[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
G06F 1/00

[12] 发明专利申请公开说明书

[21] 申请号 02820178.7

[43] 公开日 2005 年 1 月 19 日

[11] 公开号 CN 1568446A

[22] 申请日 2002.9.12 [21] 申请号 02820178.7
[30] 优先权
[32] 2001.10.12 [33] EP [31] 01203911.1
[86] 国际申请 PCT/IB2002/003751 2002.9.12
[87] 国际公布 WO2003/034190 英 2003.4.24
[85] 进入国家阶段日期 2004.4.12
[71] 申请人 皇家飞利浦电子股份有限公司
地址 荷兰艾恩德霍芬
[72] 发明人 D·P·凯利 W·J·范格斯特

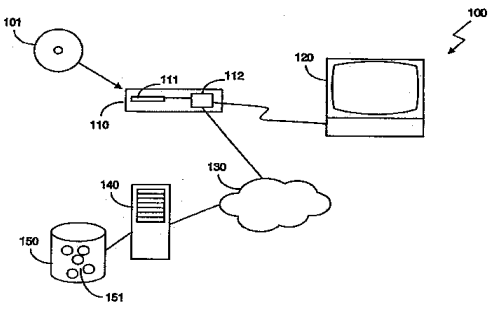
[74] 专利代理机构 中国专利代理(香港)有限公司
代理人 杨 凯 王 勇

权利要求书 2 页 说明书 11 页 附图 4 页

[54] 发明名称 安全的内容分发方法和系统

[57] 摘要

一种以安全的方式使与基本内容有关的附加内容 151 可用的方法。 基本内容在记录载体(101)上进行分发，并通过采用至少一个秘密的安全机制加以保护。 例如，DVD 内容加扰系统(CSS)可与诸如 ACC、字幕密钥和盘密钥之类的秘密一起使用。附加内容(151)在服务器(140)上可用，并可通过再现装置(112)下载。 附加内容(151)受与基本内容一样的安全机制保护，且采用至少一个用于保护基本内容的相同秘密。 这样，再现装置(112)只在成功通过与 DVD 驱动器(111)的认证之后才可访问附加内容(151)，因为通过其它方式它无法获悉访问附加内容(151)所需的秘密。



ISSN1008-4274

知识产权出版社出版

1. 一种使与基本内容有关的附加内容可用的方法，所述基本内容在记录载体（101）上进行分发，并通过采用至少一个秘密的安全机制加以保护，所述方法包括将所述附加内容从服务器分发到客户机，其特征在于，所述附加内容受与所述基本内容一样的安全机制保护，采用至少一个所述用于保护基本内容的相同秘密。

2. 如权利要求 1 所述的方法，其特征在于，所述方法包括使用所述记录载体上的秘密认证控制代码（ACC）与所述客户机执行认证协议以及利用所述会话密钥对所述附加内容加密。

3. 如权利要求 1 所述的方法，其特征在于，所述方法包括利用亦用于对至少一部分所述基本内容加密的加密密钥对所述附加内容加密。

4. 如权利要求 3 所述的方法，其特征在于，所述加密密钥是 DVD 字幕密钥和 DVD 盘密钥之一。

5. 如权利要求 1 所述的方法，其特征在于，所述记录载体是 DVD 盘。

6. 一种用于再现从重放设备接收的基本内容的再现装置，所述基本内容通过采用至少一个秘密的安全机制加以保护，所述再现装置包括利用所述至少一个秘密获取所述基本内容的条件访问部件和从服务器接收与所述基本内容相关的附加内容的接收部件，其特征在于，所述附加内容受与所述基本内容一样的安全机制保护，采用至少一个所述用于保护基本内容的相同秘密，以及设置所述条件访问部件以利用所述至少一个秘密获取所述附加内容。

7. 如权利要求 6 所述的装置，其特征在于还包括用于使所述基本内容的获取与所述附加内容的获取同步的同步部件。

8. 如权利要求 6 所述的装置（120），其特征在于，设置所述条件访问部件以利用所述记录载体上的秘密认证控制代码（ACC）

与所述服务器执行认证协议，从而创建会话密钥，并利用所述会话密钥对所述附加内容加密。

9. 如权利要求 6 所述的装置，其特征在于，设置所述条件访问部件以利用亦用于对至少一部分所述基本内容解密的解密密钥对所述附加内容解密。

10. 一种适于再现从重放设备接收的基本内容的计算机程序产品，所述基本内容通过采用至少一个秘密的安全机制加以保护，所述计算机程序产品包括利用所述至少一个秘密获取所述基本内容的条件访问方法和从服务器接收与所述基本内容相关的附加内容的接收方法，其特征在于，所述附加内容受与所述基本内容一样的安全机制保护，采用至少一个所述用于保护基本内容的相同秘密，以及所述条件访问方法用于利用所述至少一个秘密获取所述附加内容。

安全的内容分发方法和系统

本发明涉及一种使与基本内容有关的附加内容可用的方法，基本内容在记录载体上进行分发，并通过采用至少一个秘密的安全机制加以保护，该方法包括将附加内容从服务器分发到客户机。

