[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04N 7/16 (2006.01)

[12] 发明专利申请公开说明书

[21] 申请号 200510109841.7

[43] 公开日 2006 年 3 月 8 日

[11] 公开号 CN 1744708A

[22] 申请日 2005.7.14
[21] 申请号 200510109841.7
[30] 优先权
[32] 2004. 7.14 [33] KR [31] 54814/04
[71] 申请人 三星电子株式会社
地址 韩国京畿道
[72] 发明人 康龙镇

[74] 专利代理机构 北京市柳沈律师事务所
代理人 黄小临 王志森

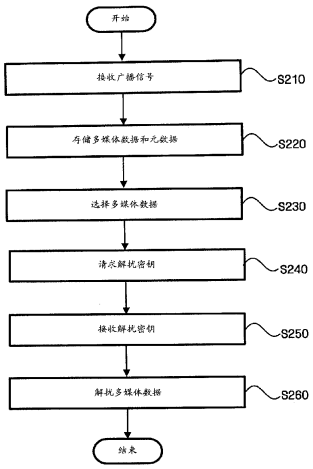
权利要求书 3 页 说明书 13 页 附图 5 页

[54] 发明名称

多媒体数据交易系统和方法

[57] 摘要

一种多媒体数据交易方法、以及执行该方法的设备和系统，所述方法包括：从由广播站服务器接收的广播信号中提取加扰的多媒体数据；请求并接收解扰密钥，以解扰用户选购的包含在所述广播信号中的多媒体数据；以及利用解扰密钥，解扰所选的多媒体数据。



1、一种广播接收设备，包括:

广播信号处理单元，接收从广播站服务器发送的广播信号，并提取包含在接收的广播信号中的加扰的多媒体数据和元数据;

存储单元，存储提取的多媒体数据和元数据;

数据发送机/接收机，发送请求解扰密钥的消息，以解扰用户想要购买的多媒体数据，并接收解码密钥；以及

控制单元，利用接收的解扰密钥，解扰用户想要购买的多媒体数据。

2、根据权利要求 1 所述的设备，其中，所述数据发送机/接收机是执行有线或无线通信服务的通信调制解调器。

3、根据权利要求 2 所述的设备，其中，从提供有线或无线通信服务的通信服务器接收所述解扰密钥。

4、根据权利要求 3 所述的设备，其中，将与用户购买的多媒体数据有关的费用与和有线或无线通信服务有关的通信费用一起由操作通信服务器的公共载体征收。

5、根据权利要求 1 所述的设备，其中，从广播站服务器接收解扰密钥。

6、根据权利要求 5 所述的设备，其中，将与用户购买的多媒体数据有关的费用与和广播站服务器提供的广播节目的接收有关的视听费用一起征收。

7、根据权利要求 1 所述的设备，还包括执行解扰的多媒体数据的应用单元。

8、根据权利要求 1 所述的设备，其中，预定数量的加扰的多媒体数据和元数据在其制造时存储在存储单元中。

9、根据权利要求 8 所述的设备，其中，控制单元从接收的多媒体数据和元数据中，选择并存储未预先存储在存储单元中的多媒体数据和元数据。

10、根据权利要求 1 所述的设备，其中，广播站服务器通过单独的信道而不是普通广播节目传输信道发送加扰的多媒体数据和元数据。

11、根据权利要求 1 所述的设备，其中，广播站服务器在没有发送普通广播节目的时区内发送加扰的多媒体数据和元数据。

12、根据权利要求 1 所述的设备，其中，解扰密钥在发送前被加密。

13、根据权利要求 12 所述的设备，其中，用于加密的变量包括第一识别

信息、第二识别信息或其组合中的至少一个，第一识别信息用于识别经解扰密钥解扰的多媒体数据，第二识别信息用于识别数据发送机/接收机。

14、根据权利要求 13 所述的设备，其中，第一和/或第二识别信息与解扰密钥请求一同发送。

15、一种多媒体数据交易方法，所述方法包括:

接收从广播站服务器发送的广播信号，并从广播信号中提取加扰的多媒体数据和元数据;

请求解扰密钥，以解扰所提取的用户想要购买的多媒体数据;

响应于所述请求，接收解扰密钥; 以及

利用接收的解扰密钥，解扰用户想要购买的多媒体数据。

16、根据权利要求 15 所述的方法，其中，根据解扰密钥的发送来征收与用户购买的多媒体数据有关的费用。

17、根据权利要求 15 所述的方法，其中，解扰密钥的请求和接收由通信调制解调器来执行，所述调制解调器执行有线或无线通信服务。

18、根据权利要求 17 所述的方法，其中，解扰密钥从提供有线或无线通信服务的通信服务器接收。

19、根据权利要求 18 所述的方法，其中，将与用户购买的多媒体数据有关的费用与和有线或无线通信服务有关的通信费用一起由操作通信服务器的公共载体根据解扰密钥的传送来征收。

20、根据权利要求 15 所述的方法，其中，从广播站服务器接收解扰密钥。

21、根据权利要求 20 所述的方法，其中，根据解扰密钥的发送，将与用户购买的多媒体数据有关的费用与和广播站服务器提供的广播节目的接收有关的视听费用一起征收。

22、根据权利要求 15 所述的方法，其中，广播站服务器通过单独的信道而不是普通广播节目传输信道，发送加扰的多媒体数据和元数据。

23、根据权利要求 15 所述的方法，其中，广播站服务器在没有发送普通广播节目的时区内发送加扰的多媒体数据和元数据。

24、根据权利要求 15 所述的方法，其中，解扰密钥在发送前被加密。

25、根据权利要求 15 所述的方法，其中，用于加密的变量包括第一识别信息、第二识别信息或其组合中的至少一个，第一识别信息用于识别经解扰密钥解扰的多媒体数据，第二识别信息用于识别执行用于解扰密钥的请求和

接收的有线或无线通信服务的通信服务。

26、根据权利要求 25 所述的方法，其中，第一和/或第二识别信息与解扰密钥请求一同发送。

27、一种广播接收设备，包括:

广播信号处理单元，接收从广播站服务器发送的广播信号，并提取包含在接收的广播信号中的加扰的多媒体数据；以及

数据发送机/接收机，请求和接收解扰密钥，以解扰用户选购的多媒体数据。

28、一种多媒体数据交易方法，所述方法包括:

从由广播站服务器接收的广播信号中提取加扰的多媒体数据;

请求并接收解扰密钥，以解扰用户选购的包含在所述广播信号中的多媒体数据；以及

利用解扰密钥，解扰所选的多媒体数据。

多媒体数据交易系统和方法

发明领域

本发明涉及一种多媒体数据交易系统和方法，更具体而言，涉及一种多媒体数据交易系统和方法，用于从广播站服务器接收加扰的多媒体数据，并获得解扰密钥来解扰用户通过公共载体所选择的多媒体数据，以购买该多媒体数据。

