



[12] 发明专利说明书

[21] ZL 专利号 92103389.3

[51] Int.Cl⁶

H04N 7 / 167

[45]授权公告日 1996 年 2 月 7 日

[24]颁证日 95.10.22

[21]申请号 92103389.3

[22]申请日 92.3.28

[30] 优先权

[32]91.3.29 [33]US[31]677,460

[73]专利权人 亚特兰大科研公司

地址 美国佐治亚州

[72]发明人 K·甘米 R·K·米田 胡业新

W·谢尔德里克

H04L 9 / 00

[74] 专利代理机构 中国专利代理(香港)有限公司

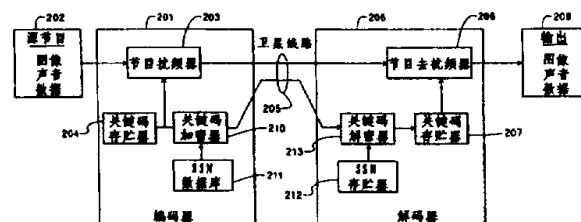
代理人 程天正 栾本生

权利要求书 9 页 说明书 33 页 附图页数 12 页

[54]发明名称 用于数字式可改进的电视信号解码器的独立外部安全性模块

[57]摘要

用于传输信号的安全系统包括：(1) 对信号编码的编码装置 (701)，它包括：对信号扰频并输出被扰频的信号和用于对被扰频信号去除扰频的关键码的扰频装置 (703)，连接到此扰频装置上的第一关键码加密装置 (710)，和第二关键码加密装置 (711)；和 (2) 用来接收并对被扰频信号去除扰频的解码装置 (706)，它包括：第一关键码解密装置 (719)，一个包含第二关键码解密装置 (718) 的可更换的安全模块 (714)，连接到第一和第二关键码解密装置上的信号去扰频装置 (708)。



1. 一种用于接收信号并对信号去除扰频的解码器，所述信号是用密钥进行扰频后的信号，所述的密钥用第一机密序号代码和第二机密序号代码之中至少一个进行了选择性的加密，其特征在于所述的解码器包括：

第一密钥解密装置(713)，当用第一机密序号代码对密钥进行选择加密时，使用该装置；

第二密钥解密装置(718)，当用第二机密序号代码对密钥进行选择加密时使用该装置，所述的第一和第二密钥解密装置之一包括在可更换的安全模块(714)中，安全模块(714)可拆卸地连接在所述解码器上，而其它则包括在解码器的固定安全部件(719)之中；

控制装置，用于操纵所述第一和第二密钥解密装置中的至少一个，产生出解密的密钥，将该解密的密钥用于对信号去除扰频。

2. 根据权利要求1的解码器，其特征在于所述的控制装置操纵第一密钥解密装置，对选择加密的密钥进行解密以产生解密的密钥。

3. 根据权利要求1的解码器，其特征在于所述的控制装置操纵第二密钥解密装置，对选择加密的密钥进行解密，以产生解密的密钥。

4. 根据权利要求1的解码器，其特征在于所述的控制装置操纵第一密钥解密装置，对选择加密的密钥进行解密，以产生部分解密的密钥，然后，操纵第二密钥解密装置，对所述部分解密的密钥进行解密，以产生完全解密的密钥。

5. 根据权利要求1的解码器，其特征在于所述的控制装置可工作

在第一、第二和第三种模式中的一种；

当工作在第一种模式时，所述的控制装置操纵所述第一密钥解密装置，对选择加密的密钥码进行解密，以产生解密的密钥码；

当工作在第二种模式时，所述的控制装置操纵所述第二密钥解密装置，对选择加密的密钥码进行解密，以产生解密的密钥码；

当工作在第三种模式时，所述的控制装置操纵第一密钥解密装置，对选择加密的密钥码进行解密，以产生部分解密的密钥码，然后，操纵第二密钥解密装置，对所述部分解密的密钥码进行解密，以产生完全解密的密钥码。

6. 根据权利要求1 的解码器，其特征在于所述的解码器还包括有信号去扰频装置(708)，利用所述的解密密钥码对所述扰频信号去除扰频。

7. 根据权利要求1 的解码器，其特征在于，还包括分别连接到所述第一和第二密钥解密装置(713,718) 的第一和第二密钥存贮装置(707,720)，用于存贮所述解密的密钥码。

8. 根据权利要求1 的解码器，其特征在于，还包括分别连接到所述第一和第二密钥解密装置(713,718) 的第一和第二机密代码存贮装置，用于存贮第一和第二机密序号代码。

9. 根据权利要求8 的解码器，其特征在于，在可更换的安全模块(714) 和固定安全部件(719) 中，所述第一和第二机密序号代码存贮装置还包括一安全装置，它只允许所述第一和第二密钥解密装置(713,718) 读取所述各自的第一和第二机密序号代码存贮装置(712,717) 的内容。

10. 根据权利要求1 的解码器，其特征在于所述的信号是电视信号。

11. 根据权利要求1 的解码器，其特征在于所述的信号是B-MAC

型电视信号。

12. 根据权利要求1的解码器,其特征还在于还包括电话接口装置(875),用于传输数据到电视提供者和从电视提供者接收数据。

13. 根据权利要求12的解码器,其特征还在于由可更换的安全模块(714)通过所述电话接口装置(875)来传输用户输入数据。

14. 根据权利要求1的解码器,其特征还在于,将所述的第一机密序号代码分配给所述解码器(706)的固定安全部件(719)。

15. 根据权利要求1的解码器,其特征还在于将所述的第二机密序号代码分配给所述可更换的安全模块(714)。

16. 根据权利要求1的解码器,其中选择加密的关键码是用第一机密序号代码,第二机密序号代码,或用两者进行加密的;其特征还在于所述的解码器还包括一转换装置(708),响应于探测到的信号,在固定安全部件(719)和可更换安全模块(714)之间自动地进行转换,对选择加密的关键码进行有效的解密,产生解密的关键码。

17. 根据权利要求1的解码器,其中选择加密的关键码是用第一机密序号代码,第二机密序号代码,或用两者进行加密的;其特征还在于,所述的解码器还包括一转换装置(708),根据接收到的信号,在第一和第二关键码解密装置(713,718)之间自动地进行转换,对关键码有效地进行解密。

18. 根据权利要求1的解码器,其特征还在于所述的解码器接收对单个解码器或一组解码器编址的合成数据包,所述合成数据包包括:

第一数据包(9a),含有对单个或一组解码器编址的未加密数据;

第二数据包(9c),含有用于确定在解码器中是否启动了第一和第二关键码解密装置(714,719)中的至少一个的未加密数据;

第三数据包(9d),含有解码器所用的被加密数据。

19. 根据权利要求18的解码器,其特征还在于所述的合成数据包还

包括第四数据包(9b)，含有未加密的数据，用于确定当第三数据包是被两次加密时通过第一和第二密钥解密装置对第三数据包解密的顺序。

20. 根据权利要求1的解码器，其特征在于还包括：

解码电路(1368)，内中包含有第一和第二密钥解密装置(1314, 1319)；

解调器(1366)；

接收装置(1391)，用于接收带有多个地址的多个压缩数字信号，每个地址对应一个特定的数字信号；

选择装置(1392)，通过识别特定的地址来选择特定的数字信号；

解压缩装置(1393)，用于对选择的数字信号进行解压缩；

选择连接装置(1397)，将解码电路(1368)选择地连接到解压缩装置(1393)和解调器(1366)之一。

21. 根据权利要求20的解码器，其特征在于还包括连接在选择装置(1392)和解压缩装置(1393)之间的用于对数字信号解密的装置(1399)。

22. 根据权利要求1的解码器，其特征在于所述可更换的安全模块包括：

第二密钥解密装置；

连接到所述第二密钥解密装置，用于从解密的关键码中产生解码器控制信息的装置，该控制信息可用于对扰频信号解扰，

安全装置，确保第二密钥解密装置产生的解密关键码只能由产生解码器控制信息的装置来使用。

23. 在包括第一和第二密钥解密装置的解码器中的一种对信号的解码方法，其中将所述第一和第二密钥解密装置之一安装在可更换的安全模块中，而将其它的东西安装在固定安全部件中，其特征在于

于该方法包括步骤:

当用第一机密序号代码对密钥码进行选择加密时, 选择地起动第一密钥解密装置, 根据第一机密序号代码处理选择加密的密钥码;

当用第二机密序号代码对密钥码进行选择加密时, 选择地起动第二密钥解密装置, 根据第二机密序号代码处理选择加密的密钥码;

对第一和第二密钥解密装置中的至少一个的操作进行控制, 以产生解密的密钥码。

24. 根据权利要求23的方法, 其特征在于控制解码器以第一, 第二和第三种模式之一工作的控制步骤包括:

当解码器是以第一种方式工作时, 起动第一密钥解密装置, 对选择加密的密钥码进行解密, 产生解密的密钥码;

当解码器是以第二种方式工作时, 起动第二密钥解密装置, 对选择加密的密钥码进行解密, 产生解密的密钥码;

当解码器是以第三种方式工作时, 起动第一密钥解密装置, 对选择加密的密钥码进行解密, 产部分解密的密钥码, 然后起动第二密钥解密装置, 对部分解密的密钥码进行解密, 产生解密的密钥码。

25. 根据权利要求23的方法, 其特征在于还包括根据解密的密钥码产生解码器控制信息的步骤, 可将该解码器控制信息用于对抗扰信号进行解扰。

26. 根据权利要求23的方法, 其特征在于还包括在下面两种情况的至少一种中保证数据访问的步骤, 所述的两种情况是: (1) 确保第一机密序号代码只能由第一密钥解密装置读出; (2) 确保第二机密序号代码出能由第二密钥解密装置读出。

27. 根据权利要求23的方法, 其特征在于所述的信号是电视信号。

28. 根据权利要求23的方法, 其特征在于所述的信号是B-MAC 型电视信号。

29. 根据权利要求23的方法, 其特征在于还包括经过电话接口装置(875) 传送数据到电视提供者和从电视提供者接数据的步骤。

30. 根据权利要求29的方法, 其特征在于还包括步骤: 在可更换的安全模块中准备用户输入数据, 通过所述电话接口装置传送。

31. 根据权利要求23的方法, 其特征在于还包括步骤: 根据检测的信号, 在固定安全部件(719) 和可更换安全模块(714) 之间有效地进行转换, 以便有效地解密选择加密的关键码, 产生解密的关键码。

32. 根据权利要求23的方法, 其特征在于还包括步骤: 根据检测到的信号, 在第一和第二关键码解密装置(713, 718) 之间自动地进行转换, 以便有效地解密选择加密的关键码, 产生解密的关键码。

33. 根据权利要求23的方法, 其特征在于还包括步骤:

提供包括所述选择加密的关键码和在第一源处的所述第一及第二机密序号代码的用户信息;

在一组第二源处提供一组节目信号;

将所述用户信息传送给第二源;

将所述用户信息与所述节目信号结合, 以产生结合的信号;

把该结合的信号传送给所述的解码器。

34. 根据权利要求23的方法, 其特征在于还包括接收合成数据包 的步骤, 所述的合成数据包包括:

第一数据包(9a), 含有用于寻址单个或一组解码器的未加密数据;

第二数据包(9c), 含有用于确定在解码器里的第一和第二关键码解密装置(714, 719) 之中是否至少一个被启动的未加密数据;

第三数据(9d), 含有解码器所用的加密数据。

35. 根据权利要求34的方法, 其特征在于所述的合成数据包还包括第四数据包(9b), 当第三数据包是被两次加密的情况下, 第四数据包中含有用于确定由第一和第二关键码解密装置对第三数据包解密的

顺序的未加密数据。

36. 根据权利要求23的方法, 所述的解码器还包括其中装有第一和第二密钥解密装置的解码电路(1368), 其特征在于所述的方法还包括步骤:

接收多个带有多个地址的压缩数字信号(1391) 每个地址对应一个特定的数字信号;

通过鉴别特定的地址来选择特定的数字信号(1392);

对选择的数字信号进行解除压缩;

将解除压缩的信号(1393) 和解调信号(1366) 选择地连接(1367) 到解码电路(1368)。

37. 根据权利要求36的方法, 其特征在于还包括一个对选择数字信号解密的步骤。

38. 根据权利要求23的方法, 其特征在于还包括步骤:

从解密的关键码中产生解码器控制信息, 该解码器控制信息用于对抗频信号去除扰频;

保证将第二密钥解密装置产生的解密关键码只用于产生解码器控制信息。

39. 根据权利要求23的方法, 其中将第二密钥解密装置装在可更换的安全模块中, 初始的控制步骤只起动第一密钥解密装置, 起始用另一第一机密序号代码加密一新的关键码, 然后, 再用第二机密序号代码加密, 产生新的选择加密的关键码, 该方法的特征在于还包括步骤:

在所述第一密钥解密装置中, 用所述的另一第一机密序号代码, 对新的选择加密关键码进行解密, 产生部分解密的关键码;

在所述第二密钥解密装置中, 用所述第二机密序号代码, 对所述部分解密的关键进行解密, 恢复所述新的关键码, 其后, 只用第二

机密序号代码对后来的新的密钥进行加密，当只用第二机密序号代码对后来的新的密钥进行加密时，则控制的步骤只起动第二密钥解密装置。

40. 一种与卫星转发器(1205)相结合的系统，其特征在于，该系统包括：

主上行线，能够将一组节目信号发送到所述卫星转发器；

节目信号的第一源，该第一源将发送给所述卫星转发器的第一节目信号供给主上行线，作为该组节目信号之一，该第一节目信号包括用户信息；

附加节目信号的至少一个附加源，第一附加源将发送给所述卫星转发器的第一附加节目信号供给主上行线，该第一附加源包括：(i) 用于从第一节目信号中提取用户信息的装置；(ii) 用于将所述用户信息插入第一不同节目信号以形成所述第一附加节目信号的装置。

41. 根据权利要求40的系统，其特征在于：

所述的卫星转发器(1205)将从主上行线接收的一组节目信号重新发送出去，作为一组重新发送的节目信号；

用于提取用户信息的装置包括：(i) 用于接收对应于第一节目信号的第一重发节目信号的装置，(ii) 用于拆开除了用户信息之外的所有信号部分的装置；

用于插入用户信息的装置，该装置包括：(i) 用于将用户信息多路化到第一不同节目信号上以形成第一附加节目信号的装置，(ii) 用于对主上行线提供第一附加节目信号的装置，作为一组节目信号的附加信号发送给所述卫星转发器。

