



(12) 发明专利

(10) 授权公告号 CN 1578457 B

(45) 授权公告日 2010.04.28

(21) 申请号 200410063492.5

US 6304659 B1, 2001.10.16, 全文.

(22) 申请日 2004.07.09

US 5285497 A, 1994.02.08, 说明书第5栏第22-49行、附图3.

(30) 优先权数据

03102202.3 2003.07.17 EP

JP 特开 2000-59753 A, 2000.02.25, 全文.

审查员 戴方兴

(73) 专利权人 汤姆森许可贸易公司

地址 法国布洛里

(72) 发明人 德克·阿道夫 安德烈·舍维措

马尔科·温特

(74) 专利代理机构 中科专利商标代理有限责任

公司 11021

代理人 戎志敏

(51) Int. Cl.

H04N 7/16 (2006.01)

H04N 7/24 (2006.01)

(56) 对比文件

US 5517232 A, 1996.05.14, 全文.

US 5420866 A, 1995.05.30, 全文.

CN 1211775 A, 1999.03.24, 全文.

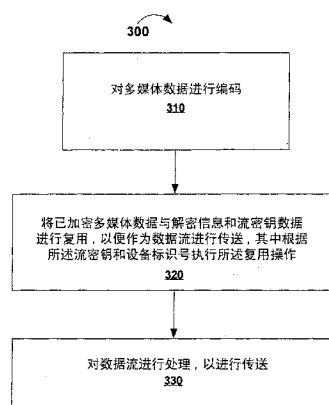
权利要求书 1 页 说明书 5 页 附图 4 页

(54) 发明名称

个人视频加密系统和方法

(57) 摘要

一种用于创建复用数据流的方法,所述复用数据流由已加密多媒体数据(310)、解密信息和流密钥数据组成。创建复用数据流(320)的处理采用根据流密钥数据和优选地与这种复用数据流的接收机相对应的设备标识号而确定的复用模式。作为复用数据流的一部分进行传输的流密钥数据位于预定位置,以便于解码器从所述预定位置中提取出该流密钥数据。然后,针对传送(330),对复用数据流进行处理。还公开了一种用于对复用数据流进行解复用的方法和设备。



1. 一种用于将数据类型复用为复用数据流的方法,包括以下步骤:
将多媒体数据编码成已加密多媒体数据 (310);以及
将所述已加密多媒体数据与流密钥数据和设备标识号进行复用 (320);
其特征在于,使用所述流密钥数据和所述设备标识号作为复用器中的种子值,以便确定复用数据流中所述已加密多媒体数据、流密钥数据和设备标识号的位置,其中流密钥数据的位置是预定的。
2. 根据权利要求 1 所述的方法,其特征在于所述编码步骤包括:
将多媒体数据编码成多媒体数据格式,以及
对所述已编码多媒体数据进行加密以获得已加密多媒体数据。
3. 根据权利要求 1 所述的方法,其特征在于针对通过数据网络的传送,对所述数据流进行处理。
4. 根据权利要求 1 所述的方法,其特征在于所述设备标识号对应于所述复用数据流的接收器。
5. 根据权利要求 1 所述的方法,其特征在于:还根据将要使用所述已加密多媒体数据的应用来执行所述复用步骤。
6. 一种用于执行复用操作的设备,所述设备包括:
编码器 (120),将多媒体数据编码成已加密多媒体数据;以及
模式复用器 (140),将所述已加密多媒体数据与流密钥数据和设备标识号进行复用;
其特征在于,所述模式复用器 (140) 还使用所述流密钥数据和所述设备标识号作为复用器中的种子值,以便确定复用数据流中所述已加密多媒体数据、流密钥数据和设备标识号的位置,其中流密钥数据的位置是预定的。
7. 一种用于将根据权利要求 1 中的方法而获得的复用数据流解复用成已加密多媒体数据、设备标识号和流密钥数据的方法,其特征在于使用所述流密钥数据和所述设备标识号来对复用数据流进行解复用,并且所述流密钥数据的位置是预定的。
8. 根据权利要求 7 所述的方法,其特征在于使用所述设备标识号,将所述已加密多媒体数据解密为适合于回放的格式。
9. 一种用于对根据权利要求 1 中的方法而获得的包括已加密多媒体数据、设备标识号和流密钥数据的复用数据流执行解复用的设备,所述设备包括:
模式解复用器 (540),使用所述流密钥数据和所述设备标识号来对所述复用数据流进行解复用,其中所述流密钥数据的位置是预定的;以及
解码器 (520),用于利用所述设备标识号将所述解复用数据流解码成适合于回放或存储的格式。

