(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 105635759 A
(43)申请公布日 2016.06.01

(21)申请号 201610055960.7

(22)申请日 2016.01.27

(71)申请人 深圳国微技术有限公司
地址 518057 广东省深圳市南山区高新技术产业园南区高新南一道国微研发大厦1楼西侧部分、2楼

(72)发明人 张华森 彭美意 李诚

(74)专利代理机构 深圳市深佳知识产权代理事务所（普通合伙） 44285
代理人 王仲凯

(51)Int.Cl.
H04N 21/254(2011.01)
H04N 21/4627(2011.01)
H04N 21/8355(2011.01)
G06F 21/10(2013.01)

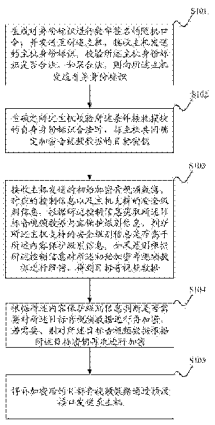
权利要求书2页 说明书6页 附图3页

(54)发明名称

一种输出内容保护方法与条件接收模块

(57)摘要

本发明公开了一种输出内容保护方法与条件接收模块，接收主机发送的主机身份标识，主机身份标识合法则向所述主机发送自身身份标识；与主机共同确定一个加密音视频数据的目标密钥；接收主机发送的初始加密音视频数据与对应的控制信息，根据控制信息对所述初始加密音视频数据进行解密，得到目标音视频数据；根据控制信息获取目标音视频数据内容保护级别信息，可以根据解密后的目标音视频数据的控制信息获取内容保护级别信息，根据内容保护级别信息需要加密的输出内容进行再加密，可以得到主机支持的安全级别信息，根据安全级别信息决定是否将需要保护的目标音视频数据输出到主机，可以对输出内容实现保护，避免非法设备窃取到解密后的内容。



CN 105635759 A

1.一种输出内容保护方法，其特征在于，应用于条件接收模块，所述方法包括：

生成对身份标识进行数字签名的随机口令，并发送至所述主机，接收主机发送的主机身份标识，校验所述主机身份标识是否合法，如果合法，则向所述主机发送自身身份标识；

当确定所述主机校验所述条件接收模块的自身身份标识合法时，与主机共同确定加密音视频数据的目标密钥；

接收主机发送的初始加密音视频数据、对应的控制信息以及主机支持的安全级别信息，根据所述控制信息获取所述目标音视频数据内容保护级别信息，判断所述主机支持的安全级别信息是否高于所述内容保护级别信息，如果是则根据所述控制信息对所述初始加密音视频数据进行解密，得到目标音视频数据；

根据所述内容保护级别信息判断是否需要对所述目标音视频数据进行再加密，若需要，则对所述目标音视频数据根据所述目标密钥再次进行加密；

将再加密后的目标音视频数据通过预设接口发送至主机。

2.根据权利要求1所述的输出内容保护方法，其特征在于，对所述目标音视频数据根据所述目标密钥再次进行加密后还包括：

为根据所述目标密钥再次进行加密后的目标音视频数据设置相应的加密标志。

3.根据权利要求1所述的输出内容保护方法，其特征在于，对所述初始加密信息进行解密，得到目标音视频数据与对应的控制信息后还包括：

判断所述目标密钥的生成时间是否超过预设周期，若超过则对所述目标密钥进行更新。

4.根据权利要求1所述的输出内容保护方法，其特征在于，所述目标密钥为对称密钥。

5.根据权利要求1所述的输出内容保护方法，其特征在于，所述控制信息为条件接收系统的控制信息和/或数字版权保护系统的控制信息。

6.根据权利要求1～5任一项所述的输出内容保护方法，其特征在于，所述预设接口为USB接口。

7.一种条件接收模块，其特征在于，包括：

接口通讯模块，用于通过预设接口接收来自主机的数据并将所述数据根据类别发送至对应的各模块；接收来自所述各模块的信息并通过所述预设接口发送至主机；

身份校验模块，用于生成对身份标识进行数字签名的随机口令，并发送至所述主机，接收来自主机的主机身份标识并进行校验，将校验结果传递至解密模块，将条件接收模块的自身身份标识传递给所述接口通讯模块；

