[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04L 9/00
G09C 1/00

[12] 发明专利说明书

专利号 ZL 98119520.2

[45] 授权公告日 2005 年 9 月 14 日

[11] 授权公告号 CN 1219381C

[22] 申请日 1998.9.18 [21] 申请号 98119520.2
[30] 优先权
[32] 1997. 9.18 [33] JP [31] 253158/1997
[71] 专利权人 松下电器产业株式会社
地址 日本国大阪府
[72] 发明人 片冈充照 原田武之助 町田和弘
增田功
审查员 许凌云

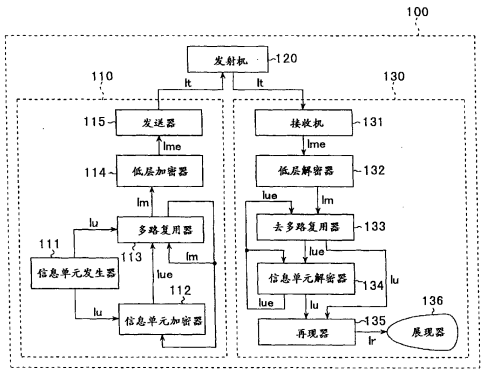
[74] 专利代理机构 上海专利商标事务所有限公司
代理人 陈 亮

权利要求书 5 页 说明书 43 页 附图 25 页

[54] 发明名称 信息传输方法及其装置

[57] 摘要

一种信息传输系统，传输包含多个信息单元的加密信息，在至少两个用户之间进行通信。每个信息单元被分层加密，并彼此多路复用。此信息传输系统由发送单元和接收单元构成。发送单元设有产生信息单元的信息单元发生器。加密信息单元以产生加密信息单元的加密器，以及至少多路复用这些信息单元和所述加密信息单元之一以产生多路信息单元的多路复用器。接收单元设有解密加密信息以产生多路信息单元的低层解密、把多路信息单元去多路复用成加密信息单元、多路信息单元或信息单元的去多路复用器，以及解密加密的信息单元的信息单元解密器。



ISSN1008-4274

1、一种用于信息传输系统的信息发射装置，其中，由多个信息单元组成的加密信息在至少两个用户之间进行通信，每个信息单元被分层加密并彼此多路复用，所述信息被加密以便于传输，其特征在于，所述装置包含：

信息单元处理装置，产生所述信息单元；

第一加密装置，用第一预定加密系统加密所述信息单元，产生加密信息单元；

第一多路复用装置，至少多路复用所述信息单元和所述加密信息单元之一，以产生多路信息单元；和

发送装置，用于发送所述加密多路信息。

2、如权利要求1所述的信息发射装置，其特征在于，还包含：

第二加密装置，用第二预定加密系统加密所述多路信息，产生所述加密多路信息；

第二多路复用装置，多路复用所述加密信息单元，以产生所述多路信息。

3、如权利要求2所述的信息发射装置，其特征在于，还包含：

第三加密装置，用第三预定加密系统加密所述多路信息，产生加密多路信息单元。

4、如权利要求3所述的信息发射装置，其特征在于，所述第三预定加密系统与应用于所述加密信息的一样。

5、如权利要求3所述的信息发射装置，其特征在于，所述第二预定加密系统与所述第三预定加密系统相同。

6、如权利要求3所述的信息发射装置，其特征在于，所述第一、第二和第三预定加密系统相同。

7、如权利要求1所述的信息发射装置，其特征在于，所述发送装置把所述加密多路信息转换成传输路径规定的格式。

8、如权利要求1所述的信息发射装置，其特征在于，所述第一加密装置用传输路径规定的加密系统加密所述信息单元。

9、一种用于信息传输系统的信息接收装置，其中，由多个信息单元组成的加密信息在至少两个用户之间进行通信，每个信息单元被分层加密并彼此多路复用，所述信息被加密以便于传输，其特征在于，所述装置包含：

第一解密装置，用第一解密系统对所述加密信息进行解密，产生第一多路信息单元；

第一去多路复用装置，把所述第一多路信息单元去多路复用成第一加密信息单元、第二多路信息单元和所述信息单元三者中的任一种；

第二解密装置，用第二解密系统对所述第一加密信息单元进行解密，产生所述信息单元或第二加密信息单元；

存储装置，设置在所述第一去多路复用装置和所述第二解密装置之间，用于存储所述第一和第二加密信息单元二者中的任何一种；和

再现装置，用于接收所述第二解密装置的所述加密信息单元，产生指示所述加密信息内容的再现信息，所述再现装置请求所述存储装置向所述第二解密装置提供所述存储的加密信息单元。

10、如权利要求 9 所述的信息接收装置，其特征在于，还包含：

第二去多路复用装置，去多路复用所述第二多路信息单元；

第三解密装置，用第三预定解密系统解密所述第二加密信息单元，产生所述信息单元。

11、如权利要求 9 所述的信息接收装置，其特征在于，所述第一解密系统与应用于所述加密信息的一样。

12、一种传输包含多个信息单元的加密信息的信息传输方法，每个信息单元被分层加密并彼此多路复用，所述加密信息在至少两个用户之间进行通信，所述信息被加密，以便传输，其特征在于，所述方法包含下列步骤：

产生所述信息单元；

用第一预定加密系统加密所述信息单元，产生加密信息单元；

多路复用至少所述信息单元和所述加密信息单元之一，以产生多路信息单元。

13、如权利要求 12 所述的信息传输方法，其特征在于，还包含下列步骤：

用第二预定加密系统加密所述多路信息，产生所述加密多路信息；

多路复用所述加密信息单元，以产生所述多路信息。

14、如权利要求 13 所述的信息传输方法，其特征在于，还包含：

用第三预定加密系统加密所述多路信息单元，产生加密多路信息单元。

15、如权利要求 14 所述的信息传输方法，其特征在于，所述第三预定加密系统与应用于所述加密信息的一样。

16、如权利要求 14 所述的信息传输方法，其特征在于，所述第二预定加密系统与所述第三预定加密系统一样。

17、如权利要求 14 所述的信息传输方法，其特征在于，所述第一、第二和第三预定加密系统相同。

18、如权利要求 12 所述的信息传输方法，其特征在于，还包含下列步骤：

把所述加密多路信息转换成传输路径规定的格式。

19、如权利要求 12 所述的信息传输方法，其特征在于，在所述加密步骤，用传输路径规定的加密系统加密所述信息单元。

20、一种接收包含多个信息单元的加密信息的信息接收方法，每个信息单元被分层加密并彼此多路复用，所述加密信息在至少两个用户之间进行通信，所述信息被加密，以便传输，其特征在于，所述方法包含下列步骤：

接收所述加密信息；

用第一解密系统解密所述加密信息，产生第一多路信息单元；

把所述第一多路信息单元去多路复用成第一加密信息单元、第二多路信息单元和所述信息单元三者中的任一种；

用第二解密系统解密所述第一加密信息单元，产生所述信息单元或第二加密信息单元；

存储所述第一和第二加密信息单元二者中的任何一种；和

接收所述加密信息单元，产生指示所述加密信息内容的再现信息，请求向第二解密装置提供所述存储的加密信息单元。

21、如权利要求 20 所述的信息接收方法，其特征在于，还包含下列步骤：

去多路复用所述第二多路信息单元；

用第三预定解密系统解密所述第二加密信息单元，产生所述信息单元。

22、如权利要求 20 所述的信息接收方法，其特征在于，所述第一解密系统与应用于所述加密信息的相同。

23、一种信息传输系统，用于传输包含多个信息单元的加密信息，每个信息单元被分层加密并彼此多路复用，所述加密信息在至少两个用户之间进行通信，所述信息被加密，以便传输，其特征在于，所述系统包含：

信息单元产生装置，产生所述信息单元；

第一加密装置，用第一预定加密系统加密所述信息单元，产生加密信息单元；

第一多路复用装置，至少多路复用所述信息单元和所述加密信息单元之一，以产生多路信息单元；

发送装置，用于发送所述加密多路信息；

第一解密装置，用第一解密系统解密所述加密信息，产生第一多路信息单元；

第一去多路复用装置，把所述第一多路信息单元去多路复用成第一加密信息单元、第二多路信息单元和所述信息单元三者中的任何一种；

第二解密装置，用第二解密系统解密所述第一加密信息单元，产生所述信息单元或第二加密信息单元。

24、如权利要求 23 所述的信息传输系统，其特征在于，还包含：

第二加密装置，用第二预定加密系统加密所述多路信息，产生所述加密多路信息；

第二多路信息，多路复用所述加密信息单元，产生所述多路信息。

25、如权利要求 24 所述的信息传输系统，其特征在于，还包含：

第三加密装置，用第三预定加密系统加密所述多路信息，产生加密多路信息单元。

26、如权利要求 25 所述的信息传输系统，其特征在于，所述第三预定加密系统与应用于所述加密信息的一样。

27、如权利要求 25 所述的信息传输系统，其特征在于，所述第二预定加密系统与所述第三预定加密系统一样。

28、如权利要求 25 所述的信息传输系统，其特征在于，所述第一、第二和第三预定加密系统相同。

29、如权利要求 23 所述的信息传输系统，其特征在于，所述发送装置把所述加密多路信息转换成传输路径规定的格式。

30、如权利要求 23 所述的信息传输系统，其特征在于，所述第一加密装置用传输路径规定的加密系统加密所述信息单元，

31、如权利要求 23 所述的信息传输系统，其特征在于，还包含：

第二去多路复用装置，去多路复用所述第二多路信息单元；

第三解密装置，用第三预定解密装置解密所述第二加密信息单元，产生所述信息单元。

32、如权利要求 23 所述的信息传输系统，其特征在于，所述第一解密系统与应用于所述加密信息的一样。

33、如权利要求 23 所述的信息传输系统，其特征在于，还包含：

存储装置，设置在所述第一去多路复用装置与所述第二解密装置之间，存储任何所述第一和第二加密信息单元二者中的任何一种。

34、如权利要求 26 所述的信息传输系统，其特征在于，还包含：

再现装置，接收所述第二解密装置的所述加密信息，产生指示所述加密信息内容的再现信息，所述再现装置请求所述存储装置向所述第二解密装置提供所述存储的加密信息单元。

信息传输方法及其装置

技术领域

本发明一般涉及在计算机通信和数据广播中加密信息和传输加密信息的方法及其装置。

背景技术

在图 25 中，示出了一种传统信息传输装置。传统信息传输装置 1900 包括发送单元 1910、发射机 1920 以及接收单元 1930。现在以两类专门的例子来描述，它们是作为例子 1 的在互联网中的信息传输，以及作为例子 2 的数字广播。多个接收单元 1910 可以对应于一个发送单元 1930。

发送单元 1930 产生发送信息，它是通过把信息单元 Iu 经过多路复用和加密而获得的，并由发送单元输出。信息单元 Iu 是对用户来说具有含义的电子数据的集合，例如文本信息、语音信息、静止图像信息、活动图像信息、HTML(超文本组成语言)信息及这些信息的组合。

发送单元 1910

发送单元 1910 包含信息单元发生器 1911、多路复用器 1912、低层加密器 1913 以及发送器 1914。

信息单元发生器 1911 产生多个信息单元，并输出。在例子 1 中，信息单元发生器 1911 输出信息单元 Iu，该信息单元 Iu 为例如用户利用键盘等输入的文本、采集到计算机中的图像以及其它已存储在计算机内的数据。信息单元发生器 1911 是例如电子邮件软件的输入屏幕部分和互联网上广播站的服务器。

另一方面，在例子 2 中，产生的所有信息单元 Iu 都预先存储在信息单元发生器 1911 内。考虑仅根据预定方案选择输出信息单元 Iu 的方法。信息单元发生器 1911 是包含数据广播发送系统内的节目管理系统、VTR 的载送机构、MPEG-2 编码器、数字广播的 EPG(电子节目指南)管理发送系统等的广播站系统。必须按长时间保持的相同内容发送诸如 EPG 等附加信息。因此，在某些情况下，在信息单元发生器 1911 内以

秒为周期重复输出相同的内容。

多路复用器 1912 接收信息单元发生器 1911 输出的多个信息单元 Iu。然后，多路复用器 1912 多路复用输入的信息单元 Iu，并输出这些被多路复用的信息单元 Iu 作为多路信息 Im。通过多路复用，多个信息单元 Iu 被转换成适用在发射机 1920 内高效传输的格式(多路信息 Im)。

在例子 1 中，多路复用器 1912 为 MIME(多用互联网邮件扩展)编码器，用于例如在互联网上通过电子邮件发送多媒体信息。在这种情况下，多路复用器 1912 分别取得文本信息、图像信息、语音信息等多个信息单元 Iu 作为要素。然后，多路复用器 1912 把这些部件转换成符合 MIME 的多部分消息，以集中多个要素，并输出该消息。MIME 的正式规范按 RFC(征求意见)1521/1522 定义。

另一方面，在例子 2 中，多路复用器 1912 为业务多路复用器，它从例如多个流数据中获得 MPEG-2 系统的 TS(传送流)。MPEG-2 系统的 TS 按 ISO/IEC CD 13818-1 标准化。在这种情况下，多路复用器 1912 把信息单元发生器 1911 输出的多个信息单元 Iu 分成数据包，称为 PEC(分组基本流)，并根据某一规则多路复用获得的数据包。

低层加密器 1913 接收多路复用器 1912 输出的多路信息，并根据预定的加密算法对多路信息进行加密，输出加密结果，作为加密多路信息 Ime。在例子 1 中，低层加密器 1913 可以是软件 PGP(颇佳保密)，其上用加密选项启动 RSA 密码，RSA 密码是例如安装在其内的公共密钥。低层加密器 1913 的输出是利用 RSA 密码加密的电子邮件的文本。RSA 密码在 R.L. Rivest、A. Shamir 以及 L. Adleman 撰写的文章中有详细描述，他们是“获得数字鉴名和公共密钥加密系统的方法”的作者(1978 年 2 月发行的 ACM 通信，第 21 卷第 2 期)。PGP 在 Simson Garfinkel 撰写的名称为“PGP：颇佳保密”一文内有详细描述(O'Reilly 及其合作者)。

另一方面，在例子 2 中，低层加密器 1913 可以是例如传送层加密器。低层加密器 1913 利用诸如 MULTI-2 以及 DES(数据加密标准)等加密算法对输入的 MPEG-2 的 TS 的有效负载部分进行加密，并输出加密结果：MPEG-2 的加密 TS。请注意，ARIB 报告第 74 期中描述的 MULTIS 是由 Hitach 公司为数字广播系统的应用开发的。

发送器 1914 接收低层加密器 1913 输出的加密多路信息 Ime，并把加密多路信息 Ime 转换成发送信息 It，输入到发射机 1920。在例子 1 中，发送器 1914 是一种程序，把由目的字段、发送者字段等组成的邮件首标加到电子邮件的文本中。发送器 1914 的输出是增加了邮件首标的电子邮件的文本。另一方面，在例子 2 中，发送器 1914

是 MPEG-2 的 TS 的纠错编码器和调制器。

发射机 1920

发射机 1920 向实际远程点发射输入的发送信息 It。发射机 1920 的输入和输出都是发送信息 It。发射机 1920 的输入不会没有任何差错地出现在接收单元 1930 的输出上。在例子 1 中，发射机 1920 为多个邮件通信灵元(代理进程)，它们通过诸如互联网等通道彼此连接，解释并执行 SMTP(简单邮件传输协议)。典型邮件通信灵元的例子包括“发送邮件”。SMTP 的正式规范按 RFC821、RFC822 以及 RFC974 定义。发送邮件在 E. Allman 撰写的题目为“发送邮件-互联网邮件路由器”Unix 程序手册”一文中有详细描述(1983 年发表，CSRG U. C. Berkeley)。

另一方面，在例子 2 中，发射机 1920 由上变频器、向卫星发送数据的抛物面天线、通信卫星以及地面接收天线组成。

接收单元 1930

接收单元 1930 接收发射机 1920 发送的发送信息 It，并向用户提供信息单元 Iu。接收单元 1930 包括接收机 1931、低层解密器 1932、去多路复用器 1933、再现器 1934、存储器 1935 以及展现器 1936。

接收机 1931 接收发射机 1920 输出的发送信息 It，并取出全部或部分信息。然后，接收机 1931 根据取出的发送信息 It 再现加密的多路信息。在例子 1 中，接收机 1931 为邮件传输的前端程序。另一方面，在例子 2 中，接收机 1931 由卫星广播调谐器、解调器和纠错解码器连接而成。

低层解密器 1932 接收接收机 1931 输出的加密多路信息 Ime，并对加密多路信息 Ime 进行解密，再现多路信息 Im。在例子 1 中，低层解密器 1932 为 PGP 程序，它由解密选项来启动。另一方面，在例子 2 中，低层解密器 1932 为传送层解密器。

去多路复用器 1933 从多路信息 Im 中分离出每个信息单元 Iu，取出分离信息单元 Iu，并输出取出的信息单元 Iu。在例子 1 中，去多路复用器 1933 为 MIME 解码器，它把文本信息、图像信息等分离成分离的信息，以取出分离信息，这些信息是各种包括在多部分消息内的各种要素。另一方面，在例子 2 中，去多路复用器 1933 是 MPEG-2 的 TS 的去多路复用器。去复用器 1933 分离由 MPEG-2 系统多路复用的多个流。

再现器 1934 接收去多路复用器 1933 输出的信息单元 Iu，产生作为可再现信息

的再现信息 Ir1。在例子 1 中，再现器 1934 可以是文本文件浏览器、图像文件显示软件等。另一方面，在例子 2 中，再现器 1934 可以是 MPEG-2 解码器，以再现用例如 MPEG-2 编码的语音或图像。在这种情况下，输出为 NTSC(国家电视制式标准委员会)信号或模拟语音信号。

存储器 1935 接收再现器 1934 输出的再现信息，并存储第一再现信息 Ir1。然后，根据再现的需要，存储器 1935 也输出第一再现信息 Ir1 作为第二再现信息 Ir2。这一操作在后面称为“再现”。请注意，第一和第二再现信息 Ir1 和 Ir2 其内容是一致的，不同之处在于展现时间上，在下文即将描述。

在例子 1 中存储器 1935 可以是 OS(操作系统)文件系统或管理电子邮件类别的软件。另一方面，在例子 2 中，存储器 1935 可以是记录和再现 NTSC 信号和模拟语音信号的 VTR(磁带录像机)或 VCR(盒式磁带录音机)。

展现器 1936 接收再现器 1934 输出的第一再现信息 Ir1 和存储器 1935 输出的第二再现信息 Ir2，向用户显示其中之一或全部信息。在例子 1 中，展现器 1936 可以是诸如 X-Window 或 Micorsoft Windows 等窗口系统，向用户展现图像和声音。另一方面，在例子 2 中，展现器 1936 可以是电视接收机，用于输入和接收例如 NTSC 信号和模拟语音信号。

在图 26 中，示出了信息传输装置 1900 产生的加密多路信息单元 Ime0d 的一个例子。根据该例子，加密多路信息单元 Ime0d 包括四个信息单元 Iu1d, Iu2d, Iu3d 和 Iu4d，在图中每个都用一个圆圈指示。虚线指示的矩形表示在低层加密器 1913 中对信息单元 Iu1d, Iu2d, Iu3d 和 Iu4d 一次加密获得的加密多路信息单元 Ime。换句话说，所有信息单元 Iu1d, Iu2d, Iu3d 和 Iu4d 都用相同的密码加密，由传输级的单个加密层保护。

信息单元 Iu1d, Iu2d, Iu3d 和 Iu4d 分别表示有天气预报的旅游地指南、旅游地的天气预报、国家天气预报，以及局部地区天气预报。对这些相对于天气预报的子分割区进行加密，产生总天气预报节目 Iue。因此，从加密的观点来看，这些子分割区没有层次。

运作

参照图 27 和 28，下面描述传统传输装置 1900 的工作情况。在图 27 中，示出了发送单元 1910 和发射机 1920 进行的工作的流程图。

在步骤S2001，信息单元发生器1911产生多个信息单元Iu，并输出产生的信息单元Iu。产生信息单元Iu的例子包括用户输入信息单元Iu和如例子1中一样指定文件的方法，以及如例子2一样，根据预定规则从存储的信息单元Iu中选择输出信息单元Iu的方法。

在步骤S2002，多路复用器1912多路复用在步骤S2001产生的信息单元Iu，并把其结果作为多路信息Im输出。多路信息Im在例子1情况下是与MIME一致的多部分数据，而在例子2中，是表示MPEG-2系统的TS的数据。

在步骤S2003，低层加密器1913对在步骤S2002多路复用获得的多路信息进行加密，产生加密多路信息Ime。在例子1中，多路信息Im是利用RSA密码等来加密的。另一方面，在例子2中，利用例如Hitachi公司制造的MULTI-2密码对MPEG-2的TS的有效负载部分进行加密。

在步骤S2004，发送器1914把步骤S2003加密获得的加密多路信息Ime转换成可以发送或适合由发射机1920发送的格式。在例子1中，把例如：“至:字段，来自:字段”的信息加到加密多路信息Ime的邮件文本的首标中，并输出该信息作为发送信息It。另一方面，在例子2中，输出利用纠错码对MPEG-2的TS进行编码，然后对编码的TS进行调制而获得的信息。

在步骤S2005，发射机1920向实际远距点发送信息It。在例子1中，安装在一台或多台连接的计算机上的邮件通信灵元根据SMTP与诸如互联网或LAN(局域网)等计算机网络进行通信。因此，邮件从一台计算机上的邮件通信灵元传输到另一台计算机上的邮件通信灵元。

另一方面，在例子2中，由抛物面天线向通信卫星发射在上变频器中变频而获得的发送信息It。通信卫星把接收到的发送信息It由转发器向地面发射。地面接收天线接收通信卫星的发送信息It。

参照图28，下面描述接收单元1930进行的操作。在图28中，具体示出了从发送信息It中实时取出信息单元Iu、向用户展现信息单元Iu、当用户需要时存储信息单元Iu以及以后再次观看信息单元Iu的操作。

在步骤S2101，当用户实时观看发送信息It的信息单元Iu时，过程进入到步骤S2102。当用户观看预先存储在存储器1935内的信息单元Iu时，过程进入到步骤S2109。

在步骤S2102，接收机1931接收发射机1920的发送信息It，并从输入的发送信

息 It 中取出部分或所有加密多路信息 Ime。在例子 1 中，进行取出一个发给特定用户的电子邮件数据处理。另一方面，在例子 2 中，通过调谐到预定的频率，进行处理，由 PID(数据包标识符)过滤出要找的特定数据包存储信息，并选择和取得该数据包。

在步骤 S2103，低层解密器 1932 接收接收机 1931 输出的加密多路信息 Ime，并对加密多路信息 Ime 解密，输出多路信息 Im。在例子 1 中，低层解密器 1932 用解密选项启动的 PGP 程序。用 PGP 程序的 RSA 密码进行解密，并输出解密结果。另一方面，在例子 2 中，对利用 MULTI-2 密码加密多路信息 Im 进行解密，获得多路信息 Im。

在步骤 S2104，去多路复用器 1933 从多路信息单元 Im 中分离出每个信息单元 Iu，取出信息单元 Iu。在例子 1 中，去多路复用器 1933 分离出根据 MIME 多路复用获得的多部分消息的每个要素。因此，分离出文本信息、图像信息、语音信息等各要素，作为离散的信息单元 Iu。

另一方面，在例子 2 中，去多路复用器 1933 根据 PID(数据包标识符)分离 MPEG-2 系统多路复用的多个流。因此，分离出诸如 MPEG-2 视频流、MPEG-1 音频流和 EPG 等附加信息作为离散信息单元 Iu。按 ITU-T H.262 对 MPEG-2 图像进行标准化，按 ISO/IEC 11172-3 标准使 MPEG-1 语音标准化。

在步骤 S2105，再现器 1934 接收去多路复用器 1933 输出的信息单元 Iu，并产生第一再现信息 Ir1 作为可再现信息。在例子 1 中，当信息单元 Iu 例如为文本信息时，则选择和列出对应于各字符码的字体，产生位图格式，作为再现信息 Ir1。当信息单元 Iu 是诸如 JPEG(联合静止图像专家组)等的图像信息格式时，把它扩展成位图格式，并输出扩展结果作为再现信息。JPEG 按 ISO/IEC 10918 进行标准化。当信息单元 Iu 为语音信息时，用与数字-模拟(D/A)转换器相同的功能把它转换成模拟语音信号。也把模拟语音信号作为再现信息输出。

另一方面，在例子 2 中，当在步骤 S2104 获得的信息单元 Iu 为 MPEG-2 视频流时，对 MPEG-2 图像进行解码，输出 NTSC 信号作为再现信息。当信息单元 Iu 为语音流时，通过 D/A 转换把它转换成模拟语音信号，并输出该模拟语音信号。

在步骤 S2106，根据再现信息的格式，展现器 1936 向用户展现在步骤 S2105 获得的第一再现信息 Ir1。在例子 1 中，当在步骤 S2105 获得的再现信息为位图格式时，展现器 1936 排列再现信息 Ir1，并在显示屏上显示该再现信息 Ir1。从这样就向用户展现再现信息 Ir1。当在步骤 S2105 获得的再现信息为模拟语音信号时，把模拟信号送到扬声器，转换成声音，并可闻地向用户展现。

另一方面，在例子 2 中，在显示器上接收到在步骤 S2105 获得的作为再现信息的 NTSC 信号，把模拟语音信息发送给扬声器，向用户展现再现信息。

在步骤 S2107，当用户想存储当前发送信息中的信息时，过程进入到步骤 S2108，而在另一种情况下，过程进入到步骤 S2101。用户意图的具体例子包括指定观看和预设定时器等。

在步骤 S2108，把步骤 S2105 产生的再现信息存储在存储器 1935 中。此后，过程进入到步骤 S2101。再现信息 Ir1 可以另外存储在存储器 1935 内，或者，用另外存储的信息 Ir1 改写已存储的信息 Ir1。另外，在原版本已存储在存储器 1935 内的情况下，可以用原版本替换该信息。

在例子 1 中，在文件系统中存储和排列再现信息。信息单元 Iu 以例如到达的顺序、发送者以及主题来排列。另一方面，在例子 2 中，把诸如图像和语音的再现信息记录在录像带上。例如，可以同时存储与图像和语音不同的在 NTSC 垂直消隐周期内多路复用的附加信息。在记录数字信息的情况下，可以同时存储不是图像和语音的多个数据流。