个人视频加密系统和方法

技术领域

[0001] 本发明涉及一种用于加密多媒体数据的方法和设备,尤其是在传输之前,对多媒体数据进行加密。

背景技术

[0002] 随着如因特网等数据网络的发展以及宽带连接的普遍接受,客户需要能够通过通信网络,根据需要选择和传递视频和音频对象(例如,电视节目、电影、视频会议、广播节目等)。因此,对点播传递系统的设计必须考虑用于传递媒体对象的编解码器(编码器/解码器程序)、在显示传递多媒体数据时的服务质量(QoS)问题、以及通过通信网络对多媒体数据的传送,如以信号形式传递的音频和视频数据。

[0003] 通常,以软件和硬件的组合来实现编解码器。此系统用于在通信网络的发射端对表示媒体对象的多媒体数据进行编码,以及在通信网络的接收器端对数据进行解码。对于编解码器的设计考虑包括以下问题:网络上带宽的可扩缩性、编码/解码数据的计算复杂度、对网络损失(数据丢失)的弹力、以及用于传输表示媒体流的数据的编码器/解码器的等待时间。采用离散余弦变换(CDT)(例如,如国际电信联盟所公布的针对低比特率通信的视频编码 H. 263 中所描述的视频编码器)和非 DCT 技术的通用编解码器是考虑了上述这些细节问题的编解码器的示例。因为在通信网络上可得到的有限带宽,编解码器也用于压缩和解压缩数据。

[0004] 服务质量问题涉及音频和视频信息的传递,以及用户观看媒体对象的整体感受。以公知为分组的离散单元通过通信网络来传递媒体对象。通过公知为服务器和路由器的数据网络节点来发送这些信息单元,所述信息单元通常按照次序进行传输。因此,因为分组可以采用不同的路径通过因特网,两个顺序传送的分组在不同的时刻到达目的设备是可能的。因此,公知为离散的 QoS 问题可能会导致在较早传送的分组之前,对在时间上较晚传送的分组进行了处理和显示,导致了显示事件的不连续性。类似地,在传输时,分组丢失也是可能的。典型地,目的设备执行错误隐藏技术,以隐藏数据的丢失。可以使用用于确保网络上的 QoS 的方法,如传输分组号的过度分配(over-allocating)或提高处于负载状态下的网络的质量等,但这些方法引入了影响通信网络性能的额外的开销需要。

[0005] 通信网络使用公知为传送协议的方案来控制数据分组的传送。在因特网工程任务组(IETF)请求说明(RFC)793 中所描述的传输控制协议(TCP)是用于控制通过通信网络的信息流的公知传送协议。传送协议试图通过维持如流量控制、差错控制等参数和数据分组的时间组织传递来稳定通信网络。通过使用位于分组报头中或与通过通信网络在设备之间传输的分组相分离的命令,对这些类型的控制进行管理。此控制信息适用于按照其中数据分组的传输趋向于有序化的“同步”方式进行操作的通信网络。

[0006] 当在通信网络上传送多媒体数据时,这些多媒体数据的制造者希望只有合法访问这些传送数据的用户能够接收和使用传送产品。在许多情况下,那些不具有对这些数据的合法访问的已知为盗用者的人们会截获并使用多媒体数据。为了最小化多媒体数据的非法

使用,制造者通过条件访问方式来保护数据,使得未授权用户难以访问和使用这些数据。

[0007] 条件访问的一些公共技术包括要求使用访问数据的口令、数据加扰、数据加密等。随着条件访问系统的频繁使用,盗用者了解了何时闯入这种系统,以非法访问这些受保护的数据。如果盗用者事先了解到使用了何种技术来保护数据,就会发生这种情况。

