(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 115955310 B
(45)授权公告日 2023.06.27

(21)申请号 202310239500.X

(22)申请日 2023.03.07

(65)同一申请的已公布的文献号
申请公布号 CN 115955310 A

(43)申请公布日 2023.04.11

(73)专利权人 杭州海康威视数字技术股份有限公司
地址 310051 浙江省杭州市滨江区阡陌路555号

(72)发明人 王滨 傅彩利 方璐 王国云 韩忠昕

(74)专利代理机构 北京博思佳知识产权代理有限公司 11415
专利代理师 杨春香

(51)Int.Cl.
H04L 9/08(2006.01)
H04L 9/32(2006.01)
H04L 9/16(2006.01)

(56)对比文件
CN 113132099 A,2021.07.16

审查员 朱星杰

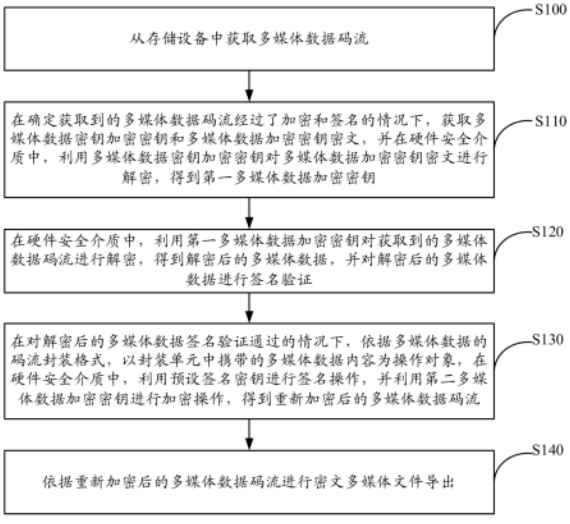
权利要求书2页 说明书12页 附图4页

(54)发明名称

信源加密多媒体数据导出安全保护方法、装置及设备

(57)摘要

本申请提供一种信源加密多媒体数据导出安全保护方法、装置及设备，该方法包括：在确定获取到的多媒体数据码流经过了加密和签名的情况下，在硬件安全介质中，利用多媒体数据密钥加密密钥对多媒体数据加密密钥密文进行解密，利用得到的第一多媒体数据加密密钥对获取到的多媒体数据码流进行解密，并对解密后的多媒体数据进行签名验证；在对解密后的多媒体数据签名验证通过的情况下，以封装单元中携带的多媒体数据内容为操作对象，在硬件安全介质中，利用预设签名密钥进行签名操作，并利用第二多媒体数据加密密钥进行加密操作；依据重新加密后的多媒体数据码流进行密文多媒体文件导出。该方法可以提高多媒体数据的安全性。



CN 115955310 B

1.一种信源加密多媒体数据导出安全保护方法,其特征在于,包括:

从存储设备中获取多媒体数据码流;

在确定获取到的多媒体数据码流经过了加密和签名的情况下,获取多媒体数据密钥加密密钥和多媒体数据加密密钥密文,并在硬件安全介质中,利用所述多媒体数据密钥加密密钥对所述多媒体数据加密密钥密文进行解密,得到第一多媒体数据加密密钥;

在所述硬件安全介质中,利用所述第一多媒体数据加密密钥对获取到的多媒体数据码流进行解密,得到解密后的多媒体数据,并对解密后的多媒体数据进行签名验证;

在对解密后的多媒体数据签名验证通过的情况下,依据多媒体数据的码流封装格式,以封装单元中携带的多媒体数据内容为操作对象,在所述硬件安全介质中,利用预设签名密钥进行签名操作,并利用第二多媒体数据加密密钥进行加密操作,得到重新加密后的多媒体数据码流;其中,所述第二多媒体数据加密密钥由所述硬件安全介质实时生成;

依据所述重新加密后的多媒体数据码流进行密文多媒体文件导出;其中,在对密文多媒体文件进行解密播放的情况下,支持边解密验签边进行播放。

2.根据权利要求1所述的方法,其特征在于,所述多媒体数据码流采用安全编码格式进行编码,所述多媒体数据码流中包括安全编码参数,所述安全编码参数包括用于标识多媒体数据是否加密的加密标识符以及用于标识多媒体数据是否签名的签名标识符。

3.根据权利要求1所述的方法,其特征在于,所述获取多媒体数据密钥加密密钥,包括:

从获取到的多媒体数据码流中获取多媒体数据密钥加密密钥的索引信息;

依据所述多媒体数据密钥加密密钥的索引信息,从密钥管理系统中获取对应的多媒体数据密钥加密密钥密文;所述多媒体数据密钥加密密钥密文利用所述硬件安全介质的公钥加密得到;

在所述硬件安全介质中,利用所述硬件安全介质的私钥对所述多媒体数据密钥加密密钥密文进行解密,得到所述多媒体数据密钥加密密钥。

4.根据权利要求1所述的方法,其特征在于,所述预设签名密钥为所述硬件安全介质的私钥。

5.根据权利要求1-4任一项所述的方法,其特征在于,所述多媒体数据为视频数据,所述封装单元为实时传输协议RTP包。

6.一种信源加密多媒体数据导出安全保护装置,其特征在于,包括:

数据获取单元,用于从存储设备中获取多媒体数据码流;

安全处理单元,还用于在确定获取到的多媒体数据码流经过了加密和签名的情况下,获取多媒体数据密钥加密密钥和多媒体数据加密密钥密文,并在硬件安全介质中,利用所述多媒体数据密钥加密密钥对所述多媒体数据加密密钥密文进行解密,得到第一多媒体数据加密密钥;

所述安全处理单元,还用于在所述硬件安全介质中,利用所述第一多媒体数据加密密钥对获取到的多媒体数据码流进行解密,得到解密后的多媒体数据,并对解密后的多媒体数据进行签名验证;

所述安全处理单元,还用于在对解密后的多媒体数据签名验证通过的情况下,依据多媒体数据的码流封装格式,以封装单元中携带的多媒体数据内容为操作对象,在所述硬件安全介质中,利用预设签名密钥进行签名操作,并利用第二多媒体数据加密密钥进行加密

操作,得到重新加密后的多媒体数据码流;其中,所述第二多媒体数据加密密钥由所述硬件安全介质实时生成;

数据导出单元,用于依据所述重新加密后的多媒体数据码流进行密文多媒体文件导出;其中,在对密文多媒体文件进行解密播放的情况下,支持边解密验签边进行播放。

7.根据权利要求6所述的装置,其特征在于,所述多媒体数据码流采用安全编码格式进行编码,所述多媒体数据码流中包括安全编码参数,所述安全编码参数包括用于标识多媒体数据是否加密的加密标识符以及用于标识多媒体数据是否签名的签名标识符。

8.根据权利要求6所述的装置,其特征在于,所述安全处理单元获取多媒体数据密钥加密密钥,包括:

从获取到的多媒体数据码流中获取多媒体数据密钥加密密钥的索引信息;

