明实施例，可以应用的场景如下所述，但不仅限于此，包括：中继服务器获取的待传输视频数据中包含 5 个视频帧，根据视频帧将所述待传输的视频数据划分为 5 个视频帧数据，并且获取到这 5 个视频帧数据在原始视频数据中所占的原始序列号分别为 1、2、3、4、5。然后按照预置排序规则调整所述多个视频帧数据在所述视频数据中所在的位置顺序，其中所述预置排序规则为按照各个视频帧数据的原始序列号降序调整各个视频帧数据的所在位置，则调整后的视频帧数据在原始视频数据中的位置顺序分别为 5、4、3、2、1，再获取调整后各个视频帧数据的原始序列号，根据所述预置对称加密规则的加密密钥和所述各个视频帧数据的原始序列号，分别生成与所述各个视频帧数据分别对应的密钥，最后通过所述各个视频帧数据分别对应的密钥对所述多个视频帧数据分别进行加密，将调整顺序后的加密的所述多个多媒体帧数据发送给客户端。在本发明实施例中，将获取的待产生的多媒体数据划分为多个多媒体数据单元，然后调整所述多媒体数据单元在多媒体数据中的位置数据，并且再通过预置对称加密规则对所述多个多媒体数据单元分别进行加密，最后将调整顺序后的加密的所述多个多媒体帧数据发送给客户端。从而替代了原有 SSL 整体加密多媒体数据的方式，解决了 SSL 加密多媒体数据所产生的额外数据的问题，进而减少了网络系统资源的浪费。

 本发明实施例提供了另一种多媒体数据加密方法，首先获取待传输的多媒体数据；然后将所述多媒体数据划分为多个多媒体数据单元；再通过预置加密规则对所述多个多媒体数据单元分别进行加密；最将加密后的所述多个多媒体数据单元发送给客户端，所述多个多媒体数据单元用于供所述客户端进行输出。与目前通过传统的 SSL 对多媒体数据进行整体加密相比，本发明实施例首先将多媒体数据划分为多个多媒体数据单元，然后对多个多媒体数据单元分别进行加密，最后输出加密后的多媒体数据单元，从而减少了网络系统资源的浪费。

 本发明实施例提供一种多媒体数据加密装置，如图 3 所示，所述多媒体数据加密装置包括：获取单元 31、划分单元 32、加密单元 33、发送单元 34。

30 获取单元 31，用于获取待传输的多媒体数据。

 划分单元 32，用于将所述获取单元 31 获取的多媒体数据划分为多个多媒体数据单元。

 加密单元 33，用于通过预置加密规则对所述划分单元 32 划分的多个多媒体数据单元分别进行加密。

35 发送单元 34，用于将加密后的所述多个多媒体数据单元发送给客户端。

其中，所述多个多媒体数据单元用于供所述客户端进行展示/输出。

需要说明的是，本发明实施例提供的一种多媒体数据加密装置所涉及各功能单元的其他相应描述，可以参考图 1 所示方法的对应描述，在此不再赘述。

本发明实施例提供了一种多媒体数据加密装置，首先获取待传输的多媒体数据；
5 然后将所述多媒体数据划分为多个多媒体数据单元；再通过预置加密规则对所述多个多媒体数据单元分别进行加密；最后将加密后的所述多个多媒体数据单元发送给客户端，所述多个多媒体数据单元用于供所述客户端进行展示/输出。与目前通过传统的 SSL 对多媒体数据进行整体加密相比，本发明实施例首先将多媒体数据划分为多个多媒体数据单元，然后对多个多媒体数据单元分别进行加密，最后输出加密后的
10 的多媒体数据单元，从而减少了网络系统资源的浪费。