音视频输入模块，用于接收来自所述接口通讯模块发送的初始加密音视频数据，并将所述初始加密音视频数据发送至解密模块；

安全级别信息处理模块，用于接收来自所述接口通讯模块发送的主机支持的安全级别信息，并将所述主机支持的安全级别信息发送至解析模块；

控制信息处理模块，用于接收所述接口通讯模块发送的初始加密音视频数据对应的控制信息，并将其发送至解析模块；

密钥生成模块，用于与主机共同确定加密音视频数据的目标密钥，将所述目标密钥传递至加密模块；

解析模块，用于解析所述主机支持的安全级别信息，将解析结果发送至解密模块，解析

初始加密音视频数据对应的控制信息，提取出解密所需密钥和内容保护级别信息，将所述解密所需密钥和内容保护级别信息发送至解密模块；

解密模块，用于判断所述主机支持的安全级别信息是否高于所述内容保护级别信息，如果是则根据所述控制信息对所述初始加密音视频数据进行解密，得到目标音视频数据，并将所述内容保护级别信息传递至加密模块；

加密模块，用于根据所述解密模块发送的内容保护级别信息判断是否需要对所述目标音视频数据进行再加密，若需要，则对所述目标音视频数据根据所述目标音视频数据再次进行加密，并将再加密后的目标音视频数据传递至所述音视频输出模块；

音视频输出模块，用于将接收到的再加密后的目标音视频数据输出至所述接口通讯模块。

8.根据权利要求7所述的条件接收模块，其特征在于，所述控制信息为条件接收系统的控制信息和/或数字版权保护系统的控制信息。

9.根据权利要求8所述的条件解析模块，其特征在于，所述解析模块包括：

CAS模块，用于解析条件接收系统控制信息，提取出解密所需密钥和内容保护级别信息，将所述解密所需密钥和内容保护级别信息发送至解密模块；

DRM模块，用于解析数字版权保护系统控制信息，提取出解密所需密钥和内容保护级别信息，将所述解密所需密钥和内容保护级别信息发送至解密模块。

10.根据权利要求7～9任一项所述的条件接收模块，其特征在于，所述预设接口为USB接口。

一种输出内容保护方法与条件接收模块

技术领域

[0001] 本发明涉及广播电视领域，特别是涉及一种输出内容保护方法与条件接收模块。

背景技术

[0002] 在广播电视领域，通常使用独立于主机的条件接收模块来解扰由条件接收系统或者数字版权保护系统控制的数字电视节目。CAM为条件接收模块，通过某种物理接口和主机相连接；接收来自主机的数据，其中包括音视频数据和其它控制信息；对音视频数据进行解密；将音视频数据和其它控制信息传回到主机；主机通过调谐器接收来自广播网络的数据，或者通过网卡接收来自因特网的数据；通过某种物理接口将数据发送到条件接收模块，并通过该物理接口接收来自条件接收模块的数据。

[0003] 目前大多数条件接收模块采用的物理接口是PCMCIA，遵循DVB-CI或者CI Plus标准，CI Plus定义了一种针对于PCMCIA条件接收模块的二次保护方案，条件接收模块使用AES对TS流进行加密后再输出到主机，但这种接口增加了主机的制造成本，同时增大了产品尺寸。存在一些条件接收模块采用USB通用串行接口作为物理接口，但这种条件接收模块对数字电视解密后直接通过USB传回到主机，第三方设备很容易将音视频内容获取并分发到未授权用户，安全性低。

发明内容

[0004] 有鉴于此，本发明的主要目的在于提供一种输出内容保护方法与条件接收模块，可以对输出内容增加保护，避免输出内容被窃取。

[0005] 为实现上述目的，本发明提供了一种输出内容保护方法，应用于条件接收模块，所述方法包括：

[0006] 生成对身份标识进行数字签名的随机口令，并发送至所述主机，接收主机发送的主机身份标识，校验所述主机身份标识是否合法，如果合法，则向所述主机发送自身身份标识；