依据所述多媒体数据密钥加密密钥的索引信息,从密钥管理系统中获取对应的多媒体数据密钥加密密钥密文;所述多媒体数据密钥加密密钥密文利用所述硬件安全介质的公钥加密得到;

在所述硬件安全介质中,利用所述硬件安全介质的私钥对所述多媒体数据密钥加密密钥密文进行解密,得到所述多媒体数据密钥加密密钥。

9.根据权利要求6所述的装置,其特征在于,所述预设签名密钥为所述硬件安全介质的私钥,和/或,所述多媒体数据为视频数据,所述封装单元为实时传输协议RTP包。

10.一种电子设备,其特征在于,包括处理器和存储器,其中,

存储器,用于存放计算机程序;

处理器,用于执行存储器上所存放的程序时,实现权利要求1-5任一项所述的方法。

信源加密多媒体数据导出安全保护方法、装置及设备

技术领域

[0001] 本申请涉及信息安全技术领域，尤其涉及一种信源加密多媒体数据导出安全保护方法、装置及设备。

背景技术

[0002] 信源加密是指从信息源头就开始对信息进行加密，以保证信息的机密性。此外，为了保证信息的完整性，还会通过签名的方式来保证信息完整。

[0003] 传统方案中，对于信源加密多媒体数据，在需要对其进行导出时，可以通过客户端从存储设备中获取信源加密多媒体数据，对其进行解密以及签名验证后导出，并在导出完成后对整个多媒体文件进行重新加密和签名，以保证多媒体数据的机密性和完整性。

[0004] 然而，上述过程中，信源加密多媒体数据导出过程中，在对整个多媒体文件进行加密之前，多媒体数据码流仍然是明文状态，存在信息泄露风险。此外，由于其采用对整个多媒体文件进行加密和签名的方式，在需要进行多媒体文件播放的情况下，需要在整个多媒体文件解密完成并验签通过的情况下，才能进行播放，导致多媒体数据播放的业务应用不顺畅。

发明内容

[0005] 有鉴于此，本申请提供一种信源加密多媒体数据导出安全保护方法、装置及设备。

[0006] 具体地，本申请是通过如下技术方案实现的：

[0007] 根据本申请实施例的第一方面，提供一种信源加密多媒体数据导出安全保护方法，包括：

[0008] 从存储设备中获取多媒体数据码流；

[0009] 在确定获取到的多媒体数据码流经过了加密和签名的情况下，获取多媒体数据密钥加密密钥和多媒体数据加密密钥密文，并在硬件安全介质中，利用所述多媒体数据密钥加密密钥对所述多媒体数据加密密钥密文进行解密，得到第一多媒体数据加密密钥；

[0010] 在所述硬件安全介质中，利用所述第一多媒体数据加密密钥对获取到的多媒体数据码流进行解密，得到解密后的多媒体数据，并对解密后的多媒体数据进行签名验证；

[0011] 在对解密后的多媒体数据签名验证通过的情况下，依据多媒体数据的码流封装格式，以封装单元中携带的多媒体数据内容为操作对象，在所述硬件安全介质中，利用预设签名密钥进行签名操作，并利用第二多媒体数据加密密钥进行加密操作，得到重新加密后的多媒体数据码流；

[0012] 依据所述重新加密后的多媒体数据码流进行密文多媒体文件导出。

[0013] 根据本申请实施例的第二方面，提供一种信源加密多媒体数据导出安全保护装置，包括：

[0014] 数据获取单元，用于从存储设备中获取多媒体数据码流；

[0015] 安全处理单元，还用于在确定获取到的多媒体数据码流经过了加密和签名的情况

下，获取多媒体数据密钥加密密钥和多媒体数据加密密钥密文，并在硬件安全介质中，利用所述多媒体数据密钥加密密钥对所述多媒体数据加密密钥密文进行解密，得到第一多媒体数据加密密钥；

[0016] 所述安全处理单元，还用于在所述硬件安全介质中，利用所述第一多媒体数据加密密钥对获取到的多媒体数据码流进行解密，得到解密后的多媒体数据，并对解密后的多媒体数据进行签名验证；

[0017] 所述安全处理单元，还用于在对解密后的多媒体数据签名验证通过的情况下，依据多媒体数据的码流封装格式，以封装单元中携带的多媒体数据内容为操作对象，在所述硬件安全介质中，利用预设签名密钥进行签名操作，并利用第二多媒体数据加密密钥进行加密操作，得到重新加密后的多媒体数据码流；

[0018] 数据导出单元，用于依据所述重新加密后的多媒体数据码流进行密文多媒体文件导出。

[0019] 根据本申请实施例的第三方面，提供一种电子设备，包括处理器和存储器，其中，

[0020] 存储器，用于存放计算机程序；

[0021] 处理器，用于执行存储器上所存放的程序时，实现第一方面提供方法。

[0022] 根据本申请实施例的第四方面，提供一种计算机程序产品，所述计算机程序产品内存储有计算机程序，当处理器执行该计算机程序时，促使处理器实现第一方面提供的方法。

[0023] 根据本申请实施例的第五方面，提供一种机器可读存储介质，所述机器可读存储介质存储有能够被处理器执行的机器可执行指令；其中，所述处理器用于执行所述机器可执行指令，以实现第一方面提供方法。

[0024] 本申请实施例的信源加密多媒体数据导出安全保护方法，对于从存储设备中获取到的多媒体数据码流，在确定获取到的多媒体数据码流经过了加密和签名的情况下，获取多媒体数据密钥加密密钥和多媒体数据加密密钥密文，并在硬件安全介质中，利用多媒体数据密钥加密密钥对多媒体数据加密密钥密文进行解密，得到第一多媒体数据加密密钥，以及，在硬件安全介质中，利用第一多媒体数据加密密钥对获取到的多媒体数据码流进行解密，得到解密后的多媒体数据，并对解密后的多媒体数据进行签名验证，通过在安全硬件介质中对多媒体数据加密密钥密文进行解密，并利用解密得到的第一多媒体数据加密密钥进行多媒体数据解密，降低了第一多媒体数据加密密钥泄露的概率，提高了第一多媒体加密密钥的安全性；在对解密后的多媒体数据签名验证通过的情况下，依据多媒体数据的码流封装格式，以封装单元中携带的多媒体数据内容为操作对象，在硬件安全介质中，利用预设签名密钥进行签名操作，并利用第二多媒体数据加密密钥进行加密操作，得到重新加密后的多媒体数据码流，通过以封装单元中携带的多媒体数据内容为操作对象进行签名和加密操作，提高了后续流程中对多媒体数据进行解密和签名验证的效率，为实现边解密验签边进行多媒体数据播放提供了技术支持；进而，依据重新加密后的多媒体数据码流进行密文多媒体文件导出，通过对加密后的多媒体数据码流进行导出的方式得到密文的多媒体文件，避免了多媒体数据导出过程中明文状态的多媒体数据泄露，提高了多媒体数据的安全性。