背景技术

随着数字时代的发展，对包括运动图像文件和音频文件的各种数字多媒体数据（以下称为多媒体数据）的需求已快速增长，所述运动图像文件诸如，例如 MPEG（运动图像专家组）或 AVI（音频视频交错），而所述音频文件诸如，例如 MP3（MPEG 音频层-3）或 OGG（Ogg Vobis）。尤其是，随着有线和无线网络通信的发展，越来越多地在线而非离线地执行多媒体数据交易。

图 1 说明了传统的多媒体数据交易系统。该系统包括：销售服务器 110，用于出售各种多媒体数据；通信设备 130，诸如个人计算机，其通过诸如因特网之类的通信网络连接至销售服务器，并允许用户下载所需的多媒体数据；以及付费服务器 120，用于为所需的多媒体数据付费。

想要购买多媒体数据的用户将通信设备 130 通过诸如因特网之类的基础网络(infrastructure network)140 连接至销售服务器 110。然后，用户在销售服务器 110 内注册的各种多媒体数据中检索所需的多媒体数据。

如果用户请求购买多媒体数据，则销售服务器 110 向用户提供付费手段，以便对该多媒体数据付费。该付费手段可以是转帐、信用卡或通信费用。

如果用户选择了付费手段，则销售服务器 110 通过诸如服务器银行设施或公共载体之类的用户所选择的手段，连同付费服务器 120 来验证该付费。

在付费之前，付费服务器 120 请求用户输入各种类型的识别信息（例如，信用卡号、用户名、和密码），来验证用户的身份。如果用户输入识别信息，则付费服务器 120 验证识别信息，并进行付费。付费后，付费服务器 120 通知用户该付费是否成功。

如果付费成功，则销售服务器 110 向通信设备 130 发送用户选择的多媒体数据。一旦在通信设备 130 接收到该发送，则用户可以下载该多媒体数据。

在某些情况下，销售服务器 110 或付费服务器 120 可用 SMS（短消息服务）向用户的诸如便携电话之类的另一通信设备发送一个鉴别号码，以便准确验证用户的身份。此时，用户可将接收的鉴别号码输入通信设备 130，来验证他/她是已验证的用户。

这种传统技术的麻烦之处在于：如上所述，用户必须通过基础网络 140 将通信设备 130 连接至销售服务器 110，以便购买多媒体数据，并且必须输入各种类型的识别信息，以便为下载多媒体数据付费。而且，下载多媒体数据花费很长时间。

另外，由于通信设备 130 通过调制解调器连接至基础网络 140，所以必须支付网络连接费。

发明内容

本发明的一个方面在于：缩短购买多媒体数据时消耗的时间，并简化购买程序。

本发明的其它方面和/或优点将部分地在下列描述中阐述、并且部分地从描述中可知、或通过本发明的实施来了解。

本发明提供一种广播接收设备，包括：广播信号交易单元，接收从广播站服务器发送的广播信号，并提取包含在接收的广播信号中的加扰的多媒体数据和元数据；存储单元，存储提取的多媒体数据和元数据；数据发送机/接收机，发送请求解扰密钥的消息，该解扰密钥用于解扰用户想要购买的多媒体数据，并接收解扰密钥；以及控制单元，利用接收的解扰密钥，解扰用户想要购买的多媒体数据。

本发明还提供一种多媒体数据交易方法，所述方法包括：接收从广播站服务器发送的广播信号，并提取包括在接收到的广播信号中的加扰的多媒体数据和元数据；请求解扰密钥，所述解扰密钥用于解扰已提取的用户想要购买的多媒体数据；响应于所述请求，接收解扰密钥；以及利用接收的解扰密钥，解扰用户想要购买的多媒体数据。

本发明提供一种广播接收设备，包括：广播信号交易单元，接收从广播站服务器发送的广播信号，并提取包含在接收的广播信号中的加扰的多媒体

数据；以及数据发送机/接收机，请求和接收解扰密钥，以解扰用户选购的多媒体数据。

本发明还提供一种多媒体数据交易方法，所述方法包括：从由广播站服务器接收的广播信号中提取加扰的多媒体数据；请求并接收解扰密钥，以解扰用户选购的、包含在所述广播信号中的多媒体数据；以及利用解扰密钥，解扰所选的多媒体数据。

附图简述

本发明的这些和/或其它方面和优点将从以下结合附图对实施例的描述中，变得明显和更加易于理解，在附图中：

图 1 说明了传统多媒体数据交易系统；

图 2 说明了根据本发明实施例的多媒体数据交易系统；

图 3 说明了根据本发明实施例的广播接收设备的框图；

图 4 是示出了根据本发明实施例的多媒体数据交易过程的流程图；以及

图 5 是示出了根据本发明实施例的广播接收设备的多媒体数据购买过程的流程图。

具体实施方式

现在将详细参照本发明的实施例，其示例在附图中说明，在附图中相同的附图标记始终指代相同的部件。下面，将通过参照附图描述实施例来说明本发明。然而，本发明可体现为诸多不同的形式，并且不应被解释为限于在此阐述的实施例。

图 2 说明了根据本发明实施例的多媒体数据交易系统。

该系统包括：广播站服务器 210，周期性或非周期性地发送加扰的多媒体数据；广播接收设备 230，接收从广播站服务器 210 发送的广播信号，并向用户提供该广播信号；以及通信服务器 220，向用户提供解扰密钥，来解扰特定多媒体数据。

广播站服务器 210 调制适于每种传输媒介，诸如无线（over-the-air）广播、卫星、或电缆广播之类的各种多媒体数据格式，并发送调制的多媒体数据。此时，使用特定加扰密钥加扰发送的多媒体数据。随着该多媒体数据，广播站服务器 210 可发送各种类型的有关该多媒体数据的信息（以下称为元数据），

诸如多媒体数据的类型（例如，MP3 或 AVI 文件）、多媒体数据的内容（例如，当多媒体数据是 MP3 音乐文件时，歌曲的曲名或歌手的名字）、多媒体数据的价格、以及用于识别多媒体数据的识别信息（例如，序列号）。

从广播站服务器 210 发送的多媒体数据可周期性或非周期性地更新。例如，如果有新的音乐，广播站服务器 210 就可组合 MP3 文件，并在每个预定周期内发送它们，或者只要该组合的 MP3 文件数量大于预定数量，就发送它们。因此，用户可接收诸如电影、音乐、或音乐视频之类的新的多媒体数据。

可从单独的多媒体数据销售商（未示出）接收多媒体数据和元数据。

另外，广播站服务器 210 也可发送要由电视接收的已广播的广播节目，并且可以与广播节目一同有选择地发送该多媒体数据和元数据。例如，可通过单独的广播信道在广播广播节目的时区内发送多媒体数据和元数据，也可通过现存的广播信道在没有发送广播节目的时区内发送它们。