[0007] 当确定所述主机校验所述条件接收模块的自身身份标识合法时，与主机共同确定加密音视频数据的目标密钥；

[0008] 接收主机发送的初始加密音视频数据、对应的控制信息以及主机支持的安全级别信息，根据所述控制信息获取所述目标音视频数据内容保护级别信息，判断所述主机支持的安全级别信息是否高于所述内容保护级别信息，如果是则根据所述控制信息对所述初始加密音视频数据进行解密，得到目标音视频数据；

[0009] 根据所述内容保护级别信息判断是否需要对所述目标音视频数据进行再加密，若需要，则对所述目标音视频数据根据所述目标密钥再次进行加密；

[0010] 将再加密后的目标音视频数据通过预设接口发送至主机。

[0011] 优选地，对所述目标音视频数据根据所述目标密钥再次进行加密后还包括：

[0012] 为根据所述目标密钥再次进行加密后的目标音视频数据设置相应的加密标志。

[0013] 优选地，对所述初始加密信息进行解密，得到目标音视频数据与对应的控制信息后还包括：

[0014] 判断所述目标密钥的生成时间是否超过预设周期，若超过则对所述目标密钥进行更新。

[0015] 优选地，所述目标密钥为对称密钥。

[0016] 优选地，所述控制信息为条件接收系统的控制信息和/或数字版权保护系统的控制信息。

[0017] 优选地，所述预设接口为USB接口。

[0018] 本发明还提供了一种条件接收模块，包括：

[0019] 接口通讯模块，用于通过预设接口接收来自主机的数据并将所述数据根据类别发送至对应的各模块；接收来自所述各模块的信息并通过所述预设接口发送至主机；

[0020] 身份校验模块，用于生成对身份标识进行数字签名的随机口令，并发送至所述主机，接收来自主机的主机身份标识并进行校验，将校验结果传递至解密模块，将条件接收模块的自身身份标识传递给所述接口通讯模块；

[0021] 音视频输入模块，用于接收来自所述接口通讯模块发送的初始加密音视频数据，并将所述初始加密音视频数据发送至解密模块；

[0022] 安全级别信息处理模块，用于接收来自所述接口通讯模块发送的主机支持的安全级别信息，并将所述主机支持的安全级别信息发送至解析模块；

[0023] 控制信息处理模块，用于接收所述接口通讯模块发送的初始加密音视频数据对应的控制信息，并将其发送至解析模块；

[0024] 密钥生成模块，用于与主机共同确定加密音视频数据的目标密钥，将所述目标密钥传递至加密模块；

[0025] 解析模块，用于解析所述主机支持的安全级别信息，将解析结果发送至解密模块，解析初始加密音视频数据对应的控制信息，提取出解密所需密钥和内容保护级别信息，将所述解密所需密钥和内容保护级别信息发送至解密模块；

[0026] 解密模块，用于判断所述主机支持的安全级别信息是否高于所述内容保护级别信息，如果是则根据所述控制信息对所述初始加密音视频数据进行解密，得到目标音视频数据，并将所述内容保护级别信息传递至加密模块；

[0027] 加密模块，用于根据所述解密模块发送的内容保护级别信息判断是否需要对所述目标音视频数据进行再加密，若需要，则对所述目标音视频数据根据所述目标音视频数据再次进行加密，并将再加密后的目标音视频数据传递至所述音视频输出模块；