在步骤 S2109，输出存储在存储器 1935 内的第一再现信息 Ir1，作为第二再现信息 Ir2。在例子 1 中，输出用户从文件系统内排列和存储的再现信息 Ir1 选出的再现信息 Ir2(Ir1)。另一方面，在例子 2 中，从录像带等再出图像和语音。虽然用户希望的选择再现信息 Ir2(Ir1)可以利用作为存储器 1935 的功能实现的方法自动进行，但用户自己也可以选择录像带等，并在存储器 1935 内设置所选的录像带。

在步骤 S2110，展现器 1936 向用户展现在步骤 S2109 输出的再现信息。此后，过程回到步骤 S2101。除了过程返回到步骤 S2101 之外，步骤 S2110 的操作可以与步骤 S2106 相同。

然而，如上所述，传统信息传输装置 1900 面临下列两个主要问题。第一个问题是限制了对设置防止不正当解密的密码抗解力的自由度。通常，对付不正当解密而设置的密码抗解力越大，正常解密方法进行解密过程需要的诸如计算机资源和处理时间等资源越多。因此，根据加密目的要求的保密性需要利用具有必要和足够抗解力的密码进行加密。

例如，当作为要发送的信息的一部分的信息单元 Iu 需要保密性高的加密时，作为要素的信息单元 Iu 必须利用具有高抗解力的密码进行加密。例如，在天气预报节目中，全国天气预报是免费的，则不加密。然而，详细的本地预报是要收费的，所以

每个用户专门定制的天气预报是要额外收费的。因此，本地的详细天气预所必须经过保密性比全国天气预报更高的加密，并且，专门定制的天气预报必须经过保密性比本地详细天气预报更高的加密。

虽然在许多密码中，理论上增加密码分析钥的长度可以调整密码的抗解力，但由于例如通常所用的加密硬件的限制，密码的抗解力未必具有足够的自由度。

然而，当使用自由度可以增加的密码的加密硬件时，会产生一些缺点。例如，接收单元 1930 变得复杂，必须准备专用的硬件。在对利用抗解力不同的密码加密的信息单元 Iu 改变密钥时，在最差的情况下，必须对每个信息单元 Iu 进行加密和解密，这样效率不高。

第二个问题是信息单元 Iu 必须在存储之前解密。通常，以所有人可以接入的媒体发送收费信息，例如通过广播。进行这种收费广播时，往往在发送单元 1910 中以加密状态发送信息，在接收单元 1930 解密信息的时间点上进行收费。这是为了防止不付费的用户不正当地观看。

传统信息传输装置 1900 必须在用户不实时观看信息单元 Iu 之前，有时在传输之后，存储解密发送信息 It 产生的再现信息 Ir，该发送信息 It 是通过对发送单元 1910 发送的信息单元 Iu 进行加密产生的。考虑这样的情况，即预先存储可以观看的信息单元 Iu，在以后观看。

当存储了相当大量的可以以后观看的信息单元 Iu 时，即使它们已根据发送信息 It 解密，但最终某些信息单元 Iu 也不观看。在存储时解密信息单元 Iu 的同时进行收费的情况下，这对用户是不利的。相反，当仔细地选择和存储少量的总是在以后观看的信息单元 LU 时，由于没有存储，即使用户以后希望观看信息单元 Iu，也不能看到信息单元 Iu。其原因是通常用户自己预先确定以后要观看的信息单元是相当困难的。

另一方面，也考虑了改变接收单元和存储发送信息 It 的结构的方法。原方法中，当重复发送诸如具有相同内容的 EPG 等附加信息时，这些信息彼此重叠。而且，包括旧的和新的内容的信息单元 Iu 都存储，而与其版本无关，不惜它们中最新的信息单元，例如空难幸存者数目和版本更新的软件。因此，浪费了存储容量，这是不现实的，取出新的信息单元 Iu 需要额外的处理。

发明内容

本发明解决了上述的传统问题。在本发明的第一方面，提供了一种用于信息传输

系统的信息传输装置，其中，由多个信息单元组成的加密信息在至少两个用户之间进行通信，每个信息单元被分层加密并彼此多路复用，所述信息被加密以便于传输，所述装置包含：

信息单元处理装置，产生所述信息单元；

第一加密装置，用第一预定加密系统加密所述信息单元，产生加密信息单元；

第一多路复用装置，至少多路复用所述信息单元和所述加密信息单元之一， 以产生多路信息单元。

从上面可以看出，根据本发明的第一方面，可以产生由多个信息单元组成的加密信息，它们被分层加密，并彼此以各种组合方式被多路复用。

根据本发明的第二方面，在本发明的第一方面中，该信息传输装置还包含：

第二加密装置，用第二预定加密系统加密所述多路信息，产生所述加密多路信息；

第二多路复用装置，多路复用所述加密信息单元，以产生所述多路信息。

从上可以看出，根据本发明的第二方面，可以用不同的加密系统加密每个信息单元，确保对非法接入信息的解密力。

根据本发明的第三方面，在本发明的第二方面的信息传输装置中，还包含：

第三加密装置，用第三预定加密系统加密所述多路信息，产生加密多路信息单元。

根据第四方面，在本发明的第三方面的信息传输装置中，所述第三预定加密系统与应用于所述加密信息的一样。

根据第五方面，在根据本发明的第三方向的信息传输装置中，所述第二预定加密系统与所述第三预定加密系统相同。

根据第六方面，在本发明的第三方面的信息传输装置中，所述第一、第二和第三预定加密系统相同。

根据第七方面，在根据本发明的第一方面的信息传输装置中，还包含：

发送装置，用于把所述加密多路信息转换成适合有效发送的格式。

根据第八方面，在本发明的第一方面的信息传输装置中，所述第一加密装置用适合信息发送的加密系统加密所述信息单元。

根据本发明第九方面，提供一种用于信息传输系统的信息传输装置，其中，由多个信息单元组成的加密信息在至少两个用户之间进行通信，每个信息单元被分层加密

并彼此多路复用，所述信息被加密以便于传输，所述装置包含：

第一解密装置，用第一解密系统对所述加密信息进行解密，产生第一多路信息单元；

第一去多路复用装置，把所述第一多路信息单元去多路复用成第一加密信息单元、第二多路信息单元和所述信息单元三者中的任一种；

第二解密装置，用第二解密系统对所述第一加密信息单元进行解密，产生所述信息单元或第二加密信息单元。

根据第十方面，在本发明的第十方面的信息传输装置中，还包含：

第二去多路复用装置，去多路复用所述第二多路信息单元；

第三解密装置，用第三预定解密系统解密所述第二加密信息单元，产生所述信息单元。

根据第十一方面，在根据本发明的第九方面的信息传输装置中，所述第一解密系统与应用于所述加密信息的一样。

根据第十二方面，在根据本发明的第九方面的信息传输装置中，还包含：

存储装置，设置在所述第一去多路复用装置和所述第二解密装置之间，用于存储所述第一和第二加密信息单元二者中的任何一种。

根据第十三方面，在本发明的第十二方向的信息传输装置中，还包含：

再现装置，用于接收所述第二解密装置的所述加密信息单元，产生指示所述加密信息内容的再现信息，所述再现装置请求所述存储装置向所述第二解密装置提供所述存储的加密信息单元。

根据第十四方面，提供一种传输包含多个信息单元的加密信息的信息传输方法，每个信息单元被分层加密并彼此多路复用，所述加密信息在至少两个用户之间进行通信，所述信息被加密，以便传输，所述方法包含下列步骤：

产生所述信息单元；

用第一预定加密系统加密所述信息单元，产生加密信息单元；

多路复用至少所述信息单元和所述加密信息单元之一，以产生多路信息单元。

从上面可以看出，根据本发明的第十四方向，可以产生包含多个信息单元的加密信息，它们被分层加密，并彼此以不同组合被多路复用。

根据第十五方面，在本发明的第十四方面的信息传输方法中，还包含下列步骤：

用第二预定加密系统加密所述多路信息，产生所述加密多路信息；

多路复用所述加密信息单元，以产生所述多路信息。

从上可以看出，根据本发明的第十五方面，可以用不同的加密系统加密每个信息单元，确保对非法接入信息的解密力。

根据第十六方面，在本发明的第十五方面的信息传输方法中，还包含：

用第三预定加密系统加密所述多路信息单元，产生加密多路信息单元。

根据第十七方面，在本发明的第十六方面的信息传输方法中，所述第三预定加密系统与应用于所述加密信息的一样。

根据第十八方面，在本发明第十六方面的信息传输方法中，所述第二预定加密系统与所述第三预定加密系统一样。

根据第十九方面，在本发明的第十六方面的信息传输方法中，所述第一、第二和第三预定加密系统相同。

根据第二十方面，在本发明的第十四方面的信息传输方法中，还包含下列步骤：

把所述加密多路信息转换成适合有效发送的格式。

根据第二十一方面，在根据本发明的第十四方面的信息传输方法中，在所述加密步骤，用适合信息发送的加密系统加密所述信息单元。

根据第二十二方面，提供一种传输包含多个信息单元的加密信息的信息传输方法，每个信息单元被分层加密并彼此多路复用，所述加密信息在至少两个用户之间进行通信，所述信息被加密，以便传输，所述方法包含下列步骤：

用第一解密系统解密所述加密信息，产生第一多路信息单元；

把所述第一多路信息单元去多路复用成第一加密信息单元、第二多路信息单元和所述信息单元三者中的任一种；

用第二解密系统解密所述第一加密信息单元，产生所述信息单元或第二加密信息单元。

根据第二十三方面，在本发明的第二十二方面的信息传输方法中，还包含下列步骤：

去多路复用所述第二多路信息单元；

用第三预定解密系统解密所述第二加密信息单元，产生所述信息单元。

根据第二十四方面，在本发明的第二十二方面的信息传输装置中，所述第一解密系统与应用于所述加密信息的相同。

根据第二十五方面，在本发明的第二十四方面的信息传输装置中，还包含下列步

骤：

存储所述第一和第二加密信息单元二者中的任何一种。

根据第二十六方面，在本发明的第二十五方面的信息传输装置中，还包含下列步骤：

接收所述加密信息单元，产生指示所述加密信息内容的再现信息，请求向第二解密装置提供所述存储的加密信息单元。

根据第二十七方面，提供一种信息传输系统，用于传输包含多个信息单元的加密信息，每个信息单元被分层加密并彼此多路复用，所述加密信息在至少两个用户之间进行通信，所述信息被加密，以便传输，所述系统包含：

信息单元产生装置，产生所述信息单元；

第一加密装置，用第一预定加密系统加密所述信息单元，产生加密信息单元；

第一多路复用装置，至少多路复用所述信息单元和所述加密信息单元之一，以产生多路信息单元；

第一解密装置，用第一解密系统解密所述加密信息，产生第一多路信息单元；

第一去多路复用装置，把所述第一多路信息单元去多路复用成第一加密信息单元、第二多路信息单元和所述信息单元三者中的任何一种；

第二解密装置，用第二解密系统解密所述第一加密信息单元，产生所述信息单元或第二加密信息单元。

从上面可以看出，根据本发明的第二十七方面，可以产生包含多个信息单元的加密信息，它们被分层加密，并彼此以各种组合被多路复用。也可以根据如此分层加密和多路复用的信息中再出信息。

根据第二十八方面，在本发明第二十七方面的信息传输系统中，还包含：

第二加密装置，用第二预定加密系统加密所述多路信息，产生所述加密多路信息；

第二多路信息，多路复用所述 加密信息单元，产生所述多路信息。

从上可以看出，根据本发明的第二方面，可以用不同的加密系统加密每个信息单元，确保对非法接入信息的解密力。

根据第二十九方面，在本发明第二十八方面的信息传输系统中，还包含：

第三加密装置，用第三预定加密系统加密所述多路信息，产生加密多路信息单元。

根据第三十方面，在本发明第二十九方面的信息传输系统中，所述第三预定加密系统与应用于所述加密信息的一样。

根据第三十一方面，在本发明第二十九方面的信息传输系统中，所述第二预定加密系统与所述第三预定加密系统一样。

根据第三十二方面，在本发明的第二十九方面的信息传输系统中，所述第一、第二和第三预定加密系统相同。

根据第三十三方面，在本发明的第二十七方面的信息传输系统中，还包含：

发送装置，把所述加密多路信息转换成适合有效发送的格式。

根据第三十四方面，在本发明的第二十七方面的信息传输系统中，所述第一加密装置用适合信息发送的加密系统加密所述信息单元，

根据第三十五方面，在本发明的第二十七方面的信息传输系统中，还包含：

第二去多路复用装置，去多路复用所述第二多路信息单元；

第三解密装置，用第三预定解密装置解密所述第二加密信息单元，产生所述信息单元。

根据第三十六方面，在本发明的第二十七方面的信息传输系统中，所述第一解密系统与应用于所述加密信息的一样。

根据第三十七方面，在本发明的第二十七方面的信息传输系统中，还包含：

存储装置，设置在所述第一去多路复用装置与所述第二解密装置之间，存储任何所述第一和第二加密信息单元二者中的任何一种。

根据第三十八方面，在本发明的第三十方面的信息传输系统中，还包含：

再现装置，接收所述第二解密装置的所述加密信息，产生指示所述加密信息内容的再现信息，所述再现装置请求所述存储装置向所述第二解密装置提供所述存储的加密信息单元。

附图说明

图 1 是根据本发明第一实施例的信息传输装置的框图；

图 2 是解释图 1 的信息传输装置产生的加密多路信息单元的辅助图；

图 3 是图 1 的信息传输装置中的发送单元和发射机进行的操作流程图；

图 4 是根据图 1 的信息传输装置内接收单元进行的操作流程图；

图 5 是根据本发明第二实施例装置的框图；

图 6 解释图 5 的信息传输装置产生的加密多路信息单元的辅助图；

图 7 是图 5 的信息传输装置中的发送单元和发射机进行的操作流程图；

图 8 是根据图 5 的信息传输装置内接收单元进行的操作流程图；

图 9 是图 5 的信息传输装置的另一个例子的框图；

图 10 是根据本发明第三实施例装置的框图；

图 11 是解释图 10 的信息传输装置产生的加密多路信息单元的辅助图；

图 12 是根据图 10 的信息传输装置内接收单元进行的操作流程图；

图 13 是图 10 的信息传输装置的另一个例子的框图；

图 14 是根据本发明第四实施例装置的框图；

图 15 是图 14 的信息传输装置中的发送单元和发射机进行的操作流程图；

图 16 是根据图 14 的信息传输装置内接收单元进行的操作流程图；

图 17 是图 14 的信息传输装置内的存储器进行的操作的流程图；

图 18 是根据本发明第五实施例装置的框图；

图 19 是图 18 的信息传输装置中的发送单元和发射机进行的操作流程图；

图 20 是根据图 18 的信息传输装置内接收单元进行的操作流程图；

图 21 是图 18 的信息传输装置的另一个例子的框图；

图 22 是根据本发明第六实施例装置的框图；

图 23 是图 22 的信息传输装置中的发送单元和发射机进行的操作流程图；

图 24 是图 22 的信息传输装置的另一个例子的框图；

图 25 是传统信息传输装置的框图；

图 26 是解释图 25 的信息传输装置产生的加密多路信息单元的辅助图；

图 27 是图 25 的信息传输装置中的发送单元和发射机进行的工作流程图；

图 28 是图 25 的信息传输装置中的接收单元进行的工作流程图。

具体实施方式

现在参照附图的图 1 至 24 详细描述根据本发明的较佳实施例。

(第一实施例)

下面参照图 1 至 3 描述根据本发明的第一实施例的信息传输装置。描述分两类具体的例子进行，例子 1 为互联网内的信息传输，例子 2 为数字广播。信息传输装置 100 包括发送单元 110、发射机 120 和接收单元 130。

发送单元 110

发送单元 110 包括信息单元发生器 111、信息单元加密器 112、多路复用器 113、低层加密器 114 和发送器 115。信息单元发生器 111 产生多个信息单元 Iu，并输出。在例子 1 中，信息单元发生器 111 输出例如用户用键盘等输入的文本、采集到计算机内的图像以及已存储在计算机内的其它信息的信息单元 Iu。信息单元发生器 111 可以是例如电子邮件软件的输入屏幕部分以及互联网上广播站的服务器。

另一方面，在例子 2 中，产生的所有信息单元 Iu 都预先存储在信息单元发生器 111 内。考虑采用仅根据预定方案选择输出信息单元 Iu 的方法。信息单元发生器 111 是包含数据广播发送系统内的节目管理系统、VTR 的载送机构、MPEG-2 编码器、数字广播的 EPG(电子节目指南)管理发送系统等的广播站系统。必须按长时间保持的相同内容发送诸如 EPG 等附加信息。因此，在某些情况下，在信息单元发生器 111 内以秒为周期重复输出相同的内容。

信息单元加密器 112 连接到信息单元发生 111 器上，接收信息单元 Iu，以加密输入的信息单元 Iu。然后信息单元加密器 112 输出加密结果作为加密信息单元 Iue。一次加密的对象是具有信息单元 Iu 或加密结果的集合。加密信息单元 Iue 定义如下：

定义 1：加密信息单元 Iue 也是信息单元 Iu。

定义 2：一组信息单元 Iu 或加密信息单元 Iu 也是加密信息单元 Iue。

定义 3：对加密信息单元 Iue 进行加密的结果也是加密信息单元 Iue。

多路复用器 113 连接到信息单元发生器 111 和信息单元加密器 112 上，分别接收信息单元 Iu 和加密信息单元。然后，多路复用器 113 多路复用从信息单元发生器 111 和/或信息单元加密器 112 接收到的信息，并输出多路复用结果作为多路信息单元 Im。

多路复用器 113 还连接到其本身的输出端，接收产生的多路信息 Im，以再次进行多路复用。而且，多路复用器 113 的输出端也连接到信息单元加密器 112 的输入端，这样，信息单元加密器 112 可以对多路信息单元 Im 进行加密，以产生加密信息单元 Iue。

因此，多路复用器 113 处理信息单元加密器 112 输出的加密信息单元 Iue，与信息单元发生器 111 输出的信息单元 Iu 相似，作为其多路复用的对象。在认为等于一个信息单元 Iu 的条件下，处理信息单元加密器 112 每次交出的加密信息单元 Iue。多

路复用器 113 可以把信息单元发生器 111 输出的信息单元 Iu 加到预先从信息单元加密器 112 输出的加密信息单元 Iue 上，并对它们多路复用。

具体地说，多路复用器 113 接收信息单元发生器 111 输出的多个信息单元 Iu。然后，多路复用器 113 多路复用输入的信息单元 Iu，并输出多路复用的信息单元 Iue，作为多路信息 Im。通过多路复用，把多个信息单元 Iu 转换成适合发射机 120 高效发送的格式(多路信息 Im)。

在例子 1 中，多路复用器 113 为 MIME(多用互联网邮件扩展)编码器，用于例如在互联网上通过电子邮件发送多媒体信息。在这种情况下，多路复用器 113 分别取得文本信息、图像信息、语音信息等多个信息单元 Iu，作为要素。然后，多路复用器 1113 把这些要素转换成符合 MIME 的多部分消息，以集中多个要素，并输出该消息。MIME 的正式规范按 RFC(征求意见)1521/1522 来定义。

另一方面，在例子 2 中，多路复用器 113 为业务多路复用器，它从例如多个流数据中获得 MPEG-2 系统的 TS(传送流)。MPEG-2 系统的 TS 按 ISO/IEC CD 13818-1 来标准化。在这种情况下，多路复用器 113 把信息单元发生器 111 输出的多个信息单元 Iu 分成数据包，称为 PEC(分组基本流)，并根据某一规则多路复用获得的数据包。

低层加密器 114 连接到多路复用器 113 上，接收多路信息 Im，并对其加密。然后，从低层加密器 114 输出加密结果作为加密多路信息。具体地说，低层加密器 114 接收多路复用器 113 输出的多路信息 Im，并根据预定的加密算法对多路信息 Im 进行加密。然后，低层加密器 114 输出加密结果作为加密多路信息 Ime。

在例子 1 中，低层加密器 114 可以是软件 PGP(颇佳保密)，其上用加密选项启动 RSA 密码，RSA 密码是例如安装在其内的公共密钥。低层加密器 114 的输出是利用 RSA 密码加密的电子邮件的文本。RSA 密码在 R.L. Rivest、A. Shamir 以及 L. Adleman 撰写的文章中有详细描述，他们是“获得数字鉴名和公共密钥加密系统”的方法的作者(1978 年 2 月发行的 ACM 通信，第 21 卷第 2 期)。PGP 在 Simson Garfinkel 撰写的名称为“PGP：颇佳保密”一文内有详细描述(O'Reilly 及其合作者)。

另一方面，在例子 2 中，低层加密器 114 可以是例如传送层加密器。低层加密器 114 利用诸如 MULTI-2 等加密算法对输入的 MPEG-2 的 TS 的有效负载部分进行加密，并输出加密结果：MPEG-2 的加密 TS。

发送器 115 连接到低层加密器 114 上，接收加密多路信息 Ime，产生发送信息 It，并输出产生的发送信息 It。具体地说，发送器 115 把低层加密器 114 输出的加密多路

信息 Ime 转换成可以输入给发射机 120 的发送信息 It。

在例子 1 中，发送器 115 是一种程序，把由目的字段、发送者字段等组成的邮件首标加到电子邮件的文本中。发送器 115 的输出是增加了邮件首标的电子邮件的文本。另一方面，在例子 2 中，发送器 115 是 MPEG-2 的 TS 的纠错编码器和调制器。

发射机 120

发射机 120 接收发送器 115 输出的发送信息 It，并向实际远距点发该信息 It。发射机 120 的输入和输出都是发送信息 It。发射机 120 的输入不会没有任何差错地出现在接收单元 130 的输出上。在例子 1 中，发射机 120 为多个邮件通信灵元(代理进程)，它们通过诸如互联网等通道彼此连接，解释并和执行 SMTP(简单邮件传输协议)。典型邮件通信灵元的例子包括“发送邮件”。SMTP 的正式规范按 RFC821、RFC822 以及 RFC974 定义。发送邮件在 E. Allman 撰写的题目为“发送邮件-互联网邮件路由器”Unix 程序手册”一文中有详细描述(1983 年发表，CSRG U. C. Berkeley)。

另一方面，在例子 2 中，发射机 120 由上变频器、向卫星发送数据的抛物面天线、通信卫星以及地面接收天线组成。

接收单元 130

接收单元 130 从发射机 120 接收发送信息 It。然后，接收单元 130 以不同方式处理发送信息 It，再现包括在其内的信息单元 Iu，最后向用户提供信息单元 Iu 的内容的再现信息 Ir。接收单元 130 包括接收机 131、低层解密器 132、去多路复用器 133、信息单元解密器 134、再现器 135 和展现器 136。

接收机 131 连接到发射机 120 上，接收发送信息 It，产生加密多路信息 Ime。具体地说，接收机 131 接收发射机 120 输出的发送信息 It，并取出部分或全部信息，然后，接收机 131 根据发送信息 It 产生加密多路信息 Ime。

在例子 1 中，接收机 131 为邮件传输的前端程序。另一方面，在例子 2 中，接收机 131 由卫星广播调谐器、解调器和纠错解码器连接而成。

低层解密器 132 连接到接收机 131 上，接收加密多路信息 Ime，产生多路信息 Im。低层解密器 132 接收接收机 131 输出的加密多路信息 Ime，并对加密多路信息 Ime 进行解密，产生多路信息 Im。在例子 1 中，低层解密器 132 为 PGP 程序，它由解密选项来启动。另一方面，在例子 2 中，低层解密器 132 为传送层解密器。

请注意，低层解密器 132 产生的加密多路信息 Ime 的内容基本上与发送单元 110 的低层加密器 114 产生的加密多路信息 Ime 相同，只是加密格式或加密方法不同。当然，也可以再现与低层加密器 114 产生的加密多路信息完全相同的加密多路信息 Ime。

去多路复用器 133 连接到低层解密器 132 上，从其接收多路信息 Im。去多路复用器 133 从多路信息 Im 中分离出加密信息单元 Iue，并输出分离的加密信息单元 Iue。当根据多路信息解密的信息包括不需要解密的信息单元 Iu 时，去多路复用器 133 分开输出加密信息单元 Iue 和信息单元 Iu。

具体地说，在例子 1 中，去多路复用器 133 为 MIME 解码器，它把文本信息、图像信息等分离成分离的信息，以取出分离信息，这些信息是包括在多部分消息内的各种要素。另一方面，在例子 2 中，去多路复用器 133 是 MPEG-2 的 TS 的去多路复用器。去多路复用器 133 分离由 MPEG-2 系统多路复用的多个流。

信息单元解密器 134 连接到去多路复用器 133 上，仅接收加密信息单元 Iue。然后，信息单元解密器 134 对接收到的加密信息单元 Iue 进行解密，产生信息单元 Iu。然而，如上所述，加密信息单元 Iue 为多路加密信息单元，由信息单元加密器 112 重复加密，或由多路复用器 113 重复多路复用。

在前一种情况下，加密器 112 已重复加密加密信息单元 Im，即使在信息单元解密器 134 本身解密之后，仍留有另一个加密的信息单元 Iue。信息单元解密器 134 从其分立输出端分别输出该余留加密信息单元 Iue 和信息单元 Iu。为了对该余留加密信息单元 Iue 进行解密，信息单元解密器 134 还连接到其输出端之一，以向其送回余留的加密信息单元 Iue。信息单元解密器 134 重复该反馈操作，直到在解密之后不再出现余留的加密信息单元 Iue。

在后一种情况下，加密信息单元 Iue 已由多路复用器 113 重复多路复用，即使在去多路复用器 133 进行去多路复用之后仍留有另一个多路信息单元 Im。由于该余留的多路信息单元受到分层多路复用和加密，所以在信息单元解密器 134 解密之前，首先必须对余留的加密(重复多路复用)信息单元 Iue 的外壳解密。因此，把该余留的多路复用的加密(重复多路复用)信息 Iue 送回给去多路复用器 133。于是，去多路复用器 133 和/或解密器 134 连续重复进行去多路复用解密，直到在解密之后不再有多路信息单元 Im，而是已解密的信息单元 Iu。然后，信息单元解密器 134 仅输出信息单元 1。