广播接收设备 230 可接收从广播站服务器 210 发送的广播信号，并且包括例如，机顶盒或数字电视。广播接收设备 230 从该广播信号中提取并存储该多媒体数据和元数据。

广播接收设备 230 检查与多媒体数据一同发送的元数据，从而不再存储先前已存储的多媒体数据。

用户可检查存储在广播接收设备 230 中的元数据，以选择他/她想要购买的多媒体数据。

如果用户选择了要购买的多媒体数据，广播接收设备 230 就请求解扰密钥，以解扰相应的多媒体数据。广播接收设备 230 可在解扰密钥请求消息中插入识别信息（下文称为多媒体数据 ID），以识别用户所选择的多媒体数据。此多媒体数据 ID 可包含在从广播站服务器 210 发送的元数据中。

解扰密钥的请求和接收可通过诸如普通电话之类的有线通信系统、或通过诸如移动电话之类的无线通信系统来执行。广播接收设备 230 可包括数据发送机/接收机（未示出），其可以使用诸如 Wi-Fi、GPRS（通用分组无线业务）、DSL（数字用户线）、或电话调制解调器之类的技术，以有线或无线方式进行通信。该数据发送机/接收机可起通信调制解调器的作用，其可打包数据以进行发送，也可接收已打包的数据。因此，广播接收设备 230 可具有由公共载体分配的唯一通信号码，诸如移动电话号码或电话号码，而该公共载体操作通信服务器 220。

如果广播接收设备 230 请求解扰密钥，则提供有线或无线通信服务的通信服务器 220 向广播接收设备 230 发送所请求的解扰密钥。该解扰密钥可预先由多媒体数据提供商或广播站服务器 210 提供。而且，通信服务器 220 可接收用解扰密钥解扰的多媒体数据的多媒体数据 ID。因此，如果通信服务器 220 从广播接收设备 230 接收到了解扰密钥请求消息，它就可使用多媒体数据 ID 检索通信服务器 220 所请求的解扰密钥。

当向广播接收设备 230 的用户征收通信费用时，发送解扰密钥的通信服务器 220 还可加上多媒体数据的购买费用。而且，通信服务器 220 可向广播站服务器 210 通知多媒体数据的购买，以便广播运营商能够计算费用。

在本发明的另一实施例中，通信服务器 220 可加密并发送请求的解扰密钥。用于加密解扰密钥的变量可包含多媒体数据 ID，该多媒体数据 ID 包含在从广播接收设备 230 发送的解扰密钥请求消息中。因此，为了解密该加密的解扰密钥，必须知道该多媒体数据 ID。即使另一广播接收设备截获该加密的解扰密钥，它也不能轻易解密该加密的解扰密钥。

在本发明的另一实施例中，用于加密该解扰密钥的变量可包含广播接收设备 230 的识别信息，诸如广播接收设备 230（具体而言为广播接收设备的数据发送机/接收机）的通信号码。当请求解扰密钥时，该广播接收设备 230 可发送它的识别信息。

当请求解扰密钥时，广播接收设备 230 可加密并发送各种信息（例如，识别信息和多媒体元数据）。

在本发明的实施例中，加密可通过会话密钥执行，该会话密钥由通信服务器 220 和广播接收设备 230 之间的预定鉴别过程产生。因此，通信服务器 220 和广播接收设备 230 可基于初始连接执行鉴别过程。可用诸如 Diffie-Hellman、RSA、EIGamal 或 Elliptic Curve 之类的公共密钥加密技术 (cryptography)，或诸如 DES 或 AES 方法之类的对称密钥加密技术，进行加密，并且可用传统技术进行鉴别。

在本发明的另一实施例中，解扰密钥可通过广播站服务器 210 直接提供给广播接收设备 230。此时，通信服务器 220 可执行广播站服务器 210 和广播接收设备 230 之间的有线或无线通信功能。广播站服务器 210 可验证谁是通过请求解扰密钥的广播接收设备 230 的通信号码来购买多媒体数据的用户，并且当征收广播节目的接收视听费用时，它可加上多媒体数据的费用。

甚至这里，广播站服务器 210 可加密并发送该解扰密钥，并且广播接收设备 230 在请求解扰密钥时，也可一同加密并发送各种类型的信息。而且，可执行广播站服务器 210 和广播接收设备 230 之间的鉴别过程，从而提高通信的安全性（例如，引入上述加密技术和鉴别）。

广播接收设备 230 可利用接收的解扰密钥，来解扰用户所选择的多媒体数据。用户可通过该广播接收设备 230 使用该解扰的多媒体数据，并且他/她可将其发送至另一应用终端。

图 3 说明了根据本发明实施例的广播接收设备 230 的框图。

广播接收设备 230 包括：广播信号处理单元 310，接收并处理从广播站服务器 210 发送的信号；存储单元 350，存储该广播信号的多媒体数据和元数据；数据发送机/接收机 340，请求并接收解扰密钥；以及控制单元 330，利用从数据发送机/接收机 340 接收的解扰密钥来解扰多媒体数据。

另外，广播接收设备 230 可进一步包括：显示单元 320，显示经广播信号处理单元 310 处理的广播节目；以及用户接口单元 360，接收来自用户的控制信息。

广播信号处理单元 310 包括：调谐器 312，调谐到接收从广播站服务器 210 发送的广播信号的频道；解调单元 314，从接收到的、在载波中携带的广播信号中提取原始广播信号；去多路复用器 316，将解调的广播信号分成视频信号、音频信号、例如 EPG（电子节目向导）信息的数字广播信息、和加扰的多媒体数据和元数据；以及解码器 318，解码该视频信号、音频信号和数字广播信息。

如果从广播站服务器 210 发送来的广播信号由调谐器 312 和解调单元 314 接收和处理，则去多路复用器 316 就会将处理后的广播信号分成视频信号、音频信号、数字广播信息以及加扰的多媒体数据和元数据。视频信号、音频信号、和数字广播信息用于广播普通广播节目。解码器 318 可包括例如用于解码该视频信号、音频信号和数字广播信息的 MPEG 解码器。

控制单元 330 在存储单元 350 中存储由去多路复用器 316 分类的多媒体数据和元数据。此时，控制单元 330 检查元数据，从而不再存储该多媒体数据。

在根据本发明另一实施例的广播接收设备 230 中，各种类型的加扰多媒体数据和元数据可在其制造时存储在存储单元 350 中。因此，控制单元 330

可在存储单元 350 中，只存储从去多路复用器 316 传递的新的多媒体数据和元数据。

在发送广播节目的时区内可通过单独的广播信道接收多媒体数据和元数据，或者也可通过现存的广播信道在未发送广播节目的时区内接收。

用户可通过用户接口单元 360 请求检索存储在存储单元 350 中的多媒体数据，而且控制单元 330 可根据用户请求，通过显示单元 320 显示元数据。该显示的元数据可包括多媒体数据的类型、内容和价格（如上所述）。用户可检查显示的元数据，以确定是否要购买该多媒体数据。