[0028] 音视频输出模块，用于将接收到的再加密后的目标音视频数据输出至所述接口通讯模块。

[0029] 优选地，所述控制信息为条件接收系统的控制信息和/或数字版权保护系统的控制信息。

[0030] 优选地，所述解析模块包括：

[0031] CAS模块，用于解析条件接收系统控制信息，提取出解密所需密钥和内容保护级别信息，将所述解密所需密钥和内容保护级别信息发送至解密模块；

[0032] DRM模块，用于解析数字版权保护系统控制信息，提取出解密所需密钥和内容保护

级别信息，将所述解密所需密钥和内容保护级别信息发送至解密模块。

[0033] 优选地，所述预设接口为USB接口。

[0034] 应用本发明提供的一种输出内容保护方法与条件接收模块，接收主机发送的主机身份标识，校验所述主机身份标识是否合法，如果合法，则向所述主机发送自身身份标识；当确定所述主机校验所述条件接收模块的自身身份标识合法时，与主机共同确定一个加密音视频数据的目标密钥；接收主机发送的初始加密音视频数据与对应的控制信息，根据所述控制信息对所述初始加密音视频数据进行解密，得到目标音视频数据；根据所述控制信息获取所述目标音视频数据内容保护级别信息，根据所述内容保护级别信息判断是否需要对所述目标音视频数据进行再加密，若需要，则对所述目标音视频数据根据所述目标密钥再次进行加密，并将再加密后的目标音视频数据通过预设接口发送至主机，可以根据解密后的目标音视频数据的控制信息获取内容保护级别信息，根据内容保护级别信息需要加密的输出内容进行再加密，可以对输出内容实现保护，避免非法设备窃取到解密后的内容。

附图说明

[0035] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据提供的附图获得其他的附图。

[0036] 图1为本发明一种输出内容保护方法实施例的流程图；

[0037] 图2为本发明一种输出内容保护方法实施例实施的架构图；

[0038] 图3为本发明一种条件接收模块实施例的结构示意图；

[0039] 图4为本发明一种条件接收模块实施例的又一结构示意图。

具体实施方式

[0040] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0041] 本发明提供了一种输出内容保护方法，应用于条件接收模块，图1示出了本发明输出内容保护方法实施例一的流程图，包括：

[0042] 步骤S101：生成对身份标识进行数字签名的随机口令，并发送至所述主机，接收主机发送的主机身份标识，校验所述主机身份标识是否合法，如果合法，则向所述主机发送自身身份标识；

[0043] 主机向条件接收模块发送自己的身份标识，条件接收模块检查主机的身份标识是否合法，如果合法，条件接收模块向主机发送自己的身份标识，否则条件接收模块停止处理来自主机的加密音视频流。所述主机身份标识和所述条件接收模块的身份标识以数字签名的形式进行保护，条件接收模块每次接收所述主机身份标识前产生一个随机口令并发送到所述主机，用于对所述主机身份标识和所述条件接收模块的身份标识进行数字签名。

[0044] 步骤S102：当确定所述主机校验所述条件接收模块的自身身份标识合法时，与主

机共同确定一个加密音视频数据的目标密钥；

[0045] 主机检查条件接收模块的身份标识符，如果合法则进入下一处理步骤，否则停止向条件接收模块发送加密音视频流。身份标识通常由第三方信任机构颁布并内嵌于设备中，可以采用X509证书实现，当确定所述主机校验所述条件接收模块的自身身份标识合法时，条件接收模块和主机协商生成加密音视频数据的密钥，通常使用对称密钥，可以使用例如Diffie-Hellman密钥交换协议或者其它变种形式。

[0046] 步骤S103：接收主机发送的初始加密音视频数据、对应的控制信息以及主机支持的安全级别信息，根据所述控制信息获取所述目标音视频数据内容保护级别信息，判断所述主机支持的安全级别信息是否高于所述内容保护级别信息，如果是则根据所述控制信息对所述初始加密音视频数据进行解密，得到目标音视频数据；

[0047] 主机将加密音视频数据发送到条件接收模块，同时将其它一些和条件接收系统或者数字版权保护系统相关的控制信息也发送到条件接收模块，另外通过可信通道发送主机所主机支持的安全级别信息。条件接收模块根据所述主机支持的安全级别信息决定是否对所述目标音视频数据进行解密，提取出条件接收系统或者数字版权保护系统的控制信息，根据所述控制信息获取所述目标音视频数据内容保护级别信息，判断所述主机支持的安全级别信息是否高于所述内容保护级别信息，如果是则根据所述控制信息对所述初始加密音视频数据进行解密，得到目标音视频数据。

[0048] 步骤S104：根据所述内容保护级别信息判断是否需要对所述目标音视频数据进行再加密，若需要，则对所述目标音视频数据根据所述目标密钥再次进行加密；

[0049] 根据目标音视频数据的内容保护级别信息决定对数据是否实现保护。如果属于高价值数据，则使用和主机协商好的密钥对音视频数据进行再加密，同时设置相应加密标志。