42. 根据权利要求40的系统，其特征在于所述的用戶信息包括系统数据包和编址数据包中的至少一个。

43. 根据权利要求40的系统，其特征在于，所述一组节目信号中

的至少一个是电视信号。

44. 根据权利要求40的系统，其特征在于，所述一组信号中的至少一个是B-MAC 型电视信号。

45. 在按照权利要求40的与卫星转发器(1205)相结合的系统中，一种发送用户信息的方法，其特征在于包括步骤：

以第一源提供所述用户信息；

以一组第二源提供一组节目信号；

将所述用户信息发送给所述的一组第二源；

将所述用户信息与一组节目信号结合，产生一组结合的信号，每一节目信号对应于所述的一组第二源中的各个第二源；

将所述的一组结合信号发送给至少一个用户。

用于数字式可改进的电视信号解码器
的独立外部安全性模块

本发明总的涉及扰频和传输系统，具体来说涉及广播、卫星或有线电视传输系统的电视信号解码器的外部安全性模块。另外，更明确地说本发明涉及一种将用户信息传输到收费电视信号分配器的方法，和变换电视信号解码器以接受数字电视信号的方法。本发明具体应用了B-型多通道模拟分量(B-MAC) 卫星传输，但也可用于NTSC(国家电视标准委员会)，PAL，SECAM，或建议的高清晰度电视制式。还有，本发明的扰频系统可用于一些相关领域：如电子银行存，定网络，电话交换系统，蜂窝式电话网络，计算机网络，等等。该系统可特别应用于所谓的“有条件使用”的多频道电视系统，在这种系统中观看者可以收看几个“基本的”频道，一个或多个需要“额外费用”或附加费的频道，以及“计节目付费”(pay-per-view) “或自动计节目付费”(impulse pay-per-view) 节目。

在收费电视系统中，收费电视服务提供者一般的是通过扰频保护信号防止未经批准的用户和侵权者使用。

对于下面的讨论及本发明的目的，“订户”指付电视服务费的人。“订户”因而可以是在自己家中具有解码器的个人用户，或可以是系统操作人员(如当地有线电视操作人员)，或小网络的操作人员(如旅店/汽车旅店操作人员，他具有用于旅店或汽车旅店的所有电视的中心解码器)。另外，“订户”可以是工业用户，如与本申请是同一受让人的美国专利4,866,770 中所述，在此引用作为参考。

对于本发明的目的，将网络定义为包括节目源（如收费电视提供者），编码器（有时称为“前端”），传输装置（卫星，电缆，无线电波，等等）和如上所述用户所使用的一系列解码器。将一种系统定义为节目源、编码器、传输装置、和信号接收解码器。将这种系统模型用来描述在网络中的个人解码器如何与编码器互相配合。

扰频过程是通过一个本身可以由加密的关键码来完成的。对每个希望收到信号的用户提供一个解码器，该解码器有其独有的鉴别数码。只要交了合适的服务费，就可给解码器分配有一个关键码用于对扰频的信号进行解。通过将与关键码（和其它信息）结合工作的去除扰频算法分配给付款用户来实现批准，而不把这种信息分配给非用户及所有可能的侵权者。

关键码可以用隐函在正常电视传输中的数据信号形式与解码器的鉴别数码结合而被传输。在典型的电视信号中，有所谓的在每一场里出现的“垂直消隐间隔”（VBI）和在色度和亮度信号之间的每一行中发生的“水平消隐间隔”（HBI）。各种其它信号可以在垂直和水平消隐间隔中的“带内”传送，包括附加的声道，数据，和电传信息。关键码可以象已有技术熟知的那样被嵌在这些“消隐间隔”中。请注意美国专利4,829,569（转让给本申请的同一受让人），在此引入作为参考，该专利表明了这样一些数据怎样被嵌在B-MAC信号中。另外，关键码可以在分离的数据通道上或甚至在电话线上“带外”传送。

维持有条件使用电视网络中的安全性取决于下面一些要求：

(i) 信号扰频技术必须足够复杂以保证直接加密图攻击不可行。

(ii) 分配给批准的解码器上的关键码不能被读出和转移到其它解码器上。

第一个条件可以通过实际的扰频算法来满足，现在可以得到的如DES（数据加密标准）或相关的算法来满足。

第二个条件要求电视信号解码器中某些装置的物理安全性，并且相当难以满足。这样一个装置必须防止观察到关键码的解密过程和部分解密后的关键码信号。

图1 表示一个用于卫星传输的已有技术的有条件使用系统。在编码器101 中，将包括图像信号、声音信号和数据的源节目信息102 在节目扰频器103 中利用来自关键码存贮器104 的关键码进行扰频。所采用的扰频技术可以是该领域公知的任何一种这类技术，其关键码可以是用于扰频过程的信号或代码数字，该信号或代码数字在解码器106 的节目去扰频器108 中需要“打开”节目或对节目去掉扰频。实际上，可以用一个关键码(单层加密) 或多于一个关键码(未示出)。关键码通常随时间变化(如按月) 以挫败侵权者。被扰频的节目和关键码通过卫星线路105 传输，并由有条件使用解码器106 接收。解码器106 从被接收的信号中恢复关键码，把它贮存在关键码存贮器107 中，并把它用于节目去扰频器108 中，节目去扰频108 对通过卫星线路105 接收的扰频节目去除扰频，输出去除了扰频影响的节目109。这种系统不是完全安全的，这是由于关键码不设障碍地通过通道传输并可能被侵权者得到并再现。

参考已有技术图2，为克服此种困难，将分配过程中保护关键码的方法引进到图1 的系统中。在传输前，在节目扰频器203 中将用于对源节目202 扰频的关键码从关键码存贮器204 中取出，并且在关键码加密器210 中，将该关键码本身用来自秘密序号代码数据库211 的秘密序号代码(SSN) 加密，秘密序号代码数据库211 包括所有被认可用户的秘密序号代码表。这些秘密序号可以与上面提到的用于译码器网络的每个译码器独有的鉴别数字相关。现在已用关键码对源节目扰频，并且关键码本身也已用秘密序号加密。因而，与图1 的系统相比在传输过程中该关键码不会被泄露秘密或发现。为了对节目去掉扰频，

侵权者必须首先得到被个可的解码器的秘密序号，把它与已适当加密的关键码配合，对该关键码解密，然后对节目去掉扰频。该秘密序号被设置在解码器206 中，例如，在制造过程中置于解码器206 内的SSN 存贮器212 中。这样，只要解码器206 在物理上保持安全性，该秘密序号不会被侵者得到。

每个秘密序号为了它的安全性对一个解码器是唯一的，或至少对一组解码器是唯一的，通过对数据库211 的循环，将加密的关键码分别传送到每个解码器中，数据库包含了在编码器201 中该网络的所有秘密序号，并在编址数据包中形成了对网络中的每个被认可的解码器分别进行寻址的关键码分配信息，单个解码器通过读出附加在该加密关键码上的关键码分配信息识别出何时接收到它的加密关键码，一个典型的编址数据包绘在图9 上，将在下面更详细地描述。

在已知的B-MAC 系统中，关键码分配在一个编址数据包中，靠其独有的鉴别数码对特定的用户解码器进行寻址。一般将该编址数据包插到垂直消隐间隔的第4 到第8 行中。每个编址数据包一般对一个单独的解码器编址。由于在一个B-MAC 或NTSC电视信号中每秒钟产生60 场(每两个隔行场组成的30 帧) ，以每场一个编址数据包的速率，每秒钟可以对60 个不同的解码器(或解码器组) 寻址，或3600 个/分钟，215,000 个/小时，和5,000,000 个/天。由于每个解码器只有当服务等级或加密等级变化时才需要寻址，所以在大系统中对每个解码的单独寻址其至有足够的多帧。通过每场传输多于一个的编址数据包可以增加解码器的寻址速率。附加的数据包可以插到每帧的垂直消隐间隔或水平消隔间隔中。可能被寻址的解码器的总数目是解码器地址可利用的数据位数的函数。B-MAC 格式一般使用28 位作为解码器地址，允许超过268,000,000 个可能的解码器地址。现将美国先进电视系统委员会报告T2 /62 ， “多通道模拟分量电视广播系统参数说明”，在此

引入作为参考，它描述了一个B-MAC 信号中的数据格式。

在接收到编址数据包之后，关键码解密器213 利用存贮在SSN 存贮器212 中的秘密序号代码对关键码解密。如果要终止对网络中任何一个解码器206 的服务，只需简单地从SSN 数据库211 中删去该秘密序号代码，这样从下一个关键码周期开始，解码器206 就被解除认可。

在如图2 所示的这样一个解码器中，收费电视提供者必须依靠解码器盒本身的物理安全性来防止侵权者读取或改变秘密序号代码和在解码器中的关键码存贮器，或发现关键码的解密过程。为了提供必要的物理安全性，解码器盒可以配备防止破坏的封印，尤其是配备带帽螺钉和扣紧件，或其它防破坏的包装以使得解码器不易发生物理性损害。付款用户可以意识到破坏解码器将改变防破坏封印或毁坏解码器，并会在下一次的检查中被发现。

依靠解码器的物理安全性来保持系统的安全性有几个缺点。首先，收费电视提供者必须保持对网络的所有解码器的所有权及对它的控制，然后把解码器出租或租赁给付款用户。收费电视提供者因而有责任保养所有的解码器，并必须维持昂贵的另部件库存和维修人员。另外，为了开始服务，一个服务人员必须亲自到付款用户居住地去安装解码器。在收费电视卫星系统中，这样的安装和服务对于可能位于世界各地的遥远安装可能是相当昂贵的。另外，如果一个侵权者在分配过程中或从一个单独付款用户家中偷得一个解码器，解码器的物理安全性将被破坏而且他也不怕被发现。

因此，图2 的系统只有在下列条件下才是安全的：

(i) 必须不可能读出或修改SSN 和解码器中的关键码存贮器。

(ii) 必须不可能发现关键码的解密过程，或解码器的4 个元件(207, 208, 212 和213) 之间的连线。

达到这两个目的的一种方法是采用一个所谓的“安全微处理机”。

图3 表示一个典型已有技术微处理机320 的方框图，该微处理机带有处理器321 、程序存贮器322 、存贮器地址总线328 、存贮数据326 和存贮数据总线327 。在这样一个设备中，根据贮存在程序存贮器322 中的程序处理输入数据323 ，产生输出数据324 。程序存贮器322 可以通过存贮数据总线327 “读出”。即是，通过存贮器地址总线328 送进到程序存贮器322 中的相继增加的存贮地址325 ，使该存贮器步进。来自存贮数据总线327 的输出存贮数据326 将展现微处理机320 的所有程序内容，包括任何一种被贮存的去扰扰频的算法和秘密号代码。有了这些数据，一个侵要者能很容易地对一个通过图2 的卫星线路205 传输的关键码解密。

图4 表示根据本发明的一个方面用来保护算法及秘密序号代码的一个理想的安全微处理机420 的方框图。图4 的安全微处理机420 与图3 微处理机320 的主要区别在于其没有存贮地址总线328 和存贮数据总线327 ，因而没有办法为了读出或写入的目的一步步地前进程序存贮器422 。存贮器的访问是由处理器421 根据不能改变的掩模编程代码来执行。所有输入的数据423 作为需要处理的数据被处理，所有的输出数据424 是处理输入数据423 的结果。没有通过数据输入来读出或改变程序存贮器422 内容的手段。

一些现代装置很接近这种理想的安全微处理机。然而，有一个要求造成了不同于这种理想的安全微处理机。制造后，必须有一个机构可以用来把解码器特有的秘密序号代码430 及解密算法434 写入存贮器422 。如果该装置能为侵权者得到，他为了非法复制的目的可能要改变秘密序号代码。因而，在秘密序号代码已被输入之后必须永久性地损坏这个装置。

多种不同技术可用于损坏写入该存贮器的装置。可使安全微处理机420 设有在芯片上的可熔断的数据线路431 ，软件锁，或类似的使

秘密序号代码430 和去扰频算法434 在制造时加进存贮器422 上的装置。然后，例如，毁不虚线所示的可熔断的线路，使得侵权者无法得到存贮在程序存贮器422 中的去扰频算法434 或秘密序号代码430 。

在另一个实施例中，图4 中的微处理机可用一个“ E^2 位”保险。当有人企图读出存贮器的内容时，“ E^2 位”（一种形式的软件锁）将使整个存贮器（通常是EEPROM）被擦去。“ E^2 位”具备两个优点；第一，使存贮器保险以防可能的侵犯，第二，存贮的擦抹表示破坏已经发生过。

为了从这样一个安全微处理机中得到秘密，侵权者将不得不利用大批昂贵的微芯片装置和相当可观的预算。破坏处理器和内容，必须破坏处理器的实体的完好性。然而，集成电路技术不断改进和不可预测的发展有可能进行比现在可得到的更经济的更实际可行的攻击。另外，用于卫星传输的侵权解码器的世界范围的市场将对为了盗取这样一个部件秘密的更趋完善的侵权电子学工业提供经济刺激。

复制包括图4 的微处理机单独一个的解码器，这将导致基于在那个单个解码器中的单个秘密序号代码的解码器的大量非法复制。如发现将导致那个秘密序号码的终止，从而终止了所有这些非法复制品。然而，侵权者可以选择使用单个被泄露秘密的部件来再现该关键码。侵权者这样就可以开发一个解码器设计，它可接收关键码作为直接输入。这些侵权部件就可能非法地分发到用户，用户将每月付款给侵权者以取得每月更新的关键码。安全性失败的后果给收费电视的提供者造成极大的损失。

如果保险只是依靠安全微处理机的物理安全性，则收费电视的提供者将冒风险。图5 表示一个装置，它试图以可更换的安全模块514 的形式提供一个安全装置来克服图1 和图2 装置的缺陷。可更换的安全模块514 包括关键码解密器513 、秘密序号代码存贮器512 和关键

码存贮器507。如图2中一样，编码器501用来自关键码存贮器504的关键码在节目扰频器503中对包括有图像信号、声音信号和数据的源节目502进行扰频。在关键码加密器510中用来自秘密序号代码数据库511的秘密序号代码(SSN)对关键码加密，秘密序号代码数据库包括一个所有合法用户的秘密序号代码的表。