具体地说，信息单元解密器 134 接收信息单元解密器 134 输出的加密信息单元

Iue。然后，从信息单元解密器 134 输出加密信息单元 Iue 的解密结果，即加密信息单元 Iue 或信息单元 Iu。加密信息单元 Iue 是通过把信息单元 Iu 进行多次加密而获得的。因此，必须多次解密加密信息单元，以取出信息单元 Iu。

信息单元解密器 134 再次接收信息单元解密器 134 本身的输出，重复解密输入，从而可以解密进行多次加密获得的加密信息单元 Iue。因此，即使信息单元解密器 134 一次可以进行的解密次数为 1，最终也可以从加密信息单元 Iue 中取出信息单元 Iu。信息单元解密器 134 也可以同时进行多次解密。在这种情况下，可以更高速地取出信息单元 Iu。

再现器 135 连接到信息单元解密器 134 和去多路复用器 133 的另一个输出端上，接收信息单元 Iu。然后，再现器 135 把输入的信息单元 Iu 转换成可以再现的再现信息 Ir，并输出再现信息 Ir。在例子 1 中，再现器 134 可以是文本文件浏览器、图像文件显示软件等。另一方面，在例子 2 中，再现器 134 可以是 MPEG-2 解码器，以再现用例如 MPEG-2 编码的语音或图像。在这种情况下，输出为 NTSC(国家电视制式标准委员会)信号或模拟语音信号。

展现器 136 接收再现器 135 输出的再现信息，向用户展现信息单元 Iu。具体地说，展现器 136 接收再现器 135 输出的再现信息 Ir，向用户展现包含在再现信息 Ir 内的信息。在例子 1 中，展现器 136 可以是诸如 X-Window 或 Micorsoft Windows 等窗口系统，向用户展现图像和声音。另一方面，在例子 2 中，展现器 136 可以是电视接收机，用于输入和接收例如 NTSC 信号和模拟语音信号。

运作

参照图 3 和图 4，下面描述信息传输装置 100 进行的一般工作。在图 3 中，示出了发送单元 110 和发射机 20 进行的操作。

在步骤 S301，信息单元发生器 111 产生多个信息单元 Iu，并输出产生的信息单元 Iu。产生信息单元 Iu 的例子包括用户输入信息单元 Iu 以及如例子 1 中一样指定一个文件的方法，以及如例子 2 一样，根据预定规则从存储的信息单元 Iu 中选择输出信息单元 Iu 的方法。

在步骤 S302，信息单元加密器 112 对在步骤 S301 产生的信息单元 Iu 递归加密，产生其结果作为加密信息单元 Iue。

在步骤 S303，多路复用在步骤 S302 加密产生的多个加密信息单元 Iue，并输出

其结果作为多路信息 Im。多路复用器 113 多路复用在步骤 S301 产生的信息单元 Iu，并把其结果输出作为多路信息 Im。多路信息 Im 在例子 1 情况下是与 MIME 一致的多部分数据，而在例子 2 中，是表示 MPEG-2 系统的 TS 的数据。

在步骤 S304，低层加密器 114 对在步骤 S303 多路复用获得的多路信息 Im 进行加密，产生加密多路信息 Ime。在例子 1 中，多路信息 Im 是利用 RSA 密码等来加密的。另一方面，在例子 2 中，利用例如 Hitachi 公司制造的 MULTI-2 密码对 MPEG-2 的 TS 的有效负载部分进行加密。

在步骤 S305，发送器 115 把在步骤 S304 加密获得的加密多路信息 Ime 转换成适合发射机 120 发送的格式，并产生发送信息 It。在例子 1 中，把例如："至:字段，来自：字段"的信息加到加密多路信息 Ime 的邮件文本的首标中，并输出该信息作为发送信息 It。另一方面，在例子 2 中，输出利用纠错码对 MPEG-2 的 TS 进行编码，然后对编码的 TS 进行调制而获得的信息。

在步骤 S306，发射机 120 向实际远距点发送信息 It。多个接收单元 130 可以对应于一个发送部分。在例子 1 中，安装在一台或多台连接的计算机上的邮件通信灵元根据 SMTP 与诸如互联网或 LAN(局域网)等计算机网络进行通信。因此，邮件从一台计算机上的邮件通信灵元传输到另一台计算机上的邮件通信灵元。

另一方面，在例子 2 中，由抛物面天线向通信卫星发射在上变频器中变频而获得的发送信息 It。通信卫星把接收到的发送信息 It 由转发器向地面发射。地面接收天线接收通信卫星的发送信息 It。

在图 4 中，示出了接收单元 130 进行的操作。在步骤 S401，接收机 131 接收发射机 120 输出的发送信息 It，并从接收到的发送信息 It 中取出部分或全部加密多路信息 Ime。在例子 1 中，进行取出一个发给特定用户的电子邮件数据的处理。另一方面，在例子 2 中，通过调谐到预定的频率，进行处理，由 PID(数据包标识符)过波出要找的特定数据包存储信息，并选择和取得该数据包。

在步骤 S402，低层解密器 132 接收在步骤 S401 产生的加密多路信息 Ime。然后，低层解密器 132 输出解密结果作为多路信息 Im。在例子 1 中，低层解密器 132 是用解密选项启动的 PGP 程序。用 PGP 程序的 RSA 密码进行解密，并输出解密结果。另一方面，在例子 2 中，对利用 MULTI-2 密码加密的多路信息 Im 进行解密，获得多路信息 Im。

在步骤 S403，去多路复用器 133 从在步骤 S402 获得的多路信息单元 Im 中分离

出加密信息单元 Iue。在例子 1 中，去多路复用器 133 分离出根据 MIME 多路复用获得的多部分消息的每个要素。因此，分离出文本信息、图像信息、语音信息等各要素，作为离散的信息单元 Iu。

另一方面，在例子 2 中，去多路复用器 133 根据 PID(数据包标识符)分离 MPEG-2 系统多路复用的多个流。因此，分离出诸如 MPEG-2 视频流、MPEG-1 音频流和 EPG 等附加信息作为离散信息单元 Iu。按 ITU-T H.262 对 MPEG-2 图像进行标准化，按 ISO/IEC 11172-3 标准使 MPEG-1 语音标准化。

在步骤 S404，判断在去多路复用器 133 去多路复用之后的信息是否还包括加密信息单元 Iue。当判断结果为是时，表示去多路复用器 133 在步骤 S403 产生的信息需要解密，以从其中取出内容，因而过程进入到步骤 S405。

在步骤 S405，信息单元解密器 134 一对密从去多路复用器 133 输出的加密信息单元 Iue 进行一次解密。此后，过程返回到步骤 S403。重复进行步骤 S403、S404 和 S405 的操作，信息单元解密器 134 可以对包括在多路信息 Im 中的所有加密信息单元 Iue 进行解密，最后取出发送单元 110 发送的所有信息单元 Iu。

另一方面，当在步骤 S404 的判断结果为否时，表示在去多路复用器 133 去多路复用之后的信息不需要解密，以从其中取出内容。换句话说，去多路复用器 133 输出的信息仅是信息单元 Iu。然后过程进入到步骤 S406。

在步骤 S406，再现器 135 接收解密器 134 输出的信息单元 Iu，并产生可再现的再现信息单元 Ir。在例子 1 中，当信息单元 Iu 例如为文本信息时，选择并列出对应于各字符码的字体，产生位图格式，作为再现信息 Ir1。当信息单元 Iu 是诸如 JPEG(联合静止图像专家组)等的图像信息格式时，把它扩展成位图格式，并输出扩展结果作为再现信息。JPEG 按 ISO/IEC 10918 进行标准化。当信息单元 Iu 为语音信息时，用与数字-模拟(D/A)转换器相同的功能把它转换成模拟语音信号。也把模拟语音信号作为再现信息输出。

另一方面，在例子 2 中，当在步骤 S301 获得的信息单元 Iu 为 MPEG-2 视频流时，对 MPEG-2 视频进行解码，输出 NTSC 信号作为再现信息。当信息单元 Iu 为语音流时，通过 D/A 转换把它转换成模拟语音信号，并输出该模拟语音信号。

在步骤 S407，展现器 136 接收再现器 135 输出的再现信息单元 Ir，然后根据再现信息的格式向用户展现再现信息 Ir 的内容。在例子 1 中，当在步骤 S406 获得的再现信息为位图格式时，展现器 136 排列再现信息 Ir，并在显示屏上显示该再现信息

Ir。这样就向用户展现再现信息 Ir。当在步骤 S406 获得的再现信息为模拟语音信号时，把模拟信号送到扬声器，转换成声音，并可闻地向用户展现。

另一方面，在例子 2 中，在显示器上接收到在步骤 S406 作为再现信息的 NTSC 信号，把模拟语音信息发送给扬声器，向用户显示再现信息。

如上所述，在第一实施例中，可以处理已递归加密多次的信息单元 Iu。因此，可以把分层结构引入到信息单元 Iu 的加密中。在选购一组信息单元 Ir 的一部分的情况下，对应于程序结构的分层结构使得可仅用一种类型的加密以较少的次数对信息单元 Iu 进行加密。

信息单元解密器 134 在接收单元 130 中重复进行解密，取出信息单元 Iu。因此，接收单元可以不需要这种高级的或特殊的解密器对应于多种类型的密码就可以构成，每次进行多次的解密处理，从而可以简化和降低成本。

把信息单元编码成加密多路信息单元

参照图 2 描述信息传输装置 100 产生的加密多路信息单元 Ime。信息单元的各个处理层用不同的后缀表示，以便于更好地对其辨认。例如，用虚线矩形表示的低层加密器 114 的输出为加密多路信息 ImeOA。

用圆圈指示的信息单元发生器 111 的四个输出分别是信息单元 Iu1a, Iu2a, Iu3a 和 Iu4a。这些信息单元 Iu1a, Iu2a, Iu3a 和 Iu4a 分别表示例如包含天气预报的旅游地指南、旅游地天气预报、全国天气预报以及本地天气预报。

用实线指示的矩形 Iue1a、Iue12a 和 Iue4a 表示信息传输装置 100 的发送单元 110 内在各加密阶段产生的加密信息的单元。具体地说，矩形 Iue1a 表示在步骤 S302，产生的第一加密信息单元 Iue，该步骤中，信息单元加密器 112 在第一预定加密系统 CS1 下用第一预定密码 C1 对信息单元发生器 111 产生的信息单元 Iu1a 进行加密。因而，产生第一加密信息单元 Iue1a。

矩形 Iue12a 还表示下列两个步产生的第二加密信息单元 Iue。在步骤 S303，多路复用器 113 多路复用从信息单元加密器 112 产生的第一加密信息单元 Iue1a 和信息单元 Iu2a，产生多路信息单元 Im12a(未图示)。在步骤 S302，信息单元加密器 112 在第二预定加密系统 CS2 用第二预定密码 C2 对从多路复用器 113 接收到的多路信息单元 Im12a 进行加密。因而，产生信息单元 Iu1a 加密两次的第二加密信息单元 Iue12a。

矩形 Iue4a 表示在步骤 S302，产生的第三加密信息单元 Iue，该步骤中，信息单元加密器 112 在第三加密系统 CS3 下用第三预定密码 C3 对信息单元发生器 111 输出的信息单元 Iu4a 进行加密。因而，产生第三加密信息单元 Iue4a。

矩形 Ime0a 表示如下产生的加密多路信息单元 Ime。首先，在步骤 303，多路复用器 113 多路复用第二加密信息单元 Iue12a、信息单元 3a 和第三加密信息单元 Iue4a，产生多路信息单元 Im1234a(未图示)。其次，在步骤 S304，低层加密器 114 在第四预定加密系统 CS4 下用第四预定密码 C4 对多路复用单元 Im1234 进行加密。

结果，第一信息单元 Iu1aet 用第一、第二和第四预定密码 C1、C2 和 C4 加密三次。第二信息单元 Iu2a 用第二和第四预定密码 C2 和 C4 加密两次。第三信息单元 Iu3a 用第四预定密码 C4 加密一次。第三信息单元 Iu4a 用第三和第四预定密码 C3 和 C4 加密两次。

因此，在这些信息单元 Iu1a、Iu2a、Iu3a 和 Iu4a 之间存在表示天气预报节目的不同内容的分层顺序。具体地说，加密多路信息 Ime0a 是一组对用户具有含义的信息。该组信息例如是一个电子邮件或一个信息节目。加密多路信息单元 Ime0a 递归包括没有加密的部分(Iu3a)和加密的部分(Iue12a 和 Iue4a)。

请注意，根据保护信息单元不被非法访问所需的适当密码抗解力，可以把所有密码 C1、C2、C3 和 C4 赋予相同的值或选择的值。同样，所有每个加密系统 CS1、CS2、CS3 和 CS4 可以从相同的加密系统或各种不同的加密系统(例如上面引用的)中选择。

作为一个例子，把未加密部分(Iu3a)和加密部分(Iue12a 和 Iue4a)包括在一个加密多路信息单元(Ime0a)中。整个加密多路信息单元 Ime0a 为天气预报节目，未加密部分(Iu3a)是免费的全国天气预报，加密部分(Iue12a 和 Iue4a)是收费的本地详细天气预报。而且，也可以考虑预览电影和加密电影、软件介绍资料、加密软件执行方式等。

在这种情况下，用户通过解密加密多路信息单元 Ime0a 可以观看全国天气预报(Iu3a)，通过解密加密信息单元 Iue2a 可以观看旅游地的天气预报(Iu2a)，通过解密加密信息单元 Iue1a 可以观看包含天气预报的旅游地指南(Iu1a)，通过解密加密信息单元 Iu34a 可以观看本地天气预报(Iue4a)。

因此，被离散的密码加密多次的信息单元对非法解密来说，具有与用单个密码加密(它具有对应于多个离散密码的抗解力)的情况相同的抗解力。而且，根据定义 2 的多个信息单元(例如信息单元 Iue 1a 和 Iu2a)在同一加密层同时被加密，能减轻启动

解密操作的负担。

把加密多路信息解密成信息单元

重复使用具有简单结构装置的单个解密器可以解密用由发送单元 110 分层排列的密码加密的加密信息，具体描述如下。把加密多路信息单元 Ime0a 通过发射机 120 以发送信息 It 的格式提供给接收单元 130。

在步骤 S401，接收单元 130 的接收机从接收到的发送信息 It 中取出部分或全部加密多路信息 Ime0a。在步骤 S402，低层解密器 132 用第三预定密码 C4 对接收到的加密多路信息 Ime0a 进行解密，获得由第二加密信息单元 Iue12a、第三信息单元 Iu3a 和第三加密信息单元 Iue4a 构成的多路信息单元 Im1234a(未图示)。请注意，如此获得的多路信息单元 Im1234a 能以与多路复用器 113 在步骤 S303 产生的多路信息单元 Im1234a 不同的格式产生。

去多路复用器 133 去多路复用在步骤 S402 产生的多路信息单元 Im1234a，并在步骤 S403 从其中分离出每个加密信息单元 Iue 和/或信息单元 Iu。因此，在步骤 S403 产生第二加密信息单元 Iue12a、第三信息单元 Iu3a 和第三加密信息单元 Iue4a。请注意，如此获得的信息单元 Iue12a、Iu3a 和 Iue4a 能按与发送单元 110 的信息单元加密器 112 产生的不同的格式产生。无需说明的是，那些信息单元 Iue12a、Iu3a 和 Iue4a 可以是与发送单元 110 的信息单元加密器 112 产生的相同的格式，从而再现那些信息单元 Iue12a、Iu3a 和 Iue4a。

把第二加密信息单元 Iue12a 发送到信息单元解密器 134，在步骤 S405，通过用第二预定密码 C2 对加密信息单元 Iue12a 进行解密，产生多路信息单元 Im12a(未图示)。把如此产生的多路信息单元 Im12a 送回到去多路复用器 133 中，在步骤 S403 对多路信息单元 Im12a 进行去多路复用，产生第一加密信息单元 Iue1a 和第二信息单元 Iu2a。

把第一加密信息单元 Iue1a 发送到信息单元解密器 134，在步骤 S404，用第一预定密码 C1 对加密信息单元 Iue1a 进行解密，产生第一信息单元 Iu1a。同样，把第三加密信息单元 Iue4a 发送到信息单元解密器 134 中，产生第四信息单元 Iu4a。

把每个在步骤 S404 产生的信息单元 Iu1a、在步骤 S405 产生的 Iu2a、在步骤 S403 产生的 Iu3a，以及在步骤 S405 产生的 Iu4a 发送到再现器 135，在步骤 S406 从这些信息单元 Iu1a、Iu2a、Iu3a 和 Iu4a 产生再现信息 Ir。请注意，所有信息单元 Iu1a、

Iu2a、Iu3a 和 Iu4a 能按与信息单元发生器 111 产生的基本上相同的内容产生，但是加密格式或加密方法可以不同。当然，也可以完全再现与信息单元发生器 111 产生的 Iu1a、Iu2a、Iu3st Iu4a 相同的信息单元。

(第二实施例)

下面参照图 5 至 8 描述根据本发明第二实施例的信息传输装置。信息传输装置 500 包括发送单元 510、发射机 120 和接收单元 530。发射机 120 与信息传输装置 100 中所用的一样。下面一般将省略对构成信息传输装置 100 的相同部件的描述，以减少重复。

请注意，解密器 532 产生的加密多路信息 Ime 的内容基本上与发送单元 110 的低层加密器 114 产生的加密多路信息 Ime 相同，但加密格式或加密方法可以不同。当然，也可以再现与低层加密器 114 产生的完全相同的加密多路信息 Ime。

发送单元 510

发送单元 510 的结构与图 1 所示的发送单元 110 非常相似，由信息单元加密器 512 代替了信息单元加密器 112。与信息单元加密器 112 相比，信息单元加密器 512 应当能对信息单元 Iu 进行与发射机 120 进行的低层传输一致的加密。换句话说，信息单元加密器 512 仅在诸如发射机 120 等执行的低层所用的某些加密系统下进行加密，无需说明的是，信息单元加密器 512 能在各种加密系统下进行加密，包括适用于上述低层传输系统。

具体地说，作为信息单元加密器 512 中所用的密码，可以选择能通过共用低层加密器 514 用于解密的高抗窜改器件进行解码的密码。高抗窜改器件可采取措施，使得非法分解内容，则擦除该内容，因而 LSI(大规模集成电路)不会泄漏出与保密有关的信息，没有具体的设备难以分析。例如，用于 CS 数字广播的接收机中的 IC 板就是一种抗窜改器件。

接收单元 530

接收单元 530 的结构与图 1 所示的接收单元 130 相似，由解密器 532 和去多路复用器 533 替换了低层解密器 132 和信息单元解密器 134。解密器 532 连接到接收机 131 上，接收加密多路信息单元 Ime。然后，解密器 532 对接收到的多路信息单元 Ime 进

行一次解密，产生多路信息 Im。请注意，解密器 532 可以解密任何一个在各种加密系统(包括发送单元 110 内的低层加密器 114 采用的某些加密系统)下加密的加密多路信息单元。

去多路复用器 533 连接到解密器 532 上，接收多路信息 Im，对接收到的多路信息 Im 去多路复用，产生信息单元 Iu。然而，当解密器 532 产生的多路信息 Im 其内包括重复多路复用的信息单元时，在去多路复用之后，仍有加密信息单元 Iue。

解密器 532 还连接到去多路复用器 533 上，接收余留的加密单元 Iue。然后，解密器 532 对加密单元 Iue 进行解密，产生多路信息单元 Im，并把它提供给去多路复用器 533。当从去多路复用器 533 接收到的加密信息单元 Iue 只是加密而没有被多路复用时，则从其中产生信息单元 Iu，并把它直接提供给再现器 135。因此，去多路复用器 533 不需要能对重复多路信息单元 Im 进行去多路复用，只要能对一次多路复用的信息单元 Im 去多路复用即可。

这样，从第一实施例的结构中去除信息单元加密器 112 递归加密多次的限制，就可以获得第二实施例的结构。在第一实施例中进行解密的低层解密器 132 和信息单元解密器 134 被综合到本实施例的解密器 532 中。这种集成也可认为是由低层解密器 132 的功能实现了信息单元解密器 134 的功能。

运作

下面参照图 7 和图 8 描述信息传输装置 500 进行的一般操作。图 7 所示的发送单元 110 和发射机 120 进行的操作与已参照图 3 描述的操作非常相似。因此，这里简要的描述一下，以说明它们之间的区别。

在步骤 S601，信息单元发生器 111 产生多个信息单元 Iu，并输出产生的信息单元 Iu。

在步骤 S602，信息单元加密器 512 对在步骤 S601 产生的信息单元 Iu 进行一次加密，输出其结果作为加密信息单元 Iue。具体地说，信息单元加密器 512 加信息单元 Iu 进行符合发射机 120 低层传输的加密。这里所用的密码的类型与低层加密器 114 内所用的密码相同。“相同”意味着例如当低层加密器 114 使用 RSA 密码时，信息单元加密器也利用 RSA 密码进行加密。在第一实施例的步骤 S302 中进行对信息单元 Iu 递归加密多次的处理，而在本步骤中不限制对信息单元 Iu 进行多次加密。

在步骤 S603，多路复用器 113 多路复用在步骤 S602 加密产生的多个加密信息单

元 Iue，并输出其结果，作为多路信息单元 Im。

在步骤 S604，低层加密器 114 用与步骤 S602 所用的相同的密码加密在步骤 S603 多路复用获得的多路信息 Im。如对信息单元加密器 512 的描述那样，低层加密器 114 中所用的密码与信息单元加密器 112 中所用的密码一样。

在步骤 S605，发送器 115 把在步骤 S604 加密获得的加密多路信息 Ime 转换成适合发射机 120 发送的格式，并产生发送信息 It。

在步骤 S606，发射机 120 向实际远距点发送信息 It。

在图 8 中，接收单元 530 进行的操作与已参照图 4 描述的操作相似。因此，对操作作简要的描述，以说明它们之间的区别。在步骤 S701，接收机 131 接收发射机 120 输出的发送信息 It，从接收到的发送信息 It 中取出部分或全部加密多路信息 Ime。

在步骤 S702，解密器 532 接收在步骤 S701 产生的加密多路信息 Ime，并对接收到的加密多路信息 Ime 进行解密。然后，解密器 532 输出解密结果作为多路信息 Im。

在步骤 S703，去多路复用器 533 从在步骤 S702 获得的多路信息单元 Im 中分离出加密信息单元 Iue。去多路复用器 533 虽然对重复多路复用的信息单元 Im 进行去多路复用，但只对一次多路复用的信息单元 Im 去多路复用即可。

在步骤 S704，解密器 532 对接收机 131 的加密多路信息单元 Ime 和/或去多路复用器 533 的加密信息单元 Iue 解密。从加密信息单元 Ime 或一次加密的加密信息单元 Iue 产生的是将直接提供给再现器 135 的信息单元 Iu。从加密信息单元 Ime 或加密且多路复用的加密信息单元 Iue 产生的是提供给去多路复用器 533 的多路信息单元 Im。

具体地说，当信息单元 Iu 加密一次时，加密信息单元 Iue 也解密一次，从而使它可以产生信息单元 Iu。虽然在第一实施例中有对信息单元 Iu 递归加密多次的限制，但在第二发明中没有限制。

在步骤 S705，再现器 135 接收解密器 532 和去多路复用器 533 输出的信息单元 Iu，并产生可再现的再现信息 Ir。

在步骤 S706，展现器 136 接收再现器 135 输出的再现信息 Ir。

如上所述，信息单元加密器 512 进行的加密与低层加密器 114 进行的加密相同。因此，不仅可以用一个解密器 532 对低层加密器 114 中所用的密码进行解码，也可以对信息单元加密器 512 中所用的密码进行解码。即可以仅准备一个非专用的解密器就可以解密信息单元 Iu。

把信息单元编码成加密多路信息单元

参照与图 2 相似的图 6，描述信息传输装置 500 产生的加密多路信息单元 Ime。由虚线矩形代表的低层加密器 114 的输出为加密多路信息 Ime0b。

圆圈指示的信息单元发生器 111 的四个输出分别为信息单元 Iu1b, Iu2b, Iu3b 和 Iu4b。这些信息单元 Iu1b, Iu2b, Iu3b 和 Iu4b 分别表示例如包含天气预报的旅游地指南、旅游地天气预报、全国天气预报以及本地天气预报。

用虚线指示的矩形 Iue12b 和 Iue4b 每个表示信息传输装置 500 在各加密阶段时产生的加密信息的单元。产生矩形 Iue12b 的方法是，先在步骤 S603 中，由多路复用器 113 对从信息单元发生器 111 接收到的信息单元 Iu1b 和 Iu2b 进行多路复用，产生多路信息单元 Im12b(未示出)。然后，信息单元加密器 512 在第五预定加密系统 CS5 下用第五预定密码 C5 对从多路复用器 113 接收到的多路信息单元 Im12b 进行一次加密，接着在步骤 S602 产生加密信息单元 Iue12b。

矩形 Iue4b 也表示在步骤 S602，产生的加密信息单元 Iue，该步骤中，信息单元加密器 512 在第六预定加密系统 CS6 下用第六预定密码 C6 加密信息单元 Iu4b。

产生加密多路信息单元 Ime0b 的方法是，先在步骤 S603 中，由多路复用器 113 对加密信息单元 Iue12b、信息单元 Iu3b 和加密信息单元 Iue4b 进行多路复用，产生多路信息单元 Im1234b(未示出)。然后，在步骤 S604，低层加密器 114 在第七预定加密系统 CS7 下用第七预定密码 C7 加密多路信息单元 Im1234b。

因此，信息单元 Iu1b 和 Iu2b 都用第五和第七预定密码 C5 和 C7 加密两次。信息单元 Iu3a 用第七预定密码 C7 加密一次。信息单元 Iu4b 用第六和第七预定密码 C6 和 C7 加密两次。

因此，在这些信息单元 Iu1b、Iu2b、Iu3b 和 Iu4b 之间存在表示天气预报节目的不同内容的分层顺序。具体如图 6 所示，根据本实施例的分层顺序与第一实施例不同。