[0050] 步骤S105：将再加密后的目标音视频数据通过预设接口发送至主机。

[0051] 将进行再加密并设置加密标志后的目标音视频数据通过预设接口，如USB接口回传到主机。使用USB作为物理接口，可减少主机所需的硬件部件，主机无需实现PCMCIA通讯功能，可以复用现有的USB通讯功能，降低了主机成本，且可以减少条件接收模块尺寸，降低成本，有利于用户接受。也可使用其他接口，包括无线或有线连接方式。主机接收到音视频数据后检查其中的加密标志，如果其表示数据被条件接收模块加密，则使用协商的密钥对数据进行解密。

[0052] 本实施例实施的实施方式如图2所示，条件接收模块以USB条件接收模块为例数据源用于提供未加密的音视频流；

[0053] 条件接收系统用于对音视频流进行加密，并加上条件接收信息；数字版权保护系统用于对音视频流进行加密，并加上数字版权信息；前端用于对加密的音视频流进行调制复用；流服务器用于负责向主机传输加密后的音视频流；广播网络用于传输来自前端的数据；因特网用于传输来自流服务器的数据；主机用于接收来自广播网络或者因特网的音视频数据，并与USB条件接收模块协同处理这些数据；USB条件接收模块用于对音视频数据进行解密并根据数据价值实行不同级别的保护。

[0054] 应用本实施例提供的一种输出内容保护方法，条件接收模块在通过USB将音视频内容返回到主机前，对其进行再次加密，主机在接收到音视频内容后，对内容解密后再输出到显示设备。条件接收模块和主机之间进行设备认证，避免非法设备获取到内容。条件接收

模块和主机使用对称密钥协商协议生成相同密钥。条件接收模块和主机定期对密钥进行刷新。条件接收模块根据音视频内容价值对其进行不同级别的保护。

[0055] 本发明还提供了一种条件接收模块，图3示出了本发明条件接收模块实施例的结构示意图，包括：

[0056] 接口通讯模块101，用于通过预设接口接收来自主机的数据并将所述数据根据类别发送至对应的各模块；接收来自所述各模块的信息并通过所述预设接口发送至主机；

[0057] 所述预设接口可为USB接口，也可使用其他接口，包括无线或有线连接方式。

[0058] 身份校验模块102，用于生成对身份标识进行数字签名的随机口令，并发送至所述主机，接收来自主机的主机身份标识并进行校验，将校验结果传递至解密模块，将条件接收模块的自身身份标识传递给所述接口通讯模块；

[0059] 音视频输入模块103，用于接收来自所述接口通讯模块发送的初始加密音视频数据，并将所述初始加密音视频数据发送至解密模块；

[0060] 安全级别信息处理模块104，用于接收来自所述接口通讯模块发送的主机支持的安全级别信息，并将所述主机支持的安全级别信息发送至解析模块；

[0061] 控制信息处理模块105，用于接收所述接口通讯模块发送的初始加密音视频数据对应的控制信息，并将其发送至解析模块；

[0062] 密钥生成模块106，用于与主机共同确定加密音视频数据的目标密钥，将所述目标密钥传递至加密模块；

[0063] 密钥生成模块也可将协商所需信息传递到接口通讯模块，周期性刷新加密密钥。

[0064] 解析模块107，用于解析所述主机支持的安全级别信息，将解析结果发送至解密模块，解析初始加密音视频数据对应的控制信息，提取出解密所需密钥和内容保护级别信息，将所述解密所需密钥和内容保护级别信息发送至解密模块；

[0065] 所述控制信息为条件接收系统的控制信息和/或数字版权保护系统的控制信息。

[0066] 所述解析模块包括：

[0067] CAS模块，用于解析条件接收系统控制信息，提取出解密所需密钥和内容保护级别信息，将所述解密所需密钥和内容保护级别信息发送至解密模块；

[0068] CAS:Conditional Access System，广播电视领域中对数字电视内容进行保护，防止盗版的系统。

[0069] DRM模块，用于解析数字版权保护系统控制信息，提取出解密所需密钥和内容保护级别信息，将所述解密所需密钥和内容保护级别信息发送至解密模块。

[0070] DRM:Digital Right Management，数字版权保护系统，通常应用于因特网的流服务领域，对音视频内容进行加密和授权控制。

[0071] 解密模块108，用于判断所述主机支持的安全级别信息是否高于所述内容保护级别信息，如果是则根据所述控制信息对所述初始加密音视频数据进行解密，得到目标音视频数据，并将所述内容保护级别信息传递至加密模块；