本发明实施例提供另一种多媒体数据加密装置，如图 4 所示，所述多媒体数据加密装置包括：获取单元 41、划分单元 42、加密单元 43、发送单元 44。

获取单元 41，用于获取待传输的多媒体数据。

划分单元 42，用于将所述获取单元 41 获取的多媒体数据划分为多个多媒体数
15 据单元。

加密单元 43，用于通过预置加密规则对所述划分单元 42 划分的多个多媒体数据单元分别进行加密。

发送单元 44，用于将加密单元加密后的所述多个多媒体数据单元发送给客户端。

20 其中，所述多个多媒体数据单元用于供所述客户端进行展示/输出。

进一步地，所述装置还包括：生成单元 45 和/或接收单元 46。

生成单元 45，用于生成所述预置加密规则对应的加密密钥。

接收单元 46，用于接收外部设备发送的所述预置加密规则对应的加密密钥。

所述划分单元 42，具体用于按照预置规则将所述多媒体数据划分为多个多媒体
25 帧数据。

所述加密单元 43，具体用于通过预置对称加密规则和所述加密密钥，对所述多个多媒体帧数据分别进行加密。

进一步地，所述装置还包括：调整单元 47。

调整单元 47，用于按照预置排序规则调整所述多个多媒体帧数据在所述多媒体
30 数据中所在的位置顺序。

所述发送单元 44，具体用于将调整顺序后的加密的所述多个多媒体帧数据发送给客户端。

进一步地，

所述获取单元 41，还用于获取各个多媒体帧数据的原始序列号；

35 所述生成单元 45，还用于根据所述加密密钥和所述各个多媒体帧数据的原始序

列号，分别生成与所述各个多媒体帧数据分别对应的密钥。

所述加密单元 43，用于通过所述各个多媒体帧数据分别对应的密钥对所述多个多媒体帧数据分别进行加密。

所述发送单元 44，还用于将所述加密密钥发送给所述客户端。

5 对于本发明实施例，所述多媒体数据为视频数据或音频数据。

需要说明的是，本发明实施例提供的另一种多媒体数据加密装置所涉及各功能单元的其他相应描述，可以参考图 2 所示方法的对应描述，在此不再赘述。

本发明实施例提供了另一种多媒体数据加密装置，首先获取待传输的多媒体数据；然后将所述多媒体数据划分为多个多媒体数据单元；再通过预置加密规则对所述多个多媒体数据单元分别进行加密；最后将加密后的所述多个多媒体数据单元发送给客户端，所述多个多媒体数据单元用于供所述客户端进行输出。与目前通过传统的 SSL 对多媒体数据进行整体加密相比，本发明实施例首先将多媒体数据划分为多个多媒体数据单元，然后对多个多媒体数据单元分别进行加密，最后输出加密后的多媒体数据单元，从而减少了网络系统资源的浪费。

15 在此处所提供的说明书中，说明了大量具体细节。然而，能够理解，本发明的实施例可以在没有这些具体细节的情况下实践。在一些实例中，并未详细示出公知的方法、结构和技术，以便不模糊对本说明书的理解。

类似地，应当理解，为了精简本公开并帮助理解各个发明方面中的一个或多个，在上面对本发明的示例性实施例的描述中，本发明的各个特征有时被一起分组到单个实施例、图、或者对其的描述中。然而，并不应将该公开的方法解释成反映如下意图：即所要求保护的本发明要求比在每个权利要求中所明确记载的特征更多的特征。更确切地说，如下面的权利要求书所反映的那样，发明方面在于少于前面公开的单个实施例的所有特征。因此，遵循具体实施方式的权利要求书由此明确地并入该具体实施方式，其中每个权利要求本身都作为本发明的单独实施例。

25 本领域那些技术人员可以理解，可以对实施例中的设备中的模块进行自适应性地改变并且把它们设置在与该实施例不同的一个或多个设备中。可以把实施例中的模块或单元或组件组合成一个模块或单元或组件，以及此外可以把它分成多个子模块或子单元或子组件。除了这样的特征和/或过程或者单元中的至少一些是相互排斥之外，可以采用任何组合对本说明书（包括伴随的权利要求、摘要和附图）中公开的所有特征以及如此公开的任何方法或者设备的所有过程或单元进行组合。除非另外明确陈述，本说明书（包括伴随的权利要求、摘要和附图）中公开的每个特征可以由提供相同、等同或相似目的的替代特征来代替。