[0008] 除此之外,现有技术并未教导多媒体数据制造者如何简单地保护多媒体数据,而不会向盗用者揭示正在使用哪种特定的技术来保护这些数据。例如,在 1998 年 12 月 10 日、由 CM COMMUNITY MEDIA GMBH&CO, ET AL. 出版的文件 DE-U-29814544 公开了一种借助于密钥对视频流进行加密的操作。还对密钥进行加密,并通过卫星发送给客户。客户接收已加密密钥,并对这些已加密数据进行解密。

发明内容

[0009] 本发明的主题是一种用于保护多媒体数据的方法,其包括以下步骤:

[0010] 将多媒体数据编码成已加密多媒体数据;以及

[0011] 将所述已编码多媒体数据与流密钥数据和解密信息进行复用;其特征在于

[0012] 根据流密钥数据和设备标识号执行所述复用步骤。

[0013] 本发明的一个方面示出了一种用于将多媒体数据复用成复用数据流的设备。

[0014] 本发明的一个方面示出了一种用于根据包括在数据流中的流密钥数据,对复用数据流进行解复用的方法。

[0015] 本发明的一个方面示出了一种用于根据包括在数据流中的流密钥数据,对复用数据流进行解复用的设备。

附图说明

[0016] 现在,将参照试图描述而不是限制本发明的范围的附图,对本发明的多种特征和优点及其优选实施例进行描述,其中:

[0017] 图 1 是依照本发明的典型实施例,将多媒体数据处理为受保护的复用数据流的编码器的系统图;

[0018] 图 2 依照本发明的典型实施例,描述了受保护的复用数据流的内容;

[0019] 图 3 是依照本发明的典型实施例,将多媒体数据编码成受保护的复用数据流的方法的方框图;

[0020] 图 4 是依照本发明的单性实施例,用于对受保护的复用数据流进行解复用的方法的方框图;以及

[0021] 图 5 是依照本发明的典型实施例,将复用数据流解复用成多媒体数据的解码器的系统图。

具体实施方式

[0022] 如这里所用,多媒体数据表示文字、图像、视频和音频数据的任意组合。流媒体包括通过因特网或其他通信数据网络传递给用户的音频、视频、多媒体、文字和交互数据,其中在完整地接收到媒体的所有多媒体数据之前,可以对该媒体进行回放。

[0023] 典型实施例涉及视频点播服务器领域,所述视频点播服务器通过数据网络将电

影、电视节目、广播节目等多媒体数据传递给用户。但是,本发明并不仅仅局限于此典型实施例,而是可以应用于其中向用户传送多媒体数据,并且需要保护数据不受到第三方的未经授权访问的任何系统。

[0024] 图 1 是依照本发明的典型实施例,将媒体对象的多媒体数据处理成受保护的复用数据流的编码器的系统图。在本实施例中,服务供应商针对去往数据订户的传输,对多媒体数据进行处理,其中,对该数据进行保护以防止第三方使用该数据。优选地,数据订户操作具有惟一标识号 (UID) 的解码器,所述标识号用于识别数据订户的指示符。可以根据对数据网络的 IEEE 802.3 兼容连接中的网络接口卡 (NIC) 所使用的标识号、在解码操作中使用的媒体访问控制 (MAC) 地址、或服务供应商分配给数据订户的 UID 等,将该号码分配给解码器。可选地,服务供应商使用 UID 来识别和确定与该 UID 相对应的数据用户的访问特权。

[0025] 作为编码系统 100 的一部分的多媒体数据服务器 110 存储和传送多媒体数据,优选地,向数据订户传送。多媒体数据表示如电影、电视节目、广播节目等媒体对象的音频和/或视频数据。多媒体数据服务器 110 可以是硬盘驱动器、移动硬盘、光盘、数字通用盘或其中的多个,以及针对编码操作,用于存储和传递多媒体数据的任何其他设备。在本发明的可选实施例中,以针对传输最终编码的实时产生的多媒体数据的数据馈送器 (data feed) 来代替多媒体数据服务器 110。