请注意，根据保护信息单元不被非法访问所需的适应密码抗解力，可以把所有密码 C5、C6 和 C7 赋予相同的值或选择的值。同样，所有每个加密系统 CS5、CS6 和 CS7 可以从相同的加密系统或各种不同的加密系统(例如上面引用的)中选择。而且，所有密码和加密系统可以从第一实施例所选择的密码和加密系统中进行选择。

把加密多路信息解密成信息单元

重复使用具有简单结构装置的单个解密器可以解密用由发送单元 510 分层排列

的密码加密的加密信息，具体描述如下。把加密多路信息单元 Ime0b 通过发射机 120 以发送信息 It 的格式提供给接收单元 530。

在步骤 S701，接收单元 530 的接收机 131 从接收到的发送信息 It 中取出部分或全部加密多路信息 Ime0b。在步骤 S702，低层解密器 532 用第七预定密码 C7 对接收到的加密多路信息 Ime0b 进行解密，获得由加密信息单元 Iue12b、信息单元 Iu3b 和加密信息单元 Iue4b 构成的多路信息单元 Iml234b(未图示)。请注意，如此获得的多路信息单元 Iml234b 能按与多路复用器 113 在步骤 S603 产生多路信息单元 Iml234b 不同的格式产生。

去多路复用器 533 去多路复用在步骤 S603 产生的多路信息单元 Iml234b，并在步骤 S703 从其中分离出每个加密信息单元 Iue 和信息单元 Iu。因此，在步骤 S703 产生加密信息单元 Iue12b、信息单元 Iu3b 和加密信息单元 Iue4b。请注意，如此获得的信息单元 Iue12b、Iu3b 和 Iue4b 能按与发送单元 510 的信息单元加密器 512 产生的不同的格式产生。无需说明的是，那些信息单元 Iue12b、Iu3b 和 Iue4b 可以是与发送单元 510 的信息单元加密器 512 产生的相同的格式，从而再现那些信息单元 Iue12b、Iu3b 和 Iue4b。

把加密信息单元 Iue12b 发送到解密器 532，在步骤 S704，通过用第五预定密码 C5 解密加密的信息单元 Iue12b，产生多路信息单元 Iml2b(未图示)。把如此产生的多路信息单元 Iml2b 送回到去多路复用器 533 中，在步骤 7403 对多路信息单元 Iml2b 进行去多路复用，产生信息单元 Iu1b 和 Iu2b。同样，把加密信息单元 Iue4b 发送到解密器 532，在步骤 S704 产生信息单元 Iu4b。

把每个在步骤 S703 产生的信息单元 Iu1b、在步骤 S703 产生的 Iu2b、在步骤 S703 产生的 Iu3b 和在步骤 S704 产生的 Iu4b 发送到再现器 135，在步骤 S705 根据这些信息单元 Iu1b、Iu2b、Iu3b 和 Iu4b 产生再现信息 Ir。请注意，所有这些信息单元 Iu1b、Iu2b、Iu3b 和 Iu4b 都能以其内容与信息单元发生器 111 产生的相同的方式产生，但加密格式或加密法可以不同。当然，也可以完全再现与信息单元发生器 111 产生的 Iu1b、Iu2b、Iu3b 和 Iu4b 相同的信息单元。

参照图 9，图 9 示出了信息传输装置 500 另一个例子。图 9 所示的信息传输装置 500R 的结构是从信息传输装置 500 中去除了低层加密器 114。在该装置中，低层传输的加密不是由低层加密器 114(图 5)进行的，而是由信息单元加密器 512(图 9)进行的。因此，信息单元加密器 512 仅在低层(例如发射机 120 工作的传输层)中使用的某

些加密系统下进行加密。无需说明的是，信息单元加密器 512 可以在各种加密系统下进行加密，包括适用于上述低层传输的系统。

(第三实施例)

下面参照图 10、11 和 12 描述根据本发明的第三实施例的信息传输装置。在本实施例中，信息传输装置 800 包括发送单元 810、发射机 120 和接收单元 830。下面一般将省略对构成信息传输装置 100、500 或 500R 的相同部件的描述，以减少重复。

请注意，解密器 832 产生的加密多路信息 Ime 的内容基本上与发送单元 810 的低层加密器 114 产生的加密多路复有信息 Ime 相同，但加密格式或加密方法可以不同。当然，也可以再现与低层加密器 114 产生的完全相同的加密多路信息 Ime。

发送单元 810

发送单元 810 的结构与已参照图 5 描述的发送单元 510 相同。然而，产生加密多路信息 Ime 的发送单元 810 的操作与发送单元 510 不同，这将在下面参照图 11 和图 12 来描述。

接收单元 830

接收单元 830 的结构与图 5 所示的接收单元 530 相似，由解密器 832 和去多路复用器 833 替换了低层解密器 532 和去多路复用器 533。解密器 832 连接到接收机 131 上，接收加密多路信息单元。然后，解密器 832 对加密多路信息单元 Ime 解密一次，产生多路信息 Im。请注意，解密器 832 可以解密分层和重复加密的多路信息单元。解密器 832 对加密 n(n 为整数)次并产生 n-1 次加密信息单元的信息单元解密。因此，根据从接收机 131 输入的加密多路信息单元的加密次数，解密器 832 重复解密单元 Ime，直到不再获得加密多路信息单元 Ime。

去多路复用器 833 连接到解密器 832 上，接收多路信息 Im，对接收到的多路信息 Im 进行去多路复用，产生信息单元 Iu。然而，当解密器 832 产生的多路信息单元 Iue 其内包括加密信息单元 Iue 时，把加密信息单元 Iue 送回到解密器 832。

运作

下面参照图 12 描述信息传输装置 800 的接收单元 830 进行的一般操作。如上所

述，发送单元 810 的结构基本上与发送单元 510 相同，因此，其进行的操作也基本上与参照图 7 描述的相同。

接收单元 830 进行的一般操作如下。

在步骤 S901，接收机 131 从发射机 120 接收发送信息 It，从输入的发送信息 It 中取出部分或全部加密多路信息 Ime。

在步骤 S902，解密器 832 接收在步骤 S901 产生的加密多路信息 Ime。然后，解密器 832 对输入的加密多路信息 Ime 进行解密，输出解密结果作为多路信息 Im。

在步骤 S903，去多路复用器 833 对每个加密信息单元 Iue 分离出在步骤 S902 产生的多路信息 Im，取出加密信息单元 Iue 和/或信息单元 Iu。

在步骤 S904，判断解密器 832 或去多路复用器 833 输出的信息单元 Iu 是否被加密。如果判断为“是”，则表示信息单元 Iu 被加密，把解密器 832 或去多路复用器 833 的信息单元 Iu(Iue)送回到解密器 832。然后，过程进入到步骤 S905。

然而，如果判断为“否”，则表示解密器 832 或去多路复用器 833 输出的信息单元 Iu 不再被加密。把解密器 832 或去多路复用器 833 的信息单元 Iu 发送到再现器 135。然后，过程进入到步骤 S906。

在步骤 S905，解密器 832 对加密信息单元 Iue 解密一次，并从其输出解密结果。然后过程返回到步骤 S903，重复进行步骤 S903、S904 和 S905，解密器 832 可以解密信息单元 Iu，最终取出没有加密的信息单元 Iu。

在步骤 S906，再现器 135 接收解密器 832 和/或去多路复用器 833 输出的信息单元 Iu，并产生再现信息 Ir。

在步骤 S907，展现器 136 根据再现信息的格式向用户展现在步骤 S906 获得的再现信息 Ir 的内容。然后过程进入到步骤 S903。

如上所述，在信息单元加密器 512 中进行多次递归加密。在低层加密器 114 中使用与信息单元加密器 512 中所用的相同的密码系统。因此，可以使解密器 832 对所有多次的加密进行解密。

<u>把信息单元编码成加密多路信息单元</u>

参照与图 2 非常相似的图 11，描述信息传输装置 800 产生的加密多路信息单元 Ime。由虚线矩形代表的低层加密器 114 的输出为加密多路信息 Ime0c。

圆圈指示的信息单元发生器 111 的四个输出分别为信息单元 Iu1c, Iu2c, Iu3c 和

Iu4c。这些信息单元 Iu1c, Iu2c, Iu3c 和 Iu4c 分别表示例如包括天气预报的旅游地指南，旅游地天气预报、全国天气预报以及本地天气预报。

用虚线指示的矩形 Iue1c、Iue12c 和 Iue4c 每个表示信息传输装置 800 的发送单元 810 在各加密阶段时产生的加密信息的单元。具体地说，矩形 Iue1c 表示产生的信息单元 Iue，其方法是信息单元加密器 512 在第八预定加密系统 CS8 下用第八预定密码 C8 对信息单元发生器 111 输出的信息单元 Iu1c 进行加密。因此，产生加密信息单元 Iue1c。

矩形 Iue12c 也表示下面两个步产生的加密信息单元 Iue。首先，多路复用器 113 对从信息单元加密器 512 接收到的第一加密信息单元 Iue1c 和信息单元 Iu2c 进行多路复用，产生多路信息单元 Im12c(未示出)。其次，信息单元加密器 512 在第九预定加密系统 CS9 下用第九预定密码 C9 对从多路复用器 113 接收到的多路信息单元 Im12c 进行加密。因此，产生信息单元 Iu1c 加密两次的加密信息单元 Iue12c。

矩形 Iue4c 表示产生的加密信息单元 Iue，其方法是信息单元加密器 512 在第十预定加密系统 CS10 下用第十预定密码 C10 对从信息单元发生器 111 输出的信息单元 Iu4c 进行加密。因而，产生加密信息 Iue4c。

矩形 Ime0c 表示下列方法产生的加密多路信息 Ime。首先，多路复用器 113 多路复用加密信息单元 Iue12c、信息单元 Iu3c 和加密信息单元 Iue4c，在步骤 S303 产生多路信息单元 Im1234c(未示出)。其次，低层加密器 114 在第十一预定加密系统 CS11 下用第十一预定密码 C11 加密多路信息单元 Im1234。

因此，信息单元 Iu1c 被第八、第九和第十一预定密码 C8、C9 和 C11 加密三次。信息单元 Iu2c 被第九和第十一预定密码 C9 和 C11 加密两次。信息单元 Iu3c 被第十一预定密码 C11 加密一次。信息单元 Iu4c 被第十和第十一预定密码 C10 和 C11 加密两次。

请注意，根据保护信息单元不被非法访问所需的适当密码抗解力，可以把所有密码 C8、C9、C10 和 C11 赋予相同的值或选择的值。同样，所有每个加密系统 CS8、CS9、CS10 和 CS11 可以从相同的加密系统或各种不同的加密系统(例如上面引用的)中选择。而且，所有密码和加密系统可以从第一实施例和第二实施例中所选择的密码和加密系统中进行选择。

把加密多路信息解密成信息单元

重复使用具有简单结构装置的单个解密器可以解密用由发送单元 810 分层排列的密码加密的加密信息，具体描述如下。把加密多路信息单元 Ime0c 通过发射机 120 以发送信息 It 的格式提供给接收单元 830。

在步骤 S901，接收单元 830 的接收机 131 从接收到的发送信息 It 中取出部分或全部加密多路信息 Ime0c。在步骤 S902，解密器 832 用第十一预定密码 C11 对接收到的加密多路信息 Ime0c 进行解密，获得由加密信息单元 Iue12c、信息单元 Iu3c 和加密信息单元 Iue4c 构成的多路信息单元 Im1234c(未图示)。请注意，如此获得的多路信息单元 Im1234c 能以与多路复用器 113 产生多路信息单元 Im1234c 不同的格式产生。

去多路复用器 133 去多路复用在步骤 S902 产生的多路信息单元 Im1234c，并在步骤 S903 从其中分离出每个加密信息单元 Iue 和信息单元 Iu。因此，在步骤 S903 产生加密信息单元 Iue12c、信息单元 Iu3c 和加密信息单元 Iue4c。请注意，如此获得的信息单元 Iue12c、Iu3c 和 Iue4c 能以与发送单元 810 的信息单元加密器 512 产生的不同的格式产生。无需说明的是，那些信息单元 Iue12c、Iu3c 和 Iue4c 可以是与发送单元 810 的信息单元加密器 512 产生的相同的格式，从而再现那些信息单元 Iue12c、Iu3c 和 Iue4c。

通过步骤 S904 和 S905 的动作，在步骤 S906，从这些信息单元 Iu1c、Iu2c、Iu3c 和 Iu4c 产生再现信息 Ir。请注意，所有这此信息单元 Iu1c、Iu2c、Iu3c 和 Iu4c 都能以其内容与信息单元发生器 111 产生的相同的方式产生，但加密格式或加密方法可以不同。当然，也可以完全再现与信息单元发生器 111 产生的 Iu1c、Iu2c、Iu3c 和 Iu4c 相同的信息单元。

参照图 13，图 13 示出了图 10 的信息传输装置 800 的另一个例子。图 13 所示的信息传输装置 800R 的结构是从信息传输装置 800 中去除了低层加密器 114。在该装置中，低层传输的加密不是由低层加密器 114(图 10)进行的，而是由信息单元加密器 512(图 14)进行的。因此，信息单元加密器 512 仅在低层(例如发射机 120 工作的传输层)中使用的某些加密系统下进行加密。无需说明的是，信息单元加密器 512 可以在各种加密系统下进行加密，包括适用于上述低层传输的系统。

(第四实施例)

下面参照图 14、15、16 和 17 描述根据本发明第四实施例的信息传输装置。该信

息传输装置 1000 包括发送单元 1010、发射机 120 和接收单元 1030。下面为减少重复，一般省略了对构成信息传输装置 100、500、500R、800 或 800R 基本相同的部分的描述。

发送单元 1010

发送单元 1010 的结构与第一实施例的发送单元 110 非常相似，只是用信息单元加密器 1012 代替了信息单元加密器 112。信息单元加密器 1012 对信息单元发生器 111 输出的信息单元 Iu 递归加密多次，产生加密信息单元 Iue。进行递归加密多次的方法可以与第一实施例的信息单元加密器 112 进行的相同。

信息单元加密器 1012 增加了信息单元标识符，它是从输出的加密信息单元 Iue 中区别出信息单元 Iu 的标识符。下面把加密信息单元标识简称为信息单元 ID。虽然加密信息单元 Iue 由所谓的子加密信息单元 Iue 组成，但是加密信息单元 ID 不应加到子加密信息单元 Iue 上，而是应加到母加密信息单元 Iue 上。把相同的值分配给按时间更新的信息单元 Iu 作为加密信息单元 ID。例如，相同的加密信息单元 ID 分配给昨天的全国天气信息单元 Iu 和今天的全国天气信息单元 Iu。

接收单元 1030

接收单元 1030 包括接收机 131、低层解密器 132、去多路复用器 1033、存储器 1034、信息单元解密器 1036、展现器 136。具体地说，在本实施例中，接收单元 1030 的结构与图 1 所示的第一实施例的接收单元 130 相似，去多路复用器 133 和再现器 135 分别由去多路复用器 1033 和再现器 1036 代替。

而且，在去多路复用器 1033 与再现器 1036 之间另外插入一个存储器 1034。存储器 1034 连接到去多路复用器 1033 和再现器 1036 上，分别接收加密信息单元 Iue 和再现指示信息 Idr。存储器 1034 还连接到信息单元解密器 1035 上，在它们之间交换加密信息单元 Iue。

存储器 1034 在其内存储从去多路复用器 1033 和信息单元解密器 1035 输入的加密信息单元 Iue。然后，存储器 1034 用更新时新输入的加密信息 Iue 替换加密信息 Iue。因此，存储在存储器内的加密信息单元 Iue 被更新成新的信息单元。当输入再现指定信息 Idr 指定存储的加密信息单元 Iue 时，存储器 1034 输出加密信息单元 Iue。

信息单元解密器 1035 的输出还连接到其本身的输入端上，以提供加密信息单元 Iue(按照前面的定义，没有被加密的信息单元 Iu 也是加密信息单元 Iue)。信息单元解密器 1035 还连接到去多路复用器 1033 的输入端上，以提供加密信息单元 Iue。

再现器 1036 还连接到去多路复用器 1033 上，以接收信息单元 Iu，产生再现信息 Ir 和再现指定信息 Idr。再现指定信息 Idr 为指定信息单元 Iu 的信息。具体地说，再现指定信息 Idr 指定包括在存储器 1034 内存储的加密信息单元 Iue 的信息单元 Iu。再现指定信息 Idr 指定的信息单元 Ir 可以由用户直接输入来确定，或者可以由信息传输装置 1000 本身独立地确定。

展现器 136 连接到再现器 1036 上，接收再现信息 Ir。然后，展现器 136 向用户展现包括在再现信息 Ir 内的内容。

运作

下面参照图 15、16 和 17 描述信息传输装置 1000 进行的操作。

在图 15 中，示出了发送单元 1010 和发射机 120 进行的操作。

在步骤 S1101，信息单元发生器 111 产生多个信息单元 Iu。

在步骤 S1102，信息单元加密器 1012 递归地加密在步骤 S1101 产生的信息单元 Iu，把其结果作为加密信息单元 Iue。

在步骤 S1103，把加密信息单元 ID 加到在步骤 S1102 产生的加密信息单元 Iue 上。不需要解密加密的信息单元 Iue，就可以方便地取出加密信息单元 ID，这是因为它加到步骤 S1102 时的信息单元 Iu 加密结果上。

在步骤 S1104，多路复用器 113 多路复用在步骤 S1103 加密产生的加密信息单元 Iue，并把其结果作为多路信息 Im 输出。

在步骤 S1105，低层加密器 114 加密步骤 S1104 多路复用获得的多路信息 Im，产生加密多路信息 Ime。步骤 S1105 进行的加密应使用与步骤 S1102 进行的加密使用的相同的密码。

在步骤 S1106，发送器 115 把步骤 S1105 加密获得的加密多路信息 Ime 转换成适合发射机 20 传输的格式，并产生发送信息 It。

在步骤要 1107，发射机 120 向实际远距点发射发送信息 It。在这种情况下，多个接收单元 1030 可以对应于一个发射单元 1010。

在图 16 中，示出了接收单元 1030 进行的操作流程图。

在步骤S1201，接收机131从发射机120接收发送信息It，从输入的发送信息It中取出部分或全部加密多路信息Ime。

在步骤S1202，低层加密器132接收在步骤S1201获得的加密多路信息Ime，解密输入的加密多路信息Ime。

在步骤S1203，去多路复用器1033分离在步骤S1202获得的每个加密信息单元Iue的多路信息Im，取出加密信息单元Iue。

在步骤S1204，存储器1034利用加密信息单元ID存储加密信息单元Iue。

在图17，将详细描述存储器1034在步骤S1204进行的操作。

在步骤S1301，从去多路复用器1033输入加密信息单元Iue。

在步骤S1302，获得在步骤S1301输入的加到加密信息单元Iue上的加密信息单元ID的值i。

在步骤S1303，通过检索查验增加了值为i的加密信息单元ID的加密信息单元Iue是否已存储在存储器1034内。

在步骤S1304，判断加密信息单元Iue是否存储在存储顺1034内。当判断为“是”时，过程进入到步骤S1305。然而，当判断为“否”时，过程进入到步骤S1306。

在步骤S1305，增加在步骤S1301输入的加密信息单元Iue并存储。然后，过程返回到步骤S1301。从步骤S1301开始重复该过程。

在步骤S1306，去除当前存储的增加了值为i的加密信息单元ID的加密信息单元Iue，并存储步骤S1301输入的加密信息单元Iue作为替换。此后，过程返回到步骤S1301。从步骤S1301开始重复该过程。

如上所述，存储在存储器1034内的信息单元Iu被加密成加密信息单元Iue。因此，即使存储器1034的内容被非法引用，也确保了其保密性。在更新的情况下，加密信息单元ID被分配到母加密信息单元Iue，从而容易从去多路复用器1033输出的加密信息单元Iue中取出加密信息单元ID。仅使用能容易取出的加密信息单元ID，所以能非常简单地进行存储器1034的内容的更新处理。

通过增加指示是否对加密信息单元ID进行更新的信息，可以简单地处理多次发送的加密信息单元Iue，而不通过存储器1034进行改更。指示是否进行了更新的信息的例子如下：

(1)指示进行更新的标记，

(2)表示版本的数值，以及

(3)全部信息的校验和。

在步骤S1205，当再现器1036输出再现指定信息Idr时，过程进入到S1206，而当没有输出再现指定信息Idr时，过程进入到步骤S1201。

在步骤S1206，存储器1034取出在步骤S1205输出的再现指定信息Idr指定的具有加密信息单元ID的加密信息单元Iue。然后，存储器1034输出加密信息单元Iue。

在步骤S1207，当要取出的信息单元Iu处于信息单元解密器1035所输入加密信息单元Iue中没有被加密的状态时，过程进入到步骤S120。

在步骤S1208，信息单元解密器1035对存在有要取出的信息单元Iu的加密信息单元Iue解密一次。然后，过程返回到步骤S1207。在步骤S1209，再现器1036接收信息单元解密器1035输出的信息单元Iu。然后，再现器1036产生再现信息Ir。

在步骤S1210，展现器136根据再现信息的格式向用户展现在步骤S1209获得的再现信息。

如上所述，加密信息单元ID被加到加密信息单元Iue上。另外增加了存储器1034。因此，存储在存储器1034内的加密信息单元Iue可以被更新到最新，而不需要在信息单元解密器1035中进行解密处理。当用户实际观看加密信息单元Iue时，信息单元解密器1035才对加密的信息单元Iue解密。

请注意，前述实施例中使用的信息单元解密器134应能同时解密多路加密信息单元Iu(Ime)。相反，信息单元解密器1035则没有这种针对信息单元解密器134的限制，这是由于加密信息是一次加密的结果。具体地说，从存储器1034一点一点地接收信息，与发射机120发送的速度相比，能以较慢处理速度加密信息的解密。

而且，还可以仅当在预定时间内没有完成处理时，向存储器1034暂时输出加密信息单元Iue。这种暂时存储的加密信息被输出到信息单元解密器1035进行处理。

如上所述，从存储器1034把加密信息单元Iue一点一点提供给信息单元解密器1035，然后把如此提供的加密信息单元Iue一点一点从信息单元解密器1035输出。结果，去多路复用器1033可以进行去多路复用，以低于发射机120的传输速率，把多路信息分解成每个信息单元。

再现器1036根据用户请求指示要提供给存储 1034的信息内容。因此，再现器1036产生再现指定信息Idr。由于该再现信指定信息Idr，所以能在选定的时间上进行解密。因此，即使在加密信息(It)以后提供密钥，接收单元1030也可以处理该加密信息。

(第五实施例)

参照图 18、19 和 20 描述根据本发明第五实施例的信息传输装置。该信息传输装置 1400 包括发送单元 1410、发射机 120 以及接收单元 1430。下面，为了减少重复，一般省略对构成信息传输装置 100、500、500R、800、800R 或 1000 基本相同的部分的描述。

通过去除第四实施例信息传输装置 1000 中，对信息单元加密器 1012 加密信息递归多次的限制，构成信息传输装置 1400。而且，第四实施例中的低层解密器 132 和信息单元解密器 1035 在第五实施例中被综合成解密器 1432。

可以认为这种综合使解密器 1432 能取代信息单元解密器 1035 的功能。

发送单元 1410

发送单元 1410 的结构基本上与图 14 所示的发送单元 1010 相同。因此省略对其描述。

接收单元 1430

接收单元 1430 的结构与接收单元 1030 非常相似，只是低层解密器 132 和信息单元解密器 1035 被解密器 1432 代替。

解密器 1432 连接到接收机 131 和存储器 1034 上，接收多路信息单元 Iue。于是，当向其输出加密多路信息 Ime 时，解密器 1432 输出多路信息 Im。而且，当向其输出加密信息单元 Iue 时，解密器 1432 解密输入的加密信息单元 Iue，并输出其解密结果的信息单元 Iu。把如此获得的信息单元 Iu 直接提供给再现器 1036。

去多路复用器 1433 连接到解密器 1432 上，从其接收多路信息单元 Im，以去多路信息单元 Im。然后，当解密器 1432 的多路信息单元 Im 加密时，去多路复用器 1433 产生加密信息单元 Iue，并把它发送给存储器 1034。当解密器 1432 的多路信息单元 Im 没有加密时，去多路复用器 1433 产生信息单元 Iu，并把它发送给再现器 1036。

存储器 1034 分别连接到去多路复用器 1433 和再现器 1036 上，接收加密信息单元 Iue 和再现指定信息 Idr。存储器 1034 还连接到解密器 1432 的输入端。存储器 1034 把接收到的加密信息单元 Iue 存储在其内，并且当更新加密信息单元 Iue 时，替换存储的加密信息单元 Iue。因此，存储在存储器 1034 内的加密信息单元 Iue 保持最新。

当接收到的再现指定信息 Idr 指定存储的加密信息单元 Iue 时，存储器 1034 输出加密信息单元 Iue。把该加密信息单元 Iue 直接馈送到解密器 1432。

再现器 1036 连接到去多路复用器 1433，接收信息单元 Iu，还连接到存储器 1034，向其提供再现指定信息 Idr。

请注意，解密器 1432 能以与发射机 120 的信息传输速率不一致的较低速率进行解密处理，这是因为是从存储器 1034 一点一点向解密器 1432 提供加密信息 Iue。这对开头部分和较靠内部分(从外壳看)的加密信息单元的来说更有效。

如上所述，加密信息单元 Iue 的结果一点一点地从存储器提供给解密器 1432。结果，去多路复用器 1433 可以进行去多路复用，以比发射机 120 的传输速率低的速率分解开头部分和较靠内部分(从外壳看)的多路信息单元。

运作

参照图 19 和 20，简要描述信息传输装置 1400 的操作。在图 19 中，示出了发送单元 1410 和发射机 120 进行的操作的流程图。

在步骤 S1501，信息单元发生器 111 产生多个信息单元 Iu，并输出产生的信息单元 Iu。

在步骤 S1502，信息单元加密器 112 分别加密步骤 S1501 产生的信息单元 Iu，并把其结果作为加密信息单元 Iue。

在步骤 S1503，把加密信息单元 ID 加到在步骤 S1502 产生的加密信息单元 Iue 上。

在步骤 S1504，多路复用器 113 多路复用在步骤 S1502 的加密产生的加密信息单元 Iue，并把其结果作为多路信息 Im 输出。

在步骤 S1505，低层加密器 114 加密在步骤 S1504 多路复用获得的多路信息 Im，并产生加密多路信息 Ime。低层加密器 114 进行的加密应使用与信息单元加密器 112 进行的加密相同的密码。