35 此外，本领域的技术人员能够理解，尽管在此所述的一些实施例包括其它实施例中所述的某些特征而不是其它特征，但是不同实施例的特征的组合意味着处于本发明的范围之内并且形成不同的实施例。例如，在下面的权利要求书中，所要求

保护的实施例的任意之一都可以以任意的组合方式来使用。

本发明的各个部件实施例可以以硬件实现，或者以在一个或者多个处理器上运行的软件模块实现，或者以它们的组合实现。本领域的技术人员应当理解，可以在实践中使用微处理器或者数字信号处理器（DSP）来实现根据本发明实施例的多媒体数据加密装置中的一些或者全部部件的一些或者全部功能。本发明还可以实现为用于执行这里所描述的方法的一部分或者全部的设备或者装置程序（例如，计算机程序和计算机程序产品）。这样的实现本发明的程序可以存储在计算机可读介质上，或者可以具有一个或者多个信号的形式。这样的信号可以从因特网网站上下载得到，或者在载体信号上提供，或者以任何其他形式提供。

例如，图 5 示出了可以实现多媒体数据加密方法的计算设备的框图。该计算设备传统上包括处理器 510 和以存储器 520 形式的计算机程序产品或者计算机可读介质。存储器 520 可以是诸如闪存、EEPROM（电可擦除可编程只读存储器）、EPROM、硬盘或者 ROM 之类的电子存储器。存储器 520 具有存储用于执行上述方法中的任何方法步骤的程序代码 531 的存储空间 530。例如，存储程序代码的存储空间 530 可以包括分别用于实现上面的方法中的各种步骤的各个程序代码 531。这些程序代码可以从一个或者多个计算机程序产品中读出或者写入到这一个或者多个计算机程序产品中。这些计算机程序产品包括诸如硬盘，紧致盘（CD）、存储卡或者软盘之类的程序代码载体。这样的计算机程序产品通常为例如图 6 所示的便携式或者固定存储单元。该存储单元可以具有与图 5 的计算设备中的存储器 520 类似布置的存储段、存储空间等。程序代码可以例如以适当形式进行压缩。通常，存储单元包括用于执行根据本发明的方法步骤的计算机可读代码 531'，即可以由诸如 510 之类的处理器读取的代码，当这些代码由计算设备运行时，导致该计算设备执行上面所描述的方法中的各个步骤。

本文中所称的“一个实施例”、“实施例”或者“一个或者多个实施例”意味着，结合实施例描述的特定特征、结构或者特性包括在本发明的至少一个实施例中。此外，请注意，这里“在一个实施例中”的词语例子不一定全指同一个实施例。

应该注意的是上述实施例对本发明进行说明而不是对本发明进行限制，并且本领域技术人员在不脱离所附权利要求的范围的情况下可设计出替换实施例。在权利要求中，不应将位于括号之间的任何参考符号构造成对权利要求的限制。单词“包含”不排除存在未列在权利要求中的元件或步骤。位于元件之前的单词“一”或“一个”不排除存在多个这样的元件。本发明可以借助于包括有若干不同元件的硬件以及借助于适当编程的计算机来实现。在列举了若干装置的单元权利要求中，这些装置中的若干个可以通过同一个硬件项来具体体现。单词第一、第二、以及第三等的使用不表示任何顺序。可将这些单词解释为名称。

此外，还应当注意，本说明书中使用的语言主要是为了可读性和教导的目的而

选择的，而不是为了解释或者限定本发明的主题而选择的。因此，在不偏离所附权利要求书的范围和精神的情况下，对于本技术领域的普通技术人员来说许多修改和变更都是显而易见的。对于本发明的范围，对本发明所做的公开是说明性的，而非限制性的，本发明的范围由所附权利要求书限定。