[0026] 与多媒体数据服务器 110 相连的编码器 120 将多媒体数据编码成适合于进行处理的格式。例如,将编码器 120 接收到的多媒体数据格式化为 MPEG-2 兼容格式。在这种类型的编码操作中,使用编码器 120 是本领域中所公知的,例如,使用编码器 120 将多媒体数据编码成不同的多媒体格式,如 MPEG-2、MPEG-4、联合视频组压缩等。

[0027] 编码器 120 也用于保护多媒体数据,使其成为第三方更加难以访问该受保护数据的格式。在典型实施例中,编码器 120 使用编码表,将 MPEG-2 格式的数据编码为加密格式。因此,限制了第三方对已编码多媒体格式的直接访问,而无需知道如何对该数据进行加密。代替地,编码器 120 可以使用如数据加密标准 (DES)、国际数据加密算法 (IDEA)、安全快速加密例程 (SAFER) 或本领域公知的其他类型的加密方法等加密处理,对多媒体数据进行加密。加密操作的产品产生了被称为已加密多媒体数据的数据。

[0028] 接下来,模式复用器 (pattern multiplexer) 140 接收来自编码器 120 的已加密多媒体数据。模式复用器 140 通过将来自编码器 120 接收到的已加密多媒体数据与其他类型的数据进行复用,执行数据保护的第二步,这种复用操作被称为复用模式 (MUXP)。

[0029] 因此, MUXP 操作以服务供应商随机选择已知为流密钥的数值或项开始,由流密钥发生器 115 执行。此外,模式复用器 140 根据设备标识号 130,获得与用户或用户设备相对应的 UID。模式复用器 140 使用流密钥和 UID,来确定如何将来自编码器 120 的数据与流密钥和用于解密来自编码器 120 的数据的解密信息进行复用。

[0030] 模式复用器 140 通过使用流密钥和 UID 作为 MUXP 中的种子值,考虑数学公式,或任何用于分配数据流中至少三种不同数据类型的位置的其他技术来执行流密钥、解密信息和已加密多媒体数据的复用。例如,尽管可以使用其他类型的公式或处理来确定 MUXP,但模式复用器 140 所使用的 MUXP 是使用流密钥和 UID 作为种子值的统计复用操作。重要的是,如果 UID 值或流密钥值任一个改变,则 MUXP 模式页发生改变。

[0031] 在图 2 中示出了由 MUXP 受控的复用操作的产品,图 2 示出了受保护的复用数据流的内容。在优选实施例中,以数据分组的形式传送受保护的复用数据流 200(此后称为数据流 200),但数据流 200 可以是任意数据格式的。数据流 200 的组成至少包括三种不同的数据类型:流密钥 210、已加密多媒体数据 220 和解密信息 230。流密钥 210 表示用于复用和/或解复用数据流 200 的流密钥数据。优选地,流密钥 210 总是占据数据流 200 中相同的分组位置,可以依照预定的顺序重复这些位置。已加密多媒体数据 220 表示从编码器 120 接收到的复用数据。

[0032] 解密信息 230 是用于对已加密多媒体数据 220 进行解密的数据,作为数据流 200 的一部分。优选地,解密信息 230 用于执行用来产生已加密多媒体数据 220 的加密处理的逆操作。解密信息的内容可以是密码信息、密钥或用于解密受保护数据的其他数据。

[0033] 在复用操作之后,由传送编码器 150 将数据流 200 格式化为适合于传输的格式,如用在 TCP/IP 兼容网络上的数据分组。传送编码器 150 通过数据网络 160 传送格式化数据,以便用在解码器中,进行解码操作。

[0034] 在本发明的可选实施例中,考虑到已解码多媒体数据的回放或存储等应用,选择用于创建数据流 200 而分配数据的 MUXP。例如,当想要在基于流的应用期间回放多媒体数据时, MUXP 模式将倾向于将大部分的解密信息设置在数据流 200 的开始,而将多媒体数据复用在数据流 200 中较后的位置。因此,当在对多媒体数据形成流时使用这种结构时,利用对多媒体数据的流缓冲的解码器的操作更为有效。相反,对于存储操作, MUXP 将解密数据均匀地分布在整個数据流 200 中,因为并不在实时操作中直接回放数据。