附图说明

[0025] 图1为本申请一示例性实施例示出的一种信源加密多媒体数据导出安全保护方法的流程示意图；

[0026] 图2为本申请一示例性实施例示出的一种信源加密视频码流下载和导出的示意图；

[0027] 图3A为本申请一示例性实施例示出的一种加密前的视频码流的示意图；

[0028] 图3B为本申请一示例性实施例示出的一种加密后的视频码流的示意图；

[0029] 图4为本申请一示例性实施例示出的一种信源加密多媒体数据导出安全保护方法的流程示意图；

[0030] 图5为本申请一示例性实施例示出的一种信源加密多媒体数据导出安全保护装置的结构示意图；

[0031] 图6为本申请一示例性实施例示出的一种电子设备的硬件结构示意图。

具体实施方式

[0032] 这里将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本申请相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本申请的一些方面相一致的装置和方法的例子。

[0033] 在本申请使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本申请。在本申请和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式，除非上下文清楚地表示其他含义。

[0034] 为了使本领域技术人员更好地理解本申请实施例提供的技术方案，并使本申请实施例的上述目的、特征和优点能够更加明显易懂，下面结合附图对本申请实施例中技术方案作进一步详细的说明。

[0035] 请参见图1，为本申请实施例提供的一种信源加密多媒体数据导出安全保护方法的流程示意图，如图1所示，该信源加密多媒体数据导出安全保护方法可以包括以下步骤：

[0036] 步骤S100、从存储设备中获取多媒体数据码流。

[0037] 示例性的，存储设备可以包括但不限于多媒体数据采集设备内部的存储卡或用于存储多媒体数据采集设备的多媒体数据的外部存储设备。

[0038] 示例性的，多媒体数据可以包括但不限于视频数据或音频数据等。

[0039] 例如，以多媒体数据为视频数据为例，对于视频采集设备(如摄像头或称为相机)的视频数据，可以依据预设录像计划，由视频管理平台从视频采集设备中获取实时视频数据，并按照录像计划，将获取到的相应录像数据存储到指定存储设备，生成录像数据。

[0040] 步骤S110、在确定获取到的多媒体数据码流经过了加密和签名的情况下，获取多媒体数据密钥加密密钥和多媒体数据加密密钥密文，并在硬件安全介质中，利用多媒体数据密钥加密密钥对多媒体数据加密密钥密文进行解密，得到第一多媒体数据加密密钥。

[0041] 步骤S120、在硬件安全介质中，利用第一多媒体数据加密密钥对获取到的多媒体数据码流进行解密，得到解密后的多媒体数据，并对解密后的多媒体数据进行签名验证。

[0042] 本申请实施例中，对于从存储设备中获取到的多媒体数据码流，可以确定获取到

的多媒体数据码流是否为经过加密和签名的多媒体数据码流。

[0043] 对于从存储设备中获取到的经过加密和签名的多媒体数据码流(可以称为内部加密的多媒体数据码流,即信源加密多媒体数据),为了保证内部密钥的安全性,在对获取到的多媒体数据码流进行导出的情况下,需要进行内部密钥和外部密钥的切换,即将多媒体数据码流利用内部密钥加密的多媒体数据码流切换为利用外部密钥加密的多媒体数据码流。

[0044] 相应地,在确定获取到的多媒体数据码流为经过了加密和签名的多媒体数据码流的情况下,需要对获取到的多媒体数据码流进行解密和签名验证。

[0045] 示例性的,为了保证多媒体数据加密密钥的安全性,在对加密后的多媒体数据进行解密的过程中,需要先获取多媒体数据加密密钥密文(即加密后的多媒体数据加密密钥),并在硬件安全介质,如Ukey(一种通过USB (通用串行总线接口)与计算机相连、具有密码验证功能、可靠高速的小型存储设备)中,利用多媒体数据密钥加密密钥(用于对多媒体数据加密密钥进行加解密的密钥)对多媒体数据加密密钥密文进行解密,得到多媒体数据加密密钥(即内部多媒体数据加密密钥,本文中称为第一多媒体数据加密密钥)。

[0046] 在得到第一多媒体数据加密密钥的情况下,为了保证多媒体数据的安全性,可以在硬件安全介质中,利用第一多媒体数据加密密钥对获取到的多媒体数据码流进行解密,得到解密后的多媒体数据,并对解密后的多媒体数据进行签名验证。

[0047] 在一个示例中,上述获取到的多媒体数据码流可以利用多媒体数据采集设备的私钥进行签名,相应地,在按照上述方式得到解密后的多媒体数据的情况下,可以利用多媒体数据采集设备的公钥对解密后的多媒体数据进行签名验证。

[0048] 需要说明的是,在本申请实施例中,对于获取到的多媒体数据码流为未经过加密和/或未经过签名的情况,其具体导出实现可以采用常规数据导出方案,本申请实施例对此不作限定。

[0049] 步骤S130、在对解密后的多媒体数据签名验证通过的情况下,依据多媒体数据的码流封装格式,以封装单元中携带的多媒体数据内容为操作对象,在硬件安全介质中,利用预设签名密钥进行签名操作,并利用第二多媒体数据加密密钥进行加密操作,得到重新加密后的多媒体数据码流。

[0050] 本申请实施例中,为了避免多媒体数据在导出过程中出现明文状态的数据泄露,在对多媒体数据进行导出之前,需要利用外部密钥对解密后的多媒体数据重新进行加密。

[0051] 此外,为了避免多媒体文件整体加密和签名导致的解密和签名验证效率过低,在进行多媒体数据导出的过程中,不再采用对整个多媒体文件进行签名和加密的方式,而是结合多媒体数据的码流封装格式,以封装单元中携带的多媒体数据内容为操作对象,对多媒体数据进行签名和加密。

[0052] 相应地,在对解密后的多媒体数据签名验证通过的情况下,依据多媒体数据的码流封装格式,以封装单元中携带的多媒体数据内容为操作对象,在硬件安全介质中,利用预设签名密钥进行签名操作,并利用外部多媒体数据加密密钥(本文中称为第二多媒体数据加密密钥)进行加密操作,得到重新加密后的多媒体数据码流。

[0053] 步骤S140、依据重新加密后的多媒体数据码流进行密文多媒体文件导出。

[0054] 本申请实施例中,在按照上述方式得到重新加密后的多媒体数据码流的情况下,

可以依据重新加密后的多媒体数据码流进行密文多媒体文件导出。

[0055] 示例性的，在多媒体文件导出完成的情况下，码流数据中不保存相关的密钥数据(包括视频加密密钥和验签密钥)，相关的密钥数据保存在硬件安全介质中，即外部密钥保存与码流数据密文分离，提高数据的安全性。在需要播放导出的密文多媒体文件的情况下，需要用到硬件安全介质中保存的相关密钥数据去解密、验签和播放。