权 利 要 求

- 1、一种多媒体数据加密方法，包括：
获取待传输的多媒体数据；
5 将所述多媒体数据划分为多个多媒体数据单元；
通过预置加密规则对所述多个多媒体数据单元分别进行加密；
将加密后的所述多个多媒体数据单元发送给客户端。
- 2、根据权利要求1所述的多媒体数据加密方法，其中，所述方法还包括：
生成所述预置加密规则对应的加密密钥；或者
10 接收外部设备发送的所述预置加密规则对应的加密密钥。
- 3、根据权利要求2所述的多媒体数据加密方法，其中，所述将所述多媒体数据划分为多个多媒体数据单元的步骤进一步包括：
按照预置规则将所述多媒体数据划分为多个多媒体帧数据。
- 4、根据权利要求3所述的多媒体数据加密方法，其中，所述通过预置加密规则
15 对所述多个多媒体数据单元分别进行加密的步骤进一步包括：
通过预置对称加密规则和所述加密密钥，对所述多个多媒体帧数据分别进行加密。
- 5、根据权利要求4所述的多媒体数据加密方法，其中，所述按照预置规则将所述多媒体数据划分为多个多媒体帧数据之后，所述方法还包括：
20 按照预置排序规则调整所述多个多媒体帧数据在所述多媒体数据中所在的位置顺序。
- 6、根据权利要求5所述的多媒体数据加密方法，其中，所述将加密后的所述多个多媒体数据单元发送给客户端的步骤进一步包括：
将调整顺序后的加密的所述多个多媒体帧数据发送给客户端。
- 25 7、根据权利要求4所述的多媒体数据加密方法，其中，所述通过预置对称加密规则和所述加密密钥，对所述多个多媒体帧数据分别进行加密之前，所述方法还包括：
获取各个多媒体帧数据的原始序列号；
根据所述加密密钥和所述各个多媒体帧数据的原始序列号，分别生成与所述各个多媒体帧数据分别对应的密钥。
- 30 8、根据权利要求7所述的多媒体数据加密方法，其中，所述通过预置对称加密规则和所述加密密钥，对所述多个多媒体帧数据分别进行加密的步骤进一步包括：
通过所述各个多媒体帧数据分别对应的密钥对所述多个多媒体帧数据分别进行加密。
- 9、根据权利要求2所述的多媒体数据加密方法，其中，所述将加密后的所述多
35 个多媒体数据单元发送给客户端之后，所述方法还包括：

将所述加密密钥发送给所述客户端,所述加密密钥用于供所述客户端对加密后的所述多个多媒体数据单元进行解密。

10、根据权利要求 1-9 任一所述的多媒体数据加密方法,其中,所述多媒体数据为视频数据或音频数据。

5 11、一种多媒体数据加密装置,包括:

获取单元,用于获取待传输的多媒体数据;

划分单元,用于将所述获取单元获取的多媒体数据划分为多个多媒体数据单元;

加密单元,用于通过预置加密规则对所述划分单元划分的多个多媒体数据单元分别进行加密;

10 发送单元,用于将加密单元加密后的所述多个多媒体数据单元发送给客户端。

12、根据权利要求 11 所述的多媒体数据加密装置,其中,所述装置还包括:

生成单元,用于生成所述预置加密规则对应的加密密钥;

接收单元,用于接收外部设备发送的所述预置加密规则对应的加密密钥。

13、根据权利要求 12 所述的多媒体数据加密装置,其中,

15 所述划分单元,具体用于按照预置规则将所述多媒体数据划分为多个多媒体帧数据。

14、根据权利要求 13 所述的多媒体数据加密装置,其中,

所述加密单元,具体用于通过预置对称加密规则和所述加密密钥,对所述多个多媒体帧数据分别进行加密。

20 15、根据权利要求 14 所述的多媒体数据加密装置,其中,所述装置还包括:

调整单元,用于按照预置排序规则调整所述多个多媒体帧数据在所述多媒体数据中所在的位置顺序。

16、根据权利要求 15 所述的多媒体数据加密装置,其中,

25 所述发送单元,具体用于将调整顺序后的加密的所述多个多媒体帧数据发送给客户端。

17、根据权利要求 14 所述的多媒体数据加密装置,其中,

所述获取单元,还用于获取各个多媒体帧数据的原始序列号;

所述生成单元,还用于根据所述加密密钥和所述各个多媒体帧数据的原始序列号,分别生成与所述各个多媒体帧数据分别对应的密钥。

30 18、根据权利要求 17 所述的多媒体数据加密装置,其中,

所述加密单元,具有用于通过所述各个多媒体帧数据分别对应的密钥对所述多个多媒体帧数据分别进行加密。

19、根据权利要求 12 所述的多媒体数据加密装置,其中,

35 所述发送单元,还用于将所述加密密钥发送给所述客户端,所述加密密钥用于供所述客户端对加密后的所述多个多媒体数据单元进行解密。

20、根据权利要求 11-18 任一所述的多媒体数据加密装置，其中，所述多媒体数据为视频数据或音频数据。

21、一种计算机程序，包括计算机可读代码，当所述计算机可读代码在计算设备上运行时，导致所述计算设备执行根据权利要求 1 至 10 中任一项所述的多媒体数据加密方法。