[0035] 图 3 是依照本发明的典型实施例,将多媒体数据编码成受保护的复用数据流的方法的方框图。在步骤 310 中,编码器 120(参照图 1)依照本发明的原理,对表示音频和/或视频媒体对象的多媒体数据进行编码,优选地,加密成已加密多媒体数据。如前所述,编码和加密处理可以是任意类型的。

[0036] 在步骤 320 中,将已加密多媒体数据与解密信息和流密钥数据一起复用成条件访问保护的复用数据流。如前所述,模式复用器 140 根据依赖于(来自流密钥发生器 115 的)流密钥的 MUXP 和来自设备标识号 130 的 UID,将三种数据类型复用成受保护的复用数据流 200(参照图 2)。如果流密钥数据或 UID 任一个发生改变,则复用数据流中各个数据类型的位置也将发生改变。

[0037] 在步骤 330 中,传送编码器 150 将数据流 200 格式化为适合于通过数据网络 160 传送的格式。优选地,将数据流 200 传送到与 UID 相对应的解码器。

[0038] 图 4 是依照本发明的典型实施例,对条件访问保护的数据流进行解复用的方法的方框图。在优选实施例中,将数据流 200 解复用为以下数据类型:流密钥 210、已加密多媒体数据 220 和解密信息 230。然后,使用这些数据类型,将已加密多媒体数据 220 处理成适合于回放或存储的格式的未加密多媒体数据。

[0039] 依照本发明的典型实施例,作为将复用数据流解复用成多媒体数据的解码器的系统图,考虑图 5 所示的解码系统 500,来解释图 4 所示的步骤。

[0040] 在步骤 410 中,解复用方法 400 以从数据网络 560 接收到复用数据流为开始。优选地,将能够从数据网络接收数据的设备用于此步骤,如传送解码器 550 等,尽管还可以使用能够接收数据的任何设备。传送解码器 550 对接收到的数据流进行格式化,以便由模式

解复用器 540 进行处理。

[0041] 在步骤 420 中,由解复用器 540(其执行模式复用器 140 的逆操作)对接收到的复用数据流进行解复用。解复用处理使用作为复用数据流的组成部分而传送过来的流密钥信息。典型地,因为流密钥信息位于复用数据流中的预定位置,模式解复用器 540 知道从接收到的数据流的什么地方提取该流密钥信息。此外,模式解复用器 540 使用与其自身或相连的解码器相对应的 UID 来进行解复用操作。

[0042] 解复用操作是用于创建复用数据流的逆操作。具体地,模式解复用器 540 使用逆 MUXP 操作,其使用流密钥和 UID,将复用数据流重构成解密信息和已加密多媒体数据。

[0043] 在步骤 430 中,将已加密多媒体数据处理为适合于回放或存储的格式。利用如解码器 520 等解码设备(其执行编码器 120 的编码和加密的逆操作)执行此步骤。解码器 520 使用从复用数据流中解复用出的解密信息,将已加密多媒体信息解密为已编码多媒体数据。然后,将该数据解密成适合于在如电视机、计算机、CD 播放器等多媒体设备上回放或存储的数据格式,理想地,该数据表示类似于来自多媒体数据服务器 110(来自图 1)的数据的多媒体数据。

[0044] 可以以用于实现这些处理的计算机实现方法和设备来具体实现本发明。也可以以在如软盘、只读存储器(ROM)、CD-ROM、硬盘驱动器、高密度盘或任意其他计算机可读存储介质等有形介质上具体实现的计算机程序代码的形式来具体实现本发明,其中,在将计算机程序代码加载到计算机中,并执行时,该计算机成为实现本发明的设备。还可以以计算机程序代码的形式具体实现本发明,例如,是否存储在存储介质中、加载到计算机中并/或由计算机执行、或者在一些传输介质上传输,如电线或电缆、光纤,或通过电磁辐射,其中,在计算机加载计算机程序代码并执行时,该计算机成为实现本发明的设备。当在通用处理器上实现时,计算机程序代码段对处理器进行配置,以创建特定的逻辑电路。