数据发送机/接收机 340 可使用诸如 Wi-Fi、GPRS（通用分组无线业务）、DSL（数字用户线）、或电话调制解调器之类的技术，以有线或无线方式进行通信。因此，数据发送机/接收机 340 可起通信调制解调器的作用，该通信调制解调器可打包数据以进行发送，也可接收已打包的数据。广播接收设备 230 可具有从公共载体分配的唯一通信号码，例如移动电话号码或固定的电话号码，而该公共载体操作通信服务器 220。

数据发送机/接收机 340 发送解扰密钥请求消息以请求解扰密钥，该解扰密钥可解扰用户想要购买的多媒体数据。该解扰密钥请求消息可包含多媒体数据 ID（例如，序列号），该多媒体数据 ID 可识别用户所选择的多媒体数据。

数据发送机/接收机 340 在接收解扰密钥后，向控制单元 330 输出解扰密钥。可直接从通信服务器 220 接收已收到的解扰密钥。通信服务器 220 可预先接收该解扰密钥，该解扰密钥可解扰来自多媒体数据提供商或广播站服务器 210 的加扰的多媒体数据。此时，通信服务器 220 也可接收可使用解扰密钥解扰的多媒体数据的多媒体数据 ID。

通信服务器 220 可利用多媒体数据 ID 检索通过广播接收设备 230 请求的解扰密钥。然后，向广播接收设备 230 发送该检索到的解扰密钥。

在本发明另一实施例中，通信服务器 220 可加密并发送广播接收设备 230 请求的解扰密钥。用于加密解扰密钥的变量可包含多媒体数据 ID，该多媒体数据 ID 包含在解扰密钥请求消息中。因此，当解密该加密的解扰密钥时，广播接收设备 230 的控制单元 330 需要在数据发送机/接收机 340 请求解扰密钥时发送给通信服务器 220 的多媒体数据 ID。即使另一广播接收设备接收加密的解扰密钥，它也不能轻易地解密该密钥。

在本发明另一实施例中，用于加密该解扰密钥的变量可包含识别广播接

收设备 230 的信息，例如广播接收设备 230（具体而言为广播接收设备 230 的数据发送机/接收机 340）的通信号码。该广播接收设备 230 可将它的识别信息与解扰密钥请求一起发送。

广播接收设备 230 的数据发送机/接收机 340 也可在请求解扰密钥时，一同加密和发送各种类型信息（例如，广播接收设备 236 的识别信息和多媒体数据 ID）。

因此，广播接收设备 230 可进一步包括可加密和解密数据的加密单元（未示出）。

加密技术可通过会话密钥执行，该会话密钥由通信服务器 220 和广播接收设备 230 之间的预定鉴别过程产生。因此，通信服务器 220 和广播接收设备 230 可在初始连接时执行鉴别过程。可用诸如 Diffie-Hellman、RSA、EIGamal 或 Elliptic Curve 之类的公共密钥加密技术，或诸如 DES 或 AES 方法之类的对称密钥加密技术进行加密，并且可采用传统的鉴别技术。

当向广播接收设备 230 的用户收取通信费用时，通信服务器 220 可加上多媒体数据的费用。而且，通信服务器 220 可向广播站服务器 210 通知多媒体数据的购买，以便广播运营商能够计算多媒体数据的费用。

在本发明另一实施例中，可从广播站服务器 210 直接接收解扰密钥，并且通信服务器 220 可在广播站服务器 210 和广播接收设备 230 的数据发送机/接收机 340 之间执行通信转发(relay)功能，以发送解扰密钥。广播站服务器 210 可验证谁是通过数据发送机/接收机 340 的通信号码来购买多媒体数据的用户，并且当征收广播节目的接收视听费用时，可加上与用户购买的多媒体数据有关的多媒体数据费用。

即使在这种情况下，广播站服务器 210 可加密并发送该解扰密钥，而广播接收设备 230 也可在请求解扰密钥时，一同加密和发送各种类型的信息。而且，鉴别过程可在广播站服务器 210 和广播接收设备 230 之间执行。

如果已经接收到解扰密钥，则控制单元 330 利用该密钥来解扰用户购买的多媒体数据。解扰的多媒体数据可直接被广播接收设备 230 使用。此时，解码器 318 可用于执行该多媒体数据。然而，本发明不限于本实施例，而且广播接收设备 230 可包括单独的应用单元（未示出），以执行解扰的多媒体数据。

而且，用户可向另一个能够使用该多媒体数据的应用终端发送该解扰的

多媒体数据。

图 4 是示出了根据本发明实施例的多媒体数据交易过程的流程图。

首先，在操作 S110，广播站服务器 210 以适于一个或多个传输媒介（例如，无线广播、卫星、和/或电缆广播）的格式，调制各种多媒体数据和元数据，并将其发送。

从广播站服务器 210 发送的多媒体数据可周期性或非周期性地更新。例如，如果有新的音乐，则广播站服务器 210 可组合例如 MP3 文件之类的文件，并在每个预定周期内发送它们，或者只要该组合的 MP3 文件数量大于预定数量，就发送它们。因此，用户可从广播站服务器 210 接收诸如电影、音乐视频或音乐之类的新的多媒体数据。

广播站服务器 210 可从单独的多媒体数据销售商（未示出）获得多媒体数据和元数据。

广播接收设备 230 可接收从广播站服务器 210 发送的广播信号，并且可包括例如，机顶盒或数字电视。在操作 S120，广播接收设备 230 从该广播信号中提取该多媒体数据和元数据，并存储该数据。

在操作 S130，用户可检查存储在广播接收设备 230 中的元数据，以选择他/她要购买的多媒体数据。

在操作 S140，如果用户选择了要购买的多媒体数据，则广播接收设备 230 请求解扰多媒体数据的解扰密钥。解扰密钥的请求和接收可通过诸如普通电话和移动电话之类的通信连接来执行。因此，广播接收设备 230 可包括数据发送机/接收机 340，该数据发送机/接收机 340 可使用诸如 Wi-Fi、GPRS（通用分组无线业务）、DSL（数字用户线）、或电话调制解调器之类的技术，以有线或无线方式进行通信。包括在广播接收设备 230 中的数据发送机/接收机可具有唯一的通信号码，诸如从公共载体分配的移动电话号码或电话号码，而该公共载体操作通信服务器 220。

在操作 S150，如果广播接收设备 230 请求解扰密钥，则提供有线或无线通信服务的通信服务器 220 就向广播接收设备 230 发送所请求的解扰密钥。通信服务器 220 可从多媒体数据提供商或广播站服务器 210 预先获得解扰密钥。

在本发明另一实施例中，通信服务器 220 可加密和发送该请求的解扰密钥。用于加密该解扰密钥的变量可包含多媒体数据 ID，该多媒体数据 ID 包

含在从广播接收设备 230 发送的解扰密钥请求消息中。因此，当解密该加密的解扰密钥时，必须知道该请求的多媒体数据的多媒体数据 ID。因此，即使另一广播接收设备接收了该加密的解扰密钥，它也不能轻易解密该密钥。