[0056] 可见，在图1所示方法流程中，对于从存储设备中获取到的多媒体数据码流，在确定获取到的多媒体数据码流经过了加密和签名的情况下，获取多媒体数据密钥加密密钥和多媒体数据加密密钥密文，并在硬件安全介质中，利用多媒体数据密钥加密密钥对多媒体数据加密密钥密文进行解密，得到第一多媒体数据加密密钥，以及，在硬件安全介质中，利用第一多媒体数据加密密钥对获取到的多媒体数据码流进行解密，得到解密后的多媒体数据，并对解密后的多媒体数据进行签名验证，通过在安全硬件介质中对多媒体数据加密密钥密文进行解密，并利用解密得到的第一多媒体数据加密密钥进行多媒体数据解密，降低了第一多媒体数据加密密钥泄露的概率，提高了第一多媒体加密密钥的安全性；在对解密后的多媒体数据签名验证通过的情况下，依据多媒体数据的码流封装格式，以封装单元中携带的多媒体数据内容为操作对象，在硬件安全介质中，利用预设签名密钥进行签名操作，并利用第二多媒体数据加密密钥进行加密操作，得到重新加密后的多媒体数据码流，通过以封装单元中携带的多媒体数据内容为操作对象进行签名和加密操作，提高了后续流程中对多媒体数据进行解密和签名验证的效率，为实现边解密验签边进行多媒体数据播放提供了技术支持；进而，依据重新加密后的多媒体数据码流进行密文多媒体文件导出，通过对加密后的多媒体数据码流进行导出的方式得到密文的多媒体文件，避免了多媒体数据导出过程中明文状态的多媒体数据泄露，提高了多媒体数据的安全性。

[0057] 在一些实施例中，多媒体数据码流采用安全编码格式进行编码，多媒体数据码流中包括安全编码参数，安全编码参数包括用于标识多媒体数据是否加密的加密标识符以及用于标识多媒体数据是否签名的签名标识符。

[0058] 示例性的，为了更好地适配以封装单元中携带的多媒体数据内容为操作对象的加密和签名，提高数据加密和签名状态的确定效率，在多媒体数据进行码流编码的过程中，可以采用安全编码格式进行编码。

[0059] 示例性的，安全编码格式编码的多媒体数据码流中可以包括安全编码参数。该安全编码参数可以包括但不限于用于标识多媒体数据是否加密的加密标识符以及用于标识多媒体数据是否签名的签名标识符。

[0060] 举例来说，以多媒体数据为视频数据为例，对于采用RTP(Real-time Transport Protocol，实时传输协议)协议封装的视频码流，每一个RTP包(即一个封装单元为一个RTP包)中均可以携带有上述安全编码参数，可以依据RTP包中携带的安全编码参数确定该RTP包中携带的视频数据是否加密以及是否签名。

[0061] 在一些实施例中，上述获取多媒体数据密钥加密密钥，可以包括：

[0062] 从获取到的多媒体数据码流中获取多媒体数据密钥加密密钥的索引信息；

[0063] 依据多媒体数据密钥加密密钥的索引信息，从密钥管理系统中获取对应的多媒体数据密钥加密密钥密文；多媒体数据密钥加密密钥密文利用硬件安全介质的公钥加密得到；

[0064] 在硬件安全介质中，利用硬件安全介质的私钥对多媒体数据密钥加密密钥密文进行解密，得到多媒体数据密钥加密密钥。

[0065] 示例性的，为了实现对多媒体数据加密密钥密文的解密，可以获取多媒体数据密钥加密密钥的索引信息，以便依据多媒体数据密钥加密密钥的索引信息获取用于对多媒体数据加密密钥密文进行解密的多媒体数据密钥加密密钥。

[0066] 示例性的，多媒体数据密钥加密密钥的索引信息可以携带在多媒体数据码流中，可以通过从多媒体数据码流中获取多媒体数据密钥加密密钥索引信息。

[0067] 例如，多媒体数据密钥加密密钥索引信息可以包括在上述安全编码参数中。

[0068] 为了提高多媒体数据密钥加密密钥的安全性，从而进一步提高多媒体数据加密密钥的安全性，依据多媒体数据密钥加密密钥的索引获取到的多媒体数据密钥加密密钥可以为多媒体数据密钥加密密钥密文(即加密后的多媒体数据密钥加密密钥)。

[0069] 示例性的，多媒体数据密钥加密密钥密文可以利用硬件安全介质的公钥加密得到。

[0070] 例如，在依据多媒体数据密钥加密密钥的索引信息从密钥管理系统中获取多媒体数据密钥加密密钥的情况下，可以在获取请求中携带硬件安全介质的标识信息；密钥管理系统接收到该获取请求的情况下，可以依据多媒体数据密钥加密密钥的索引信息查询到对应的多媒体数据密钥加密密钥，并依据硬件安全介质查询到对应的硬件安全介质的公钥，并利用该硬件安全介质的公钥对查询到的多媒体数据密钥加密密钥进行加密，得到多媒体数据密钥加密密钥密文。

[0071] 其中，硬件安全介质在使用之前，均可以将公钥发送给密钥管理系统，由密钥管理系统对硬件安全介质的公钥进行维护。

[0072] 相应地，在获取到多媒体数据密钥加密密钥密文的情况下，可以在硬件安全介质中，利用硬件安全介质的私钥对多媒体数据密钥加密密钥密文进行解密，得到多媒体数据密钥加密密钥，进而，可以在硬件安全介质中，利用多媒体数据密钥加密密钥，对多媒体数据加密密钥密文进行解密，得到多媒体数据加密密钥。

[0073] 为了使本领域技术人员更好地理解本申请实施例提供的技术方案，下面结合具体实例对本申请实施例提供的技术方案进行说明。

[0074] 在该实施例中，以上述多媒体数据为视频数据为例。

[0075] 在该实施例中，基于信源加密视频监控系统，结合码流封装格式和编码格式的技术，在视频导出过程及导出后，对视频码流数据进行全过程的机密性和完整性保护。同时也对信源加密视频监控系统中，码流全密态应用场景的补充，在方便用户导出视频文件播放的同时，也能对导出的视频文件做全过程的机密性和完整性的保护，防止视频信息的泄露。

[0076] 可见，本申请实施例提供的方案可以实现基于全密态的视频监控系统的码流导出。

[0077] 示例性的，全密态指的是，码流从相机出来，到传输，到存储，全是密文状态的，直到播放的时候才去解密。其中，系统中密态的码流被异常截获，是无法解密的，因为密钥在密钥管理系统(如视频密钥管理中心)内部管理，且需要合法认证授权才能获取授权对象公钥加密的密钥。因此，上述方案中用于对码流进行加密的密钥可以包括系统内部密钥(如上述第一多媒体数据加密密钥)和导出视频使用的系统外部密钥(如上述第二多媒体数据加

密密钥)。因为根据全密态的监控系统的设计,系统的内部密钥是无法获取明文态的,只会保存在经过相关认证机构认证的密码硬件里面,所以当导出码流文件的时候,无法继续使用原来的系统内部密钥,需要使用系统的外部密钥。

[0078] 可见,本申请实施例中要求视频文件导出后,可以适应码流文件被拷贝到另外的PC环境播放使用的常规场景,又能够使用相关认证机构推荐的密码算法和通过相关认证机构认证的密码硬件来保护被导出的码流文件。

[0079] 为了使本领域技术人员更好地理解在全密态的视频监控系统内部,如何实现对视频文件导出的安全性,下面对本申请实施例中信源视频导出安全保护的实现流程进行说明。