22、一种计算机可读介质，其中存储了如权利要求 21 所述的计算机程序。

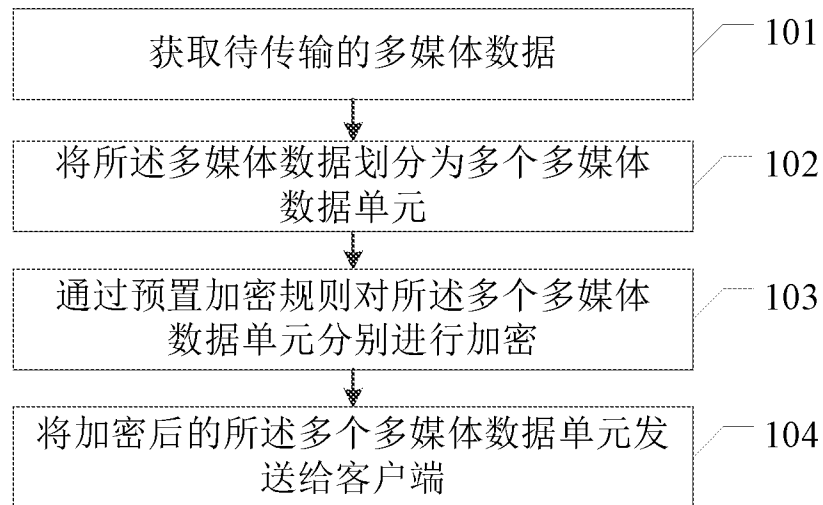


图 1

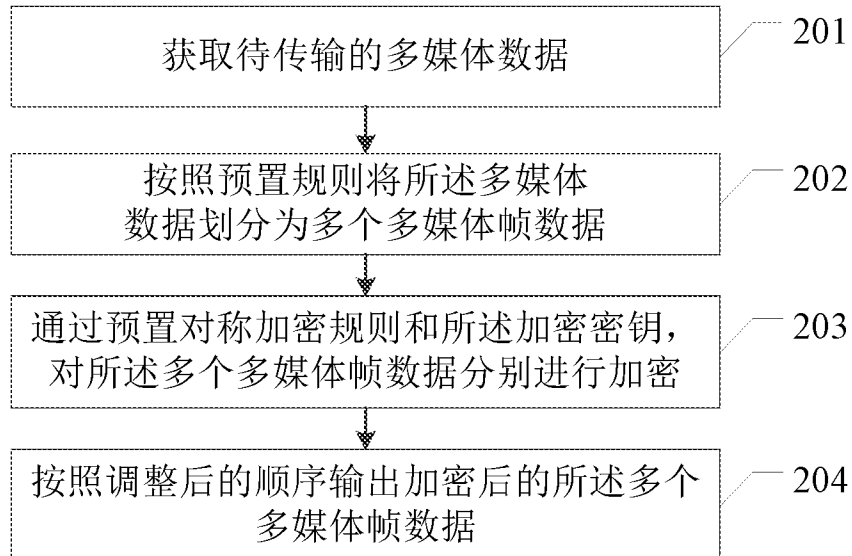


图 2

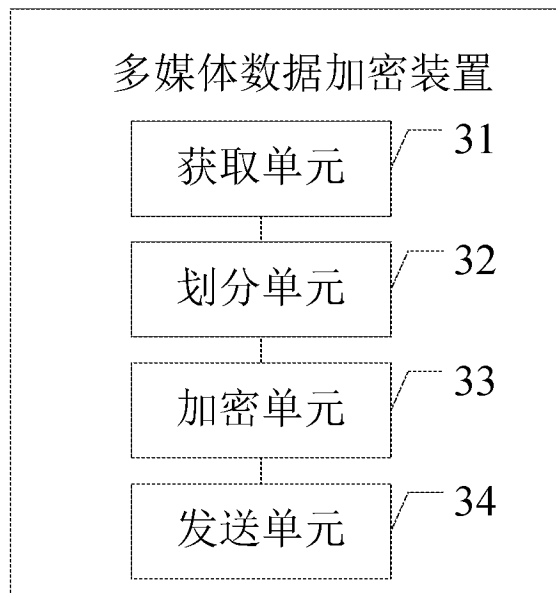


图 3

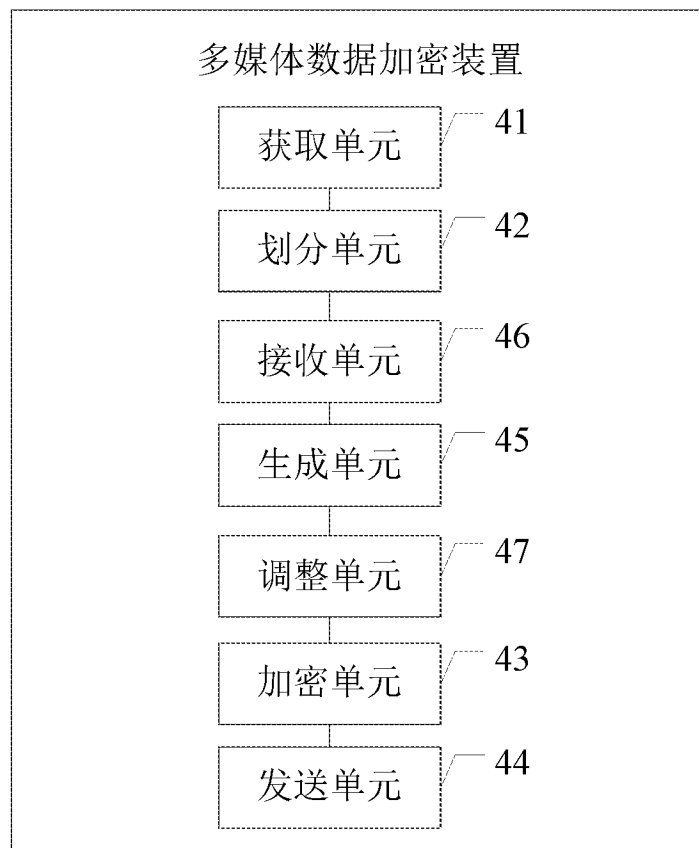


图 4

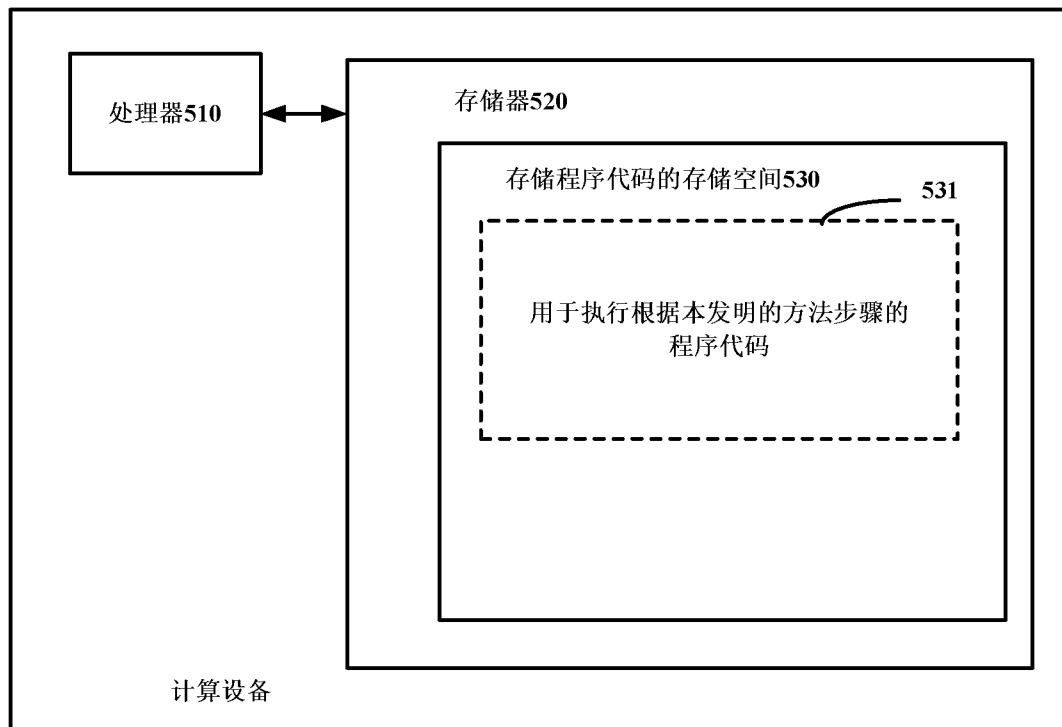