本发明还涉及一种用于再现从重放设备接收的基本内容的再现装置，基本内容通过采用至少一个秘密的安全机制加以保护，该再现装置包括利用所述至少一个秘密获取基本内容的条件访问部件和从服务器接收与基本内容相关的附加内容的接收部件。

DVD 技术允许内容制作者在盘上提供比简单电影多得多的内容。因为大存储容量可用，所以可以在盘上提供所有种类的附加内容。例如，可以包括幕后花絮、减余片、对导演和/或演员的采访、不同语言的叠印字幕（subtitle）和伴随视频片断的声轨。

因为越来越多的家庭娱乐系统可以某种方式访问因特网，所以附加内容不仅可以在 DVD 盘上提供而且可以在网站上提供。这称之为联网 DVD。在其最基本的形式下，想观看某种电影的用户连接到网站以观看该电影并查看附加信息，观看有关电影的新访谈或报道，如此等等。他也可以参与与该电影有关的在线游戏。

希望保护此附加内容以避免未授权访问和/或拷贝。具体地说，对附加内容的访问应该只限于拥有该盘的合法样品的人。

一种简单的解决方案将是首先以某种方式验证用户拥有 DVD 盘的样品，然后从服务器分发附加内容。例如，这种解决方案可以这样实现，即向网站提供盘上存储的标识符，并在该网站上将其与正确标识符列表作比较。但是，这种解决方案非常不安全，因为标识符可以从原样品被简单地拷贝，并由未授权设备用于非法访问附加内容。

本发明的目的是提供一种如前言所述的方法，此方法比已知方法安全。

此目的是通过本发明的一种方法达到的，这种方法的特征在于，附加内容受与基本内容一样的安全机制保护，采用至少一个用于保护基本内容的相同秘密。尽管利用诸如加密技术或基于认证的访问限制之类的安全机制本身是公知的，但这些机制通常采用不同的秘密，如加密密钥。这使系统总体上更易受攻击者攻击，因为系统现在需要保护更多的秘密。

通过共享安全机制和秘密，则需要保护的是较少的敏感信息。保护 DVD 内容的安全机制被设计来对抗有恶意的第三方的主动攻击，并且它们还可以用于保护同样吸引第三方的附加内容。

此外，通过引入仅在附加内容的接收者可访问记录载体时才可获悉的秘密，分发实体可以确信只有实际可访问记录载体的接收者才可对附加内容解密。

在实施例中，所述方法包括利用记录载体上的秘密认证控制代码（ACC）与客户机执行认证协议以建立会话密钥，并利用会话密钥对附加内容加密。客户机仅当知道 ACC 时才可成功地完成认证，或者如果它知道 ACC，它起码可推导出正确的会话密钥。这确保只有客户机可访问记录载体时才可对附加内容解密。

在另一个实施例中，所述方法包括利用亦用于对至少一部分基本内容加密的加密密钥对附加内容加密。加密密钥最好是 DVD 字幕密钥（title key）和 DVD 盘密钥之一。在 DVD 中，字幕密钥和盘密钥只可由客户机（通常是与 DVD 装置相连的再现装置）从 DVD 盘获得，因此这也确保了只有可访问记录载体的客户机才可以将附加内容解密。

本发明的另一目的是提供如前言所述的一种比已知方法安全的装置。

此目的是通过本发明的一种装置实现的，这种装置的特征在于，

附加内容受与基本内容一样的安全机制保护，采用至少一个用于保护基本内容的相同秘密，以及设置条件访问部件以利用所述至少一个秘密来获取附加内容。

通过共享安全机制和秘密，则需要保护的是较少的敏感信息。设计保护 DVD 内容的安全机制来对抗有恶意的第三方的主动攻击，并且它们还可以用于保护同样吸引第三方的附加内容。

此外，通过引入仅在附加内容的接收者可访问记录载体时才可获悉的秘密，分发实体可以确信只有实际可访问记录载体的接收者才可对附加内容解密。

在实施例中，所述装置还包括用于使基本内容的获取与附加内容的获取同步的同步部件。在 DVD 中，尤其是字幕密钥可以按分区变更。通过选择与字幕密钥相同的秘密来保护附加内容，则此秘密可与字幕密钥同时予以变更。然后，有必要使基本内容的获取与附加内容的获取同步，以便正确的秘密可用于对附加内容解密。

在另一实施例中，设置条件访问部件以利用记录载体上的秘密认证控制代码（ACC）与服务器执行认证协议，以建立会话密钥，并利用该会话密钥对附加内容加密。所述装置仅当知道 ACC 时才可成功地完成认证、或者如果它知道 ACC，它起码可推导出正确的会话密钥。这确保只有所述装置可访问记录载体时才可以对附加内容解密。