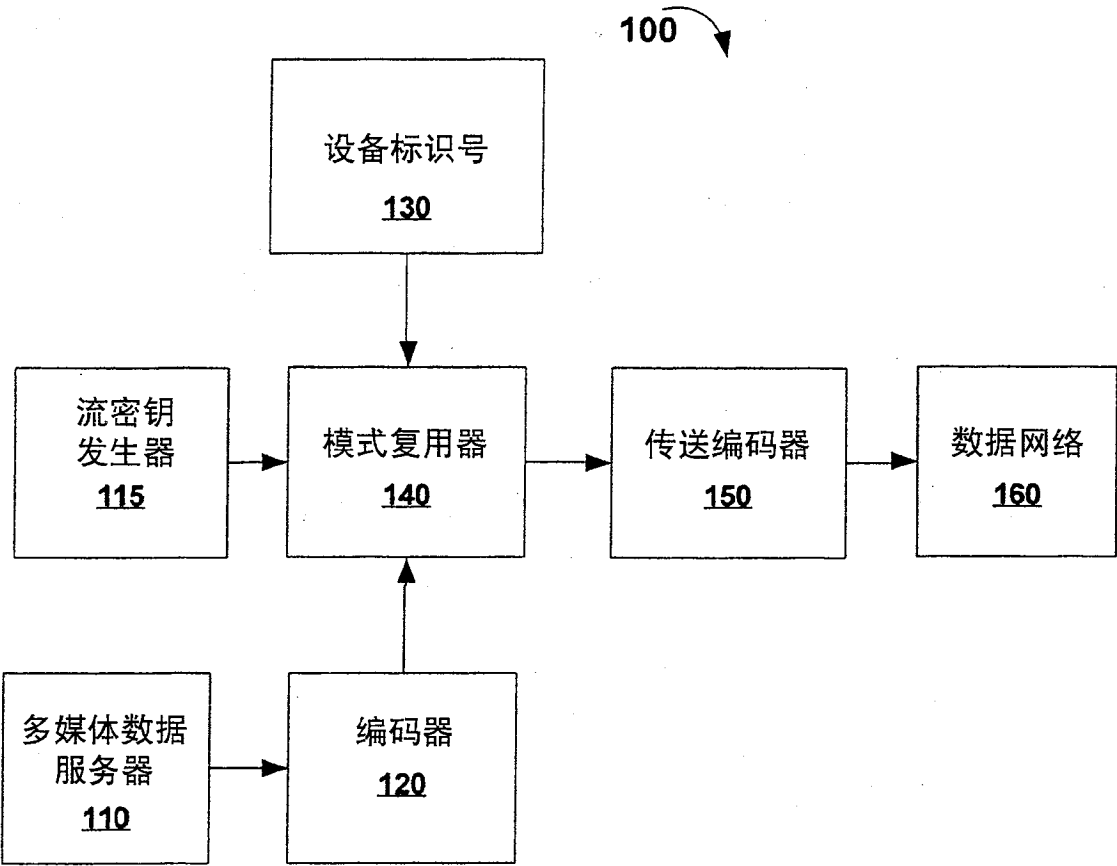


图 1

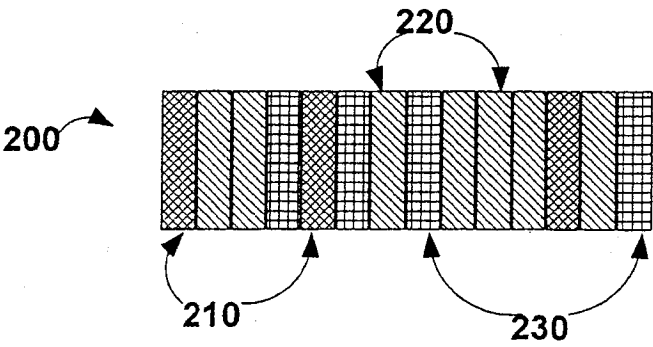