图 5

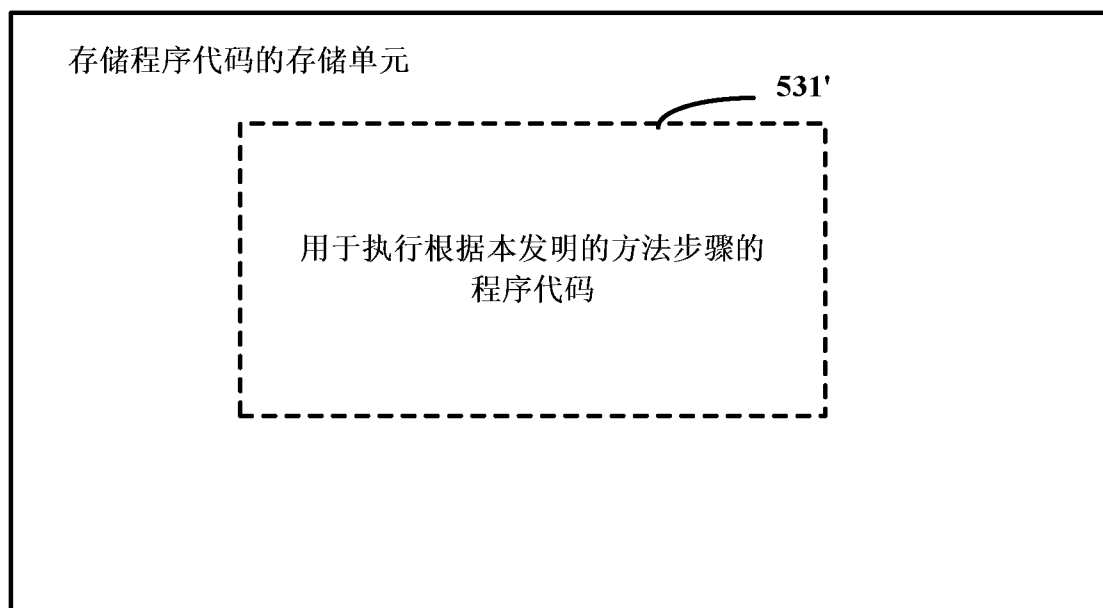


图 6

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2016/083713

A. CLASSIFICATION OF SUBJECT MATTER

H04N 21/2347 (2011.01) 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)