在实施例中，还设置条件访问部件以利用亦用于对至少一部分基本内容解密的解密密钥将附加内容解密。

本发明还涉及一种计算机程序产品。

本发明的这些和其他方面将通过参照附图所示的实施例来阐明，附图中：

图 1 示意性地显示了用于使与基本内容相关的附加内容可用的系统的主要部件，其中包括 DVD 驱动器和再现装置；

图 2 说明 DVD 驱动器和再现装置安装在一个重放设备中的情况

下的 DVD 内容加扰系统。

图 3 说明 DVD 驱动器利用数字接口或总线与外部再现装置相连的情况下的内容加扰系统；以及

图 4 更详细地示意再现装置。

在这些附图中，相同的参考标号表示类似或对应的功能。附图中所示的一些功能通常用软件实现，所述软件表示软件实体，如软件模块或对象。

图 1 示意性地显示了根据本发明的系统 100 的主要部件。系统 100 包括重放设备 110 和显示设备 120。在优选实施例中，重放设备 110 是包括 DVD 驱动器 111 和再现装置 112 的 DVD 播放器，其中再现装置 112 可以实现为解码卡。DVD 驱动器 111 和再现装置 112 也可以作为物理上独立的装置提供。例如，DVD 驱动器 111 可安装到计算机中，由此再现装置 112 作为在计算机上运行的应用软件来提供。再现装置 112 也可以如同 DVD 驱动器 111 一样安装到显示设备 120 中。

用户可以将记录载体 101（如 DVD 盘）放在 DVD 驱动器 111 中。然后读出记录载体 111 上存储的内容并将其提供给再现装置 112，在再现装置 112 中将其解码和处理，以生成音频/视频信号。此音频/视频信号然后馈送到显示设备 120，以便显示给用户。这样，例如，用户可以在其电视上观看 DVD 盘上存储的电影。

重放设备 110 还与外部网络 130 相连，外部网络 130 最好是因特网。至外部网络 130 的连接可以用电缆调制解调器、ADSL 线路、或安装在重放设备 110 中的、与电话线相连的普通调制解调器来实现。该连接还可以通过将再现装置 112 链接到以太网或其他提供至外部网络 130 的接入的局域网来实现。至外部网络 130 的连接将用于下载诸如电影或音乐之类的内容，因此最好是高带宽连接。

服务器 140 也与外部网络 130 相连。服务器 140 提供从例如存储装置 150 下载的附加内容项 151。内容项 151 涉及并扩展了记录载

体 101 上的内容。例如，内容项 151 可以包括电影声轨的不同版本、不同语言的电影配音或叠印字幕（subtitle）、幕后花絮、额外场景、不同结尾、基于电影的游戏、对演员和其他参与者的采访、与记录载体 101 上存储的内容有关的实况事件等等。

记录载体 101 通常具有某种表示这些附加内容项 151 可用的指示。这可以是打印在记录载体 101 的保护封面上的指示性信息，但也可以是记录载体 101 本身具有的计算机可读指示符。在那种情况下，DVD 驱动器 111 可以自动检测该指示符。重放设备 110 然后可以向用户提供访问附加内容项 151 的选项。如果用户同意，则重放设备 110 使用其至外部网络 130 的连接联络服务器 140。然后它可以获取可用附加内容项 151 的列表，用户可从中选择访问一个或多个内容项。可以容易地设想许多访问、显示和管理附加内容项 151 的其他方法。

记录载体 101 上的内容包括多个所谓的字幕。字幕可以是例如视频流、音频流等等。为了防止非法拷贝，记录载体 101 上的字幕可以各种方式加以保护。

如果记录载体 101 是 DVD 盘，则采用内容加扰系统（CSS）。在图 2 中，给出了在 DVD 驱动器 111 和再现装置 112 安装在一个重放设备 110 中的情况下如何使用 CSS 的概况图。此概况图以及图 3 的概况图都基于从因特网上和其他渠道公开可获得的信息，其他渠道如 2000 年 12 月 6 日由 Gregory Kesden 在 Carnegie Mellon 大学所作的有关 CSS 的公开讲演，此讲演的记录可从因特网上 http://www-2.cs.cmu.edu/~dst/DeCSS/Kesden/处获得。

记录载体 101 包含经加密的盘密钥 EDK，它存储在所谓的引导区中。引导区可以通过兼容的 DVD 驱动器读取。盘密钥对盘上的所有内容都是相同的。数据以一个分区为单位加密。每个分区在分区首部具有加密的字幕密钥 ETK。字幕密钥可以按分区变更。

重放设备 110 包括一个或多个播放器密钥，它们可用于对记录

载体 101 上加密的盘密钥 EDK 解密，这当然要假设重放设备 110 持有正确的播放器密钥。在步骤 201，从记录载体 101 获得加密的盘密钥 EDK，并在步骤 202 将其解密。在对盘密钥解密之后，重放设备 110 在步骤 203 接收加密的字幕密钥 ETK，并在步骤 204 使用解密的盘密钥对字幕密钥解密。

接着，在步骤 205 接收加密的字幕。在步骤 206 用解密的字幕密钥对数据解密。重放设备 110 然后可以将期望字幕的字幕密钥解密，从而访问这些字幕本身。可以对解密的数据进行解码，以获取音频/视频信号，此音频/视频信号在步骤 207 提供给显示设备 120 以便显示给用户。

在图 3 中，针对 DVD 驱动器 111 利用数字接口或总线与外设再现装置 112 相连的情况说明 CSS。需要执行三个主要步骤：认证、安全的总线加密/解密以及数据解密，它们在图 3 中分别用 AUTH、SECBUS 和 DDEC 表示。