[0080] 如图2所示,信源加密的视频监控系统的客户端对码流进行下载操作,密文码流会从存储设备给到客户端,客户端可以根据码流的封装结构,对接收到的密文视频码流进行解析,识别是否经过加密以及签名。

[0081] 在码流经过了加密和签名的情况下,可以根据设计的安全编码格式,进行解析,得到加密和签名的相关参数,其可以包括但不限于:视频密钥加密密钥的索引、视频加密密钥的密文、加密算法、签名算法、算法对应的IV值等信息。

[0082] 客户端可以根据对获取到的密文码流进行解密和验签(即签名验证)操作,在解密成功,且验签通过的情况下,利用安全硬件设备(也可以称为智能密码钥匙,如Ukey)的私钥对解密后的视频数据进行签名操作,同时利用智能密码钥匙生成的新的视频加密密钥对解密后的视频数据重新进行加密操作,该过程同样需要符合设计的安全编码格式。然后根据实际的配置重新组装码流的封装及编码格式,保存密文视频文件。在外部播放该密文视频文件的时候,需要根据设计的安全编码格式解析密文码流的结构,然后进行解密播放。

[0083] 在该实施例中,在对视频码流进行签名和加密的过程中,可以依据视频数据的码流封装格式,以封装单元中携带的视频内容为操作对象。

[0084] 示例性的,在以RTP协议进行视频码流封装的情况下,封装单元可以为RTP包。

[0085] 示例性的,加密前后的视频码流可以分别如图3A和图3B所示。

[0086] 如图3A和图3B所示,在RTP封装NAL 时加密,加密内容为NAL数据。在不加密情况下,RTP打包器将NAL数据打包进RTP的负载。在加密的情况下,NAL和RTP之间根据安全编码格式添加安全编码层(可以称为视频数据安全编码层),该安全编码层中的安全编码数据可以包括但不限于协议头、加密标识符、签名标识符、密码算法信息、视频加密签名数据等。RTP打包器将安全编码数据打包到RTP中。

[0087] 示例性的,添加了安全编码层的RTP负载(即安全编码格式RTP负载)可以如表1所示。

表 1

[0088]

协议头 (4Byte)	加密标识符	签名标识符 (4bit)	长度 (3Byte)	编码参数 (1Byte)	填充 (3Byte)
加密签名参数结构 …					
签名数据(64Byte) …					
视频数据 …					

[0089] 其中,表1中各字段具体说明如下:

[0090] 协议头:长度为4字节(Byte),为视频安全编码包(即表1所示数据结构)的开始,值为0x00 00 00 01;

[0091] 加密标识符:长度为4位(bit),标识内容部分是否加密。例如,取值0x0表示内容部分未加密,取值0x1表示内容部分已加密;

[0092] 签名标识符:长度为4位,标识内容部分是否签名。例如,取值0x0表示内容部分未签名,取值0x1表示内容部分已签名;

[0093] 长度:长度为3字节,表示视频安全编码包的总长度(从表1中所示的协议头开始到视频数据结束的总长度);

[0094] 编码参数:长度为1字节,为NAL header的内容,包括1bit的禁止位、2bit的优先级以及5bit的NAL类型;

[0095] 填充:长度为3个字节,保证结构体对齐;

[0096] 加密签名参数:视频数据加密和签名参数集。在加密标识符的取值表示内容部分已加密,且签名标识符的取值表示内容部分已签名的情况下启用;

[0097] 签名数据:长度为64字节,视频数据明文的签名数据,使用加密签名参数中的签名算法和视频采集设备(可以称为相机设备)的私钥计算得到。在签名标识符的取值表示内容部分已签名的情况下启用;

[0098] 视频数据:在加密标识符取值表示内容部分已加密的情况下,为加密后的视频数据;在加密标识符取值表示内容部分未加密的情况下,为原始视频数据(未加密的视频数据)。

[0099] 示例性的,加密签名参数的结构可以如表2所示:

表 2

[0100]

设备 ID			VKEK 索引
VEK 密文			
加密签名算法	位移值	填充	IV 值

[0101] 其中,表2中各字段具体说明如下:

[0102] 设备ID :长度为32字节,本项描述了视频设备的ID,该ID作为视频监控系统中能唯一确认当前视频设备的标识符。

[0103] VKEK索引:长度为20字节,本项主要描述了视频密钥加密索引,该索引号在创建VKEK时生成,可以根据该索引号查询对应的VKEK。其中VKEK由视频密钥管理中心生成。

[0104] VEK密文:长度为32字节,本项主要描述了视频加密密钥的密文。

[0105] 加密签名算法:长度为2字节,本项主要描述了加密和签名算法。

[0106] 位移值:长度为1字节,本项为视频加密算法的位移值。

[0107] 填充:1字节用于对齐。

[0108] IV值:长度为16字节,本项为视频加密算法的IV值。

[0109] 在该实施例中,如图4所示,信源加密的视频监控系统的客户端处理逻辑流程可以包括:

[0110] 步骤1、在客户端开始导出信源加密视频数据,同时调用码流分析库回调函数的设置。

[0111] 步骤2、下载信令交互完成,客户端收到码流数据。

[0112] 步骤3、将码流传输给码流分析库。

[0113] 步骤4、码流分析库根据码流的信息,判断是否是信源加密的码流。

[0114] 示例性的,码流分析库可以通过解析视频数据封装协议的协议头(如RTPHeader)中的相关信息确定码流是否为信源加密的码流。

[0115] 步骤5、在码流为信源加密码流的情况下,则将以安全编码格式打包的码流,回调给客户端。

[0116] 示例性的,在确定码流为信源加密码流的情况下,可以将以安全编码格式打包的码流,例如,RTP包中的负载数据(按照上述安全编码格式进行编码),回调给客户端。

[0117] 步骤6、在安全编码格式内,找到具体的字段,判断安全编码格式的加密标识和签名标识是否开启。

[0118] 示例性的,加密标识符开启表明视频数据内容已加密,签名标识符开启表明视频数据内容已签名。

[0119] 步骤7、在加密标识符和签名标识符取值表示内容部分已加密和已签名的情况下,根据安全编码格式解析的规则,解析出VKEK(Video Key Encryption Key,视频密钥加密密钥)的索引(即视频密钥加密密钥索引)和VEK(Video Encryption Key,视频加密密钥)的密

文(即视频加密密钥密文),并根据VKEK的索引和VEK的密文用SM2国密算法解密出VEK(可以称为第一视频加密密钥)。

[0120] 需要说明的是,在本申请实施例中,加密标识符和签名标识符通常均开启或均不开启。在加密标识符和签名标识符均未开启,或,确定码流不属于信源加密码流的情况下,可以采用针对普通码流的导出加密方式进行处理,本申请实施例对此不做限定。

[0121] 步骤8、VEK作为对称密钥,用SM4国密算法解密视频数据以及利用相机设备的公钥对码流数据的进行SM2国密算法验签。

[0122] 步骤9、解密成功且验签通过的情况下,利用硬件安全介质的私钥对解密后的视频数据进行签名操作,同时利用硬件安全介质实时生成的视频加密密钥(可以称为第二视频加密密钥)对解密后的码流重新加密,并将加密后的视频数据返回给码流分析库。