将同样的SSN安装在可更换的安全模块514里的秘密序号代码存贮器512中，可更换的安全模块514是可拆卸地连在解码器506上。可更换的安全模块514的关键码解密器513利用存贮在秘密序号代码存贮器512中的秘密序号代码对关键码解密。解密后的关键码贮存于关键码存贮器507中。不像图2，整个可更换的安全模块是可拆卸地连于解码器506上。节目去扰频器508从可更换的安全模块514中的关键码存贮器507中读出解密后的关键码，并用此关键码去除扰频并输出去扰频后的节目509。可拆卸的安全模块514被设计得可由用户更换，最好不用特殊工具，因而，最方便情况是用一个插入式模块。

使用插入式外部模块，通过将它以很低价换出，给予了收费电视提供者提高该安全装置中的工艺的能力。在发生安全性破坏时，一个新的包含节目扰频算法和SSN的可更换的安全模块可以邮寄到被认可的用户。被认可的用户可以从他们的解码器上取下旧的可更换的安全模块，并由他们自己插入新的可更换的安全模块。这样就恢复了系统的安全性，不用花钱来更换整个解码器，或花钱派一个维修人员去更换在每个解码器中的可更换的安全模块。另外，收费电视提供者不必自己拥有解码器。解码器可以是一种由用户购买的普通的商业上可得到的部件，或甚至可结合于电视机本身。为了开始服务，收费电视提供者仅需将可更换的安全模块邮寄给用户而无需上门服务。

尽管可更换的安全模块提供了保证网络的安全性破坏后可以恢复的优点，但它也有一些缺点。所有的安全性都在可更换的安全模块514

中，解码器506 本身是一个普通部件。由可更换的安全模块514 产生的密钥信号在其到解码器506 的传输点处是可以被发现的。可是，密钥应足够经常地变化以保证其对潜在的侵权者没有价值。

这种方法的问题是一个给定的可拆卸的安全模块514 将会与任何解码器506 一起工作，并且破坏可更换的安全块514 不会损坏解码器506 。结果是如果可更换的安全模块514 泄露秘密，侵权行为将会非常迅速地扩展。

尽管如上所描述的装置表示了单独一个用于对节目信号扰频的密钥(所谓的“单层加密”)，任何一个已有技术装置可采用多重密钥(“二层”，“三层”，等等) 的扰频系统。具体应用于有线电视环境的多重密钥加密系统在美国专利4,890,319(Seth-Smith, 1989年12月26公开) 中有叙述，在此作为参考。图6 表示已有技术二层加密编码器601 的一个例子。编码器601 包含秘密序号代码数据库611，数据库包含一个由所有被认可用户的秘密序号代码组成的表，这些序号代码最好是56位长。密钥码存贮器604 贮存“月密钥”(KOM)，在此实施例中“月密钥”可以是对偶数月(2、4、6月，等等) 是“偶数”密钥，或者对奇数月(1、3、5月等等) 是“奇数”密钥。取决于这样一个密钥可利用的数据位数，密钥还可以对一年中每个月都不同，或甚至可以更加独特。另外，这里所示的以每月为基础相比，密钥可以变化得更频繁或更不频繁。这些KOM 最好是56位长。

密钥码加密器610 对从密钥码存贮器604 中选取的密钥码加密，并输出一系列每个用来自秘密序号代码数据库611 的秘密序号代码加密的加密密钥ESSN[KOM] 到数据多路通道635。种子存贮器636 包含一个用于对声音和图像信号进行扰频的“种子”。该“种子”还可以是类似于上述密钥的数据代码或信号。最好，该种子每1/4 秒变

化一次。种子加密器637 对种子用该月关键码加密，并将加密的种子 EKOM[SEED] 输出到数据多路通道635 。这样，就用秘密序号代码加密 3 关键码，而对该种子用该关键码加密。在传输过程中，关键码和种子都不易被恢复。

在此实施例中，源节目602 包括带有上面提到的典型的色度及亮度信号的多路模拟图像(MAC) 信号639 ，以及可以含有几个不同声音与非声音(数据) 信号的多道声音数据638 。例如，可能至少有二个声音通道(立体声) 和一个为听力损坏的人附加的电传信息通道。另外，可能有与图像信号相关的声音附加通道，如外语翻译，非相关的声音信号(如广播节目) 或数据信号(如用户信息、计算机数据等等)。象该领域中公知的那样把所有这些信号数字化并一起多路传输，所得的是多路模拟分量、数据638 准备被扰频。

种子通过伪随机位定序器(PRBS) 643 ，然后被附加到加法器644 里的多路声音数据638 中。伪随机位定序器(PRBS) 643和加法器644 组成了一个本领域熟知的逐位加密器645 。将结果的扰频多路声音数据传至数据多路通道635 ，并与加密的种子和关键码一起多路传输。

在线路中继扰频器603 中对MAC 图像信号639 进行扰频，线路中继扰频器利用来自用于扰频算法的种子存贮器636 中的“种子”对MAC 信号线路进行扰频。然后将所得到的扰频MAC 信号送至多路复用器632 上，多路复用器将扰频后的MAC 信号与数据多路通道的输出一起多路化。把数据多路通道635 的多路传输数据输出用P. A. M. 调制器645 调制成脉冲振幅调制(PAM) 形式。输出的B-MAC 信号646 包括都用种子扰频了的MAC 图像信号639 和多路传输的PAM 声音数据638 、以及用月关键码扰频过的种子、和一系列用用户解码器的秘密序号代码加密了的月关键码，将所有这些一起多路化。

为了将B-MAC 信号646 解除扰频，侵权者必须能够对这些加密的

关键码中的一个解密，并且利用那个关键码对种子解密。然而，如图2所描述的单层编码装置中一样，为了获得一个秘密序号代码，侵权者只需获得一个这种解码器的秘密，就可对关键码解密。用此关键码，侵权者可以对种子解密，用此种子对节目信号去除扰频。附加的加密“层”（即更多的种子和关键码）使侵权更麻烦，这是由于侵权者必须对更多种子和关键码解密，然而，一旦第一关键码已被解密，接着的关键码和种子也可被解密。在图6所示的实施例中，为了能全年对节目信号解除扰频，侵权者必须每月对关键码解密。图6中所用的秘密序号代码，种子和关键码可被收费电视提供者有效地利用，通过秘密序号代码来终止一个特定的解码器，并且挫败侵权者的窃用。然而，尽管系统还没被泄露秘密，一个决意的侵权者可能借助于一个被泄密的解码器来泄露这样一个多层加密系统的秘密，这种侵权的中心是获得通向秘密序号代码的渠道。

一个具体的问题涉及将加密和种子和/或编码的月关键码(KOM)与节目信号一起传输到个人用户的问题，这些用户可以有他们自己的天线、一般是后院中的抛物面接收天线。参考图11，已有系统使用一个中心控制器1181以把编址数据包或其它与用户相关的信息插入节目信号中，直接认可那些接收加密信号的个人用户接收机，而不是通过当地的分配器。中央控制器1181通过专用线路1185把编址数据包传输到上行线广播电台1183（如Home Box Office, cinemax，等），广播电台1183再将该编址数据包与节目信号（通常被编码）一起多路传输。将这些信号传输到卫星1105，然后一般通过后院接收天线1187返回到个人接收器1189。如果个人想接收某些节目，他应通过电话线1188向中央控制器1181打电话。中央控制器再将该个人的认可要求通过专用线1185转发给广播电台1183。上行线广电台将该个人的新认可的代码与他们的特定的加密节目信号一起进行多路传输。然后，信号

通过卫星转发器1105转发给个人天线1187，并进入到其解码盒内，在那里新的请求认可将允许这些解码器对新的节目信号解密。这样的一种系统现在正被通用仪器公司的图像密码II-TM系统所用。重要的是，由于专用线1185（一般是电话线）传输的限制，一个广播电台不能迅速与所有用户联系。

已有技术的另一个问题涉及接收数字电视信号的现有电视解码器的改进。首先，当地的电缆电视分配机构必须用适合数字电视信号的新的转换盒来代替所有用户家中现有的转换盒。这将花费很大，因为必须分配新的解码器盒，收集旧的盒，且通常很费时。作为另一种办法。当地电缆电视分配机构可分配新的只接收数字电视信号的解码器盒。这样，用户可以用他们原来的接收模拟信号的解码器盒，同时也可用新盒接收数字信号。这也将花费很多，这是因为除了前面提到的其它麻烦外，在二盒中的许多电路是多余的，必须在用户家中增加分流器以提供给二个盒子的二个同轴输入。

鉴于上述已有技术装置的缺陷，在该领域中仍需要提供一种收费电视的扰频系统，该系统不只是依靠解码器部件的物理安全性来维持系统的完整性。

因而，本发明的目的之一是提供一种带有可拆卸安全模块的数据接口的解码器。

本发明的目的之二是提供一种可执行由内部安全模块执行的所有功能的可更换安全模块。

本发明的目的之三是提供一种利用对一个用户解码器和可拆卸的安全模块分别指定的两个不同的秘密序号代码对关键码进行双重加密的系统。

本发明的目的之四是电视信号解码器提供一个可更换的安全模块，该可更换的安全模块仅与一个解码器工作，而不能与另一个解码

器工作。

本发明的目的之五是提供一种解码器，其中外部的安全模块可以更换，而不用中断用户接收被认可的信号。

本发明的之六是提供一种在多通道上将一些同样的认可信号传输给各个个人收费电视接收器的方法。

本发明目的之七是提供一种低费用的、可以容易地将一个解码器盒转变成可以接收模拟和数字电视信号，而没有多余电路的方法。

用本发明的原理解决了上面提到的已有技术加密装置的许多问题及相关的问题，本发明的这种原理是能够在传输前对密钥进行二次加密，首先用的是用户的可拆卸外部安全模块的第一秘密序号代码(SSN₀)，然后再用用户解码器的第二秘密序号代码(SSN₁)。双重加密技术阻止对可拆卸的外部安全模块的复制，这是由于每个可拆卸的安全模块只与它配套的解码器一起工作。该系统在系统损坏后还允许更换该可更换的安全模块，因而可重新恢复系统的安全性。另外，在更换外部安全模块时通过提供三步解密，可以不间断地传输解密的信号。首先，在新的可更换的外部安全模块插入解码器之前，用用户解码器的第二秘密序号代码对输入信号解密。第二，将有效的月密钥(KOM)传送到内部安全模块，在那里用另一个秘密序号代码(SSN)对它解密。然后，将该软件包转到新的外部安全模块，在那对它进一步解密，并存贮有效的KOM。最后，把输入信号的解码送到外部安全模块，这样外部安全模块成了有效的安全元件。

系统包括一个编码器，用来给信号编码，该编码器包括信号扰频器、第一和第二密钥加密器。信号扰频器对信号扰频并输出被扰频的信号和为了对被扰频信号去除扰频影响用的密钥。第一密钥加密器连接到信号扰频器上，用第一秘密序号代码对密钥进行第一次加密，并输出一加密的密钥。第二密钥加密器连接到第一密钥

码加密器，并在一次加密关键码上用第二秘密序号代码进一步进行加密，并输出二次加密的关键码。

该系统还包括一个与信号扰频器和第二关键码加密器相连的发射机，用于传输被扰频的信号和二次加密的关键码。

系统还包括一个与发射机耦合的用于接收扰频信号并去除扰频影响的线路管理器解码器。该解码器包括第一和第二关键码解密器和去扰频器。在两次加密方式中，该第一关键码解密器与发射机耦合，并对二次加密的关键码用该第二秘密序号代码进行第一次关键码的解密，并输出部分解密的关键码。第二关键码解密器与第一关键码解密器耦合，并对部分被解密的关键码用该第一秘密序号代码进行第二次关键码的解密，并输出解密后的关键码。扰频器与第二关键码解密器和传输器耦合，并用被解密的关键码对扰频信号去除扰频影响，并输出去除了扰频的信号。该解码器可以在不使用可拆卸的安全模块下发挥作用。一旦发生系统损坏或服务等级的变化，一个可更换的安全模块可插入到该解码器中以“改善”解码器。

在本发明的另一实施例中，认可信号从主上行线通过卫星转发器传输到回送上行线。在回送上行线中，节目声音和图像信号与认可信号结合，并被送回卫星转发器，然后到个人收费电视信号接收器。

在本发明的一个另外的实施例中，描述了一个易连接的模块或“侧舱”，其允许标准解码器盒可接收模拟及数字电视信号两者。此数字侧舱可以改善现存转换器盒，而无需有二套非图像部件。

本发明这些及其它目的和优点，以及实施例的细节，可从下面说明书及附图更充分地理解，其中不同图中的类似元件配有最后两位数字相同的参考号（如图7的解码器706和图8的解码器806）。

图1表示一个用于卫星传输的已有技术的有条件使用系统，其中关键码不设障碍地被送到解码器。

图2 表示一个采用单独一个关键码加密技术的用于卫星传输的已有技术的有条件使用系统。

图3 表示一个不带安全存贮器的已有技术的微处理机。

图4 表示一个带有安全存贮器和可熔断的数据线路的微处理机，其适于贮存本发明的算法及秘密序号代码。

图5 表示具有包含第一秘密序号代码的可更换的安全模块的用于卫星传输的有条件使用系统。

图6 表示采用一个附加加密层的用于卫星传输的有条件使用系统。

图7 表示本发明的有条件使用系统的一个示范性实施例，该系统带有一个用第一和第二秘密序号代码对关键码加密的加密器；一个卫星传输系统；和一个解码器，该解码器含有第一秘密序号代码及包含第二秘密序号代码的可更换的安全模块。

图8 表示图7 解码器的扩展图。

图9 表示一个编址数据包的帧格式。

图9A表示一个系统数据包的帧格式。

图10表示一个安全微处理机(内部或外部的) 和线路管理器之间的联系。

图11表示在中央控制器和个人电视用户之间传输认可信号和编址数据包的已有技术系统。

图12表示将一些同样的认可信号在多种通道上从中央控制器传输到个人电视用户的另一个本发明具体实施例。

图13表示本发明的另一个实施例，其中将图7 和图8 中描绘出的解码器很容易 地进行了改善，以接收模拟及数字电视信号。

图7 表示本发明的加密系统，包括一个对源节目702 进行编码的编码器701 ，通过卫星线路705 传输到至少一个解码器706 。根据图7 ，将关键码加密并对个人解码器编址，与图5 中的装置相似。然而，

在此情况下，关键码可被两次加密。

编码器701 包括一个含有效安全性选择的有效安全性选择存贮器721。有效安全性选择可选择固定的安全元件719 或可更换的安全元件714 作为有效的安全元件。只有有效安全元件可接收B-MAC 信号并把种子传送给节目扰频器703。