在步骤 S1506，发送器 115 把步骤 S1505 加密获得的加密多路信息 Ime 转换成适合发射机 120 发送的格式，并产生发送信息 It。

在步骤要 1507，发射机 120 向实际远距点发送信息 It。在这种情况下，多个接收单元 1430 可以对应于一个发送单元 1410。

在图 20 中，示出了接收单元 1430 进行的操作流程图。

在步骤S1601，接收机131从发射机120接收发送信息It，从输入的发送信息It中取出部分或全部加密多路信息Ime。

在步骤1602，解密器1432接收在步骤S1601获得的加密多路信息Ime。然后，解密器1432解密接收到的加密多路信息Ime，并产生多路信息Im。

在步骤S1603，多路复用器1433分离在步骤S1602获得的每个加密信息单元Iue的多路信息Im，取出加密信息单元Iue。

在步骤S1604，存储器1034利用加密信息单元ID存储加密信息单元Iue。

在步骤S1605，当再现器1036输出再现指定信息Idr时，过程进入到步骤S1606，而当不输出再现指定信息Idr时返回到步骤S1601。

在步骤S1606，存储器1034取出在步骤S1605输出的再现指定信息Idr指定的具有加密信息单元ID的加密信息单元Iue。然后，存储器1034输出加密信息单元Iue。

在步骤S1607，解密器1432对加密的信息单元Iue解密，产生信息单元Iu。当信息单元Iu被加密一次时，对加密信息单元Iue解密一次，从而可以产生产单元Iu。虽然在第四发明中有对信息单元Iu递归加密多次的限制，但在本发明中没有这种限制。

在步骤S1608，再现器1036接收信息单元解密器1432输出的信息单元Iu，并产生再现信息Ir。

在步骤S1609，展现器1436根据再现信息的格式，向用户展现在步骤S1608获得的再现信息。

如上所述，信息单元加密器1012进行的加密与低层加密器114进行的加密相同。因此，可以用单个解密器1432不仅解码低层加密器114内使用的密码，而且可以解码信息单元1012内使用的密码。即，可以仅准备一个非专用的解密器，来解密信息单元Iu。

而且，加密信息单元ID被加到加密信息单元Iue上。另外增加了存储器1034。因此，存储在存储器1034内的加密信息单元Iue可以被更新到最新，而不需要在解密器1432中进行解密处理。当用户实际观看加密信息单元Iue时，解密器1432才对加密的信息单元Iue解密。

参照图21，示出了图18的信息传输装置1400的另一个例子。图21所示的信息传输装置1400R的结构是从信息传输装置1400中去除了低层加密器114。在该装置中，低层加密不是由低层加密器114(图18)进行的，而是由信息单元加密器1512(图

21)来进行。因此，信息单元加密器512仅在低层(例如发射机120工作的传输层)使用的某些加密系统下进行加密，例如发射机120进行的。无需说明的是，信息单元加密器1012能够在各种加密系统下进行加密，包括适合上述低层传输的系统。

(第六实施例)

下面参照图22、23和24描述根据本发明第六实施例的信息传输装置。该信息传输装置1700包括发送单元1710、发射机120和接收单元1730。下面为减少重复，一般省略对构成信息传输装置100、500、500R、800、800R、1000、1400和1400R基本相同的部分的描述。

在本实施例中，其发明点是把解密器1732输出的信息单元Iu回送给解密器本身，使解密器1732可以处理上述递归加密多次的信息单元。

发送单元1710

发送单元1710的结构基本上与图14所述的发送单元1010相似。因此省略其描述。

接收单元1730

接收单元1730的结构与根据第五实施例(图18) 接收单元非常相似，只是用解密器1832代替了解密器1432。

解密器1732连接到接收机131上，接收加密多路信息，产生加密信息单元Iue、多路信息Im或信息单元Iu。解密器1732具有回送如此产生的加密信息单元Iue给本身的环路。解密器1732还连接到再现器1036上，向其提供如此产生的信息单元Iu，并连接到去多路复用器1733上，向其提供如此产生的多路信息单元Iu。而且，解密器1732双向连接存储器1034，在它们之间交换加密信息单元Iue。当向其输出加密多路信息Ime时，解密器1732输出多路信息Im，当向其输入加密信息单元Iue时，解密加密的信息单元Iue，并输出其结果的信息单元Iu。

去多路复用器1733连接到解密器1732上，接收多路信息Im，并输出加密信息单元Iue和/或信息单元Iu。

存储器1034接收去多路复用器1733和去解密器1732输出的加密信息单元Iue，以及再现器1036输出的再现指定信息Idr。然后，存储器1034还向解密器1732输出

加密信息单元 Iue。

当更新加密信息单元 Iue 时，存储器 1034 存储接收到的加密信息单元 Iue，并替换存储的加密信息单元 Iue，把加密信息单元 Iue 更新到最新。

当接收到的再现指定信息 Idr 指定存储的加密信息单元 Iue 时，存储器 1034 输出加密信息单元 Iue。

再现器 1036 接收解密器 1732 输出的信息单元 Iu，输出再现信息 Ir 和再现指定信息 Idr。请注意，第三实施例中所用的解密器 832 应能同时解密多路信息单元 Iu。相反，由于作为一次解密结果的加密信息暂时存储在存储器 1034 内，所以解密器 1732 并不受解密器 832 那样的限制。

而且，还可以仅当在预定周期内不能完成处理时，把加密信息单元 Iue 暂时输出到存储器 1034 上。把这种暂时存储的加密信息输出到信息单元解密器 1732，然后进行处理。

运作

参照图 23 详细描述接收单元 1730 进行的操作。

在步骤 S1801，接收机 131 接收发射机 120 的发送信息 It，从接收到的发送信息 It 中取出部分或全部加密多路信息单元 Ime。

在步骤 S1802，解密器 1732 接收在步骤 S1801 获得的加密多路信息 Ime。然后，解密器 1732 解密接收到的加密多路信息 Ime，产生多路信息 Im。

在步骤 S1803，解密器 1433 分离在步骤 S1802 获得的每个加密信息单元 Iue 的多路信息 Im，取出加密信息单元 Iue。

在步骤 S1804，存储器 1034 利用加密信息单元 ID 存储加密信息单元 Iue。

在步骤 S1805，当再现器 1036 输出再现指定信息 Idr 时，过程进入到步骤 S1806。当不输出再现指定信息 Idr 时，过程返回到步骤 S1801。

在步骤 S1806，从存储加密信息单元 Iue 的存储器 1034 中取出具有步骤 S1805 所输出再现指定信息 Idr 指定的加密信息单元 ID 的加密信息单元 Iue，并输出取出的加密信息单元 Iue。

在步骤 S1807，当取出的信息单元 Iu 处于解密器 1732 所输入加密信息单元 Iue 中没有加密的状态时，过程进入到步骤 S1809。

在步骤 S1808，解密器 1732 对存在要取出的信息单元 Iu 的加密信息单元 Iue 解

密一次。然后过程返回到步骤S1807。

在步骤S1809，再现器1036接收解密器1732输出的信息单元Iu，处理作为可再生信息的再现信息Ir。

在步骤S1810，展现器136根据再现信息的格式向用户展现在步骤S1809获得的再现信息Ir。

如上所述，信息单元加密器1012进行递归加密多次，并且在低层加密器114中使用与信息单元加密器1012内使用的相同的密码系统，从而，可以在解密器1732中对应于所有这些多次加密进行解密。

而且，加密信息单元ID加到加密信息单元Iue中，可以把存储在存储器1034内的加密信息单元Iue更新到最新，而不用在解密器1732中进行解密处理。当用户实际观看加密信息单元Iue时，由解密器1732解密加密的信息单元Iue。

参照图24，图24示出了图22的信息传输装置1700的另一个例子。图24所示的信息传输装置1700R的结构是从信息传输装置1700中去除了低层加密器114。在该装置中，低层传输的加密不是由低层加密器114(图22)进行的，而是由信息单元加密器512(图24)进行的。因此，信息单元加密器512仅在低层(例如发射机120工作的传输层)使用的某些加密系统下进行加密。无需说明的是，信息单元加密器1012可以在各种加密系统下进行加密，包括在适合上述低层传输的系统。

如上详述，根据本发明，对信息单元Iu进行多次相同的递归加密，并由一个解密器解密多次。因此，与传统的例子相比，不仅可以进行自由度很大的加密，而且例如通过不用专用解密器和附加解密器简单化了信息传输装置。

又，在引入加密信息单元Iu之后加上加密信息单元ID，以根据ID更新新设置的存储器的内容。在实际观看信息单元Iu时，由解密器解密信息单元Iu。因此，不仅能简单地管理存储器内容的更新，而且可以防止不付费用户在观看时解密存储的信息单元Iu而非法观看信息单元Iu。因此，本发明对解密收费系统是有很高的吸引力的。

虽然详细描述了本发明，但前面的描述只是所有方面的说明，并不是限制。应当理解，不脱离本发明的范围可以作出大量的其它修改和变化。

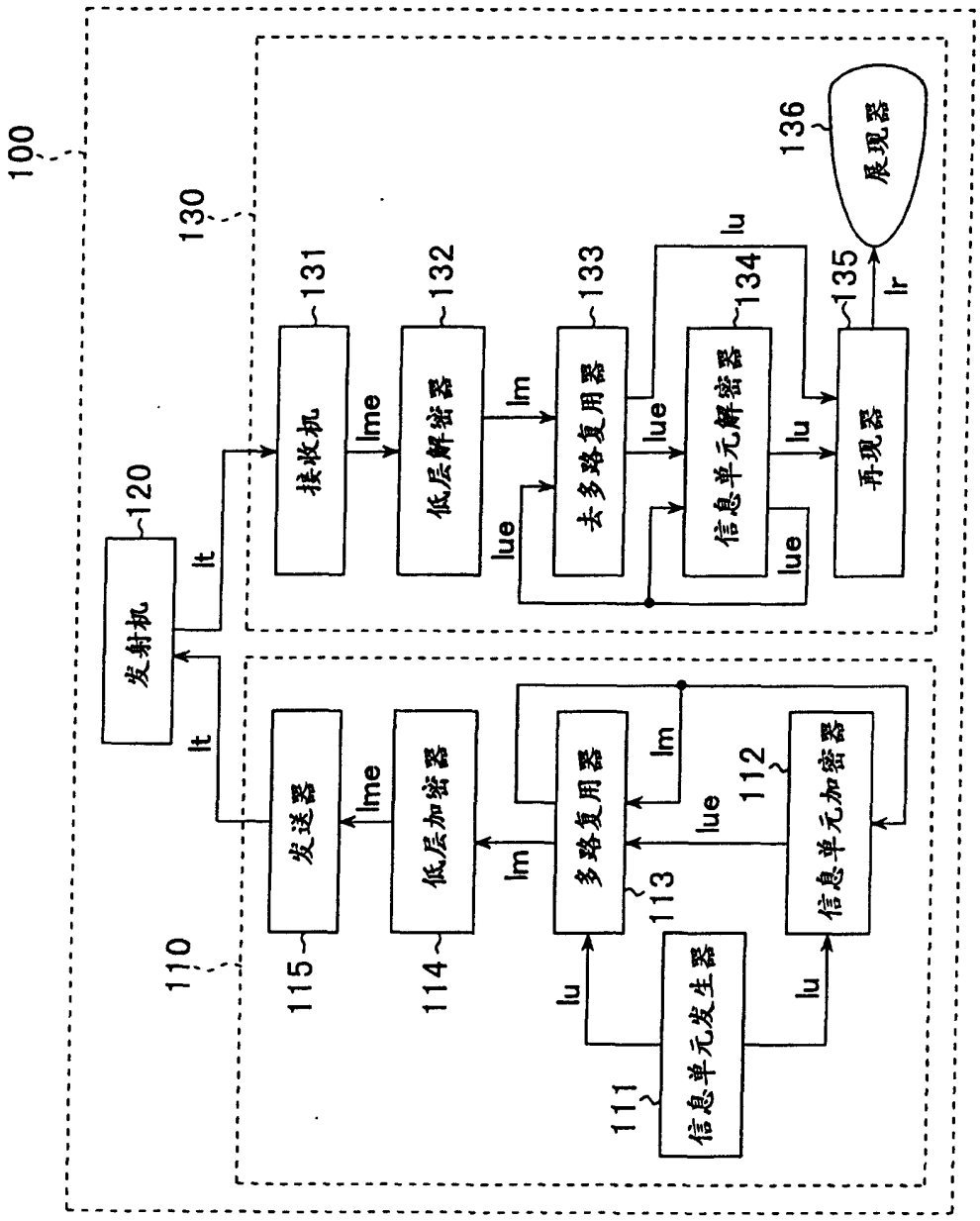

100
130
120
发射机
It
接收机
131
lme
低层解密器
132
lm
lue
去多路复用器
133
lue
信息单元解密器
134
lu
lue
再现器
135
lr
展现器
136
110
发送器
115
lme
低层加密器
114
lm
多路复用器
113
lm
lue
信息单元加密器
112
lu
lu
信息单元发生器
111

图 1

图 2

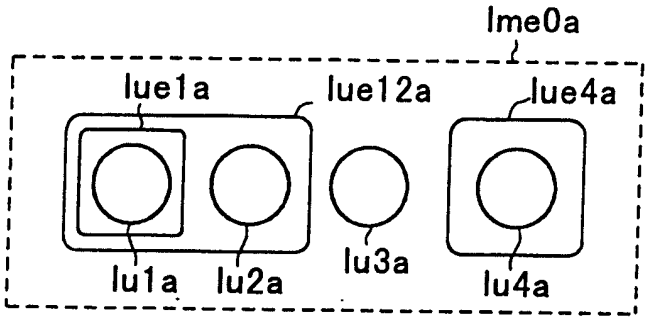

lme0a
lue1a
lue12a
lue4a
lu1a
lu2a
lu3a
lu4a

图 6

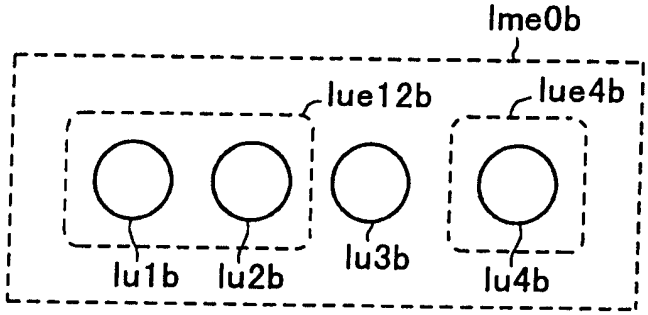

lme0b
lue12b
lue4b
lu1b
lu2b
lu3b
lu4b

图 11

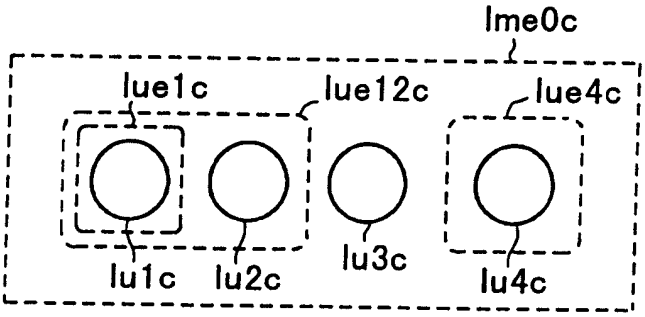
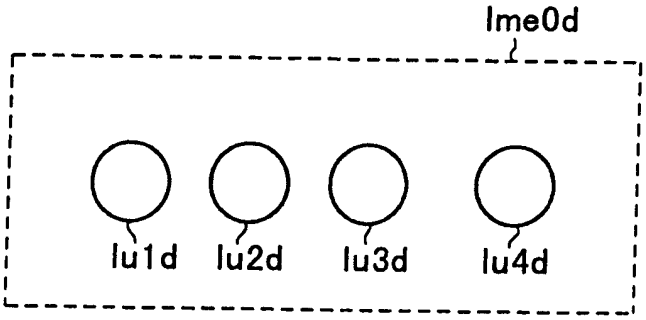

lme0c
lue1c
lue12c
lue4c
lu1c
lu2c
lu3c
lu4c

图 26


lme0d
lu1d
lu2d
lu3d
lu4d

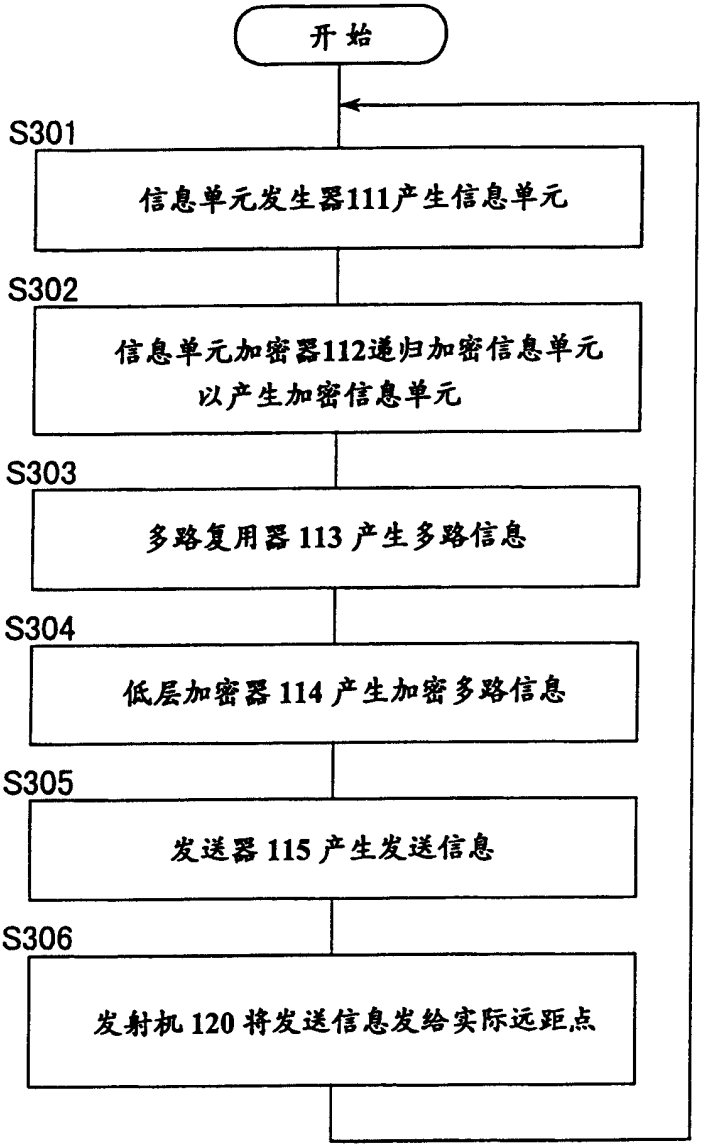

开始
S301
信息单元发生器111产生信息单元
S302
信息单元加密器112递归加密信息单元以产生加密信息单元
S303
多路复用器 113 产生多路信息
S304
低层加密器 114 产生加密多路信息
S305
发送器 115 产生发送信息
S306
发射机 120 将发送信息发给实际远距点

图 3

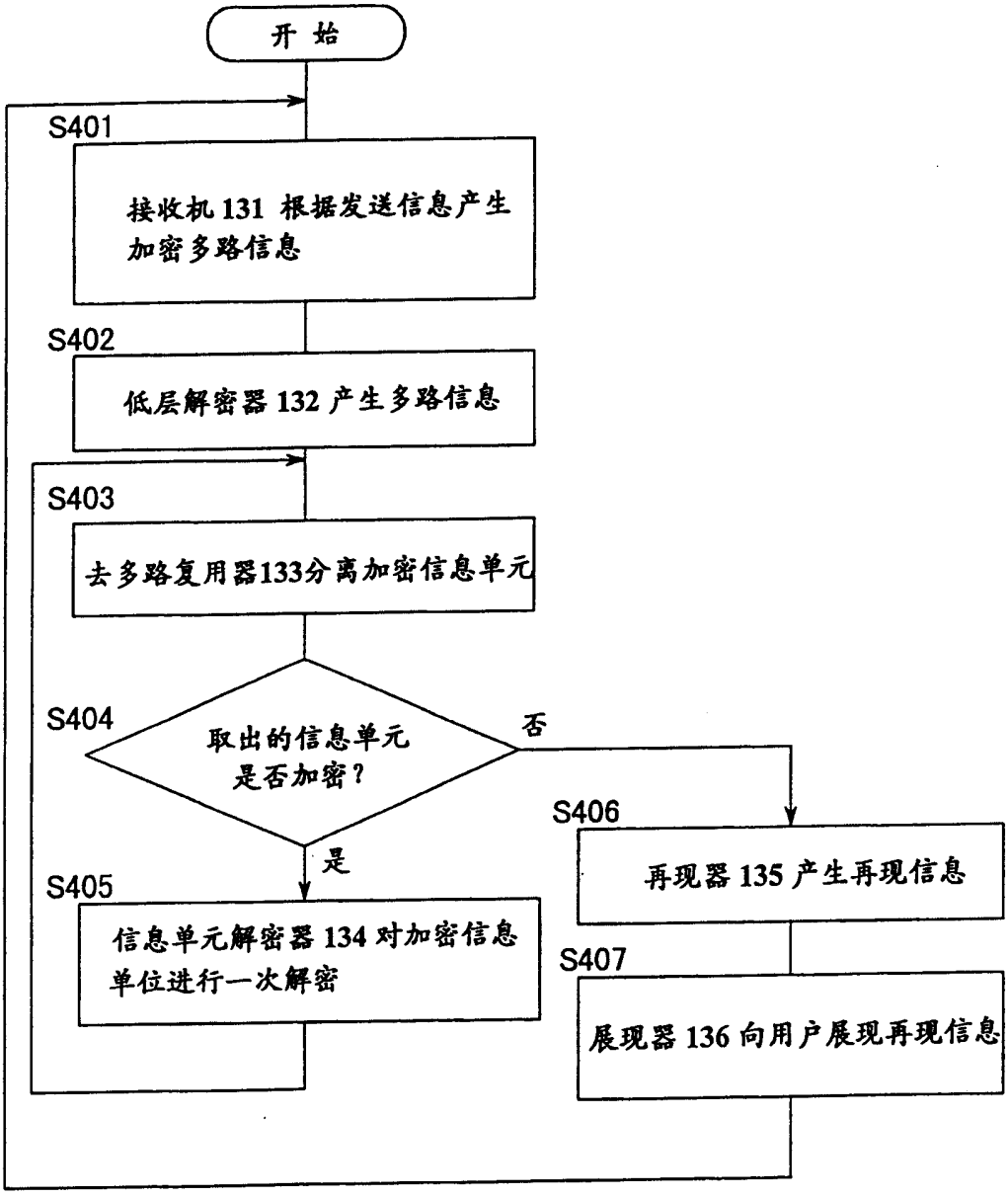

开 始
S401
接收机 131 根据发送信息产生加密多路信息
S402
低层解密器 132 产生多路信息
S403
去多路复用器133分离加密信息单元
S404
取出的信息单元是否加密？
否
是
S405
信息单元解密器 134 对加密信息单位进行一次解密
S406
再现器 135 产生再现信息
S407
展现器 136 向用户展现再现信息

图 4

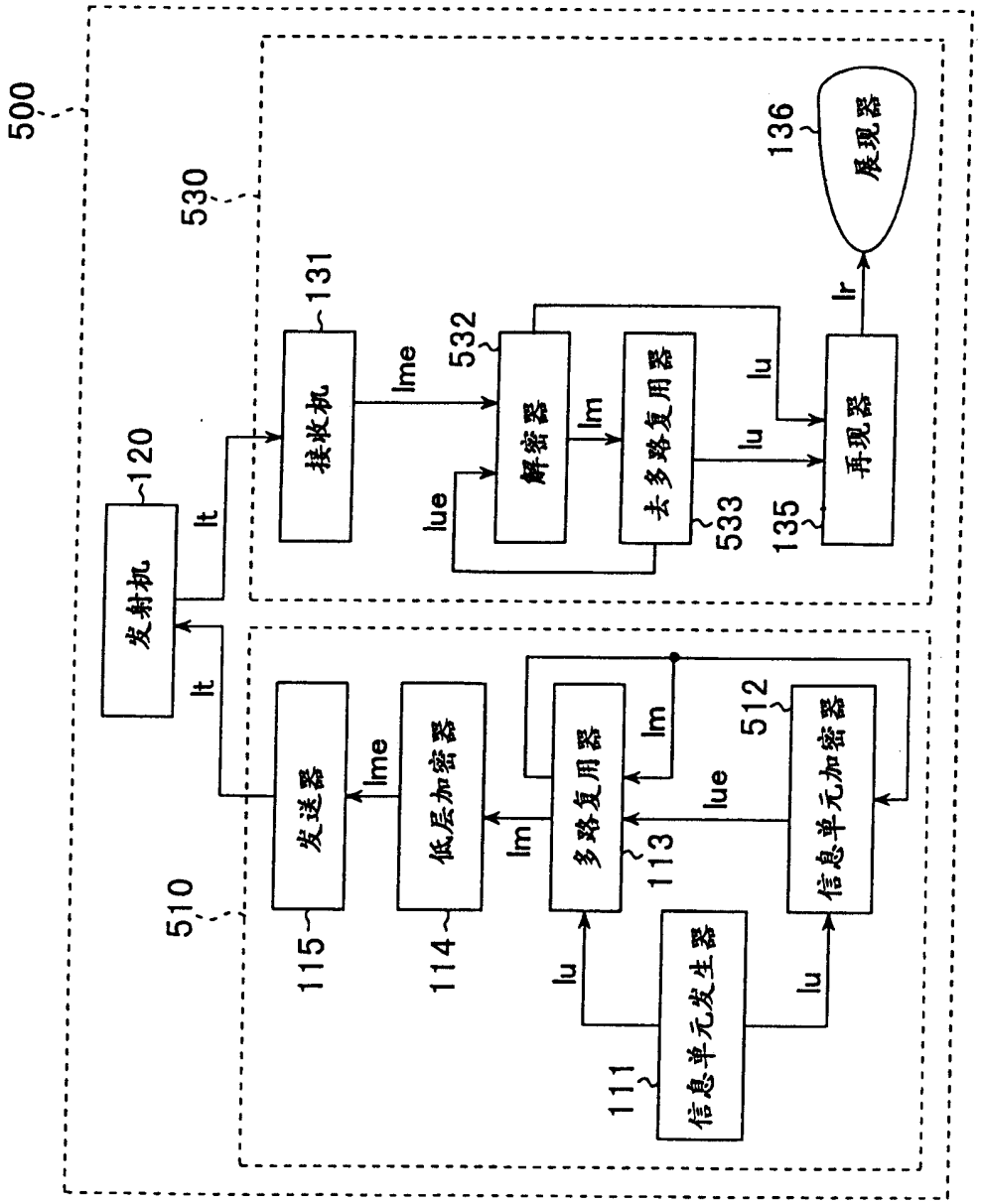

500
530
510
120
发射机
It
It
131
接收机
lme
532
解密器
lm
去多路复用器
lu
lu
533
135
再现器
lr
136
展现器
lue
发送器
lme
115
低层加密器
114
lm
多路复用器
113
lm
lue
512
信息单元加密器
lu
lu
111
信息单元发生器