[0123] 步骤10、码流分析库进行解析和打包,回调给客户端加密后的码流数据。

[0124] 步骤11、将回调给客户端的加密码流添加水印信息等信息,并保存文件(视频文件)。

[0125] 步骤12、在解密播放的情况下,将加密的码流文件路径传输给播放库,根据播放库的回调进行解密,然后将解密后的码流数据传输给播放库,进行边验签边解码播放。

[0126] 示例性的,在对视频文件进行播放的过程中,需要使用上述硬件安全介质中保存的第二视频加密密钥进行码流数据解密。

[0127] 例如,上述硬件安全介质为Ukey,在对视频文件进行播放的过程中,Ukey可以通过USB接口与视频播放设备连接,视频播放设备可以从Ukey中获取第二视频加密密钥,用于码流解密。

[0128] 可见,本申请实施例提供的技术方案可以在全密态的视频监控系统中,实现视频的正常导出,且能提高导出视频文件的安全性,同时利用设计的安全编码格式,实现边解密验签边播放的能力,提升用户体验。

[0129] 以上对本申请提供的方法进行了描述。下面对本申请提供的装置进行描述:

[0130] 请参见图5,为本申请实施例提供的一种信源加密多媒体数据导出安全保护装置的结构示意图,如图5所示,该信源加密多媒体数据导出安全保护装置可以包括:

[0131] 数据获取单元510,用于从存储设备中获取多媒体数据码流;

[0132] 安全处理单元520,还用于在确定获取到的多媒体数据码流经过了加密和签名的情况下,获取多媒体数据密钥加密密钥和多媒体数据加密密钥密文,并在硬件安全介质中,利用所述多媒体数据密钥加密密钥对所述多媒体数据加密密钥密文进行解密,得到第一多媒体数据加密密钥;

[0133] 所述安全处理单元520,还用于在所述硬件安全介质中,利用所述第一多媒体数据加密密钥对获取到的多媒体数据码流进行解密,得到解密后的多媒体数据,并对解密后的多媒体数据进行签名验证;

[0134] 所述安全处理单元520,还用于在对解密后的多媒体数据签名验证通过的情况下,依据多媒体数据的码流封装格式,以封装单元中携带的多媒体数据内容为操作对象,在所述硬件安全介质中,利用预设签名密钥进行签名操作,并利用第二多媒体数据加密密钥进行加密操作,得到重新加密后的多媒体数据码流;

[0135] 数据导出单元530,用于依据所述重新加密后的多媒体数据码流进行密文多媒体

文件导出。

[0136] 在一些实施例中,所述多媒体数据码流采用安全编码格式进行编码,所述多媒体数据码流中包括安全编码参数,所述安全编码参数包括用于标识多媒体数据是否加密的加密标识符以及用于标识多媒体数据是否签名的签名标识符。

[0137] 在一些实施例中,所述安全处理单元520获取多媒体数据密钥加密密钥,包括:

[0138] 从获取到的多媒体数据码流中获取多媒体数据密钥加密密钥的索引信息;

[0139] 依据所述多媒体数据密钥加密密钥的索引信息,从密钥管理系统中获取对应的多媒体数据密钥加密密钥密文;所述多媒体数据密钥加密密钥密文利用所述硬件安全介质的公钥加密得到;

[0140] 在所述硬件安全介质中,利用所述硬件安全介质的私钥对所述多媒体数据密钥加密密钥密文进行解密,得到所述多媒体数据密钥加密密钥。

[0141] 在一些实施例中,所述预设签名密钥为所述硬件安全介质的私钥,所述第二多媒体数据加密密钥由所述硬件安全介质实时生成。

[0142] 在一些实施例中,所述多媒体数据为视频数据,所述封装单元为实时传输协议RTP包。

[0143] 本申请实施例还提供一种电子设备,包括处理器和存储器,其中,存储器,用于存放计算机程序;处理器,用于执行存储器上所存放的程序时,实现上文描述的信源加密多媒体数据导出安全保护方法。

[0144] 请参见图6,为本申请实施例提供的一种电子设备的硬件结构示意图。该电子设备可包括处理器601、存储有机器可执行指令的存储器602。处理器601与存储器602可经由系统总线603通信。并且,通过读取并执行存储器602中与信源加密多媒体数据导出安全保护逻辑对应的机器可执行指令,处理器601可执行上文描述的信源加密多媒体数据导出安全保护方法。

[0145] 本文中提到的存储器602可以是任何电子、磁性、光学或其它物理存储装置,可以包含或存储信息,如可执行指令、数据,等等。例如,机器可读存储介质可以是:RAM(Radom Access Memory,随机存取存储器)、易失存储器、非易失性存储器、闪存、存储驱动器(如硬盘驱动器)、固态硬盘、任何类型的存储盘(如光盘、dvd等),或者类似的存储介质,或者它们的组合。

[0146] 在一些实施例中,还提供了一种机器可读存储介质,如图6中的存储器602,该机器可读存储介质内存储有机器可执行指令,所述机器可执行指令被处理器执行时实现上文描述的信源加密多媒体数据导出安全保护方法。例如,所述机器可读存储介质可以是ROM、RAM、CD-ROM、磁带、软盘和光数据存储设备等。

[0147] 本申请实施例还提供了一种计算机程序产品,存储有计算机程序,并且当处理器执行该计算机程序时,促使处理器执行上文中描述的信源加密多媒体数据导出安全保护方法。

[0148] 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。

[0149] 以上所述仅为本申请的较佳实施例而已，并不用以限制本申请，凡在本申请的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本申请保护的范围之内。