在认证过程 AUTH 中，检查再现装置 112 是否是 DVD 兼容的装置。认证以如下方式执行。DVD 驱动器 111 从记录载体 101 读取认证控制代码 ACC。在再现装置 112 中生成随机数 RN1。此数 RN1 传送到 DVD 驱动器 111。在 DVD 驱动器 111 中，在步骤 ER1 将数 RN1 连同 ACC 一起用秘密算法加密，步骤 ER1 的结果传送给再现装置 112。

在再现装置 112 中，数 RN1 在步骤 ER1’ 中作多次加密，每次使用不同的数 i。在步骤 CMP1，对各数 i 将该结果与从 DVD 驱动器 111 接收的 EA 的结果作比较。如果对 i 的某个值 ER1 和 ER1’ 的结果匹配，则再现装置 112 知道数 i 的该值与从记录载体 101 读取的 ACC 的值相同。

在 DVD 驱动器 111 生成随机数 RN2 并将其传送给再现装置 112。在步骤 ER2 将该数连同 DVD 驱动器 111 中的 ACC 数一起加密。在步骤 ER2’，在再现装置 112 中将随机数 RN2 连同在上述步

骤 CMP1 中已发现与该 ACC 相同的 i 的值一起加密。在步骤 CMP2，在 DVD 驱动器 111 中将步骤 ER2 和 ER2’ 的结果作比较，如果它们相同，则 DVD 驱动器 111 认为再现装置 112 是兼容的装置。

在安全总线功能 SECBUS 中，在 DVD 驱动器 111 和再现装置 112 中将加密的随机数 RN1 和 RN2（即 DVD 驱动器 111 中 ER1 和 ER2 的输出和再现装置 112 中 ER1’ 和 ER2’ 的输出）用于派生安全总线密钥或会话密钥 SK。注意到，如果认证过程 AUTH 成功执行，则各装置中确定的会话密钥 SK 是相同的，因此可用于数据的安全交换。

在 DVD 驱动器 111 中，从记录载体 101 读取加密的盘密钥 EDK 和加密的字幕密钥 ETK，并分别在步骤 SEDK 和 SETK 中（再次）用该安全总线密钥 SK 加密。然后将双重加密的盘密钥和字幕密钥传送给再现装置 112。

在再现装置 112 中，分别在步骤 SDDK 和 SDTK 中将安全总线密钥 SK 用于对双重加密的盘密钥和字幕密钥解密。再现装置 112 现在可以访问加密的盘密钥 EDK 和字幕密钥 ETK。之所以要执行此双重加密步骤，是为了确保通过窃听 DVD 驱动器 111 和再现装置 112 之间的接口不可能获得加密的盘密钥 EDK 和字幕密钥 ETK。

在数据解密功能 DDEC 中，以与图 2 所示一样的方式对分区解密。简要概述如下，再现装置 112 在步骤 DDK 利用其播放器密钥 PK 对盘密钥解密，然后在步骤 DTK 利用所述盘密钥对字幕密钥解密。利用如此得到的盘密钥和字幕密钥，再现装置 112 现在可以对记录载体 101 上存储的各字幕解密。

图 4 更详细地示意了再现装置 112。此处的再现装置 120 包括 IEEE 1396 联网接口模块 401，此模块与 IEEE 1394 局部总线 400 相连。在此实施例中，与 DVD 驱动器 111 的通信经过局部总线 400。其他装置也可以连到局部总线 400 上。

再现装置 112 中设有认证模块 402，它执行如参照图 3 所述的认

证功能 AUTH。还有加解密模块 403，它执行如参照图 3 所述那样的加密/解密功能 SECBUS 和数据解密功能 DDEC。

解密的内容从加解密模块 403 馈送到输出模块 404。输出模块 404 对内容进行解码和处理，以生成将分别在显示器 441 和扬声器 442 上输出的音频和/或视频信号。显示器 441 和扬声器 442 一起可视为显示设备 120。生成这种输出是本专业中众所周知的。很清楚，有许多不同的视听装置 441、442 可用于再现输出。

输出模块 404 还可以存储存储媒体 443 上的内容。当然，这只在接收内容的相关权限允许这样做时才可以这样做。存储媒体 443 可以是例如硬盘、录像带或可重写 DVD 盘。

再现装置 120 还包括联网模块 410。此联网模块 410 提供至上述外部网络 130 的接入，外部网络 130 最好是因特网。联网模块 410 可以实现为例如与电缆调制解调器相连的具有适当软件的网卡。也可以采用与 ADSL 线路相连的调制解调器、或与例如基于以太网的 LAN 相连的网卡。

如以上参照图 1 所作的说明，某些点上的联网模块 410 从服务器 140 下载附加内容项 151。希望可以防止附加内容项 151 被非法访问和/或拷贝。具体地说，对附加内容项 151 的访问应当只限于拥有记录载体 101 的合法样品的人们。