关键码存贮器704 包括有效安全性器721 和用于对节目扰频器703 中的节目702 进行扰频的种子。作为另一种选择，如图6 所示，关键码存贮器604 可以包含一些用来对种子加密的月关键码(KOM_5)。这个种子用来对源节目702 加密。在此双加密技术中，首先在第一关键码加密器710 中用贮存在SSN₀ 数据库711 中的第一秘密序号代码(SSN₀) 对KOM 加密。在第二关键码加密器715 中用来自SSN₁ 数据库716 中的第二秘密序号代码(SSN₁) 对KOM 进一步加密。对每个SSN 不断地进行这个过程，以产生出一系列加密的关键码，将这些关键码与被扰频的节目一起通过多路器732 进行多路化，并经卫星线路705 发送。

解码器706 接收并通过信号分离器733 分离被加密的节目及被加密的关键码，并且在内部安全模块719 (解码器706 的组成部分) 内进行第一次关键码的解密。第二次解密在可更换的外部安全元件714 中进行，该元件例如，作为一个插入模块被固定在解码器706 的外部。作为另一种选择，加密的关键码可与加密的节目分别送到两个分开的通道，如同未审决的473,442 号申请中所述的那样，将该申请在此引用作为参考。

内部固定的安全模块719 在可更换的外部安全模块714 没有安装时是不完整的。内部安全模块719 将接收路线管理器708 那里送来的系统数据。认可和控制数据最好包含如图9 所示的编址数据包和图9A 所示的系统数据包。编址数据包9c 最好包括一个28 位的用户鉴别数码或地址码9a，以非加密形式传送。此用户地址码对应于在内部和外部

安全模块719和714中的用户地址。线路管理器708 只续出(唯一的) 内部安全模块719 的用户地址, 并相应地将整个编址数据包9e送到该指定的安全模块。接着该用户地址的是二位未加密的二进制位9b和9c。第一位9b决定该编址数据包最终是被送入内部安全模块719 或是送入外部安全模块714 。第二位9c决定接下来的信息, 被加密的信息9d是被一次加密或两次加密。如果二进制数码9c指示双重加密, 则需要内部安全模块719 和外部安全模块714 都对它进行解密。加密的数据9d的位数包括认可和控制数据, 例如, 月关键码, 用户认可数据(如使用者层信息, 付款收看信息, 或其它用户专门的或解码器专用的数据)。通常, 认可数据决定一个特定的用户或解码器是否被认可去接收并解密一个特定的节目或收看付款收看节目, 等等。控制数据可包括确定数据包送去哪里的信号, 能量管理数据, 防盗报警数据, 或其它解码部件启动信号。

表1 表示怎样根据位9b和9c的值来确定编址数据包9e的路线。

目的地位 9d	加密位 9c	编址数据包(ADP) 结果的路线
内部	单	ADP 只到内部安全模块
内部	双	ADP 先到外部模块, 然后到内部
外部	单	ADP 只到外部安全模块
外部	双	ADP 先到内部模块, 然后到外部

表 1

图9A所示的系统数据包包含节目专门信息并被传送到所有解码器并由它们处理。系统数据包9h包括一个类似于编址数据包9e中的位9b的内部/外部目的位9f。位9f依靠路线管理器708 决定该系统数据

包送去哪里，更确切地说，决定包9h进到内部或是外部安全模块。接下来的信息，9g，是被加密的数据，该数据包括：加密种子，确定特定的节目位于哪层的节目层信息，付款收看节目的价格，核对和数位，和任何该了目或通道(系统数据包9h在其中传输)所专用的附加信息。再次说明，系统数据包9h是一个特定节目或通道所专有的，并最好由节目广播电台插入(如图11的1183和图12的1286)。每个节目最好用其特有的种子加密。

如前面参考图6 所讨论，内部和外部安全模块必须先接收并对它们的特有的编址数据包解密以再现月关键码，然后，使用此月关键码，内部和外部安全模块将使用此月关键码对来自系统数据包9h的种子解密。最后，种子从安全模块通过路线管理器传送到图像去扰频器873或声音/数据解密器874 来对节目的图像或声音解密。

所有包含在编址数据包9e和系统数据包9h中的数据由内部安全模块719 处理。类似地，当外部安全模块714 安装后，它可以代替内部安全模块719 的功能。当系统数据包9h的未加密数据位9f指示时，外部安全模块714 被用作有效安全元件。在系统把有效安全元件从内部安全模块719 换到外部安全模块714 之前，这使外部安全模块714 被配置、插入并用编址数据包信息(尤其是，KOM)加以认可。这一过程下面将详述。如前所述，编址数据包9e包含了未加密的并对每个内部安全模块719 是唯一的用户地址码9a。外部安全模块714 还有唯一的用户地址码用来追踪外部模块的位置。一旦外部安全模块714 被插入，通过把内部安全模块719 的用户地址码送到外部安全模块714 (此外部模块可在安全 存贮器720 中贮存这个地址码)中，外部安全模块714 可以自己改成内部安全模块719 的用户地址码。

编址数据包9e用来把解码器专用的信息传送到一个单个的解码器，最好采用下面按图12描述的环回方法。在B-MAC 电视信号中，编址数

据包最好如在本发明背景技术中所讨论的那样，在每帧的垂直消隐间隔期间被传输。每个用户有一个与其解码器706 对应的唯一的编址数据包。每个解码器被分配一个单独的用户地址和相应的一个秘密序号代码(SSN)。用户地址和相应的秘密序号代码不相同，相关或没有关联。最好，该秘密序号代码是由一个随机数码发生器产生。当带有相应的用户地址的编址数据包被接收时，数据包可被解密，因而显露了KOM 和数据。所有被解密的数据(例如，KOM，分层数据，PPV，等等)保存在模块(707 或720) 中的安全存贮器里。这些数据包最好包括一个核对和数，用来核实数据的正确接收和解密。所有编址数据包被路线管理器708 接收，并且，根据位9b 的值，被送到所指示的安全模块去解密。在安全模块中的有条件使用软件或节目认可软件使用被解密的贮存的数据，根据用户的分层，付款收看户头等等，决定是否要对一个特别节目解密。安全模块714 和719 还决定是否要在其安全存贮器模块中放置一个特定的加密数据部分。例如，调制解码器875 所用的回访电话号码不需要贮存在安全存贮器中，并因而被传至调制解调器。

可以根据图4 的原则构建可更换的安全模块714 和解码器706 的内部安全元件719。例如，第二秘密序号代码SSN₁ 可以通过可熔断的线路输入模块714 的SSN₁ 存贮器717 中，然后在制造中将这些线路毁掉。类似地，内部安全元件719 的SSN₀ 存贮器712 可以在制造时通过可熔断的线路被输入，然后毁掉线路。还通过可熔断的线路，在制造期间将算法输入密钥解密器718、713 中，然后毁掉可熔断的线路。

可更换的安全模块通过向所有被认可用户寄出新的可更换的安全模块为收费电视提供者提供更换系统保险的选择。通过重新对SSN₀ 和SSN₁ 数据库711 和716 编程序以对应于解码器706 的第一秘密序号代码与安全模块714 的第二秘密序号代码的结合，如果线路未被破坏，

回收的可更换的安全模块714 可为一个不同的解码器再次使用。收回的可更换的安全模块714 最好废掉，并把一个新的可更换的安全模块714 送至用户，将安全技术的变化及改进结合以挫败可能的侵权。一旦发生安全性毁坏，为了恢复系统的安全，只需更换可更换的安全模块而不必更换整个解码器。最大的优点是，不用特别的帮助用户就可以更换外部安全模块，并将旧模块还给服务提供者。

参考图8，表示编码器706 的放大图，具体地说，更详细地描绘了节目去扰频器/线路管理器708。将进来的电视信号，最好是B-MAC电视信号，输入到多路信号分离器833。多路分离器把图像、数字声音、电传信息及认可和控制数据分离。将认可和控制数据，尤其是编址数据包9c和系统数据包9h，输入到显示及通讯处理器870。多路分离器833 还为进来的信号提供纠错和数据恢复。进一步将进来的信号格式化为一种可被显示器及通讯处理器870 更易使用的形式。

将认可和控制数据，尤其是编址数据包9c输进显示及通讯处理器870 的用户接口逻辑线路871 和安全性线路管理器872。具体地说，进来的数据速率通常对处理器870 来说太快而不能处理，因而多路信号分离器833 存贮并将数据格式化，并把它平行输入到用户接口逻辑线路871 及安全性线路管理器872。如果编址数据包9c包含这个特定解码器806 的独特的用户地址9a，而且加密位9c被设置成单独一次加密，用户接口逻辑线路871 命令安全性路线管理器872 将编址数据包送到内部安全模块(机内安全元件或ISE) 819，如果目的地位9b被这样设置的话。另一种可能是，如果目的地位9b被设置到外部安全模块814，安全性路线管理器872 通过耦合器879 把编址数据包传递到外部安全模块(外侧保险元件或OSE) 814。见表1。

如果加密位9c设置为单独一次加密，则根据目的地位9b，由内部或外部安全模块对加密的编址数据包信息9d解密。一旦KOM 被解密，

将它贮存在安全存贮器720 和707 中，然后用来对种子解密。与KOM 相比最好让这个种子非常频繁地变化(例如，每1/4 秒)，然后从内部或外部安全模块通过线路管理器872 送到图像去扰频器873 或声音/数据解密器874 。将这些种子用在图像去扰频器873 或声音/数据解密器874 中，以分别对图像及声音/数据解密。由于种子变化如此频繁(每1/4 秒)，种子未加密就被送到图像去扰频器873 和声音/数据解密器874 则不是很严重的问题。

如果加密位9c 设置为双加密并且目的地位9b 被设置在外部，则进来的编址数据包9c 首先在内部安全模块中用第一秘密/机密序号代码进行部分解密，然后在外部安全模块中用第二秘密/机密序号代码进行最终解密。将KOM 再一次贮存在安全模块720 中并用来对种子解密。

将耦合器879 也连接到声音/数据解密器874 以使通过外部安全模块814 改善声音/数据解密器，该外部安全模块814 包含仅针对声音/数据的附加解密算法。如果现在的声音加密已经泄露，这将增加编码声音的安全性。

电话调制解调器875 可包括一个微处理机，该微处理机使内部或外部安全模块819 和814 通过电话线路同编码器701 或其它设施进行通讯。这一性能将在下面更详细讨论。

在图8 上还示出了前面板显示器878 ，包括用户所用的输入键和显示器(最好在解码器盒806 的前面)。屏幕显示器/电传器877 保证屏幕信息或电传信息在用户电视屏幕上重复占位或显示。

从内部安全模块到外部安全模块转移安全功能的过程将在下面描述。最初，所有安全功能由内部安全模块719 来完成。如果发生了安全性毁坏，可以通过生产和分配带有安装到解码器706 安装说明的外部安全模块来保护安全性。这时，外部安全元件在其安全存贮器720

中既没有有效的月关键码，也没有任何对该特定用户合适的层和节目号码。因而，外部安全元件714 还不能执行任何独立的安全功能。

用加密的编址数据包9c把KOM 传送到内部和外部安全模块。由于安装了外部安全元件以改善保险性，用对每个内部和外部安全模块独有的KOM 对内部安全模块和外部安全的编址数据包进行不同的加密。因而，如上面的表1 所示，未加密的位9b决定了编址数据包9c的目的地。

在此过程期间，载有下一个KOM 的编址数据包带着设置到外部安全模块上的目的地位9b、带着设置到双加密的加密位9c被传输。路线管理器708 仍首先把编址数据包9c传送到内部安全模块，但现在内部安全模块用包含在其秘密序号代码存贮器712 中的备用秘密序号代码对加密数据9d解密。这个备用秘密序号代码不是内部安全模块通常用来对加密数据9d解密的那个代码，将用备用秘密序号代码解密的结果送回到路线管理器872 并转送到外部安全模块814 以使用外部安全模块的秘密序号代码最后解密。这样，月关键码被二次加密，第一次用备用秘密序号代码，第二次用外部安全模块的秘密序号代码。由于两次解码器的专门的解密必定是成功的，这种二次加密避免了在解码器706 之间外部安全模块的偶然移动。再次说明，在过渡阶段，用存贮在内部安全模块的安全存贮器中的秘密序号代码，和存贮在外部安全模块(为现存的每个内部和外部保险模块)的安全存贮器中的秘密号代码，对KOM 进行二次加密。

如果KOM 不用备用SSN 进行二次加密，则侵权者可改变目的地位和编码位9b和9c以在安全模块之间传送一个被解密的KOM，在传送期间截取它。通过使用备用的SSN，如果发生篡改目的地位和编码位，内部安全模块会相信加密的KOM 是用普通SSN 加密的，因而不能对KOM 解密。只有部分解密的KOM 在模块间通过并只在双加密的状态下。现

在的系统在解密器之间禁止交换外部安全模块的使用，这是由于两个 SSN 必须与二次加密的 KOM 相对应。

当下一个 KOM 已经传输并贮存到所有的解码器 706 中时，编码器 701 最好把系统数据包目的地位 9f 改变成外部安全模块，并将加密位 9c 改变成双重加密。外部安全模块 714 现在就变成了有效安全元件并承担了所有的安全功能。因而，解密的种子现在用 KOM 解密，并且从外部安全模块 714 通过安全性路线管理器 872 被送到图像去扰频器 873 和声音 / 数据解密器 874 。由于外部安全模块在其不易失的安全存贮器内现在还包含用户认可数据如节目、服务层和付款收看认可，它可以有条件地把种子释放给与内部安全模块无关解密专用节目。类似地，作为一个独立的安全模块，外部安全模块可以从用户接口逻辑线路 871 记录自动付款收看过程的购买，并可以通过电话调制解调器 875 用如下所述的加密通讯把此信息加载于电话管理器上。加密位 9c 如需要可改为单加密。增加外部安全模块的原因是为了在内部安全模块已被泄密之后恢复安全性。因而，在该最佳实施例中，采用双加密，并且在内部安全模块泄露秘密时外部安全模块成为有效的安全元件。

一里安置了外部安全模块，新的安全功能(包括新的秘密序号代码，编码算法，软件或物理安全性) 可被结合到内部安全模块中，使得在分配了外部安全模后被分配的新的解码器盒中不需要外部安全模块，仍然提供一个供将来的外部安全模块用的空的耦合器 879 。在新解码器盒中的内部安全模块为对将来外部安全模块提供兼容的传输，在这些新解码器中的内部安全模块在功能上必须模仿前代的内部安全模块，并且发挥和内一外安全模块结合时同样的功能，还必须对编址数据包目的地位 9b 及位 9c 作出响应。