[0072] 加密模块109，用于根据所述解密模块发送的内容保护级别信息判断是否需要对所述目标音视频数据进行再加密，若需要，则对所述目标音视频数据根据所述目标音视频数据再次进行加密，并将再加密后的目标音视频数据传递至所述音视频输出模块；

[0073] 音视频输出模块110，用于将接收到的再加密后的目标音视频数据输出至所述接

口通讯模块。

[0074] 图4示出了本实施例中预设接口为USB的USB条件接收模块的结构示意图，使用USB作为物理接口，减少了主机所需的硬件部件，主机无需实现PCMCIA通讯功能，可以复用现有的USB通讯功能，降低了主机成本，且减少了条件接收模块尺寸，降低成本，有利于用户接受，加密模块对输出内容实现了保护，避免了非法设备窃取解密后内容，密钥生成模块周期性刷新密钥，增加了安全性。

[0075] 需要说明的是，本说明书中的各个实施例均采用递进的方式描述，每个实施例重点说明的都是与其他实施例的不同之处，各个实施例之间相同相似的部分互相参见即可。对于系统类实施例而言，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。

[0076] 最后，还需要说明的是，在本文中，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、物品或者设备中还存在另外的相同要素。

[0077] 以上对本发明所提供的输出内容保护方法与条件接收模块进行了详细介绍，本文中应用了具体个例对本发明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发明的方法及其核心思想；同时，对于本领域的一般技术人员，依据本发明的思想，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发明的限制。