H04N; 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)

WPI, EPODOC, CNPAT, CNKI, GOOGLE: fragment, slicing, partition, encrypt, media, video, audio, data, segment, divide, encrypt, key, chip

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 105337963 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 17 February 2016 (17.02.2016), description, pages 9-11	1-22
X	CN 104410828 A (BEIJING NOVEL-SUPERTV DIGITAL TV TECHNOLOGY CO., LTD.), 11 March 2015 (11.03.2015), description, pages 2-4	1-22
X	CN 103297809 A (HUAWEI TECHNOLOGIES CO., LTD.), 11 September 2013 (11.09.2013), description, pages 3-4	1-22
X	CN 103248474 A (HUAWEI TECHNOLOGIES CO., LTD.), 14 August 2013 (14.08.2013), description, pages 2-4	1-22
A	WO 2014022062 A1 (INTEL CORP.), 06 February 2014 (06.02.2014), the whole document	1-22

☐ 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 02 August 2016 (02.08.2016)	Date of mailing of the international search report 24 August 2016 (24.08.2016)
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 YANG, Weiming Telephone No.: (86-10) 62413403

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2016/083713

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 105337963 A	17 February 2016	None	
CN 104410828 A	11 March 2015	None	
CN 103297809 A	11 September 2013	None	
CN 103248474 A	14 August 2013	None	
WO 2014022062 A1	06 February 2014	EP 2880590 A1	10 June 2015
		EP 2880590 A4	17 February 2016
		CN 104145274 A	12 November 2014
		US 2014032924 A1	30 January 2014

国际检索报告

国际申请号

PCT/CN2016/083713

A. 主题的分类

H04N 21/2347 (2011.01) 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)

H04N; 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))

WPI, EPODOC, CNPAT, CNKI, GOOGLE: 视频, 音频, 媒体, 数据, 分段, 片段, 分片, 划分, 分割, 加密, media, video, audio, data, segment, divide, encrypt, key, chip

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
PX	CN 105337963 A (北京奇虎科技有限公司等) 2016年 2月 17日 (2016 - 02 - 17) 说明书第9-11页	1-22
X	CN 104410828 A (北京视博数字电视科技有限公司) 2015年 3月 11日 (2015 - 03 - 11) 说明书第2-4页	1-22
X	CN 103297809 A (华为技术有限公司) 2013年 9月 11日 (2013 - 09 - 11) 说明书第3-4页	1-22
X	CN 103248474 A (华为技术有限公司) 2013年 8月 14日 (2013 - 08 - 14) 说明书第2-4页	1-22
A	WO 2014022062 A1 (INTEL CORPORATION) 2014年 2月 6日 (2014 - 02 - 06) 全文	1-22

☐ 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 8月 2日

国际检索报告邮寄日期

2016年 8月 24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

杨威明

电话号码 (86-10) 62413403

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2016/083713

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	105337963	A	2016年 2月 17日	无			
CN	104410828	A	2015年 3月 11日	无			
CN	103297809	A	2013年 9月 11日	无			
CN	103248474	A	2013年 8月 14日	无			
WO	2014022062	A1	2014年 2月 6日	EP	2880590	A1	2015年 6月 10日
				EP	2880590	A4	2016年 2月 17日
				CN	104145274	A	2014年 11月 12日
				US	2014032924	A1	2014年 1月 30日

表 PCT/ISA/210 (同族专利附件) (2009年7月)