在本发明的另一实施例中，用于加密该解扰密钥的变量可包含广播接收设备 230 的识别信息，诸如广播接收设备 230（具体而言为广播接收设备的数据发送机/接收机 340）的通信号码。该广播接收设备 230 可将它的识别信息与解扰密钥请求一起发送。

广播接收设备 230 可加密各种类型的信息（例如，广播接收设备 230 的识别信息以及多媒体元数据），并将其与解扰密钥请求一起发送。

加密技术可通过会话密钥执行，该会话密钥由通信服务器 220 和广播接收设备 230 之间的预定鉴别过程产生。因此，通信服务器 220 和广播接收设备 230 可在初始连接时执行鉴别过程。可用诸如 Diffie-Hellman、RSA、ElGamal 或 Elliptic Curve 之类的公共密钥加密技术，或诸如 DES 方法或 AES 之类的对称密钥加密技术进行加密，并且可采用传统的鉴别技术。

在操作 S160，通信服务器 220 向广播站服务器 210 通知多媒体数据的购买，从而广播运营商能够计算该多媒体数据的费用。

发送解扰密钥的通信服务器 220 在向广播接收设备 230 的用户收取通信费用时，可加上多媒体数据的费用（S170）。

在本发明另一实施例中，解扰密钥可由广播站服务器 210 直接提供给广播接收设备 230。此时，通信服务器 220 可执行通信转发功能，以在广播接收设备 230 和广播站服务器 210 之间发送解扰密钥。广播站服务器 210 可验证谁是通过检查请求解扰密钥的广播接收设备 230 的通信号码来购买多媒体数据的用户，并且当收取广播节目的接收视听费用时，可加上多媒体数据的费用。

即使在这种情况下，广播站服务器 210 可加密并发送该解扰密钥，而且，可执行在广播站服务器 210 和广播接收设备 230 之间的鉴别过程。

广播接收设备 230 可采用接收的解扰密钥，解扰用户所选择的多媒体数据。现将参照图 5 描述广播接收设备 230 的多媒体数据购买过程。

图 5 是示出了根据本发明实施例的广播接收设备的多媒体数据购买过程的流程图。

当在操作 S210 中接收到了广播站服务器 210 发送来的广播信号时，其由

调谐器 312 接收，并由解调单元 314 进行处理。去多路复用器 316 将这些广播信号分成视频信号、音频信号、数字广播信息以及加扰的多媒体数据与元数据。

控制单元 330 在存储单元 350 中存储去多路复用器 316 分类的多媒体数据和元数据（S220）。

在根据本发明另一实施例的广播接收设备 230 中，各种类型的加扰多媒体数据可在其制造时存储在存储单元 350 中。因此，控制单元 330 可只选择和存储未在存储单元 350 中存储的多媒体数据。此操作可通过检视多媒体数据的元数据（例如，序列号）来执行。

可通过单独的广播信道在发送广播节目的时区内接收多媒体数据和元数据，或者也可通过现存的广播信道在未发送广播节目的时区内接收它们。

用户可通过用户接口单元 360 请求检索存储在存储单元 350 中的多媒体数据，而且控制单元 330 可根据用户请求，通过显示单元 320 显示存储在存储单元 350 中的元数据。在操作 S230，用户可检查显示的元数据，并选择要购买的多媒体数据。

数据发送机/接收机 340 可使用诸如 Wi-Fi、GPRS、DSL、或电话调制解调器之类的技术，以有线或无线方式进行通信，并且其可以发送解扰密钥请求消息，来获得可解扰用户选择的多媒体数据的解扰密钥（S240）。数据发送机/接收机 340 可具有由公共载体分配的唯一通信号码，而该公共载体操作通信服务器 220。

解扰密钥请求消息可包括多媒体数据 ID，其可识别用户选择的多媒体数据。

数据发送机/接收机 340 在操作 S250 中接收所请求的解扰密钥。解扰密钥可直接从通信服务器 220 接收。在解扰密钥请求之前，通信服务器 220 可从多媒体数据提供商或广播站服务器 210 接收解扰密钥。

在本发明另一实施例中，通信服务器 220 可加密并发送请求的解扰密钥。用于加密该解扰密钥的变量可包含多媒体数据 ID，该多媒体数据 ID 包含在解扰密钥请求消息中。因此，多媒体数据 ID 必须是已知的，以便解密该加密的解扰密钥。因而，即使另一广播接收设备接收了加密的解扰密钥，它也不能轻易地解密该密钥。

在本发明另一实施例中，用于加密该解扰密钥的变量可包含广播接收设

备 230 的识别信息，例如广播接收设备 230（具体而言为广播接收设备的数据发送机/接收机 340）的通信号码。该广播接收设备 230 可将它的识别信息与解扰密钥请求一起发送。

广播接收设备 230 可加密各种类型的信息（例如，广播接收设备 230 的识别信息和多媒体元数据），并将其与解扰密钥请求一起发送。

加密技术可通过会话密钥执行，该会话密钥由通信服务器 220 和广播接收设备 230 之间的预定鉴别过程产生。因此，通信服务器 220 和广播接收设备 230 可在初始连接时执行鉴别过程。可用诸如 Diffie-Hellman、RSA、EIGamal 或 Elliptic Curve 之类的公共密钥加密技术，或诸如 DES 或 AES 方法之类的对称密钥加密技术进行加密，并且可采用传统的鉴别技术。

通信服务器 220 在向广播接收设备 230 的用户收取通信费用时，可加上多媒体数据的费用。而且，通信服务器 220 可向广播站服务器 210 通知多媒体数据的购买，从而广播运营商能够计算该多媒体数据的费用。

在本发明另一实施例中，可从广播站服务器 210 直接接收解扰密钥，而且通信服务器 220 可在广播站服务器 210 和广播接收设备 230 的数据发送机/接收机 340 之间执行通信转发。广播站服务器 210 可验证谁是通过请求解扰密钥的数据发送机/接收机 340 的通信号码来购买多媒体数据的用户，并且它可在广播节目的接收视听费上加上多媒体数据的费用。

即使这种情况下，广播站服务器 210 可加密并发送该解扰密钥，并且当请求解扰密钥时，广播接收设备 230 也可一同加密并发送各种类型的信息。而且，可执行广播站服务器 210 和广播接收设备 230 之间的鉴别过程。

如果已经接收到解扰密钥，则控制单元 330 利用该解扰密钥来解扰用户购买的多媒体数据（S260）。解扰的多媒体数据可直接由广播接收设备 230 的用户使用。此时，解码器 318 可用于解码该多媒体数据。然而，本发明不限于本实施例，而且广播接收设备可包括单独的应用单元（未示出），以解码该解扰的多媒体数据。