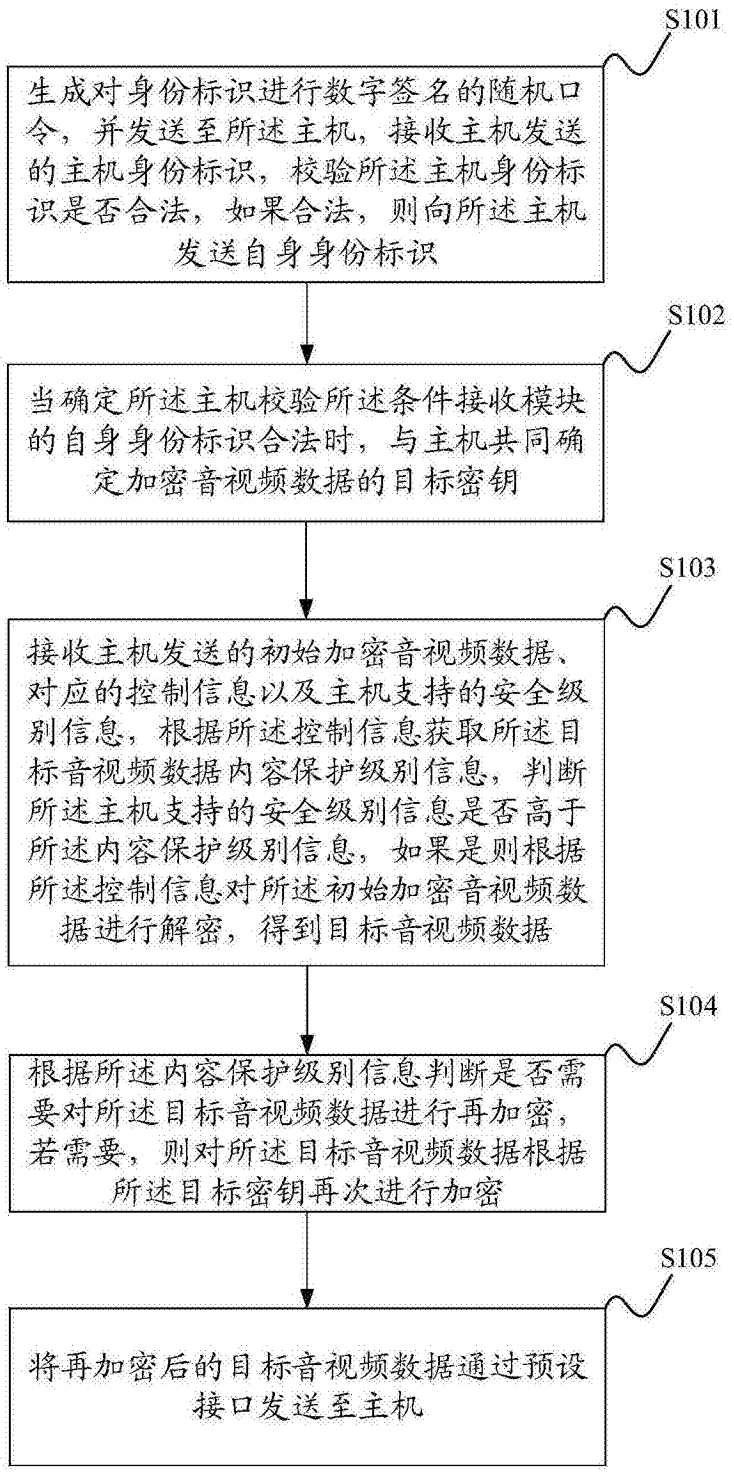

S101
生成对身份标识进行数字签名的随机口令，并发送至所述主机，接收主机发送的主机身份标识，校验所述主机身份标识是否合法，如果合法，则向所述主机发送自身身份标识
S102
当确定所述主机校验所述条件接收模块的自身身份标识合法时，与主机共同确定加密音视频数据的目标密钥
S103
接收主机发送的初始加密音视频数据、对应的控制信息以及主机支持的安全级别信息，根据所述控制信息获取所述目标音视频数据内容保护级别信息，判断所述主机支持的安全级别信息是否高于所述内容保护级别信息，如果是则根据所述控制信息对所述初始加密音视频数据进行解密，得到目标音视频数据
S104
根据所述内容保护级别信息判断是否需要对所述目标音视频数据进行再加密，若需要，则对所述目标音视频数据根据所述目标密钥再次进行加密
S105
将再加密后的目标音视频数据通过预设接口发送至主机