根据本发明，附加内容项 151 受至少一种亦用于保护记录载体 101 上内容的安全机制的保护。该安全机制采用一个或多个秘密，如 ACC、盘密钥或字幕密钥。可以在将相同的安全机制应用于附加内容项 151 时采用这些秘密中的一个或多个秘密。

一接收到受保护的附加内容项 151，联网模块 410 就将它们馈送到加解密模块 403，以便可以将它们解密并由输出模块 404 再现，正如记录载体 101 上的基本内容一样。此馈送操作可以以流传送方式完成，例如在附加内容项 151 的各块到达时将其馈送到加解密模块 403，最好是采用某种缓冲机制，例如为了有助于流式传送。

在第一实施例中，还在再现装置 112 和服务器 140 之间使用了参照图 3 所述的认证协议。再现装置 112 现在参与与服务器 140 的认证过程 AUTH，正如它之前与 DVD 驱动器 111 所做的那样。即，服务器 140 现在代替 DVD 驱动器 111。网络 130 现在取代 DVD 驱动器 111 和再现装置 112 之间的安全总线。

在图 3 所示的认证过程 AUTH 中，再现装置 112 在成功通过与 DVD 驱动器 111 的认证之后，确定与从记录载体 101 得到的 ACC 数相同的值 i。再现装置 112 可以利用该值 i 来向服务器 140 证明它可以访问记录载体 101。服务器 140 然后可以将附加内容项 151 提供给再现装置 112。

服务器 140 从与记录载体 101 完全相同的记录载体读取 ACC 数，并将此 ACC 用作认证过程的输入。与图 3 所示的 AUTH 过程不同，服务器 140 现在首先向再现装置 112 提供随机选择的数 RN2”，此数连同与 ACC 相等的所述 i 的值在再现装置 112 中用作步骤 ER2’的输入。ER2’的输出回传给服务器 140，并在 CMP2 中与使用 RN2”和 ACC 的 ER2 的输出作比较。

如果 CMP2 成功，则服务器 140 断定再现装置 112 知道 ACC 的值，因此必定可以访问记录载体 101。通过以此方式逆向交换随机数，则接收装置 112 不可能假装可以访问 ACC 或通过与服务器 140 交互获悉 ACC。

为了完成认证过程，再现装置 112 此刻生成随机数 RN1”并将其发送给服务器 140，如以上参照图 3 所述那样在服务器 140 上使用该随机数，只不过只需一次迭代，因为已经知道 i 的正确值。这样，就完成了认证过程，并且服务器 140 和再现装置 112 都拥有了生成会话密钥 SK 所必需的输入。然后可以将一个或多个附加内容项 151 以加密的方式经外部网络 130 传送到再现装置 112。在本实施例中，可以在服务器 140 中推导出来自记录载体 101 的盘密钥和字幕密钥。

由服务器 140 交付的附加内容项 151 对应该与记录载体 101 的

原始内容同步显示的所有信息使用相同的盘密钥和字幕密钥。定时信息用于检测字幕密钥的变更。这些密钥不必经由网络 130 传送。按分区打包且先用字幕密钥然后用会话密钥加密的附加内容项 151 经网络 130 传送。很清楚，在本实施例中，记录载体 101 和服务器 140 中所用的记录载体应该是相同的，且具有相同的密钥。

在第二实施例中，服务器 140 和再现装置 112 之间无需同步。在记录载体 101 上的基本内容的显示处于暂停状态的同时，可以显示附加内容项 151。派生的会话密钥用于对附加内容项 151 加密。对此附加信息不采用盘密钥或字幕密钥。因为服务器 140 已将 ACC 数用于派生会话密钥，所以需要正确的记录载体 140。

在第三实施例中，应用了来自记录载体 101 的盘密钥，并如上所述那样进行认证。盘密钥和固定字幕密钥用于对分区加密。固定的字幕密钥例如为固定模式 '00' 或随机数。在最后一种情形中，必须以安全的方式将它传送到再现装置 112。

记录载体 101 和服务器 140 所用记录载体 101 之间的同步是不需要的，因为双方都知道盘密钥。因为服务器已将 ACC 数用于派生会话密钥，以及将盘密钥用于对分区加密，所以需要正确的记录载体 101。但是，这些密钥不经由外部网络 130 传送。

在第四实施例中，服务器 140 和再现装置 112 之间不需要任何认证。此方法可用于同时将附加内容分发给记录载体 101 的所有拥有者。服务器 140 此时提供用盘密钥和字幕密钥加密的附加内容项 151。如果需要盘内容和附加内容之间的同步，则可以采用第一实施例中所述的方法。

如果不需要同步，则可以利用来自记录载体 101 的盘密钥和服务器选择的字幕密钥对附加内容 151 执行加密。如果此字幕密钥不是固定的，则以加密的方式将其传送到再现装置 112。不同的字幕密钥可用于对字幕的不同部分加密。然后可以相应地改变对附加内容项 151 解密所必需的密钥。

在另一实施例中，未使用来自 CSS 系统的秘密，但服务器 140 仍然检查再现装置 112 是否具有相同的 DVD 盘。认证利用不必与 CSS 认证一样的通用认证协议进行。用会话密钥对从服务器 140 传送给再现装置 112 的附加内容项 151 加密。会话密钥是来自此特定盘的加密的盘密钥。此会话密钥不经由网络 130 传送。