如果以前分配的外部安全模块泄露秘密，则配置新的外部安全模块，由用户取下旧的并插入新的。新的外部安全模块没有月关键码或

用户认可及控制数据(如层或节目代码)。因而,为了保持服务的连贯性,应暂时让所有安全及认可功能回到内部安全模块。在分配/寄出新的外部安全模块之前,编址数据包连同设置在内部安全模块上的目的位 $9d$ 和设置在单加密的加密位 $9c$ 一起被传输。在这之后,将加密位 $9c$ 改变成双重加密来完成前面叙述过的步骤,以允许新的KOM被二次解密并贮存在新的外部安全模块中。最后,安全性,认可和控制功能随加密位被设置到双加密而被转到外部安全模块上。

概括地说,如果一个系统发生毁损,收费电视提供者则寄出可更换的外部安全模块给用户,把解密转到内部安全模块直到所有解码器有了新的KOM,然后利用仅通过外部安全模块的解密或使用双重加密技术,这样就恢复了系统的安全性。选择使用可更换的外部安全模块还有其它吸引人的优点。没有为额外频道付款的用户不会被寄给可更换的安全模块,因为“基本”频道可能仅用一次加密密钥或甚至无障碍地传送。如果用户希望提高等级,以便能收到额外付费频道(一个或多个),收费电视提供者可给该用户邮寄合适的可更换的安全模块。

另外,可更换的安全模块可被用来增加其它附加特性。话多电缆电视系统提供选择服务如IPPV(自动计节目付费收看),这需要在解码器706和起点之间的双向联系。在过去,如果用户希望升级得到IPPV服务“侧舱”来改变用户解码器。作为另一种选择,必需更换整个解码器。所有这三种选择都需上门服务,对用户造成不便,并对收费电视提供者造成费用问题。类似地,当收费电视提供者希望改善其整个编码器/解码器系统时,它必须对每个用户提供一个新的解码器,该解码器在过渡时期将用新旧两种编码技术工作,这是由于几乎不可能同时更换所有的用户解码器。因而,为了在更换期间的几个月内使用收费电视提供者的旧编码器发挥作用,解码器生产者面临为其现有

解码器提供额外电路的附加费用。

在所有上面这些改善现有服务的例子中，可更换的安全模块714 可用来改善解码器706 而没有上门服务带来的费用和不便。可更换的安全模块714 可邮寄到用户，用户可将可更换的安全模块插入，并立即改善了解码器或增加了附加的功能(如IPPV) ，改变了解码技术，或提供了一个附加水平的安全性。最好，把IPPV加入到解码器706 中。值得注意的是，可更换的安全模块714 可以对解码器增加附加的软件功能。

可更换的安全模块714 可采取多种形式中的一种。在该最佳实施例中，该模块可包括一个“灵巧卡”，一张带有内装式微处理器(如一个68HC11微处理器) 的塑料“信用卡”，如由国际标准组织在标准ISO7816/1 和ISO7816/2 中所描述的微处理器。现将1989年6月20日公布的美国专利4,841,133 在此引入作为参考，它描述这样一种“灵巧卡”。该“灵巧卡”可以配备有一系列连接到耦合器879 触点的电触点。最好提供16个触点以允许有充足的扩充余地(以备将来增加附加功能) ，本发明只用6-8 个触点。触点可为卡提供电源、时钟信号和数据传输。可提供附加的触点以允许耦合器879 到声音/数据解密器874 之间的连接。这些附加触点允许应用附加的解密算法，这些解密算法可以与包含在解密器874 中的那些解密算法结合使用也可以独立地使用或为了其它的目的。

计节目付款收看的节目发送在此定义为用户可以要求认可收看一个特定节目的节目发送。在许多这种付款收看系统中，其节目是体育项目(拳击、摔跤、等等) ，这些节目不是以正规的时间基础传输。希望收看此节目的用户必须以特殊去扰频机构的形式，或以传输或输入一个特殊代码到用户解码器的型式接收认可。某些付款收看电视系统允许用户要求观看一个付款收看节目(如电影) 。然后付款收看电

视提供者传输该要求的节目并认可那个用户的解码器接收该信号。

自动计节目付款收看(IPPV) 节目在此定义为用户在其个人解码器中具有预先被认可的存款数的任何节目。如果一个用户希望收看一个特别节目，用户仅仅启动解码器，一个适当的存款数从用户剩下的存款中被去除，用户可立即收看节目。例如在Block 的美国专利 4,484,217 和4,163,254 中公开了付款收看电视系统，在此引入作为参考。

在本发明的付款收看实施例中，解码器通过电话控制器/调制解调器875 向起点传送一个对付款收看节目解码的认可请求。然而最好是，安全存贮器720 和707 先存贮付款收看节目的认可信息(如存款)而安全模块通过电话控制器/调制解调器875 在较后时传送实际的付款收看数据。

电话控制器940 可以是一个计算机调制解调型设备，或用按键信号工作以与起点联系。电话控制器最好是一个调制解调型设备，用移频键或FSK 方式与起点联系。1990年5月15日公布的美国专利 4,926,444 描述了FSK 操作，在此引入作为参考。收费电视提供者可向用户发送合适的认可信息(TEL)，以用户秘密电话号(STN) 对该信息加密。秘密电话号并不是常规意义上的电话号码，而是另一种类型的秘密序号代码，它可分配给一个给定的电话控制器/调制解调器875 或一系列电话控制器。一旦被解码器906 的处理器870 接收到，认可信息可被确定传送路线，并被用来启动一个或多个特别付款收看节目的去除扰频。

在另一个实施例中，它可与上述付款收看实施例结合使用，电话控制器/调制解调器可用来接收用秘密电话号加密的KOM。加密的节目信号被输入到解码器806，通过调制解调器875 进入处理器870。调制解调器875 必须能提供多路信号分离器833 的功能以分离编址数

据包9e, 把它们输入到处理器870, 然后处理器870 送它们进到规定的安全模块。

电话控制器875 可被编程在一个预定的时间或在一个预定的时间间隔内或者在接到来自起点的信号后或最好在电话使用最少的时候(如清早时间)去呼叫起点, 电话控制器可通过免费的1-800 号码, 一个所谓的“瓦特”线, 或通过一个当地电话到一个商业数据线如 TYMNET或TELENET 与起点通话。本发明最好使用在题目为“用于电视传输系统的数据返回”申请号为____的申请中所描述的数据返回系统, 在此引入作为参考。一旦通话被连接上建立了通讯, 解码器806 向起点加一个用秘密电话号STN_i加密的付款收看使用记录的负载。起点向解码器806 输送类似加密了的数据, 包括新的密钥码, 秘密序号代码, 或解密算法。可将加密的密钥码或其它加密的数据送到内部安全元件819, 或可更换的安全模块814。从起点传输来的信息借助于电话线通过调制解调器875 进入处理器870, 或最好通过卫星电视输入到盒833 并进入处理器870。

如上所讨论, 新的秘密序号代码或解密算法是用秘密电话号码加密的, 它可从起点通过电话控制器875 传送到解码器。然后将编码的秘密序号代码或解密算法解密并存贮在选定的安全模块中。这种借助于电话控制器875 对解密算法和秘密序号代码的去载方法有时被称为“E²插入码”(E² patch), 并允许收费电视提供者通过把新的信息加进解码器的EEPROM来保持或恢复系统的安全性。E²插入码不必要求改变在解码器806 中的整个解密算法。为了足以改变解密算法只需改变秘密序号代码或仅仅解密算法的一部分, 如一个特定的位或数据表就够了。E²插入码允许收费电视提供者改进加密系统以解决“故障”, 并恢复系统的安全性。

通过电话控制器875 接收信号以后, 该起点将向解码器发送回执

信号，表明信息已经收到。类似地，在数据已经通过电话控制器/调制解调器从起点到达解码器以后，解码器将通过调制解调器875 返回一个回执信号到起点，表示数据已经收到。对此，本发明最好使用在题目为“一个电视传输系统的数据返回”的申请中描述的那种数据返回系统，其申请号为____，在此引入作参考。

除了付款收看请求或记录之外，电话控制器还可用于加载其它来自解码器的信号。例如，可将如结合图4 所述的破坏防护信息发送以表明解码器是否已被破坏。另外，为了电视评估的目的(如Nittlson 评估) 可将节目观看信息加载给收费电视提供者。

通常，任何可借助于图9 的B-MAC(或NTSC, PAL, SECAM等) 输入而传送的数据也可通过电话控制器875 卸载。这种信息包括但不限于消隐码，分层信息，个人信息，可利用的款数，组鉴别号码，和其它系统数据。通常，将电话控制器875 用于不频繁的通讯，如周期性改变安全等级和IPPV请求，这是由于电话线有限的带宽和经由电话比B-MAC 输入来传送信息增加费用。

用秘密电话号码(SIN) 加密的电话信息(TEL) 在解码器806 期间仍是被加密的并只在安全模块中被解密。为了避免被侵权者探测到，解密后的电话信息并不传出该安全模块。解码器806 对被扰频的节目解除扰频时，必须有通过B-MAC 输入接收到的电话信息和编址数据包。依靠这两个信息源，窃用实际上不可能，因为潜在的侵权者必须侵入收费电视提供者的电话系统并对二次加密的关键码解密。

图10 表示在安全性微处理机(内部或外部) 和线路管理器之间的通讯。解码器1006 包括带有安全存贮器1052 的安全性微处理机1050。安全性存贮器1052 包括一组秘密序号代码SSNo，一个对那个解码器或一系列解码器是独有的秘密电话号码(该秘密电话号码在制造过程中被装入并如结合图4 讨论的那样用“E² 位”(见图4) 或其它安全措

施保证安全性)，加密算法E，和其它认可信息。加密的节目信号EKOMO(SYS)1053和一次加密的月关键码ESSNO(KOMO)1054与选择的加密电话数据ESSNO(TEL)1055一起被输入解码器1006。

安全微处理机1050用贮存在安全存贮器1052中的秘密电话号码STN_c对加密的电话数据ESTNO(TEL)解密。被解密的电话数据(TEL)也贮存在安全存贮器1052中以防止被侵权者探测到。电话数据(TEL)可为解码器1006提供认可信息，即关于现在解码器1006是否被认可对一些或所有接收到的加密节目进行解密。另外，其它信息可在解码器和起点之间传输(如结合图9的讨论)。

至于带有编址数据包9e的加密信号的传输，以前的系统在广播发送的上行线中加入一个中央控制。如以前所讨论并参考图11，以前的系统采用一中央控制器1181把编址数据包或其它用户相关信息插入节目信号中，以直接认可那些收到被加密信号的个人接收者，而不通过当地分配器。中央控制器1181通过专用线1185把编址数据包传输到上行线广播电台1183(例如，Home Box office, cinemax等等)它接着多种传输带有它们的通常总是加密的节目信号的编址数据包。

在新系统情况下并参考图12，提供一个用户认可计算机1282和监控计算机1280，它们通过编址和系统数据包9e和9h把相同的用户和系统数据输入给主上行线1284。用户认可计算机1282和监控计算机1280都是由科学—Atlanta制造并销售的现行产品。用户认可计算机1282在一个大数据库中包含所有用户或解码器特有数据。然后这个用户特别数据被格式化进入编址数据包9e以便同声音和图像一起在主上行线1284中多路传输。类似地，用户认可计算机1282在一个大数据库中包含了特定节目所特有的系统宽频信息，并被格式化进入系统数据包9h以便传输。主上行线1284多路传输带有声音和图像的系统数据包以产生典型的B-MAC信号。这个信号可以被任何一个可使用数据包

对节目解密的用户接收。然后编址和系统数据包9e和9h在一个通道中通过卫星上行线1283与声音和图像一起被传送到卫星转发器1205上。

信号从卫星转发器1205反射到卫星接收器和上行线1283。编址和系统数据包被回送上行线1286接收，在此它们与插入主上行线1284中的声音及图像节目信息分离。然后这些数据包与不同的声音及图像节目信号一起多路传输并传输到卫星转发器1205。然后该组合信号通过接收器1283被传输到个人接收器1289中并对它们解密。用此系统，编址数据包可被几个回送上行线广播电台接收，电台把这些数据包连同它们的扰频了的节目信号一起多路传输。它们还可以从系统数据包9h中取出选择的部分，例如，层信息，付款收看费用数据，等。以此方式，所有回送上行线广播电台最好传送具有数据包的广播B-MAC 节目信号到所有的用户。一个用户可以调谐到任一通道来接收扰频的节目和对节目解密的数据包，可以在回送上行线1286上被结合的系统宽频数据最好包括回呼数据，这在申请号为___，题目为“电视传输的数据返回”的申请中有描述，在此作为参考。

在此系统中，既然编址数据包可从主上行线1284传输到不同节目分配器(如，HBO, Cinemax，等)的不同回送上行线1286，可避免每个广播电台必须用专用线1185。编址和系统数据包分别为图9和9A描述的形式，并最好置成B-MAC 格式。因此，回送上行线1286必须对B-MAC 信号解密以除去回送格式，这样可取出与它们的特定的被加密的节目信号一起多路传输的每个单个加密的编址数据包9e。

另外，本发明可以全场KOM 方式操作，用此方式可迅速访问网络中所有的解码器706。在B-MAC 电视信号中，编址数据包最好如本发明背景技术中所讨论的那样在每帧的垂直消隐间隔期间传送。一般，KOM 和编址数据包在每场垂直消隐间隔的5行当中传送。这大约产生每秒6,000 个字节的数据。此数据量可在已有技术的专用线路1185上

传输。然而，如果广播电台想迅速访问所有的用户，它们被专用线1185的传输能力所限制，一般是受电话公司电话线传输能力的限制。在本发明的情况下，以全场方式大约可以传送每秒500 千字节的数据。以此方式，每场可得到204 行图像线加5 条垂直消隐间隔线以传输编址数据包。因此，如果一个广播电台想迅速认可PPV 或IPPV收看一个现在即将到来的节目(如，一场拳击比赛)，广播电台可用现在的系统达到。屏幕文字消息可出现在所有用户的电视机上以指示正在发生什么。

用此系统，具有卫星接收抛物面型天线的个人用户可接收来自所有卫星的节目信号和数据包，不管他调在哪个频道。如果他被认可对一个特定节目信号解密，此信号将包含他独有的编址数据包，该编址数据包由处理器870 发送并由特定的安全模块解密。