图 5

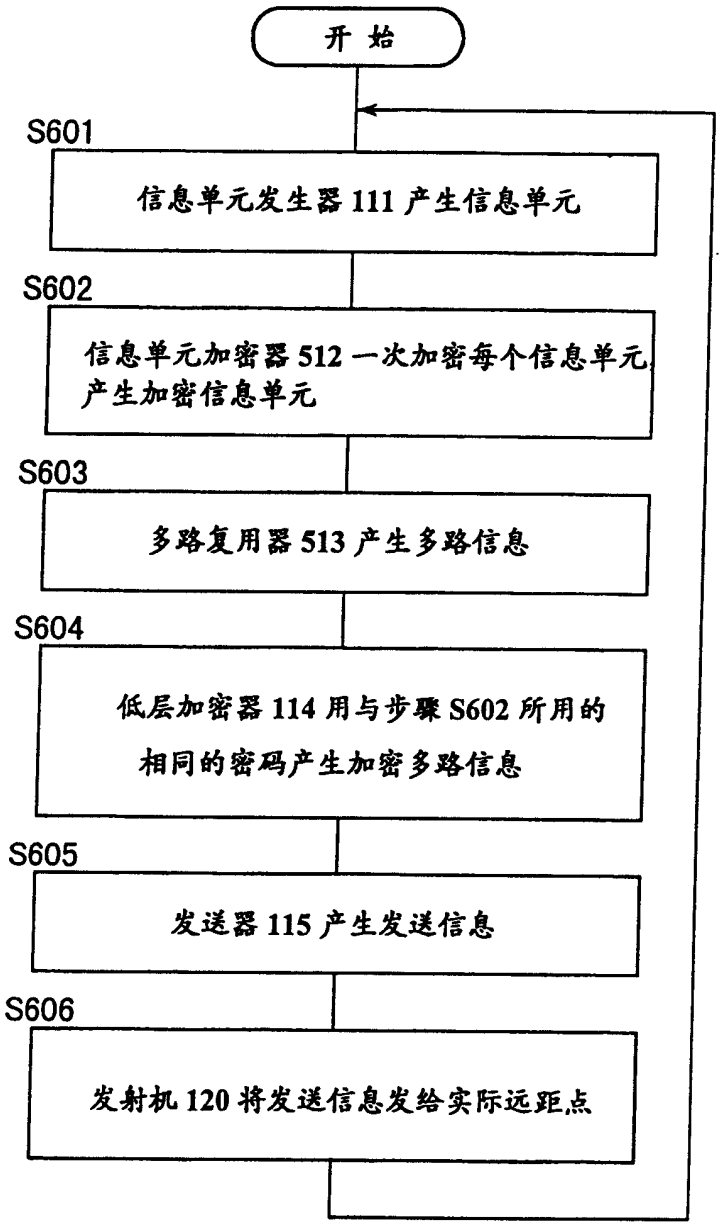

开 始
S601
信息单元发生器 111 产生信息单元
S602
信息单元加密器 512 一次加密每个信息单元，产生加密信息单元
S603
多路复用器 513 产生多路信息
S604
低层加密器 114 用与步骤 S602 所用的相同的密码产生加密多路信息
S605
发送器 115 产生发送信息
S606
发射机 120 将发送信息发给实际远距点

图 7

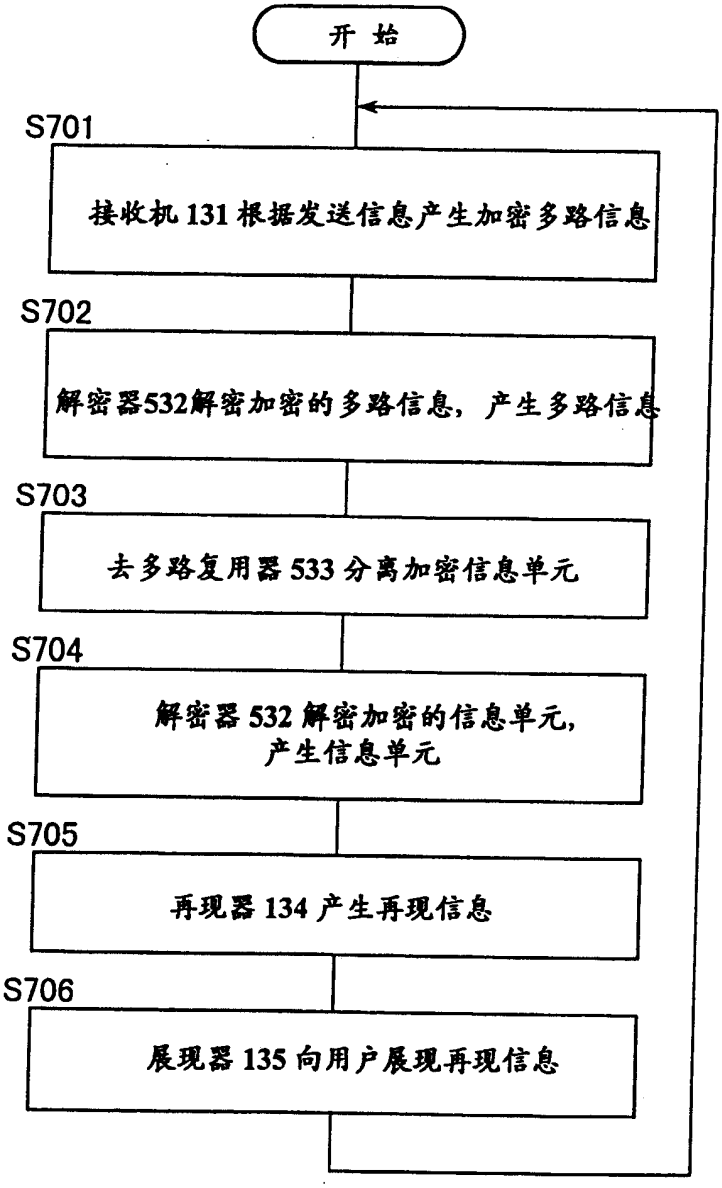

开 始
S701
接收机 131 根据发送信息产生加密多路信息
S702
解密器532解密加密的多路信息，产生多路信息
S703
去多路复用器 533 分离加密信息单元
S704
解密器 532 解密加密的信息单元，
产生信息单元
S705
再现器 134 产生再现信息
S706
展现器 135 向用户展现再现信息

图 8

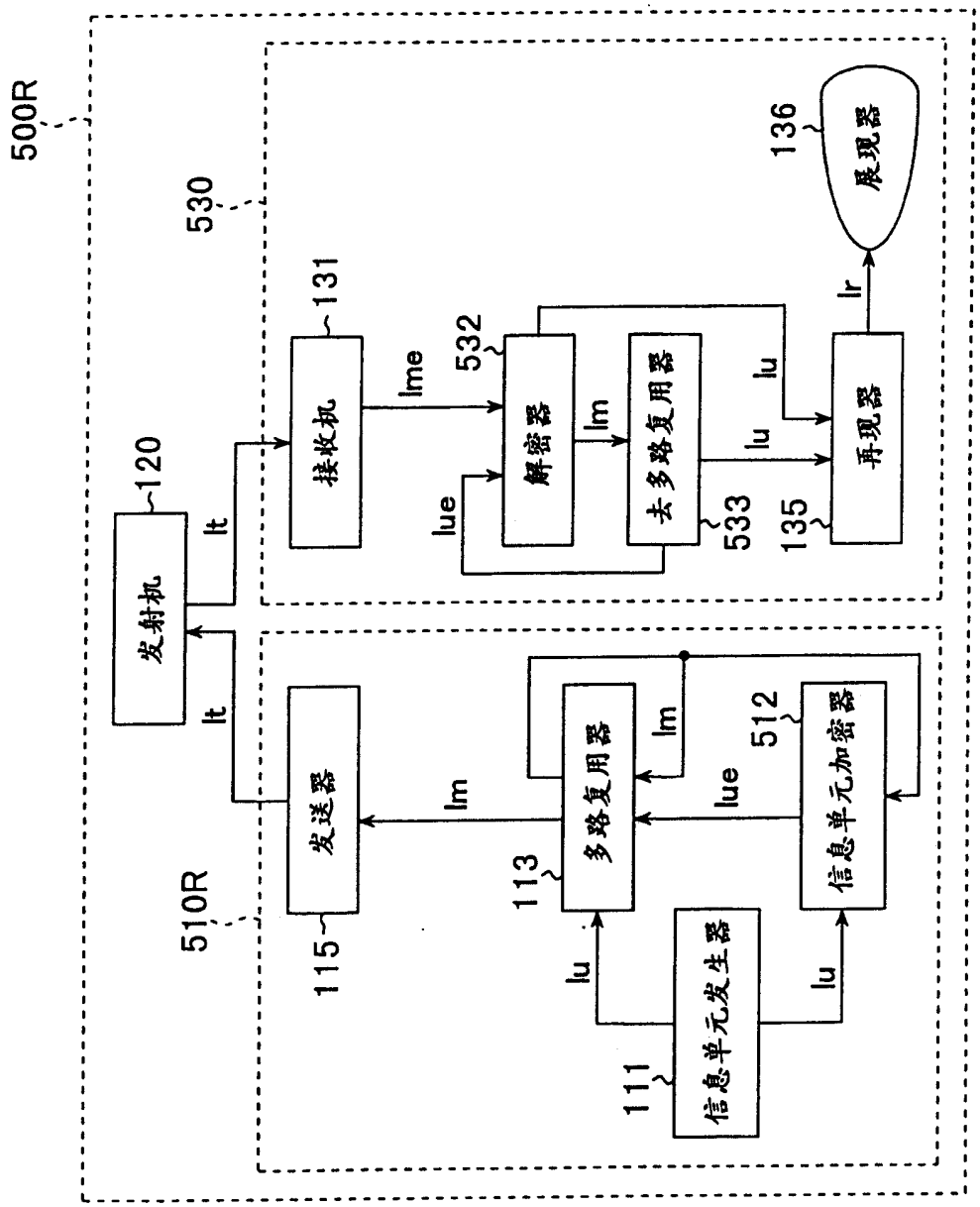

500R
530
136
展现器
131
接收机
lme
532
解密器
lm
去多路复用器
lu
lu
lue
533
135
再现器
lr
120
发射机
lt
lt
发送器
lm
113
多路复用器
lm
512
lue
信息单元加密器
510R
115
lu
lu
111
信息单元发生器

图 9

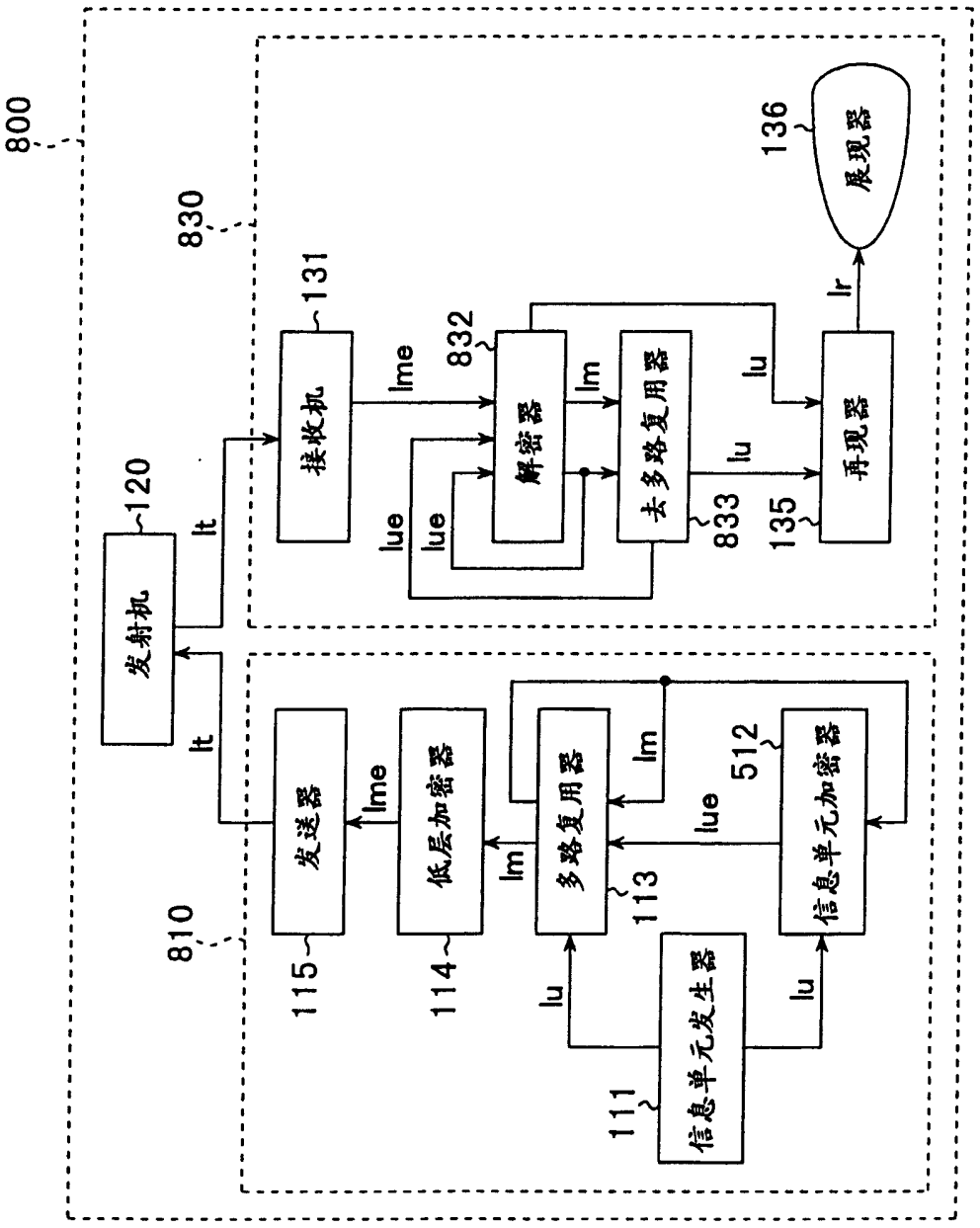

800
830
810
120
发射机
131
接收机
832
解密器
去多路复用器
833
135
再现器
136
展现器
发送器
115
低层加密器
114
多路复用器
113
512
信息单元加密器
111
信息单元发生器
lt
lme
lm
lue
lu
lr

图 10

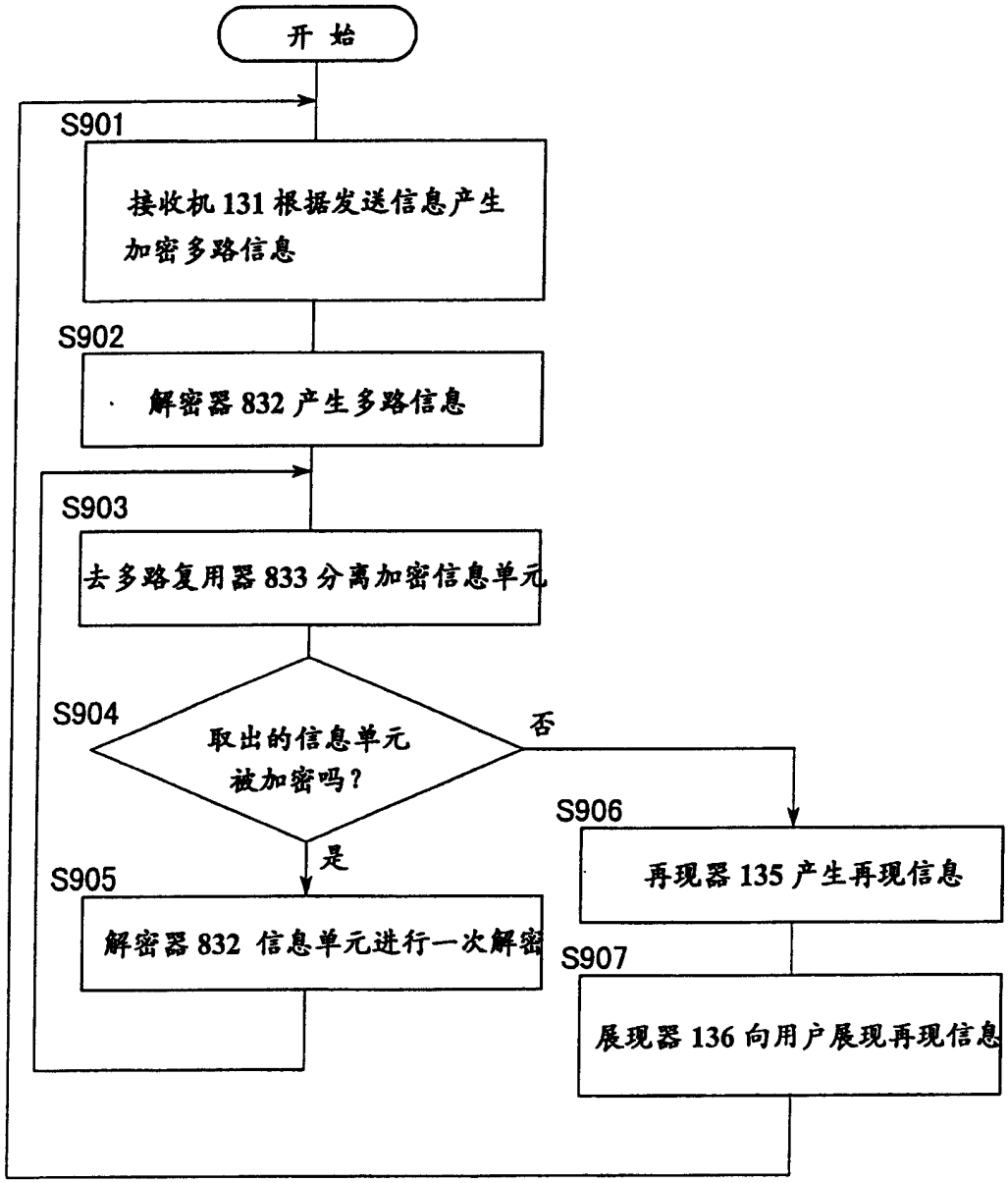

开 始
S901
接收机 131 根据发送信息产生加密多路信息
S902
解密器 832 产生多路信息
S903
去多路复用器 833 分离加密信息单元
S904
取出的信息单元被加密吗？
否
是
S905
解密器 832 信息单元进行一次解密
S906
再现器 135 产生再现信息
S907
展现器 136 向用户展现再现信息

图 12

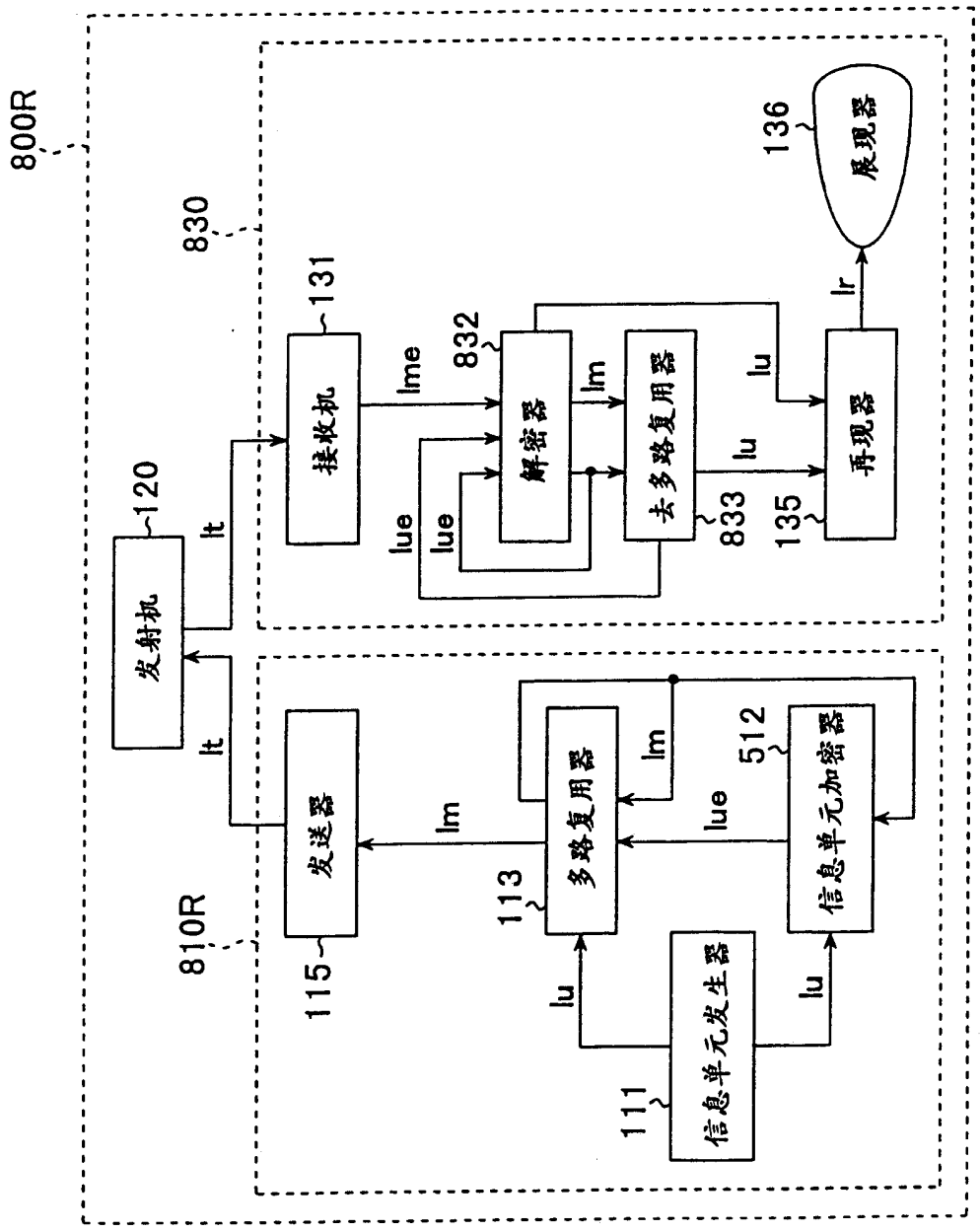
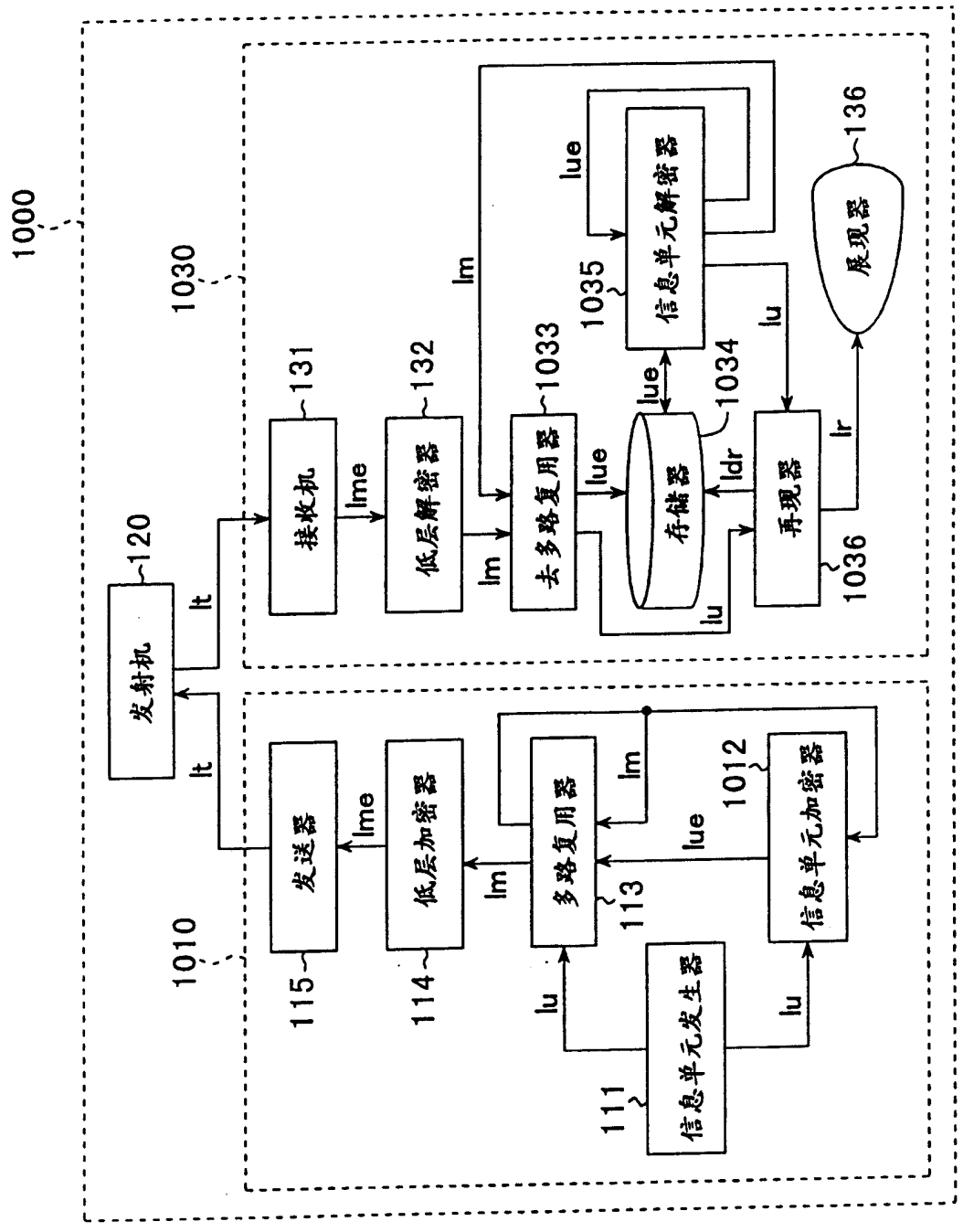