图1

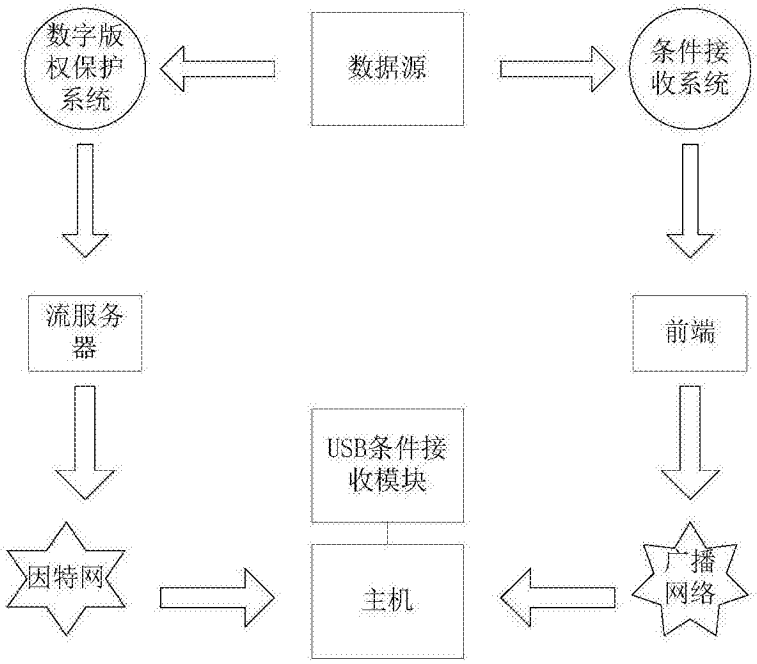

数字版权保护系统
数据源
条件接收系统
流服务器
前端
USB条件接收模块
因特网
主机
广播网络

图2

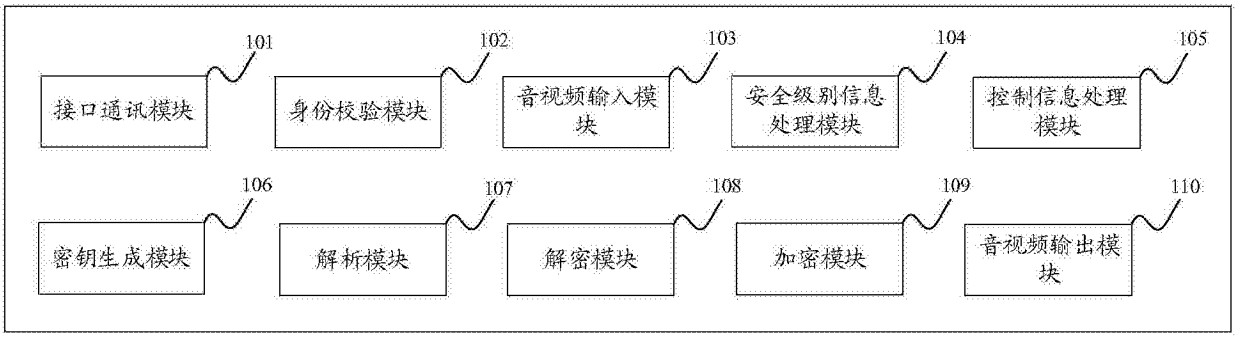

101
接口通讯模块
102
身份校验模块
103
音视频输入模块
104
安全级别信息处理模块
105
控制信息处理模块
106
密钥生成模块
107
解析模块
108
解密模块
109
加密模块
110
音视频输出模块

图3

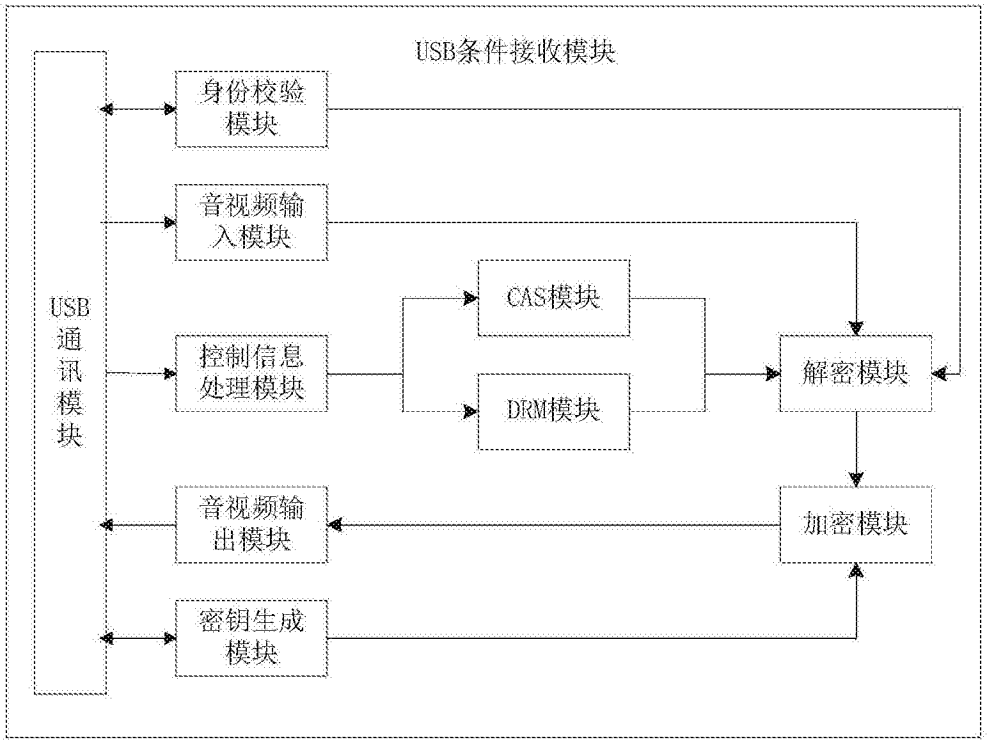

USB条件接收模块
身份校验模块
音视频输入模块
USB通讯模块
控制信息处理模块
CAS模块
DRM模块
解密模块
音视频输出模块
加密模块
密钥生成模块

图4