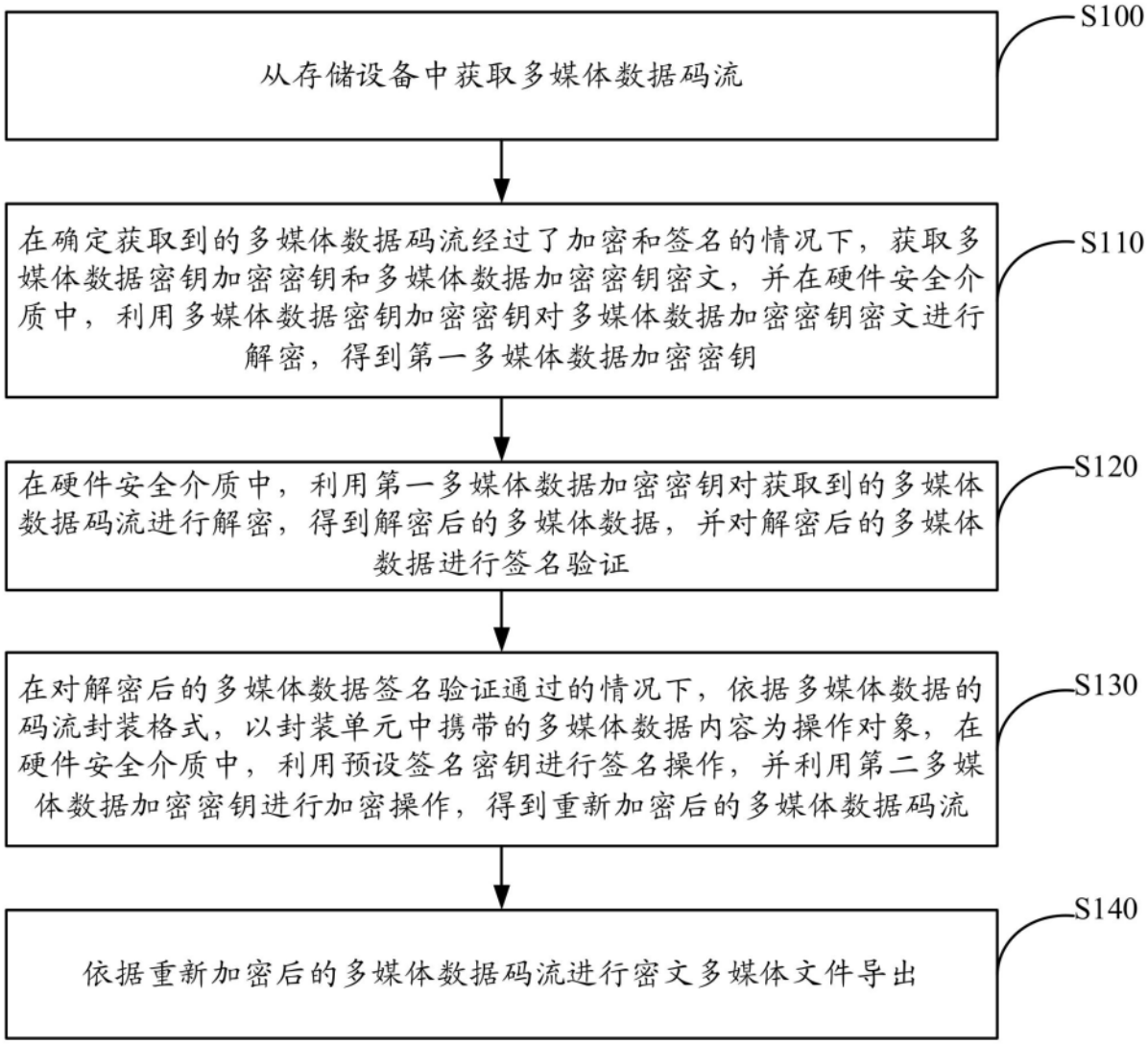

S100
从存储设备中获取多媒体数据码流
S110
在确定获取到的多媒体数据码流经过了加密和签名的情况下，获取多媒体数据密钥加密密钥和多媒体数据加密密钥密文，并在硬件安全介质中，利用多媒体数据密钥加密密钥对多媒体数据加密密钥密文进行解密，得到第一多媒体数据加密密钥
S120
在硬件安全介质中，利用第一多媒体数据加密密钥对获取到的多媒体数据码流进行解密，得到解密后的多媒体数据，并对解密后的多媒体数据进行签名验证
S130
在对解密后的多媒体数据签名验证通过的情况下，依据多媒体数据的码流封装格式，以封装单元中携带的多媒体数据内容为操作对象，在硬件安全介质中，利用预设签名密钥进行签名操作，并利用第二多媒体数据加密密钥进行加密操作，得到重新加密后的多媒体数据码流
S140
依据重新加密后的多媒体数据码流进行密文多媒体文件导出