图 2

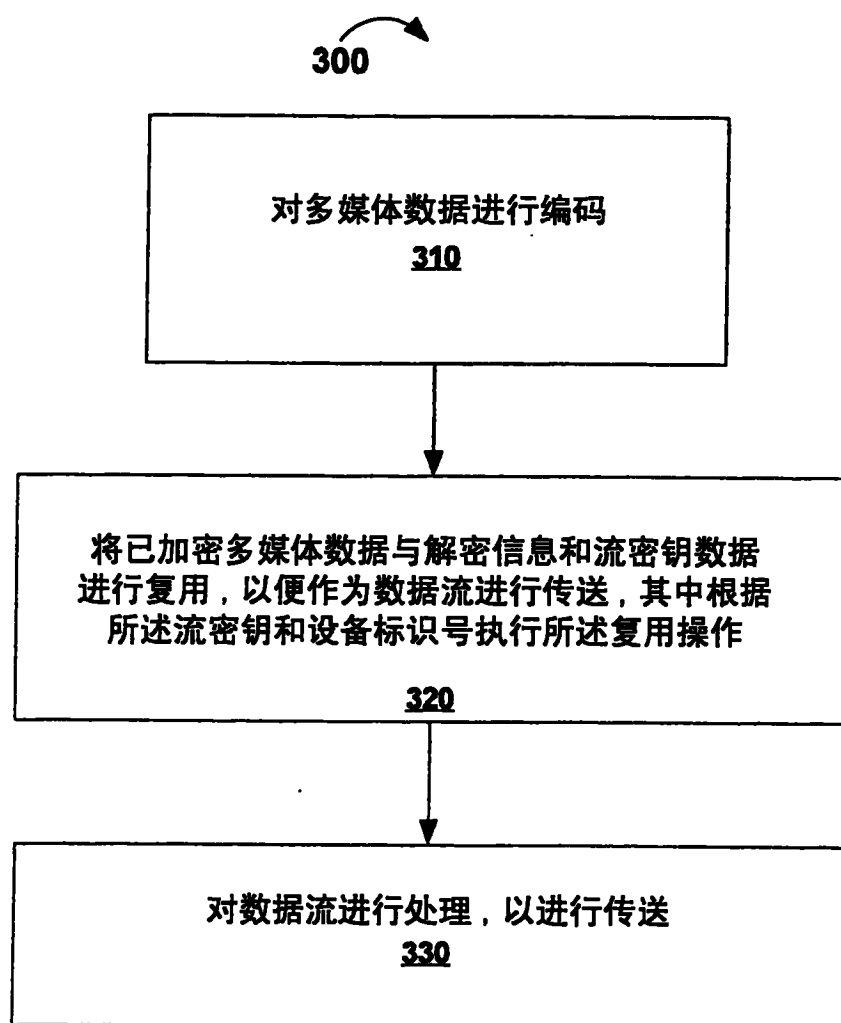


图 3