而且，用户可向另一个能够使用该多媒体数据的应用终端发送该解扰的多媒体数据。

如上所述，根据本发明的多媒体数据处理系统和方法，该系统和方法的某些方面在于，可简单化并缩短多媒体数据购买过程，并可降低在连接网络以购买多媒体数据时所征收的网络通信费用。

虽然已经示出和描述了本发明的几个实施例，但是本领域技术人员应该理解：在没有脱离本发明的原理和精神、由权利要求及其等同物所定义的范围的前提下，可以对这些实施例进行改动。示例实施例将被认为仅仅在于说明的意义，而不是出于限定的目的。因此，本发明的范围不由本发明的详细描述而是由权利要求及其等同物来定义，而且范围之内的全部差异将被视为包含在本发明内。

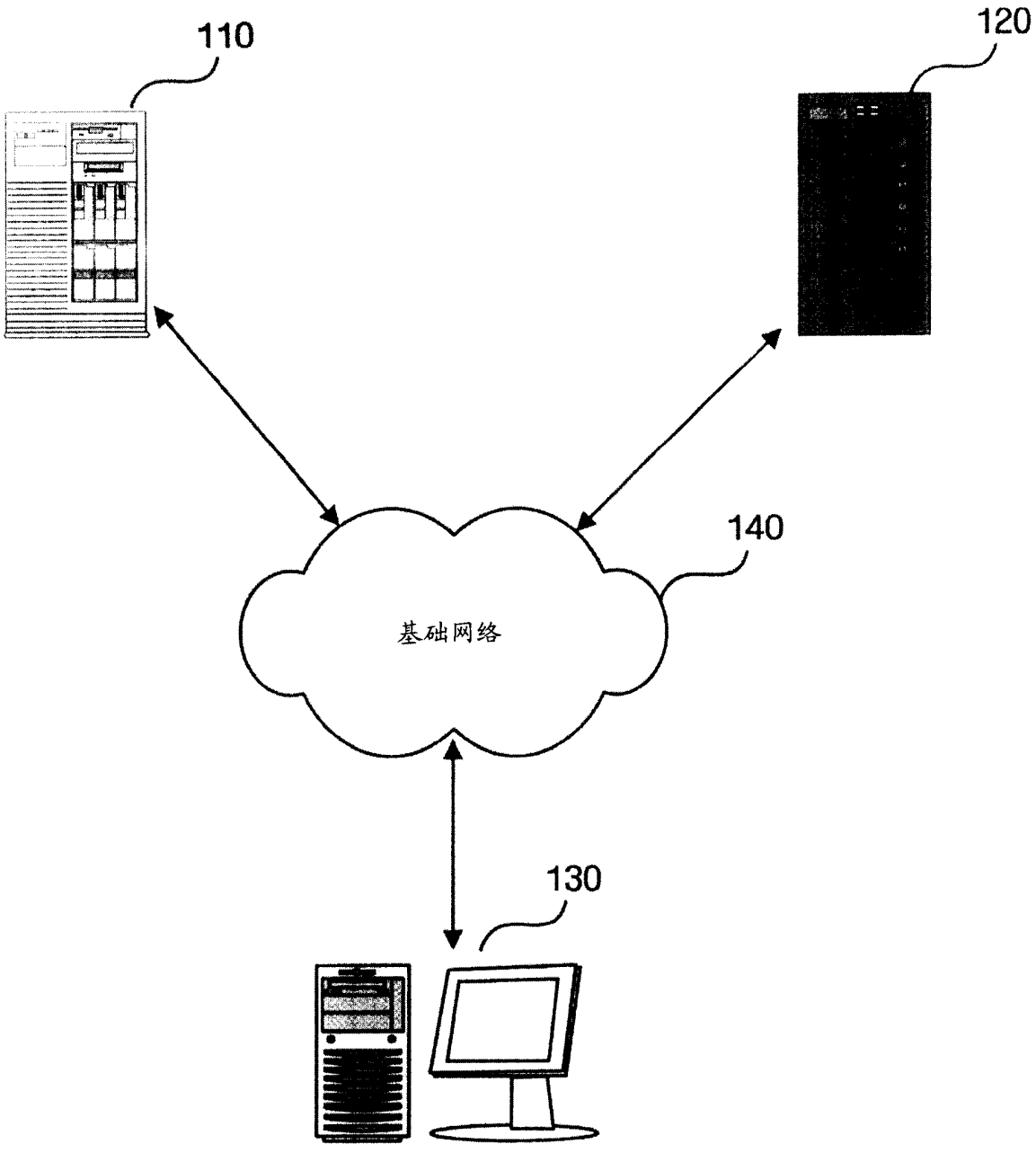


图 1

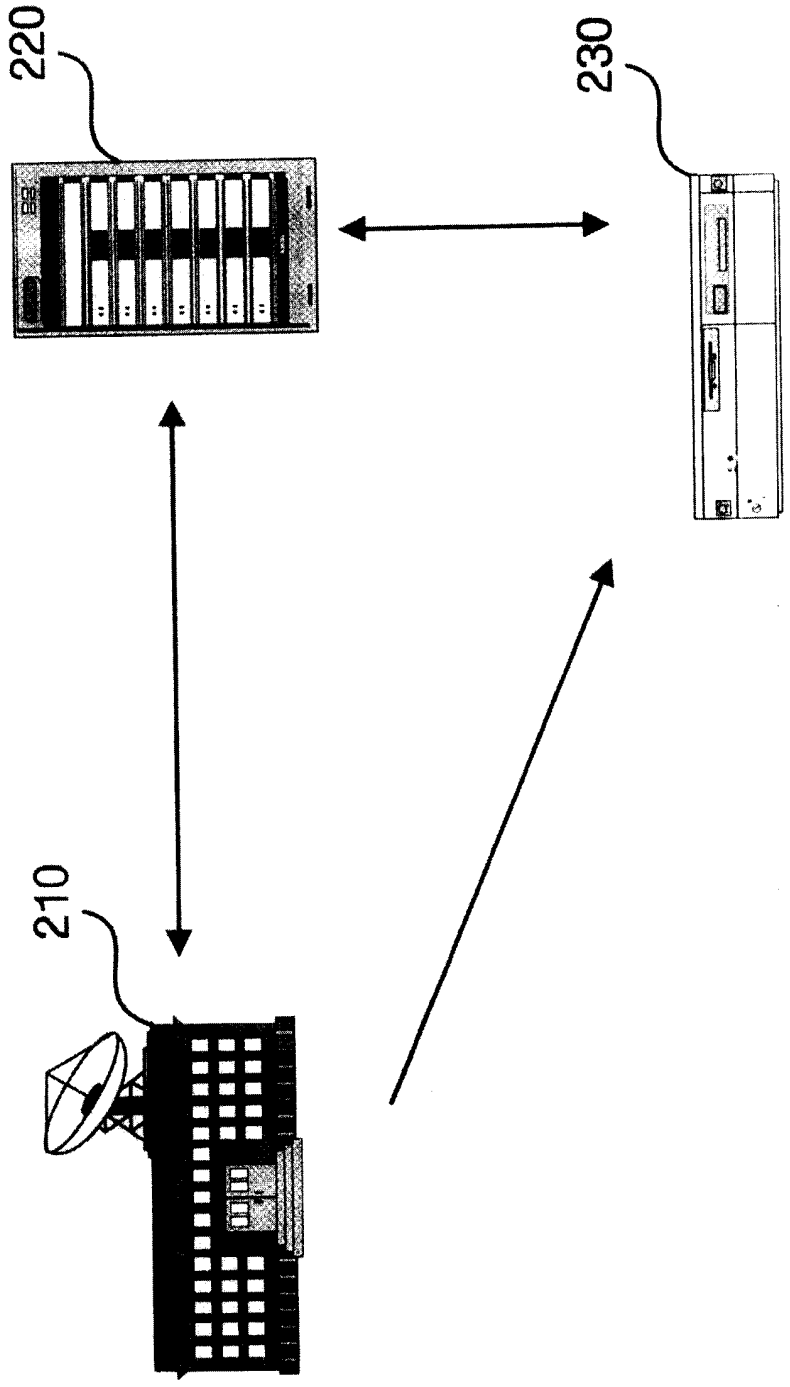


图 2

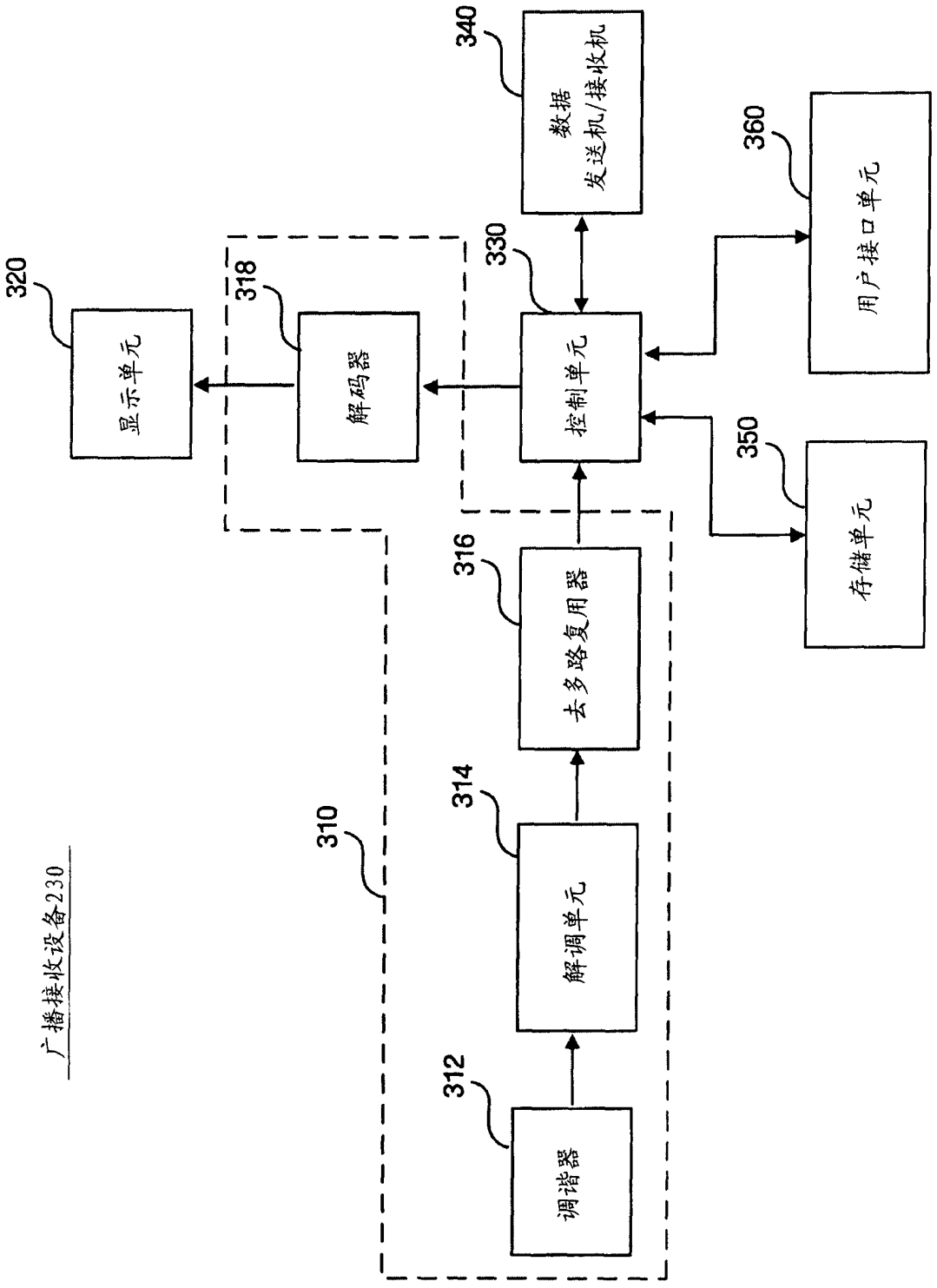

广播接收设备230
310
312
调谐器
314
解调单元
316
去多路复用器
318
解码器
320
显示单元
330
控制单元
340
数据
发送机/接收机
350
存储单元
360
用户接口单元