也可能不经任何认证就对附加内容项 151 进行分发，其中，将来自记录载体 101 的盘密钥和字幕密钥用作加密密钥，以在分发附加内容项 151 之前将其加密。

应注意，上述实施例对本发明进行说明而非限制，本专业的技术人员可以在不背离所附权利要求书的前提下，设计出许多备选实施例。

在权利要求书中，括号之间的任何引用符号不应视为对权利要求书予以限制。单词“包括”不排除不同于权利要求中所列单元或步骤的存在。单元之前的单词“一个”不排除多个这种单元的存在。本发明可以通过包括几个不同单元的硬件以及适当编程的计算机来实现。

在设备权利要求中，枚举了几个部件，这些部件中的若干部件可以通过同一件硬件来实现。互不相同的从属权利要求中记载了某些措施这一事实并不表示不能利用这些措施的组合。

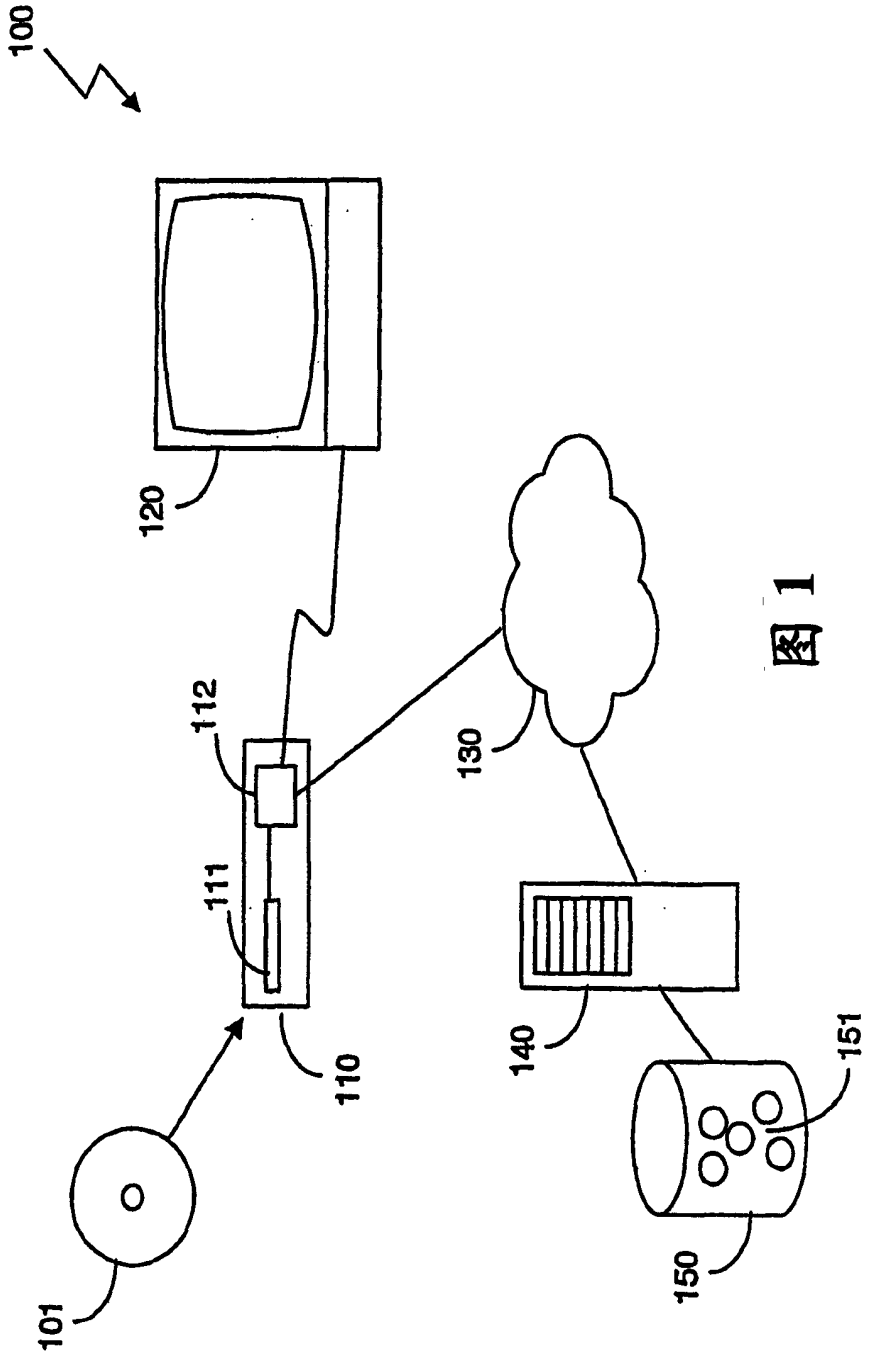


图 1

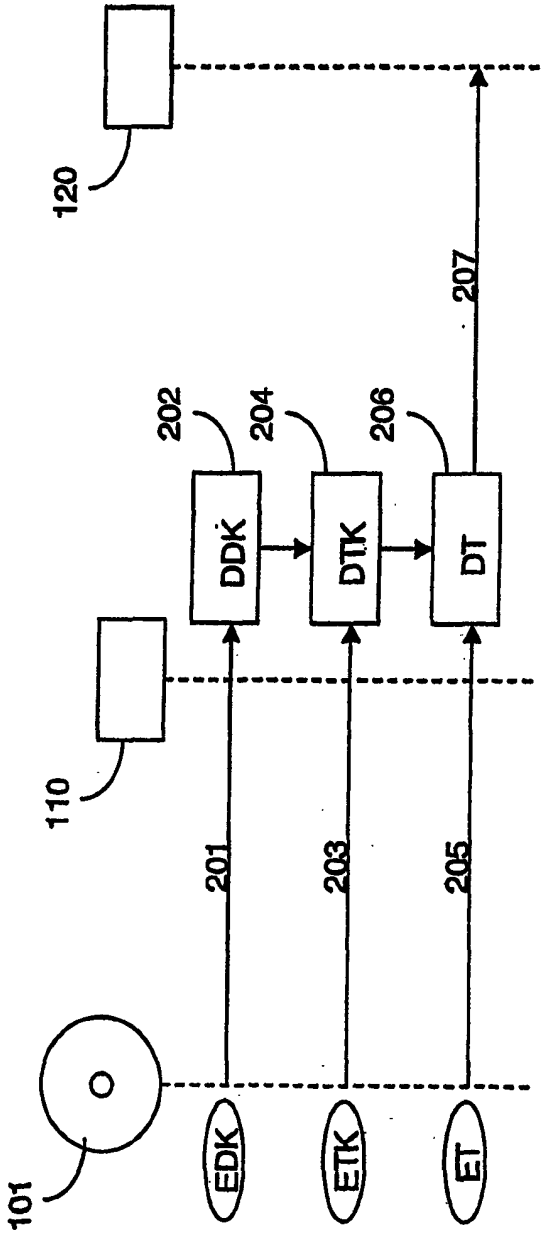


图 2