800R
830
810R
120
发射机
lt
131
接收机
lme
832
解密器
lm
去多路复用器
lu
833
135
再现器
136
展现器
lr
lue
lue
115
发送器
113
多路复用器
111
信息单元发生器
512
信息单元加密器

图 13

图 14


1000
1030
1010
发射机
120
lt
接收机
131
lme
低层解密器
132
lm
去多路复用器
1033
lue
存储器
1034
ldr
再现器
1036
lr
展现器
136
lu
信息单元解密器
1035
lue
lm
发送器
115
lme
低层加密器
114
lm
多路复用器
113
lm
lue
信息单元加密器
1012
lu
信息单元发生器
111
lu

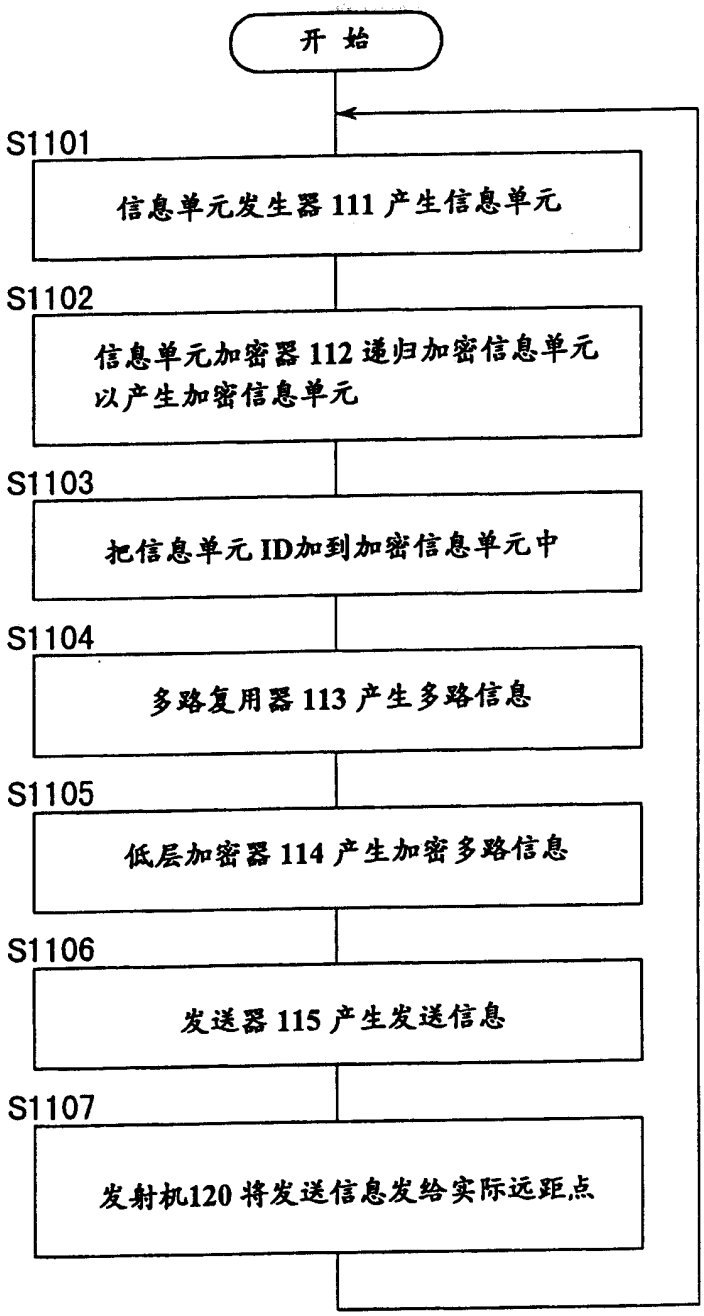

开 始
S1101
信息单元发生器 111 产生信息单元
S1102
信息单元加密器 112 递归加密信息单元
以产生加密信息单元
S1103
把信息单元 ID加到加密信息单元中
S1104
多路复用器 113 产生多路信息
S1105
低层加密器 114 产生加密多路信息
S1106
发送器 115 产生发送信息
S1107
发射机120 将发送信息发给实际远距点

图 15

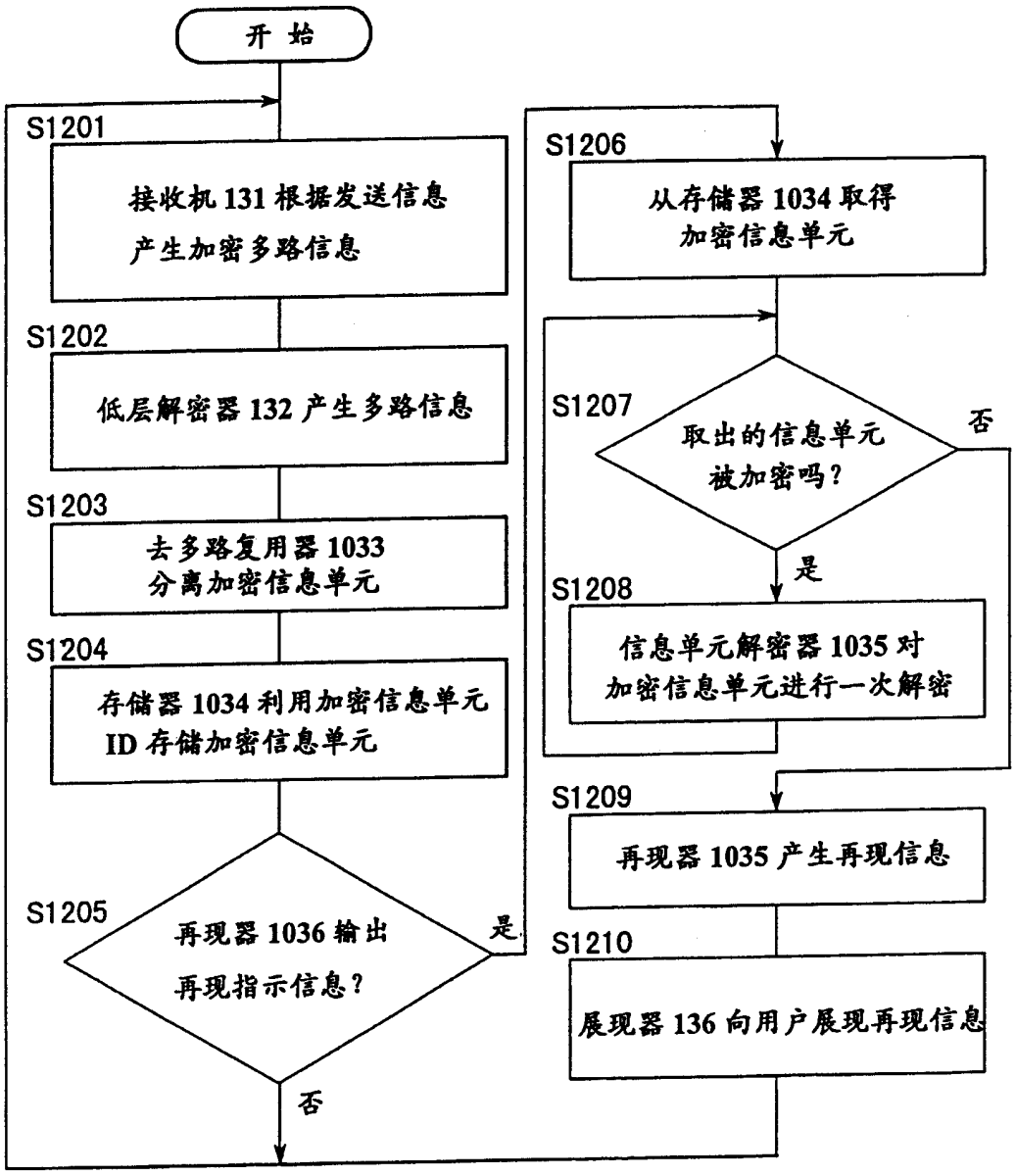

开 始
S1201
接收机 131 根据发送信息
产生加密多路信息
S1202
低层解密器 132 产生多路信息
S1203
去多路复用器 1033
分离加密信息单元
S1204
存储器 1034 利用加密信息单元
ID 存储加密信息单元
S1205
再现器 1036 输出
再现指示信息?
是
否
S1206
从存储器 1034 取得
加密信息单元
S1207
取出的信息单元
被加密吗?
否
是
S1208
信息单元解密器 1035 对
加密信息单元进行一次解密
S1209
再现器 1035 产生再现信息
S1210
展现器 136 向用户展现再现信息

图 16

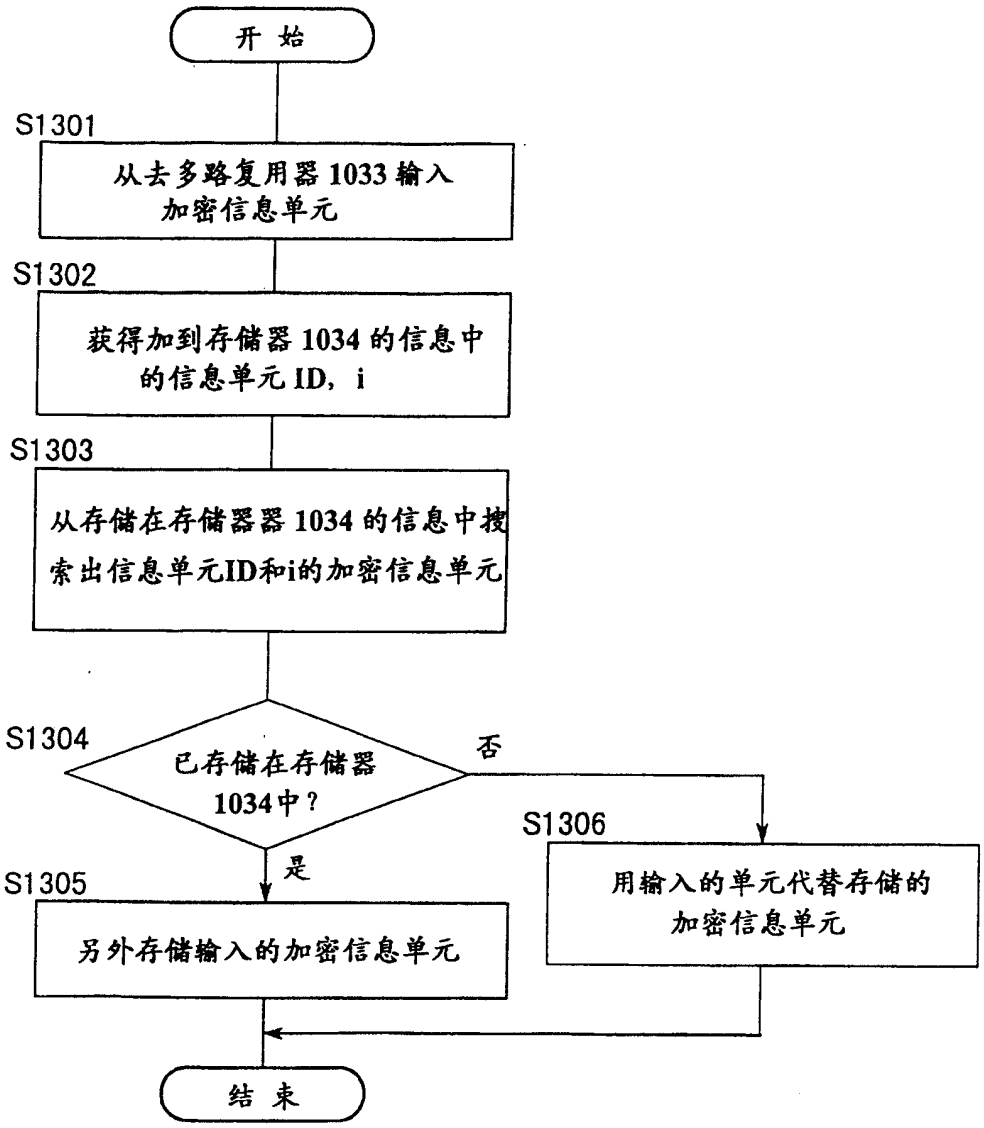
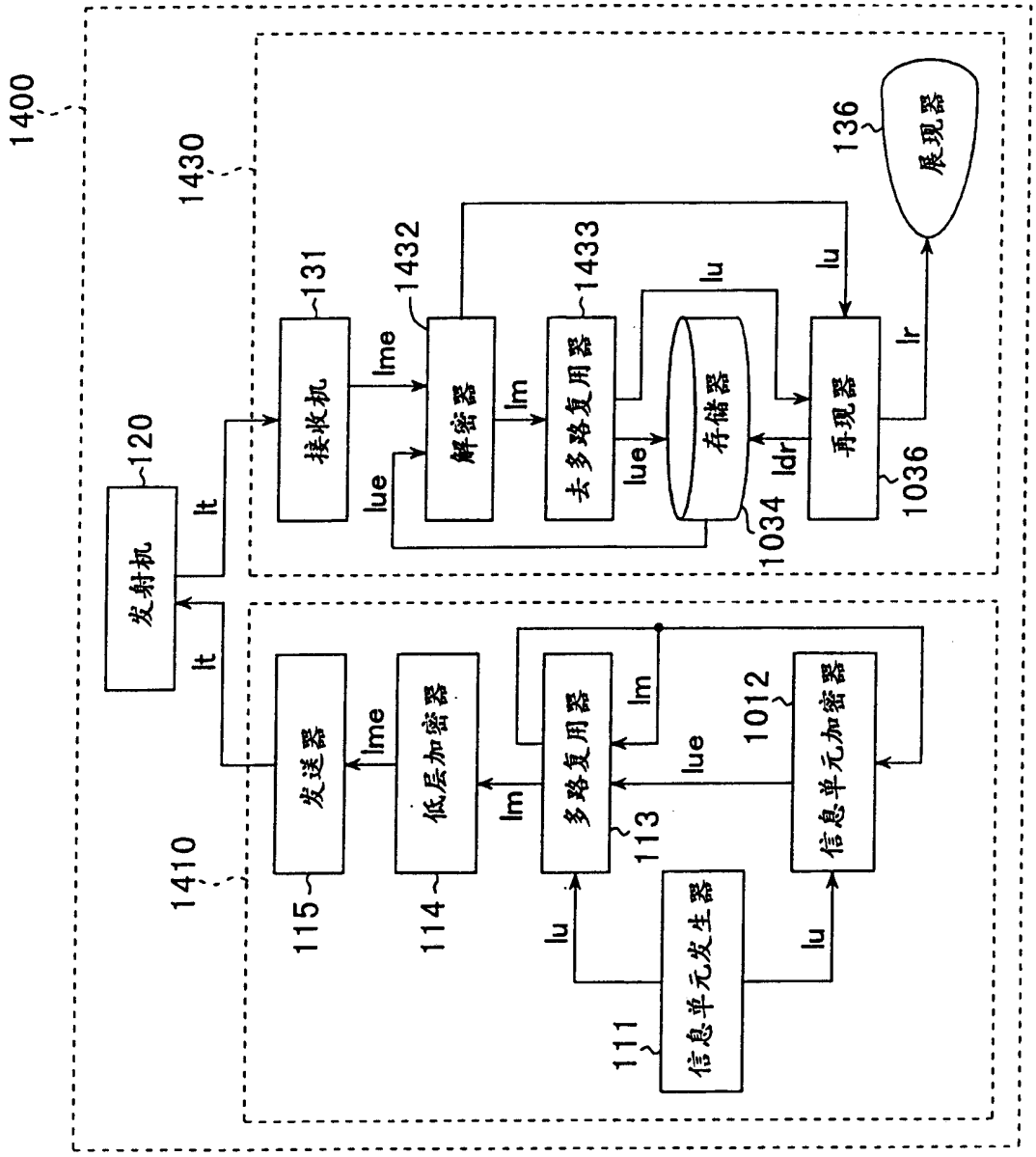

开 始
S1301
从去多路复用器 1033 输入
加密信息单元
S1302
获得加到存储器 1034 的信息中
的信息单元 ID，i
S1303
从存储在存储器器 1034 的信息中搜
索出信息单元ID和i的加密信息单元
S1304
已存储在存储器
1034中？
否
是
S1306
用输入的单元代替存储的
加密信息单元
S1305
另外存储输入的加密信息单元
结 束

图 17

图 18


1400
1430
1410
发射机
120
lt
接收机
131
lme
解密器
1432
lm
去多路复用器
1433
lue
存储器
1034
ldr
再现器
1036
lr
展现器
136
lu
发送器
115
低层加密器
114
多路复用器
113
信息单元发生器
111
信息单元加密器
1012

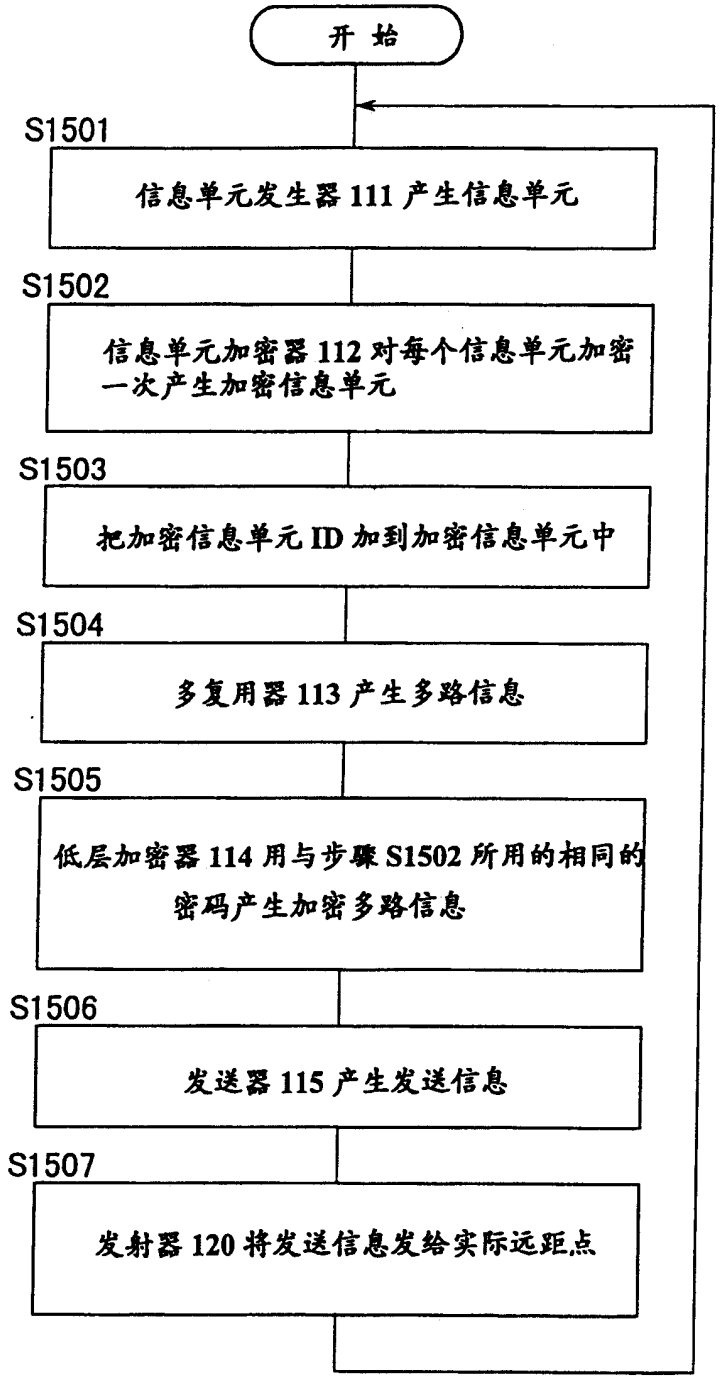

开 始
S1501
信息单元发生器 111 产生信息单元
S1502
信息单元加密器 112 对每个信息单元加密一次产生加密信息单元
S1503
把加密信息单元 ID 加到加密信息单元中
S1504
多复用器 113 产生多路信息
S1505
低层加密器 114 用与步骤 S1502 所用的相同的密码产生加密多路信息
S1506
发送器 115 产生发送信息
S1507
发射器 120 将发送信息发给实际远距点

图 19

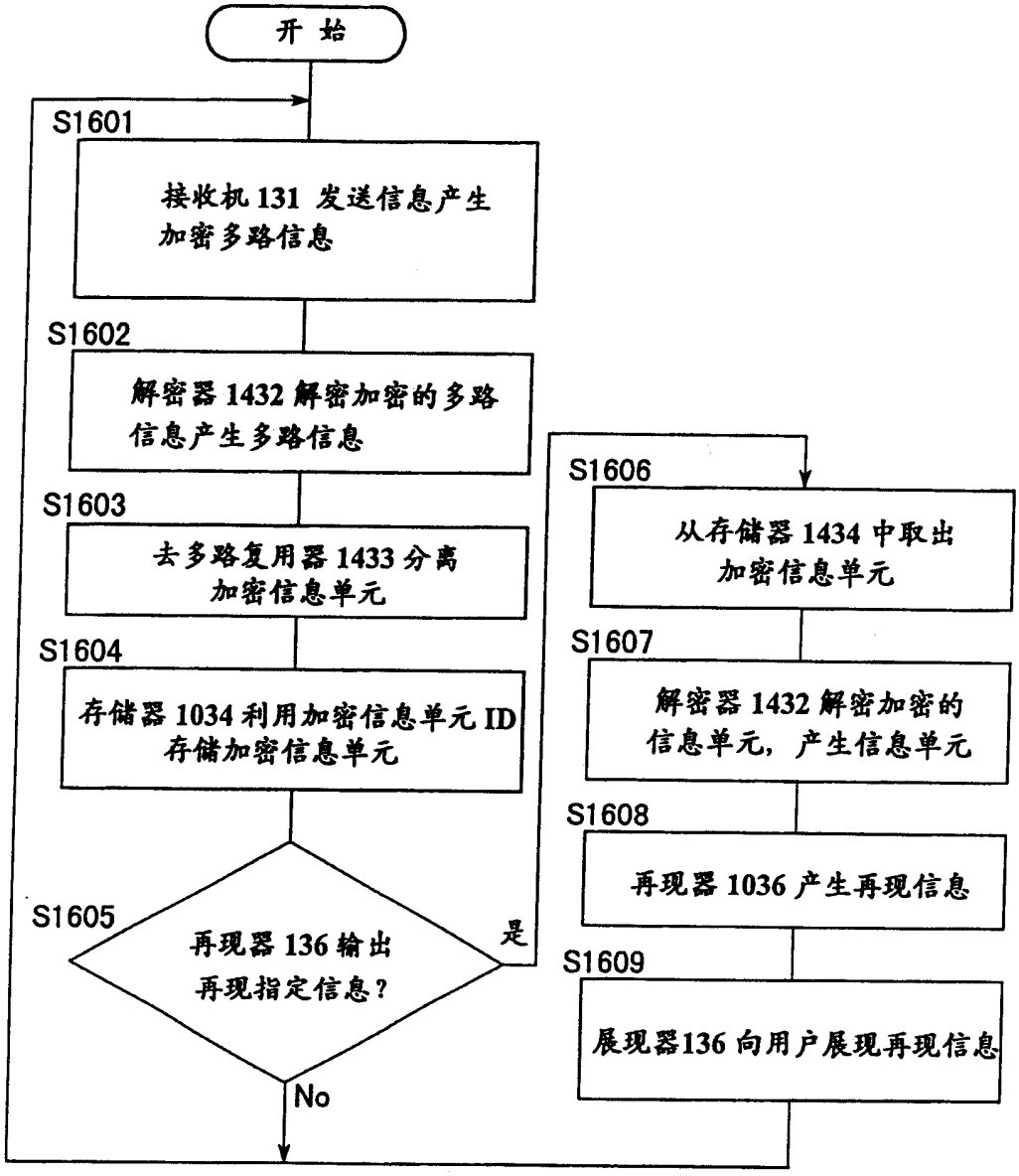

开 始
S1601
接收机 131 发送信息产生
加密多路信息
S1602
解密器 1432 解密加密的多路
信息产生多路信息
S1603
去多路复用器 1433 分离
加密信息单元
S1604
存储器 1034 利用加密信息单元 ID
存储加密信息单元
S1605
再现器 136 输出
再现指定信息？
是
No
S1606
从存储器 1434 中取出
加密信息单元
S1607
解密器 1432 解密加密的
信息单元，产生信息单元
S1608
再现器 1036 产生再现信息
S1609
展现器136 向用户展现再现信息