图 3

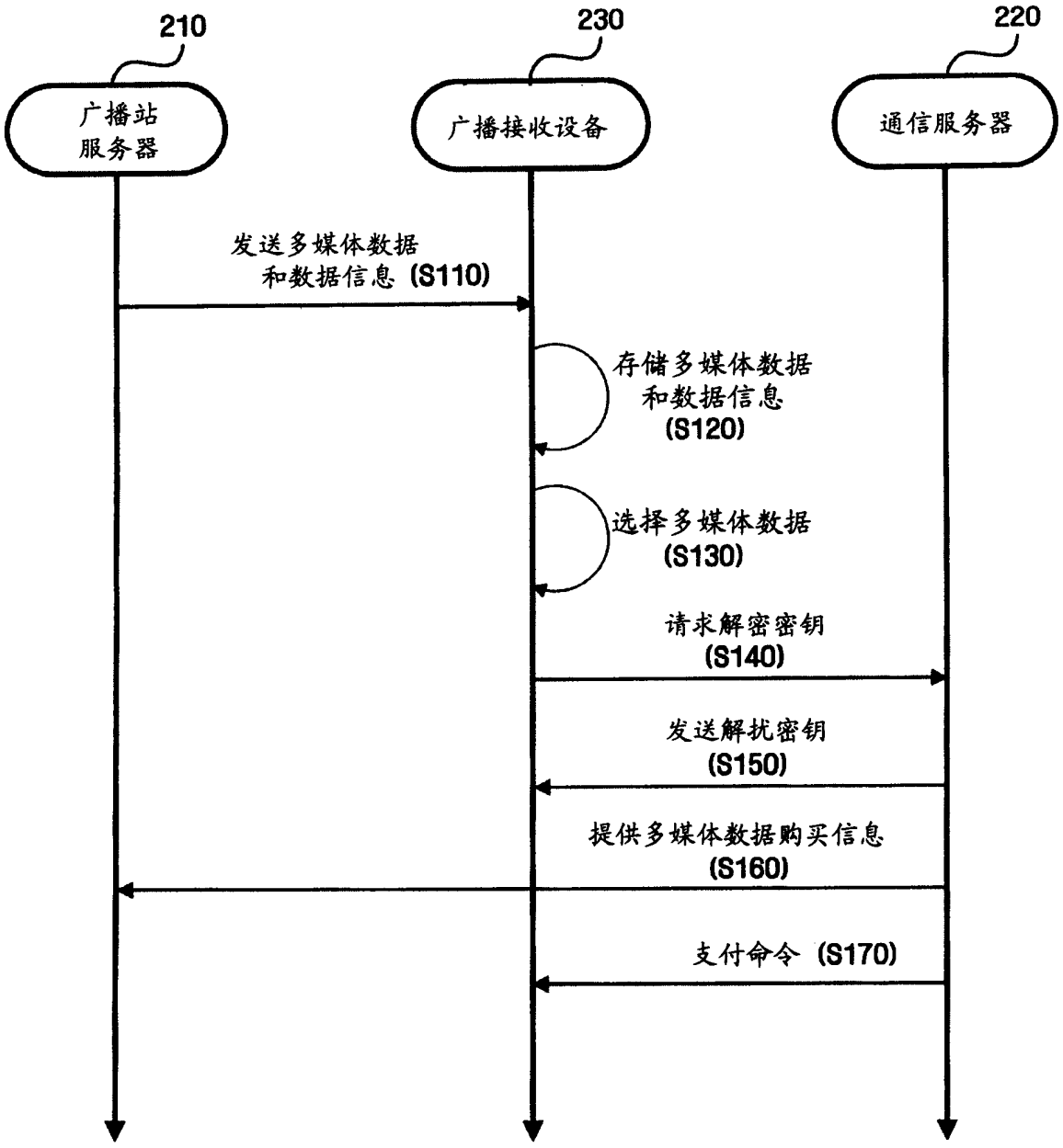

210
230
220
广播站
服务器
广播接收设备
通信服务器
发送多媒体数据
和数据信息 (S110)
存储多媒体数据
和数据信息
(S120)
选择多媒体数据
(S130)
请求解密密钥
(S140)
发送解扰密钥
(S150)
提供多媒体数据购买信息
(S160)
支付命令 (S170)

图 4

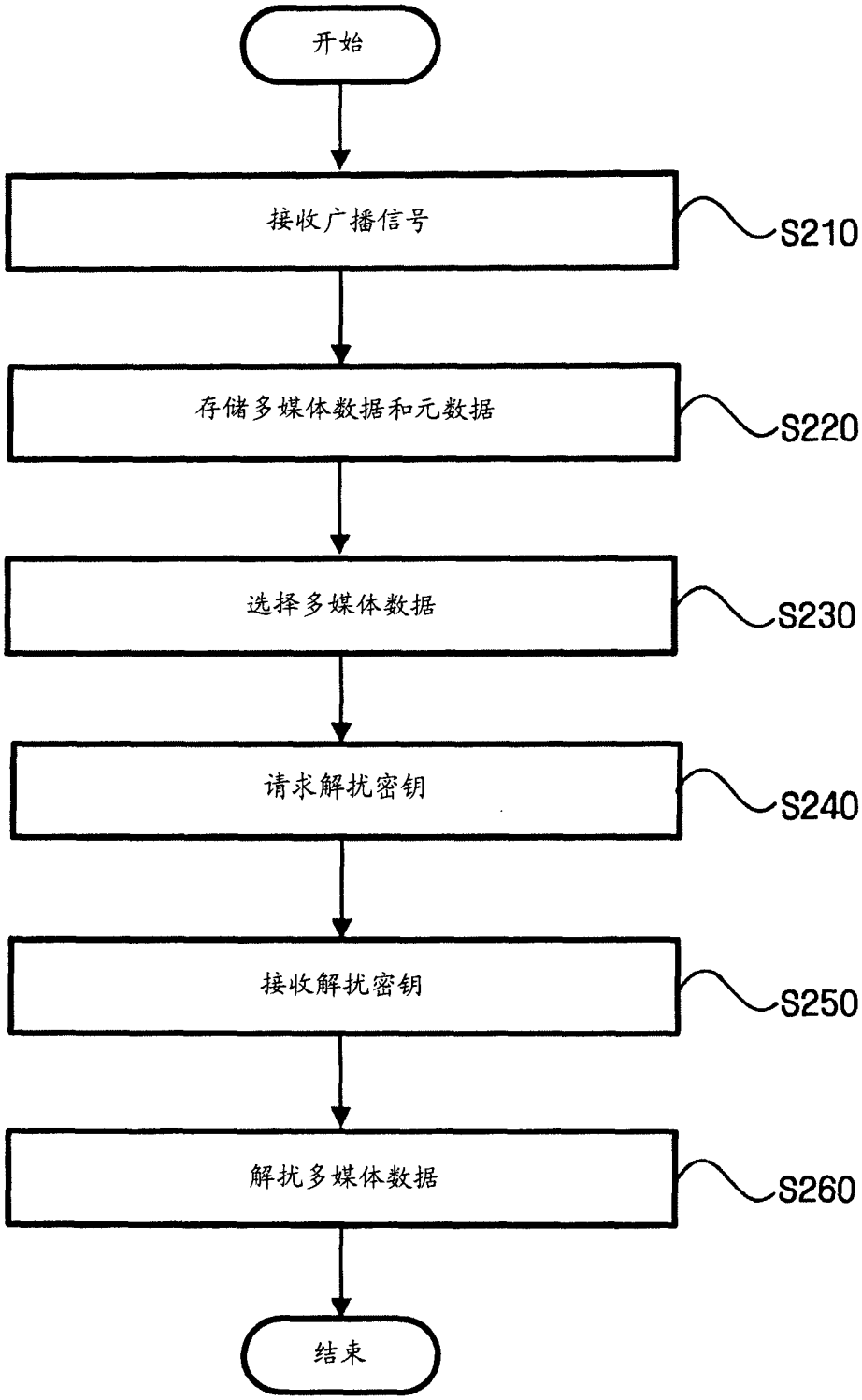

开始
接收广播信号
S210
存储多媒体数据和元数据
S220
选择多媒体数据
S230
请求解扰密钥
S240
接收解扰密钥
S250
解扰多媒体数据
S260
结束

图 5