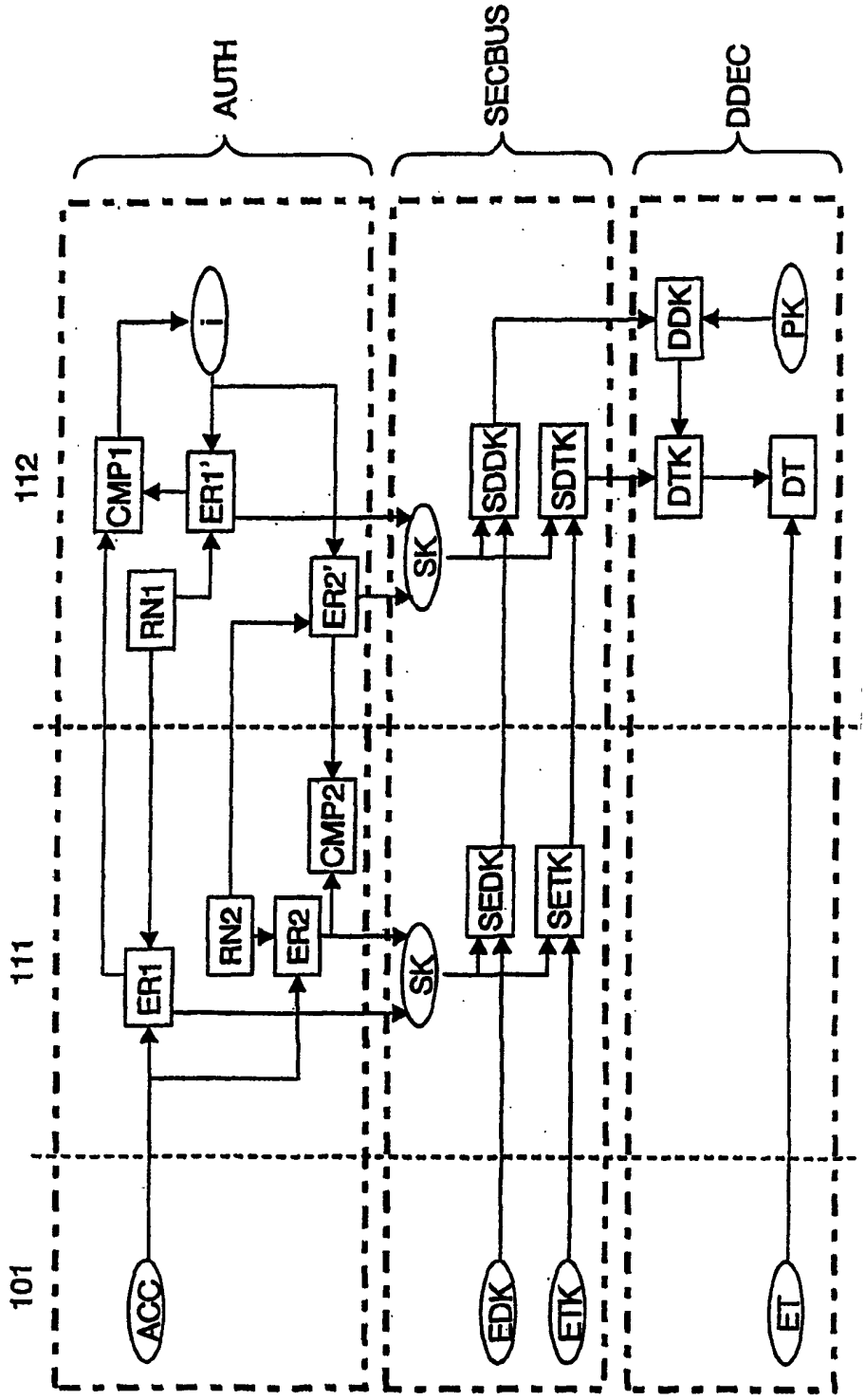

AUTH
SECBUS
DDEC
112
111
101
i
CMP1
ER1'
RN1
ER2'
SK
SDDK
SDTK
DDK
PK
DTK
DT
CMP2
RN2
ER2
ER1
SK
SEDK
SETK
ACC
EDK
ETK
ET

图 3

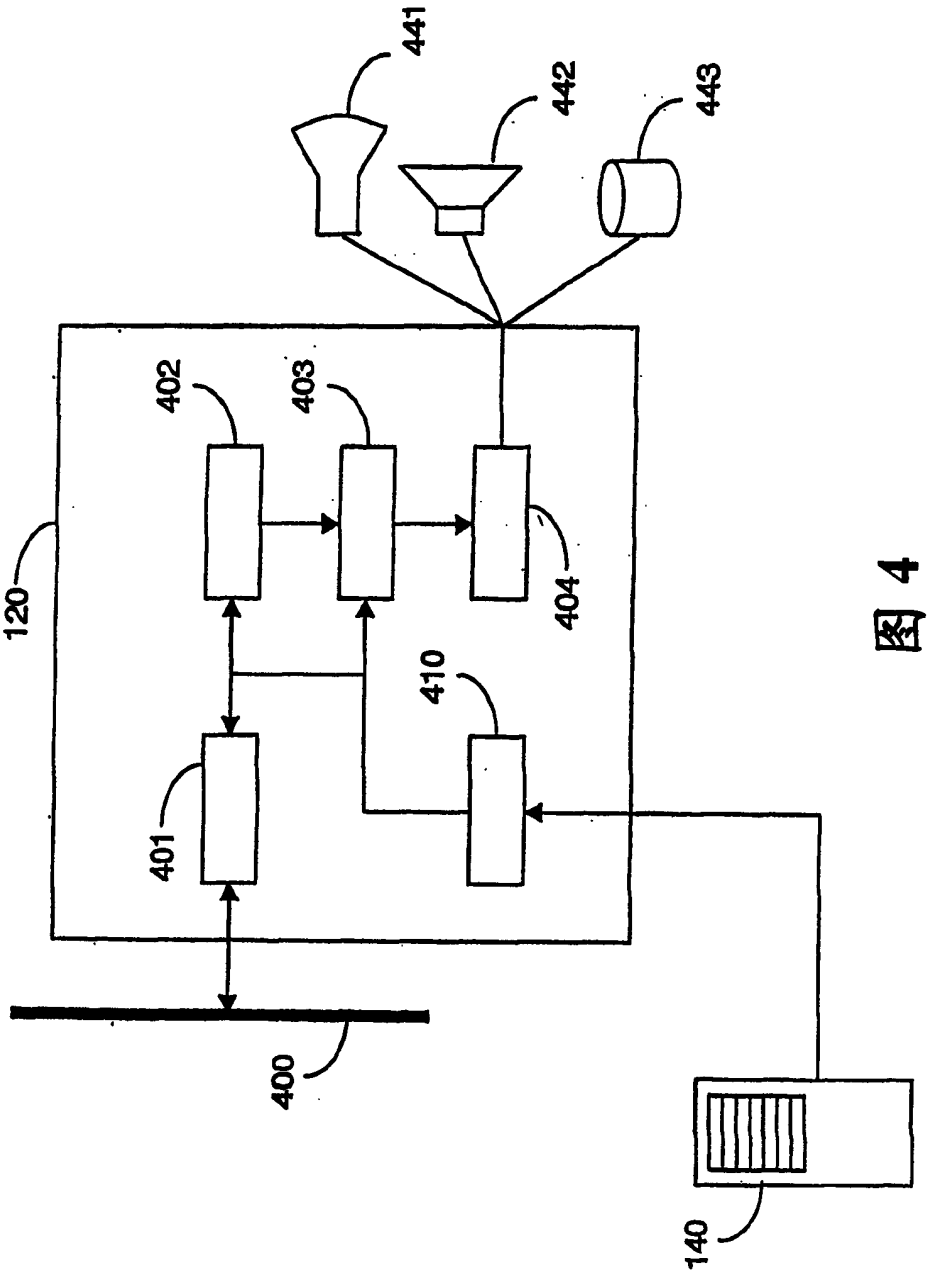


图 4