参考图13，表示一个把模拟解码器盒(图7 中所描绘706 和图8 中所描绘的806) 从一个模拟结构转变为也能接收数字电视信号的方法。原来的模拟解码器盒被绘为1306，其中进来的信号在降频转换器1365中被降频转换。进来的信号最好在L频带，频率在0.95-1.45千兆赫，然而，任何其它频率也可使用。将这些频率降频转换为一个解码器容易操作的固定频率，最好转换成612 兆赫的中频。然后信号在FM解调器1366上解调，并通过开关1367传输到解码器1368上。信号最好是B-MAC 型，因此解码器1368对该B-MAC 信号解密，解密成声音、NTSC图像和频道3 信号，以输入到一个标准电视接收器。

为改善系统以接收数字信号，可以通过使用一个简单的4 导线连接器增加一个“数字侧舱”1390。抽头1397使被降频转换的信号输入侧舱1390的直角相移关键解调器1391中。最好使用每秒40兆字节的解调器。然后当解调的信号输入到纠错和多路信号分离器1392中。块1392还为数字侧舱1390中的信号提供正确的定时。

开关1367可被置于第二位置以接收数字信号，借此将来自数模(D/A)转换器1396的模拟信号输入到解码器卡1368上。连接到解码器1368的调谐微处理机1367用来控制转发器的调谐功能。另外，调谐微处理机1367还可控制音量和在解码器盒1390的前面板上显示数据。重要的是，调谐微处理机1367通过解码器1368为盒1392提供调谐信息以使多路信号分离器1392从所有包含在一个特定通道的进来信号中选择一个特定的数据子通道。具体地说，显示和通讯处理器870接收未加密的频道地址位，用来定位和选择特定的转发器号码(或通道号码)和子转发器(或子通道号码)。关于这种通道的变换，在题目为“一个多路传输的模拟分量(MAC)电视系统的虚拟通道”，申请号为—的申请中有更详细的描述，在此引入作参考。另外，来自安全模块的图像解密种子也被传输到盒1392，以使选择的子通道被解密。

盒1392利用带有检验和或奇偶位的正向误差校正法(FEC)校正信号中的误差。以选择的子通道将信号分路后传输到图像解压缩器1393中。典型的数字图像解压缩可是离散的余弦变换(DCT)或本领域技术人员熟悉的其它数字高压压缩技术。

然后，将解压缩的/扩展的数字图像信号在解密器1399中解密。如果图像信号，要被数字化传输，最好用关键码的数字加密，而不是象以前描述的用一个种子对模拟信号扰频。结果，解码器1368的外部安全模块1314和1319分别为解密器1399提供关键码的解密。安全模块1314和1319的功能与前面叙述过的功能是一样的。

然后用本领域技术人员熟悉的技术处理解密的去压缩的/扩展的数字图像信号，以重新形成一个B-MAC信号。扩展的数字图像信号输入到YUV存贮器1395，其中存贮有每行或帧的亮度信号Y。类似地，色度信号U和V也在帧的基础上存贮。盒1392还输入B-MAC数据到存贮控制器1394，存贮控制器1394在正确的定时的间隔内通过D/A转换器

1396 向解码器1368 输出存贮的亮度和色度信息。来自转换器1396 的信号是典型的具有图像、声音和其它数据的B-MAC 信号。标准模拟信号从解码器1368 输入到电视接收机。

此实施例使数字侧舱解压缩和扩展低位速率的信号成一个全B-MAC 图像信号。系统数据、系统和编址数据包9e 和9h、电传文字和数字声音未被压缩，被送到解码器1368 而不在侧舱1390 上解压缩。

开关1376 可以是微处理机控制的，使得读出系统数据或编址数据包中的“压缩—启动”位，并使开关1367 启动解压缩的数字侧舱1390。因此，带有数字侧舱1390 的解码器可以对模拟及数字图像信号进行接收和去扰频。另外，图13 中的抽头1397 是一个环路。这个环路可以是一个单独的引线，然而，此环为扩展增加了灵活性。

尽管本发明是参照最佳实施例进行描述的，在以下权利要求的范围内，本领域的普通技术人员显然可作出一些其它的改进。本发明并不限于这些描述，其保护范围完全由下面的权利要求来确定。