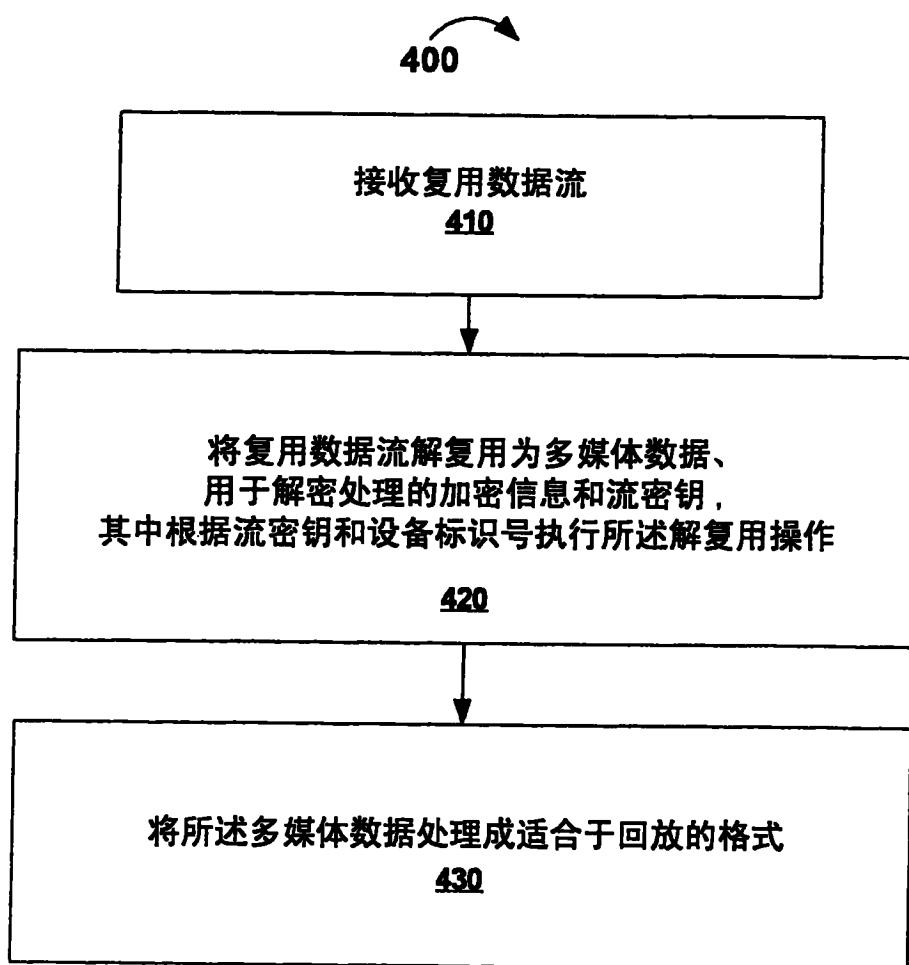


图 4

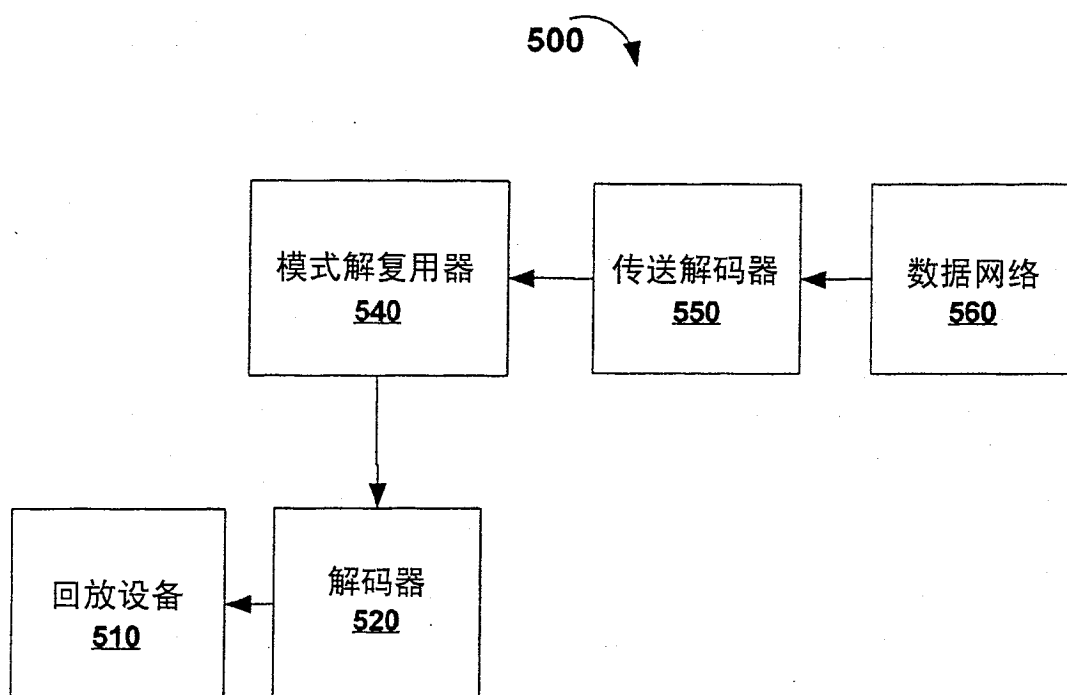


图 5