图 20

图 21

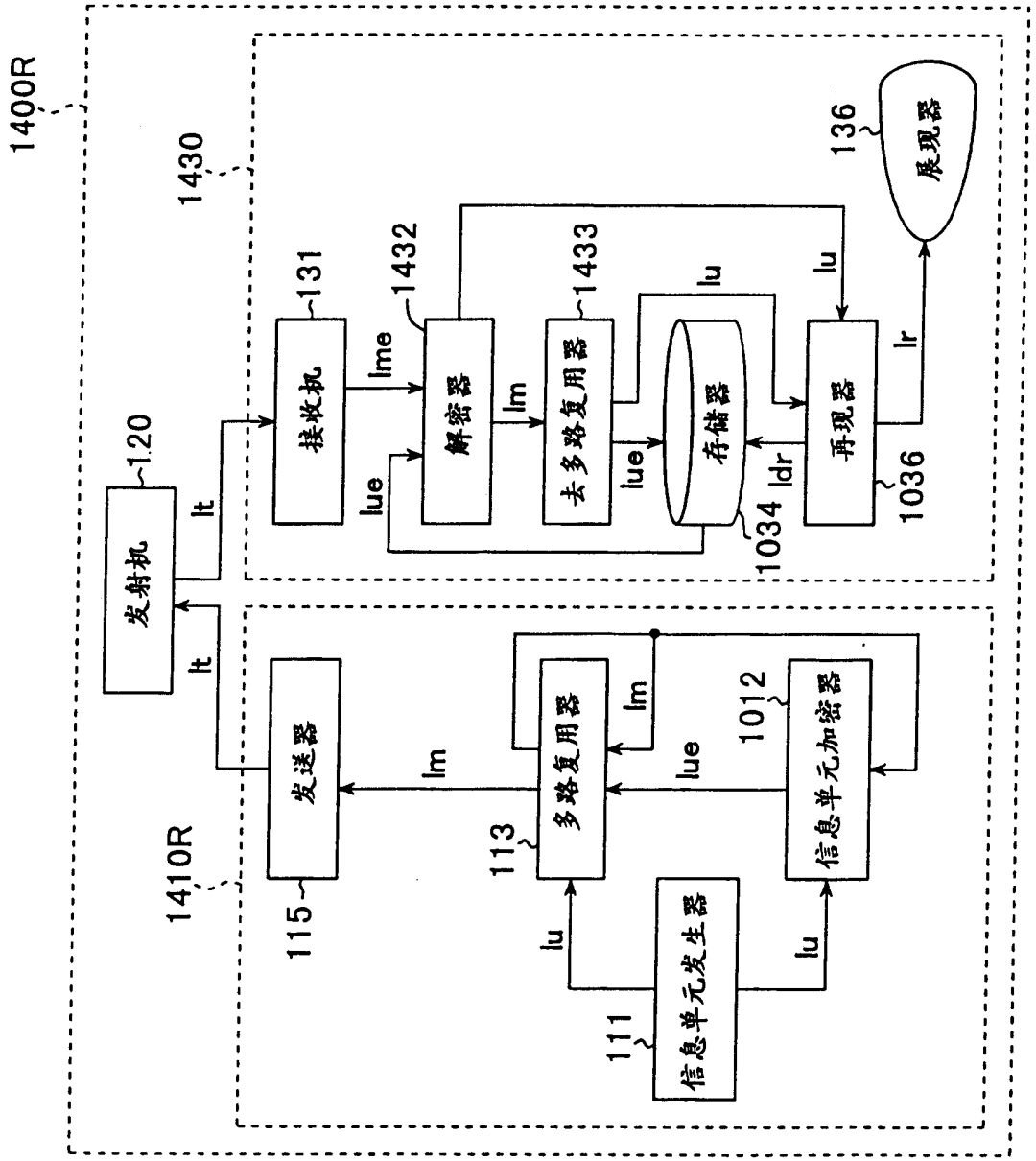
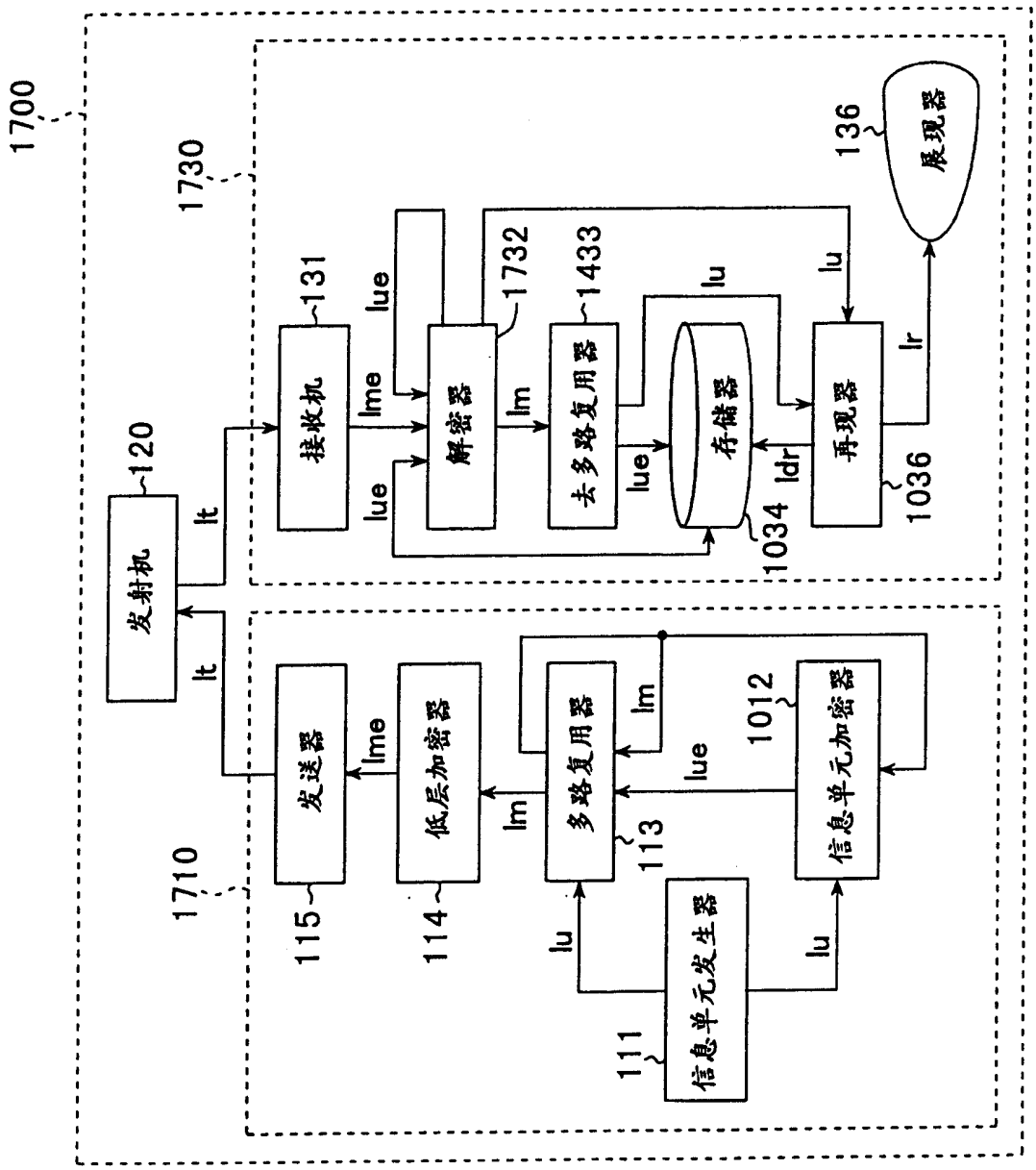

1400R
1430
1410R
120
发射机
lt
131
接收机
lme
1432
解密器
lm
1433
去多路复用器
lue
存储器
ldr
1034
lu
再现器
1036
lr
136
展现器
115
发送器
113
多路复用器
1012
信息单元加密器
111
信息单元发生器

图 22


1700
1730
1710
120
发射机
lt
131
接收机
lme
lue
1732
解密器
lm
1433
去多路复用器
lue
存储器
1034
lu
ldr
再现器
1036
lr
136
展现器
115
发送器
lme
114
低层加密器
lm
113
多路复用器
lm
lue
1012
信息单元加密器
111
信息单元发生器
lu
lu
lu

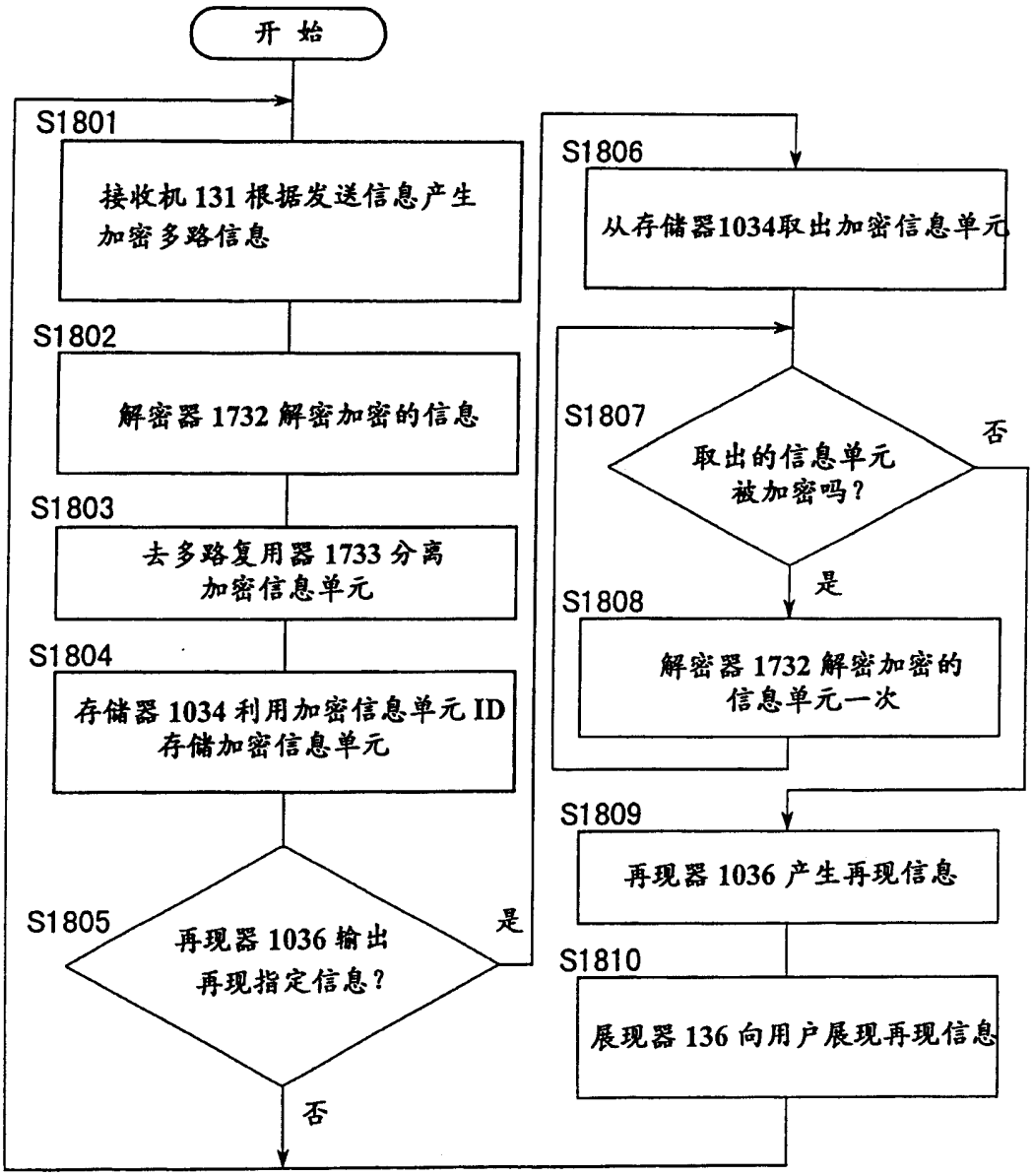
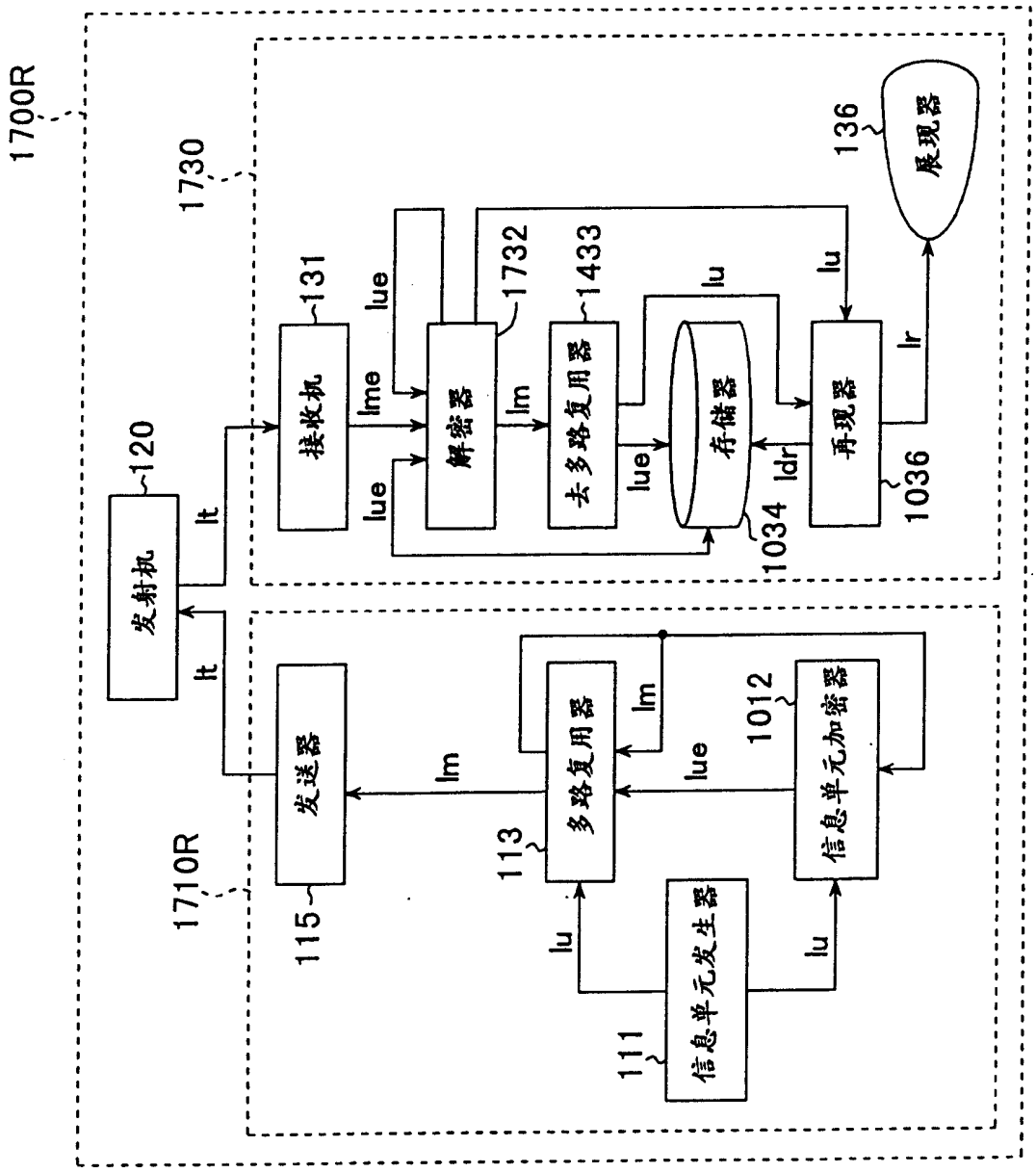

开 始
S1801
接收机 131 根据发送信息产生加密多路信息
S1802
解密器 1732 解密加密的信息
S1803
去多路复用器 1733 分离加密信息单元
S1804
存储器 1034 利用加密信息单元 ID 存储加密信息单元
S1805
再现器 1036 输出再现指定信息？
是
否
S1806
从存储器1034取出加密信息单元
S1807
取出的信息单元被加密吗？
否
是
S1808
解密器 1732 解密加密的信息单元一次
S1809
再现器 1036 产生再现信息
S1810
展现器 136 向用户展现再现信息

图 23

图 24


1700R
1730
1710R
120
发射机
lt
131
接收机
lme
lue
1732
解密器
lm
1433
去多路复用器
lue
存储器
lu
136
展现器
lr
再现器
ldr
1036
1034
115
发送器
lm
113
多路复用器
lm
lue
1012
信息单元加密器
111
信息单元发生器
lu
lu

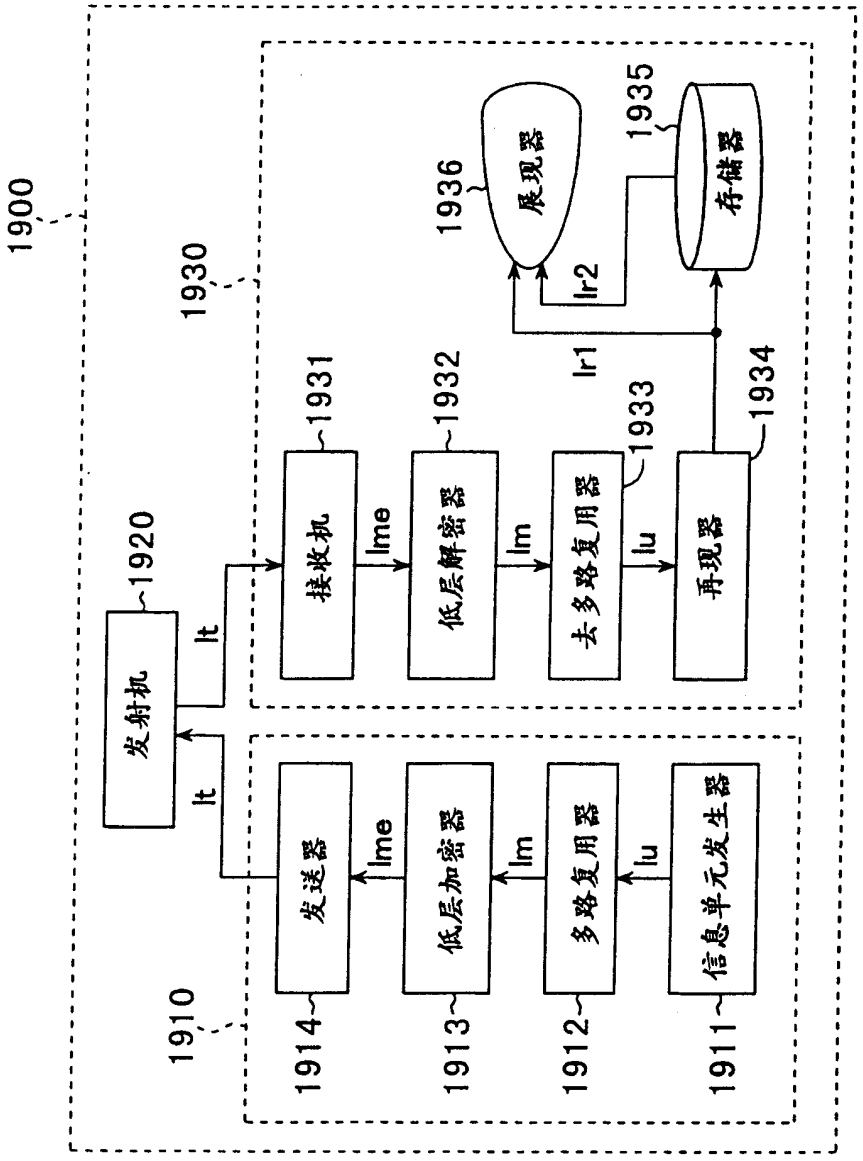

1900
1930
1910
1920
发射机
It
接收机
1931
Ime
低层解密器
1932
Im
去多路复用器
1933
Iu
再现器
1934
Ir1
展现器
1936
Ir2
存储器
1935
发送器
1914
低层加密器
1913
多路复用器
1912
信息单元发生器
1911

图 25

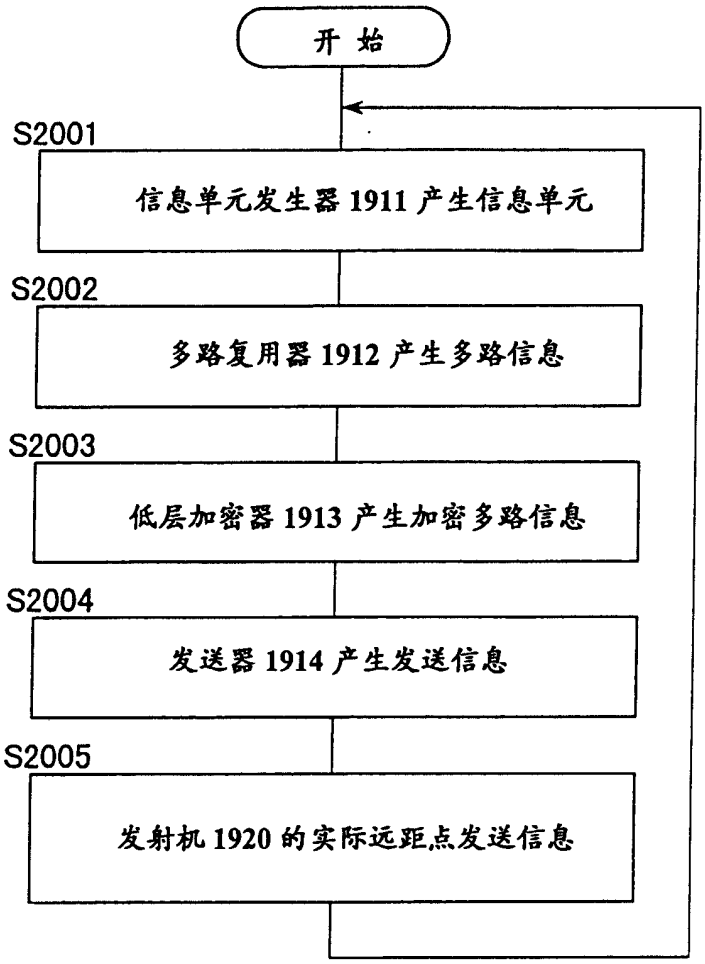

开 始
S2001
信息单元发生器 1911 产生信息单元
S2002
多路复用器 1912 产生多路信息
S2003
低层加密器 1913 产生加密多路信息
S2004
发送器 1914 产生发送信息
S2005
发射机 1920 的实际远距点发送信息

图 27

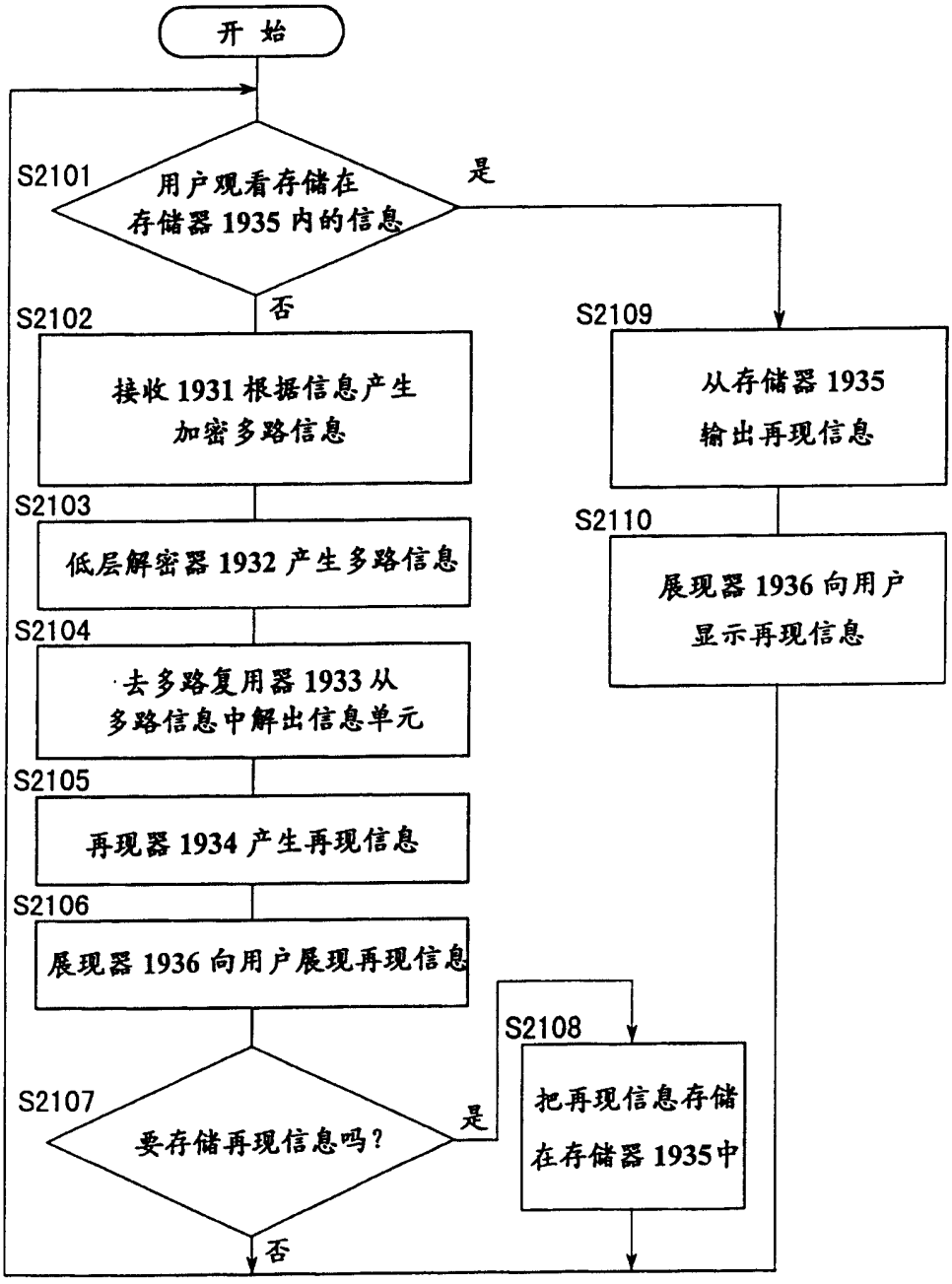

开 始
S2101
用户观看存储在存储器 1935 内的信息
是
否
S2102
接收 1931 根据信息产生加密多路信息
S2103
低层解密器 1932 产生多路信息
S2104
去多路复用器 1933 从多路信息中解出信息单元
S2105
再现器 1934 产生再现信息
S2106
展现器 1936 向用户展现再现信息
S2107
要存储再现信息吗?
是
否
S2108
把再现信息存储在存储器 1935中
S2109
从存储器 1935 输出再现信息
S2110
展现器 1936 向用户显示再现信息

图 28