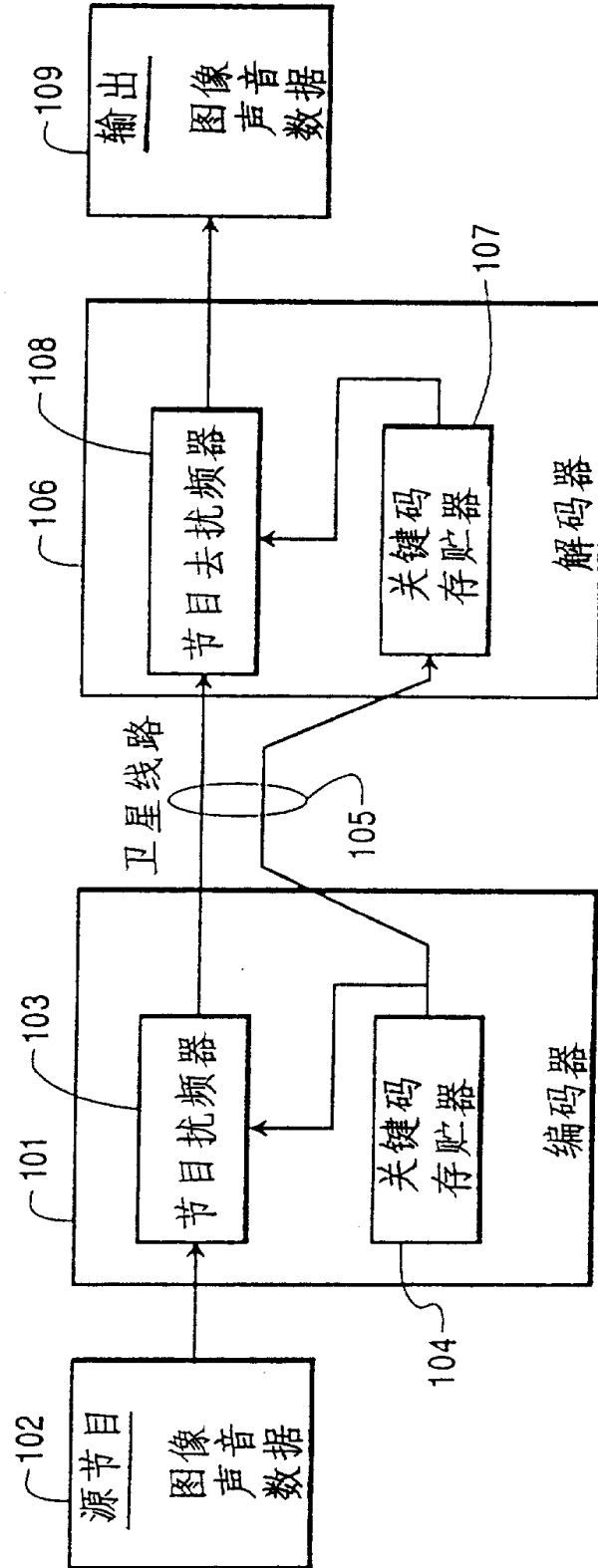


图 1

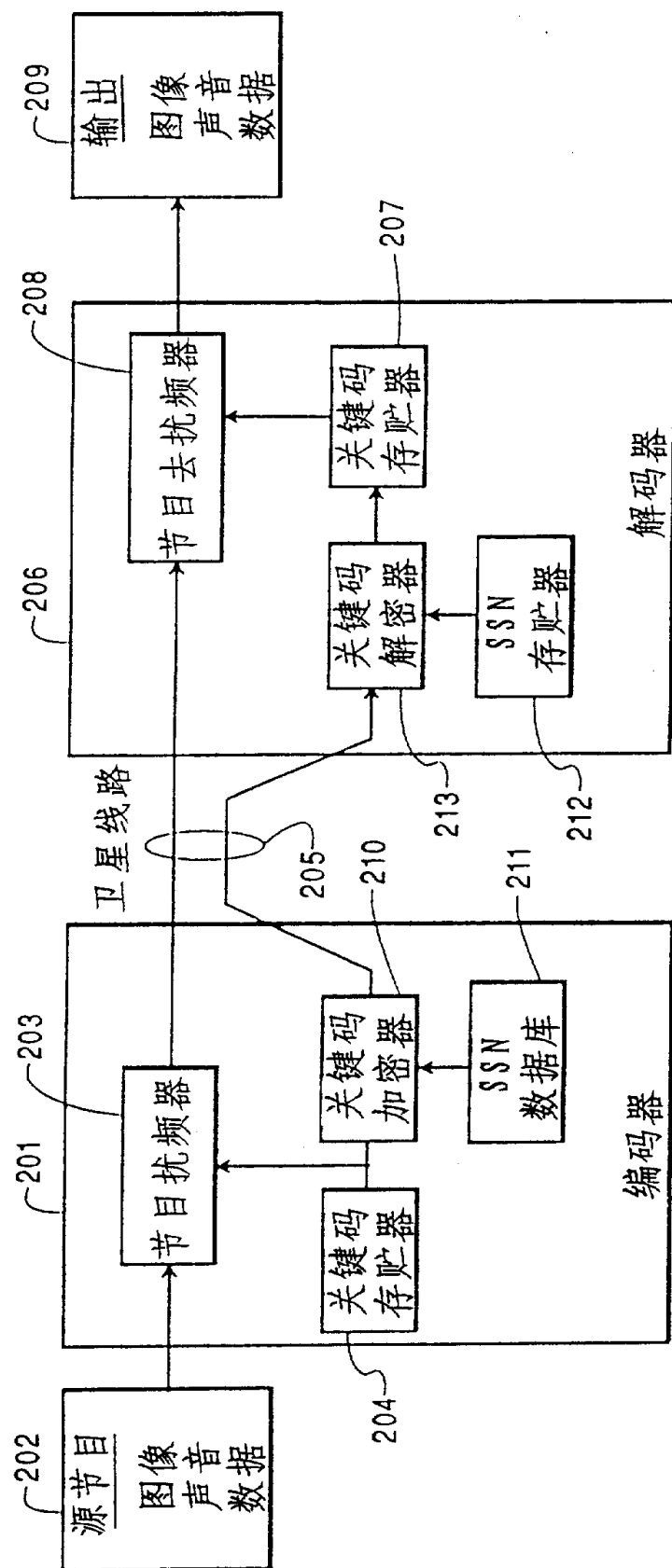


图 2

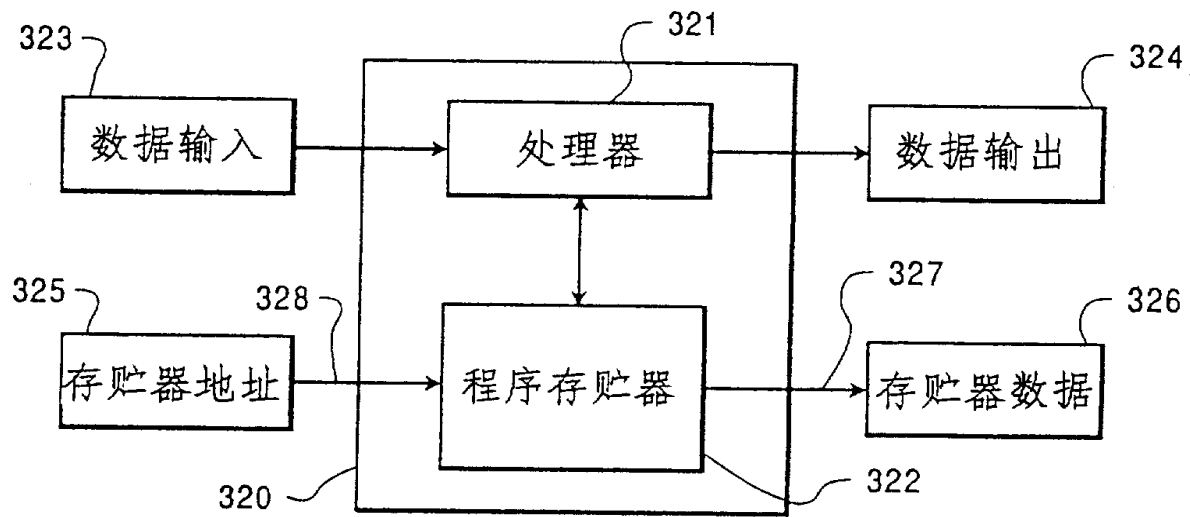


图 3

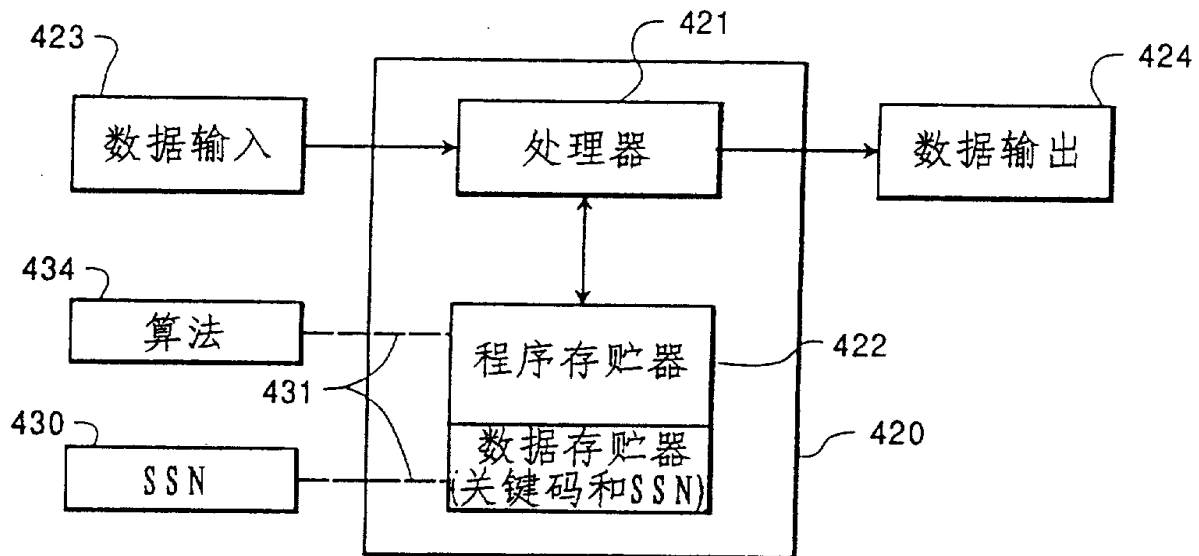


图 4

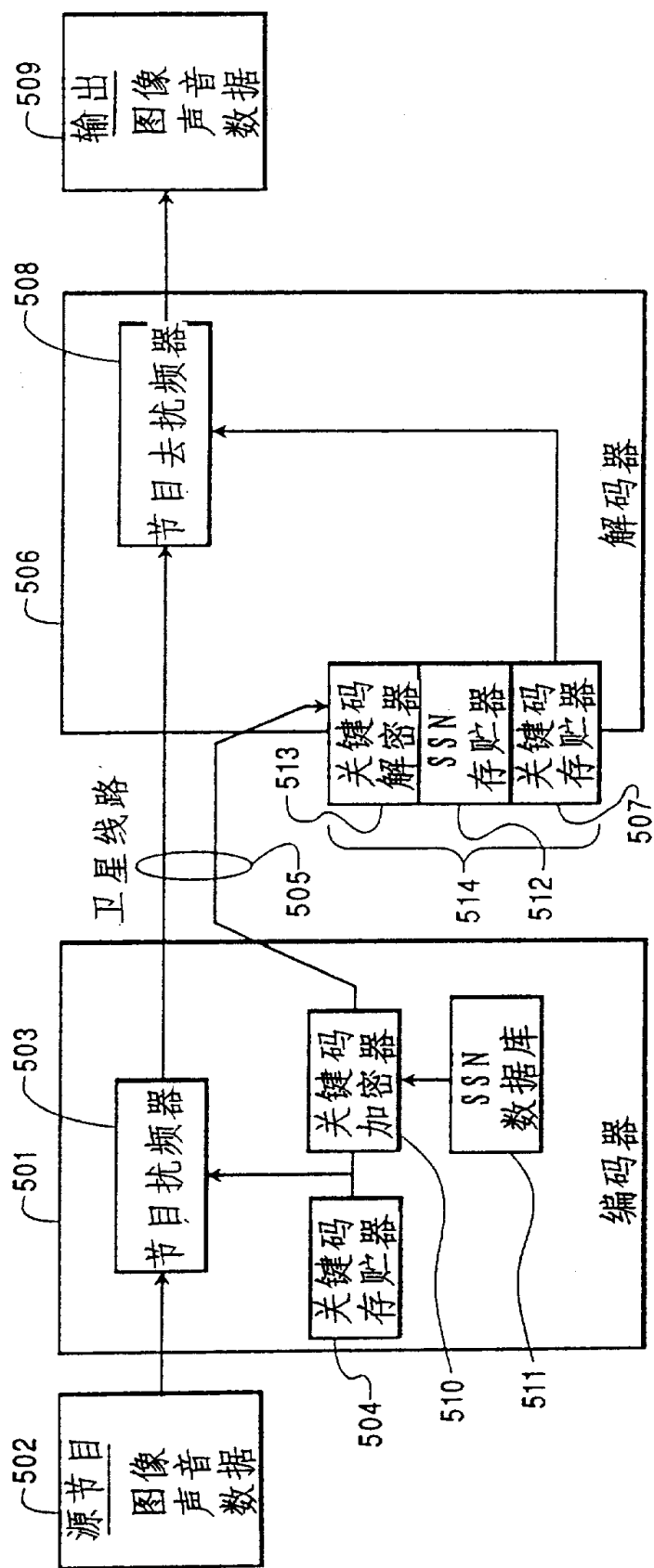


图 5

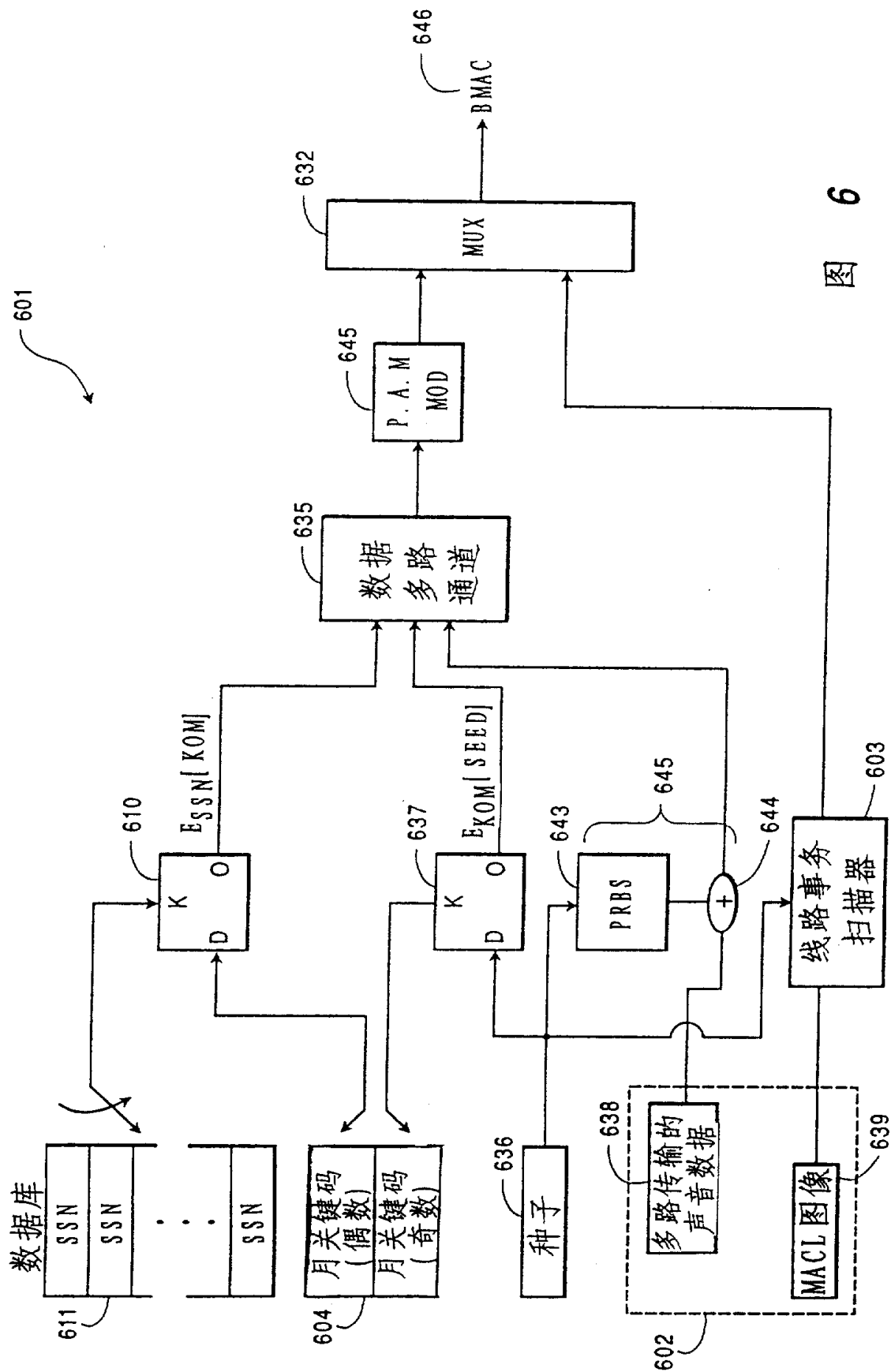
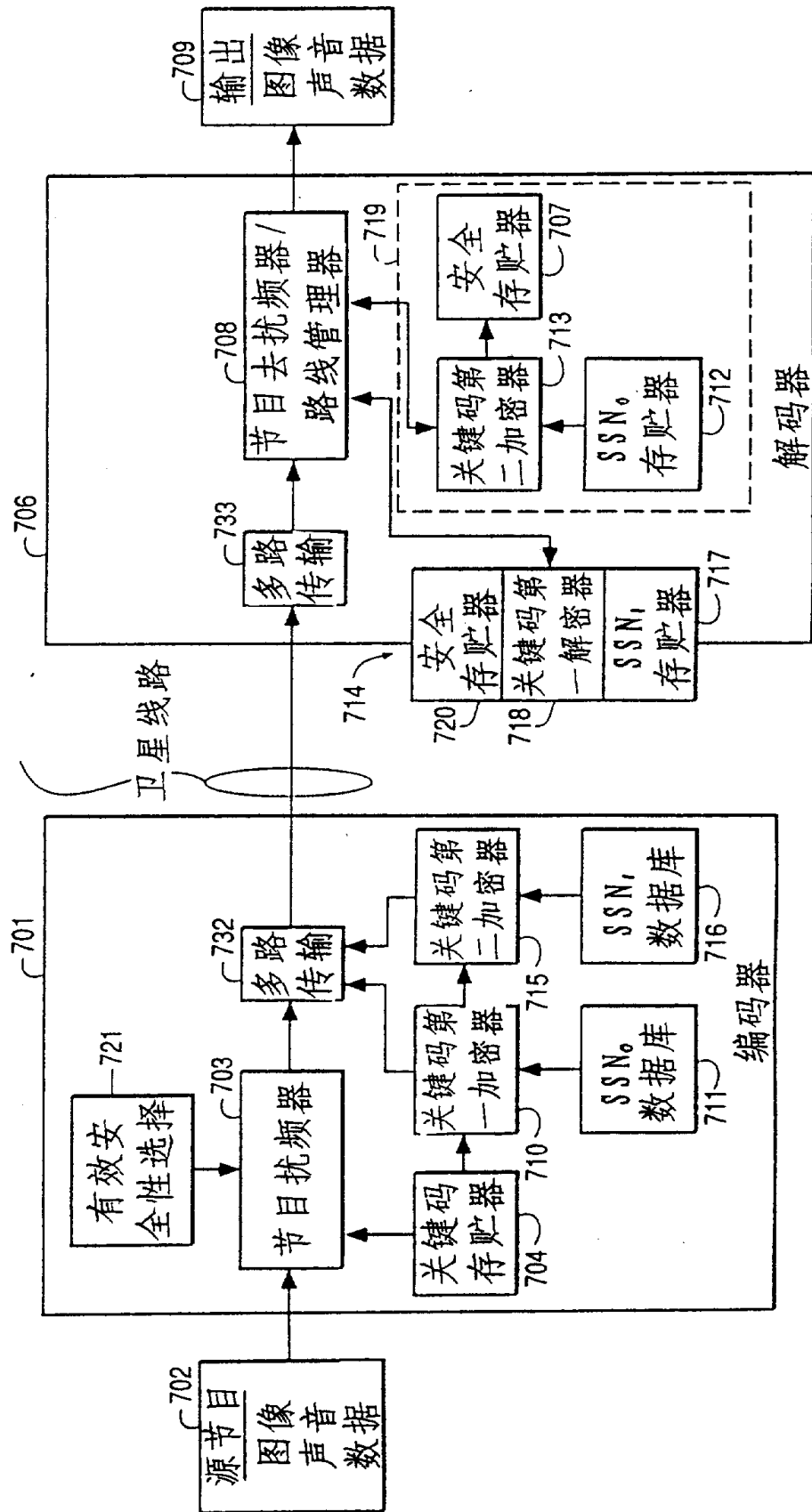