图1

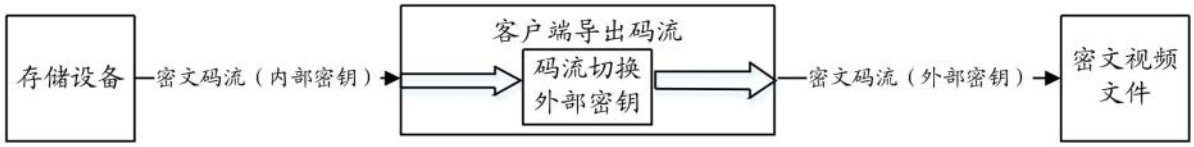

存储设备
密文码流（内部密钥）
客户端导出码流
码流切换
外部密钥
密文码流（外部密钥）
密文视频文件

图2


RTP Header
（RTP头部）
NAL
RTP Header
NAL
· · ·

图3A

图3B

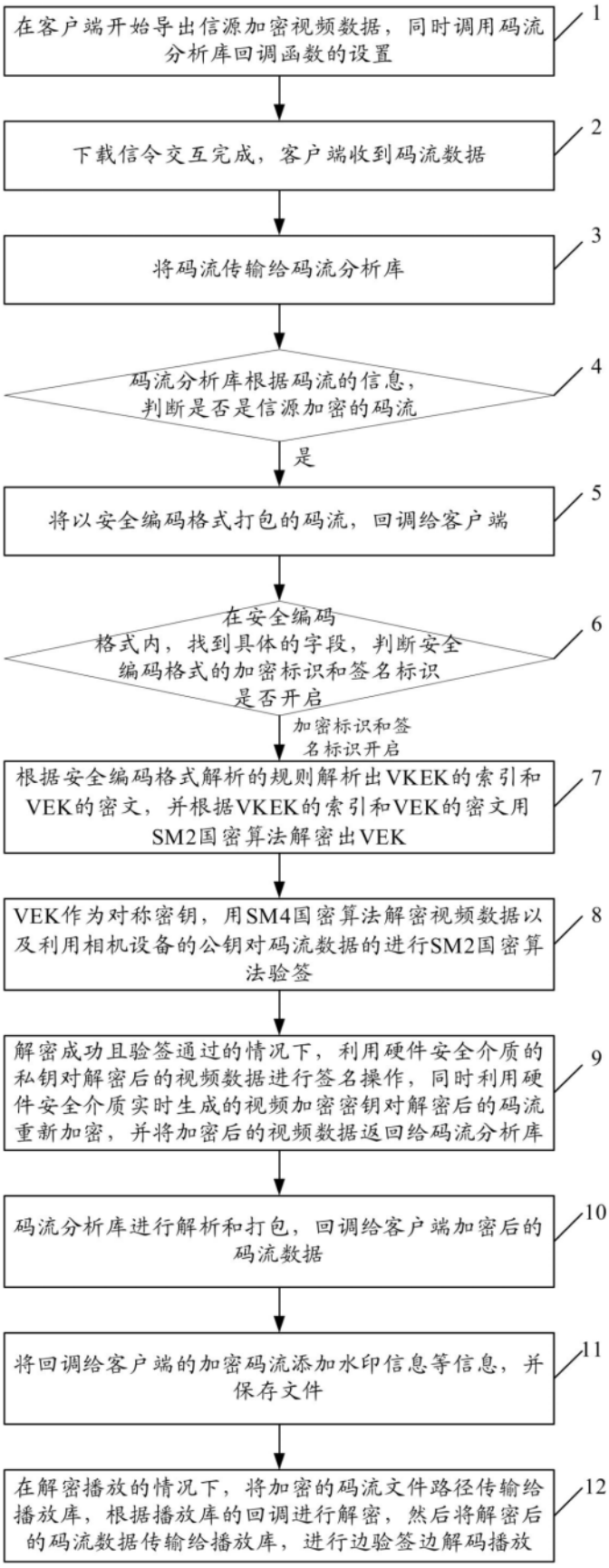

在客户端开始导出信源加密视频数据，同时调用码流分析库回调函数的设置
1
下载信令交互完成，客户端收到码流数据
2
将码流传输给码流分析库
3
码流分析库根据码流的信息，判断是否是信源加密的码流
4
是
将以安全编码格式打包的码流，回调给客户端
5
在安全编码格式内，找到具体的字段，判断安全编码格式的加密标识和签名标识是否开启
6
加密标识和签名标识开启
根据安全编码格式解析的规则解析出VKEK的索引和VEK的密文，并根据VKEK的索引和VEK的密文用SM2国密算法解密出VEK
7
VEK作为对称密钥，用SM4国密算法解密视频数据以及利用相机设备的公钥对码流数据的进行SM2国密算法验签
8
解密成功且验签通过的情况下，利用硬件安全介质的私钥对解密后的视频数据进行签名操作，同时利用硬件安全介质实时生成的视频加密密钥对解密后的码流重新加密，并将加密后的视频数据返回给码流分析库
9
码流分析库进行解析和打包，回调给客户端加密后的码流数据
10
将回调给客户端的加密码流添加水印信息等信息，并保存文件
11
在解密播放的情况下，将加密的码流文件路径传输给播放库，根据播放库的回调进行解密，然后将解密后的码流数据传输给播放库，进行边验签边解码播放
12

图4

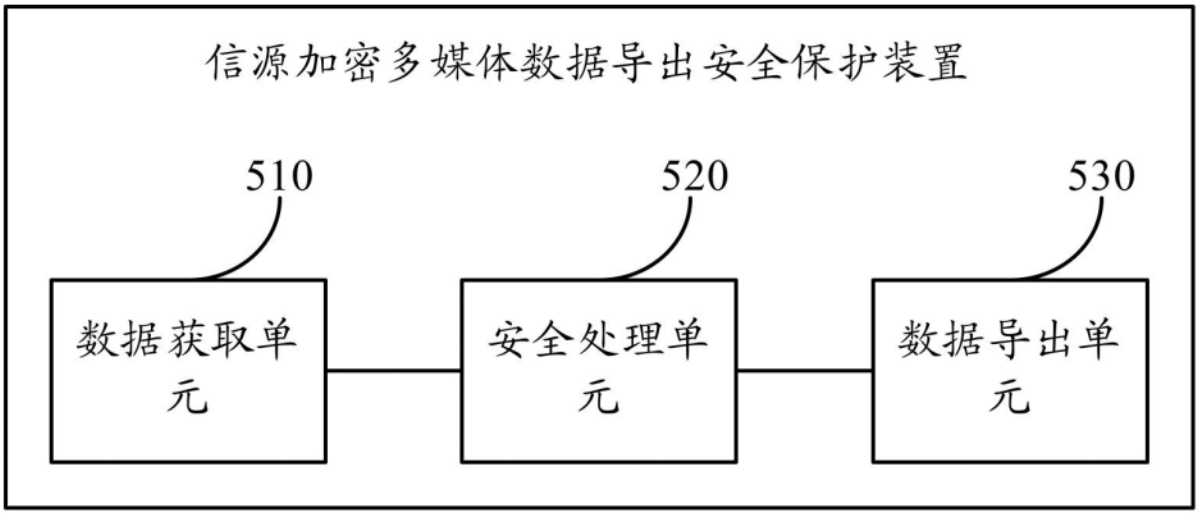

信源加密多媒体数据导出安全保护装置
510
520
530
数据获取单元
安全处理单元
数据导出单元

图5

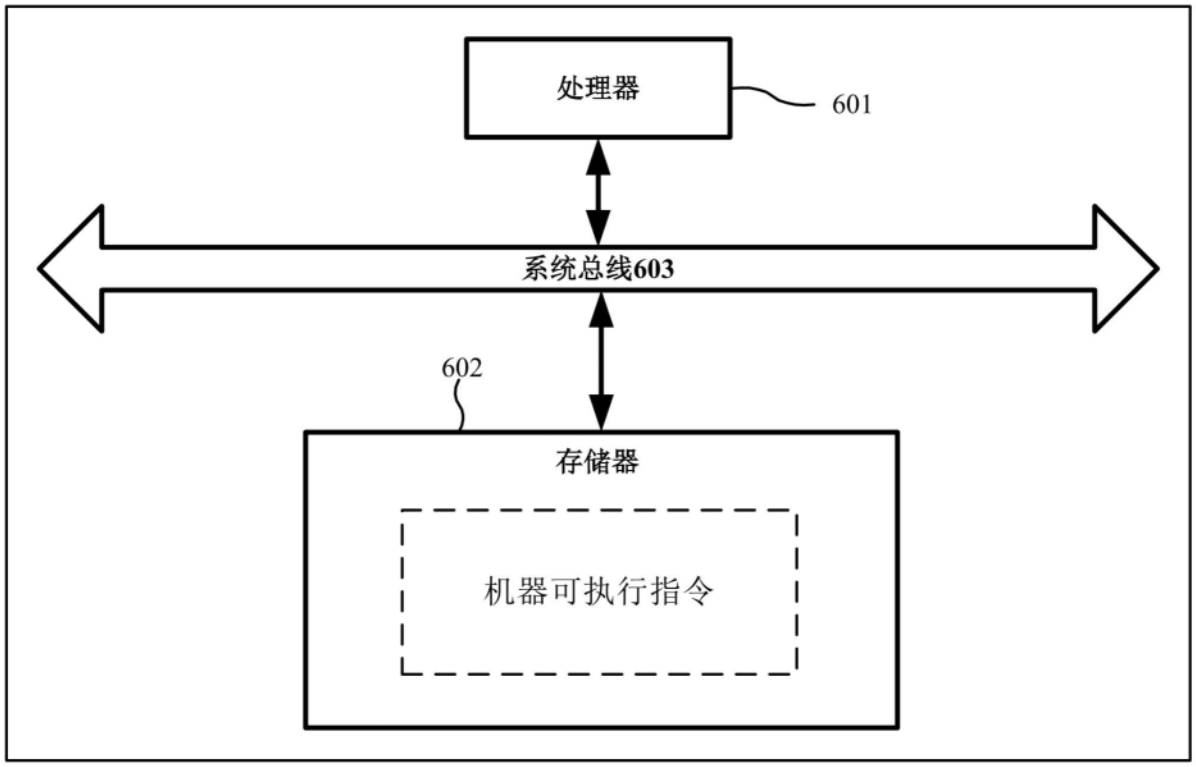

处理器
601
系统总线603
602
存储器
机器可执行指令

图6