图 6

图 7



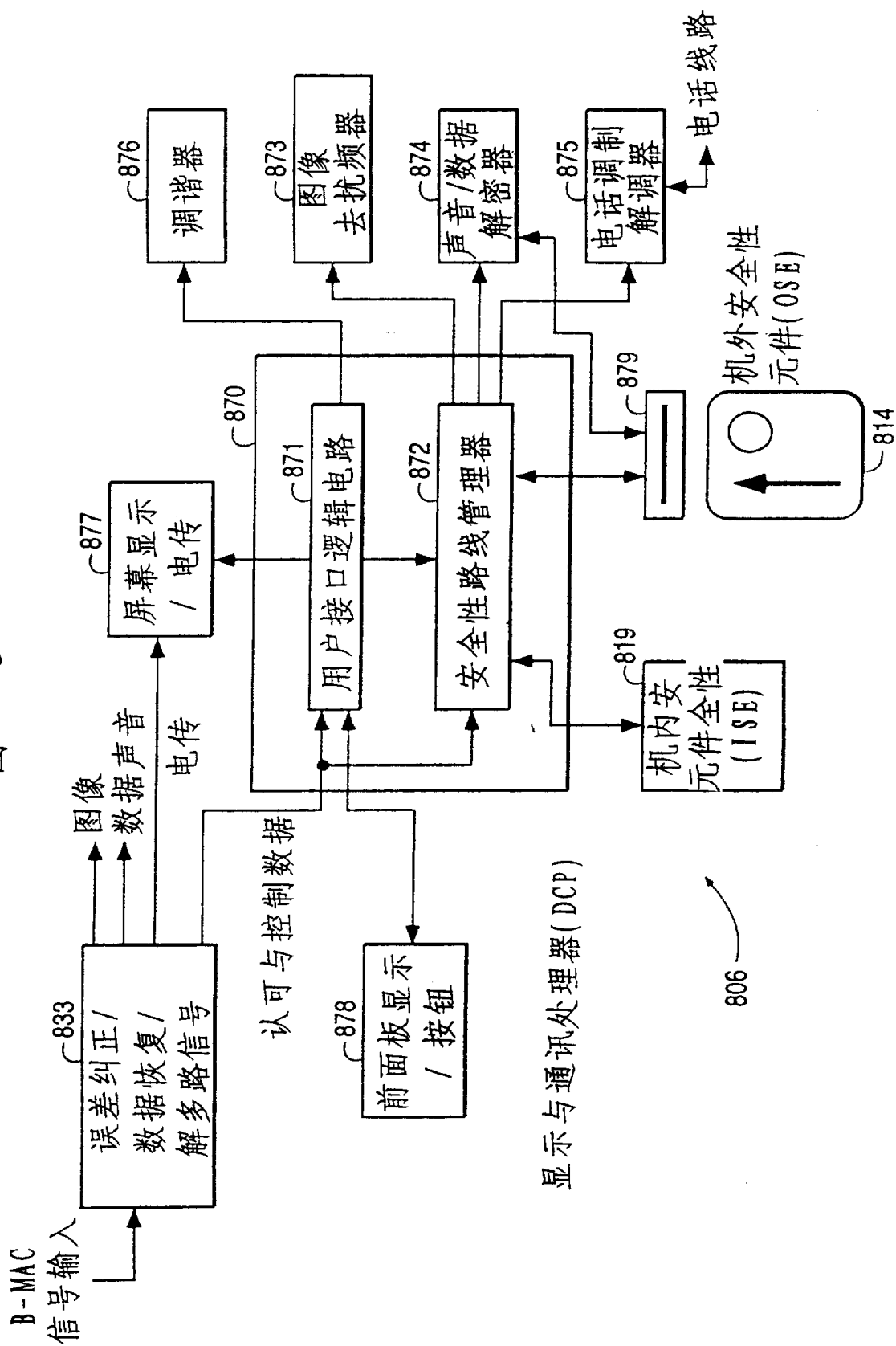


图 9

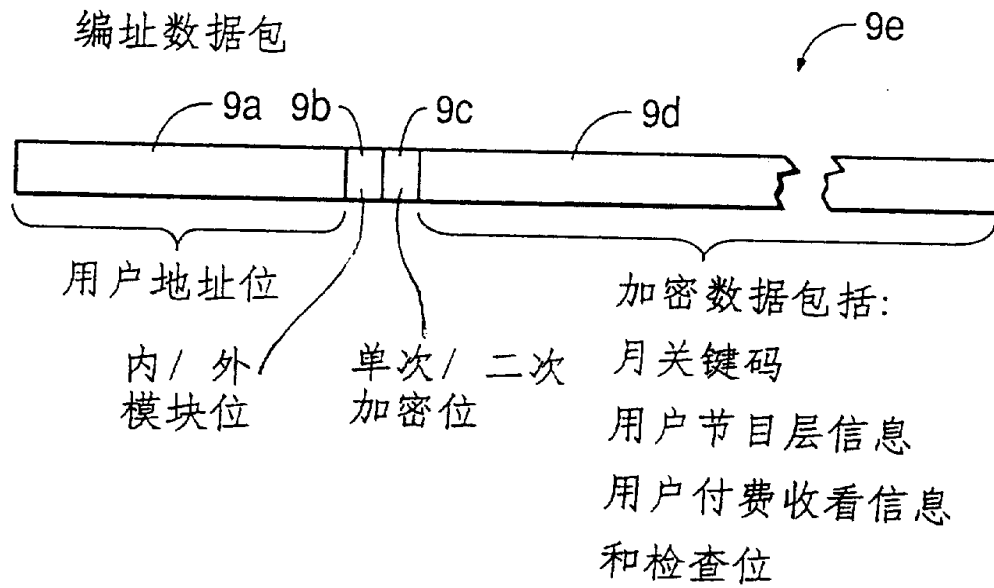


图 9A

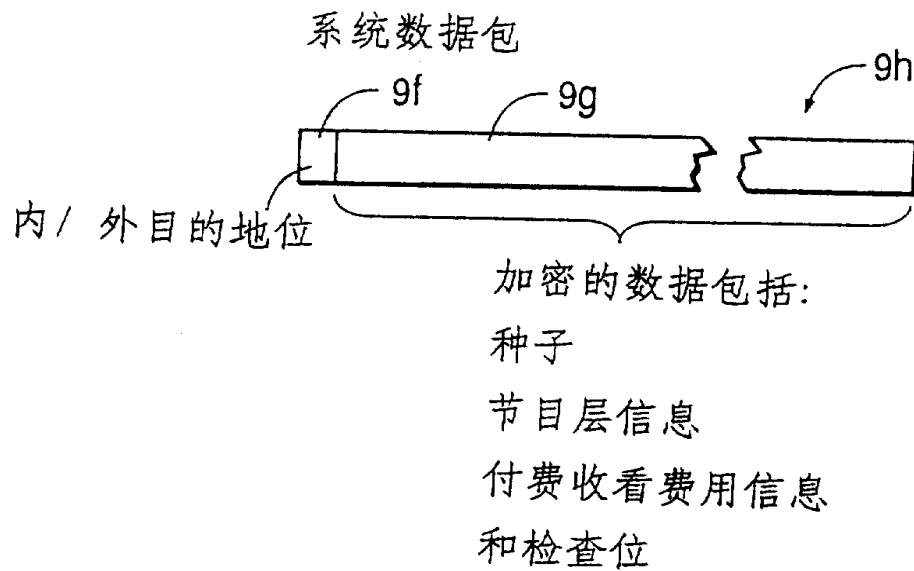
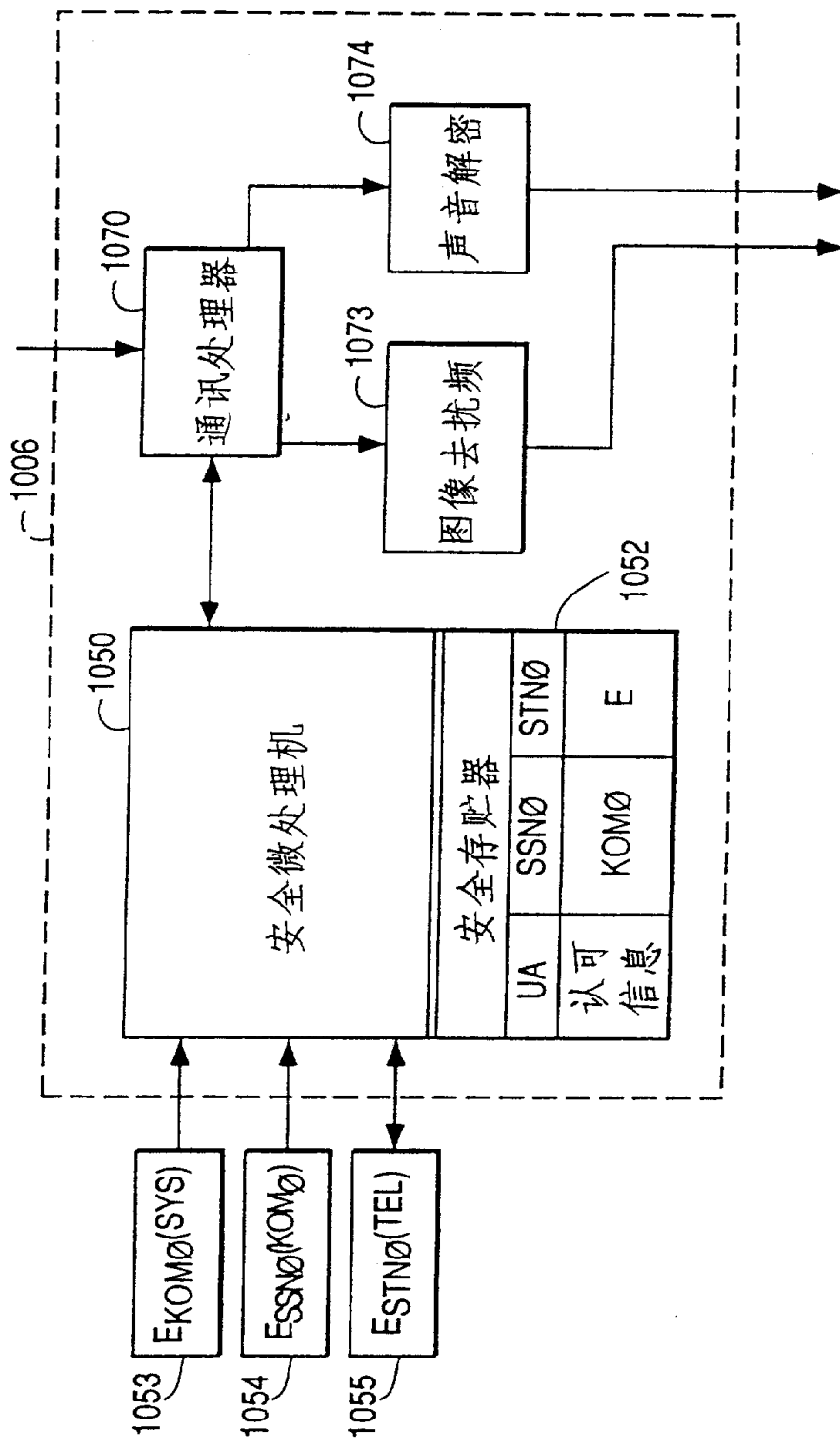


图 10



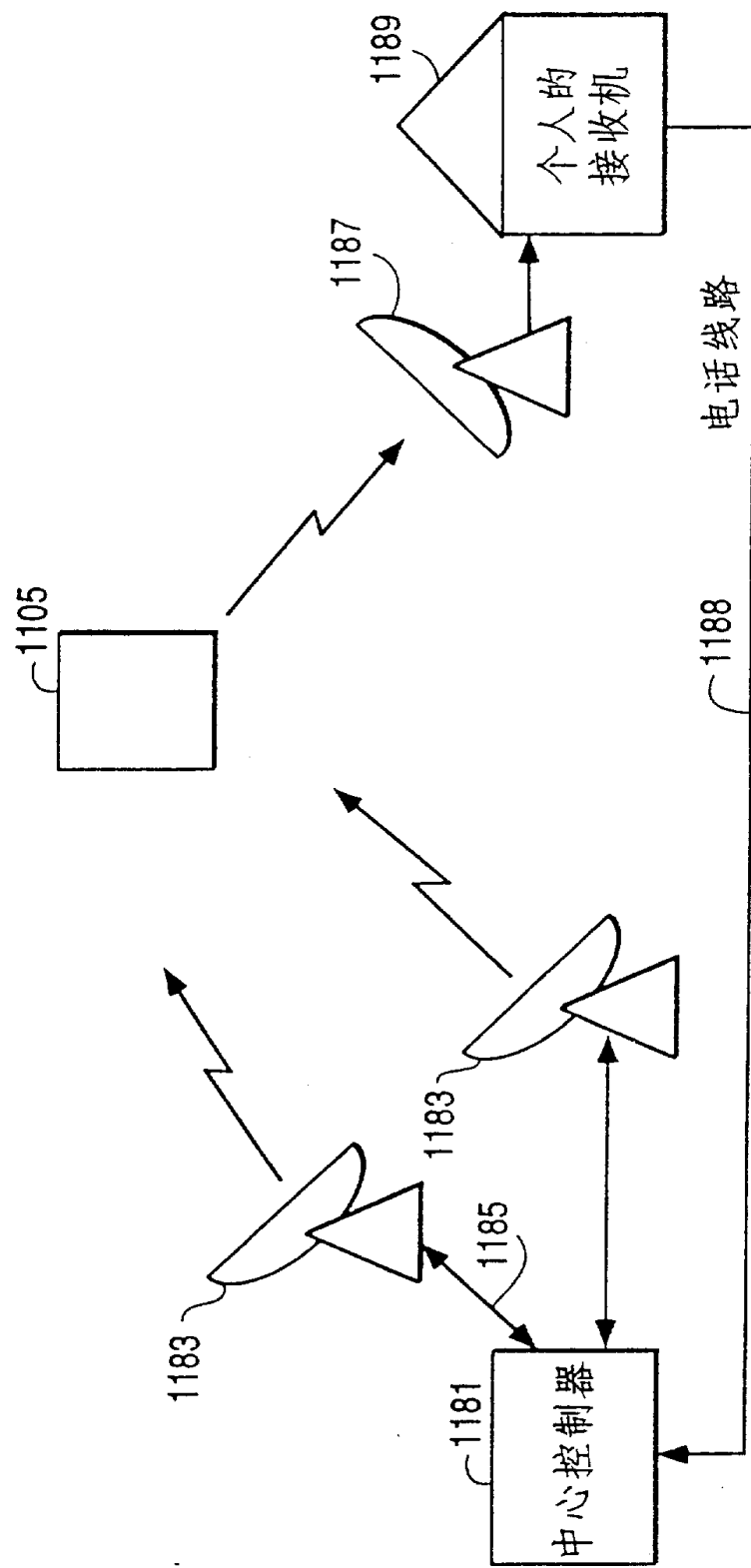


图 11

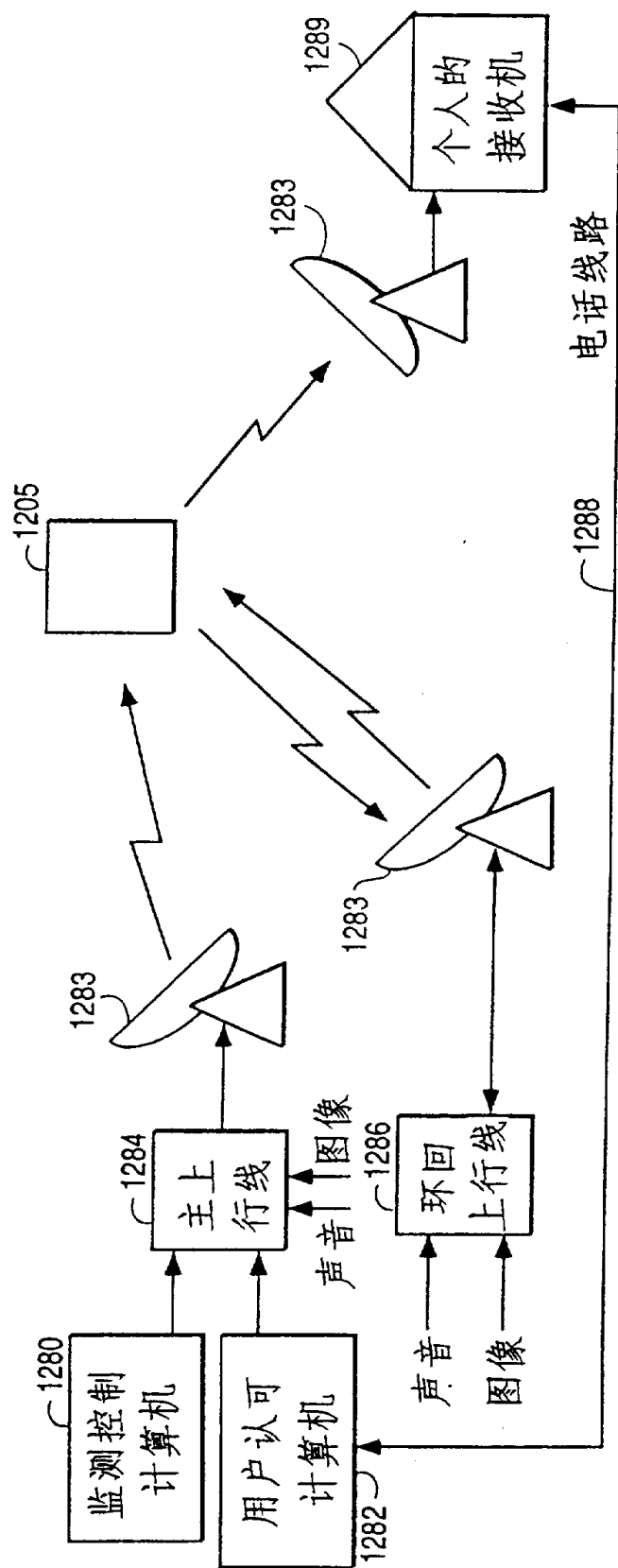


图 12

图 13

