



(12) 发明专利

(10) 授权公告号 CN 102224521 B

(45) 授权公告日 2013. 10. 23

(21) 申请号 200980146653. 8

(22) 申请日 2009. 10. 08

(30) 优先权数据

12/248, 437 2008. 10. 09 US

(85) PCT申请进入国家阶段日

2011. 05. 23

(86) PCT申请的申请数据

PCT/IB2009/054404 2009. 10. 08

(87) PCT申请的公布数据

W02010/041208 EN 2010. 04. 15

(73) 专利权人 纳格拉法国两合公司

地址 法国巴黎

(72) 发明人 O·福莱亚 D·莱斯特旺

(74) 专利代理机构 中国国际贸易促进委员会专
利商标事务所 11038

代理人 杨小明

(51) Int. Cl.

G06T 1/00 (2006. 01)

(56) 对比文件

US 2006/0164544 A1, 2006. 07. 27, 说明书第 [0025], [0032], [0074] 段 .

US 2008/0085031 A1, 2008. 04. 10, 说明书第 [0004], [0012], [0023] 段 .

US 6285774 B1, 2001. 09. 04, 说明书第 5 栏 第 20-36 行, 第 8 栏 “2. 1. MESSAGE ENCRYPTION” 部分 .

US 2002/0080964 A1, 2002. 06. 27, 说明书第 [0063] 段 .

US 2008/0085031 A1, 2008. 04. 10, 说明书第 [0004], [0012], [0023] 段 .

US 6285774 B1, 2001. 09. 04, 说明书第 5 栏 第 20-36 行, 第 8 栏 “2. 1. MESSAGE ENCRYPTION” 部分 .

US 2002/0080964 A1, 2002. 06. 26, 说明书第 [0063] 段 .

US 2006/0164544 A1, 2006. 07. 27, 说明书第 [0025], [0032], [0074] 段 .

审查员 王晓燕

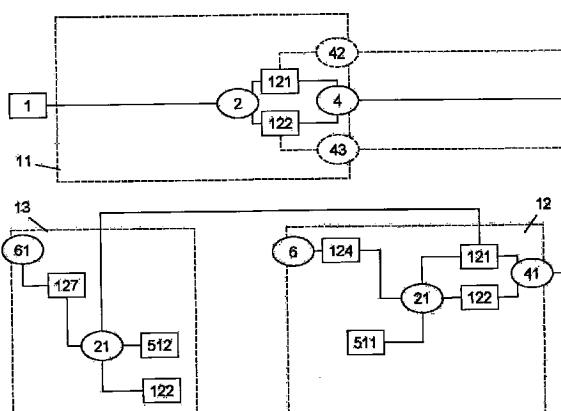
权利要求书3页 说明书7页 附图7页

(54) 发明名称

使用加扰和水印技术用于多播视听节目的记录的拷贝的安全共享的方法和装置

(57) 摘要

本发明涉及一种用于在多播视听节目的记录的拷贝的各种个人用户设备之间的安全共享的设备和方法, 通过使用加扰和水印技术的创造性方法保证再次编码的视听节目的合法消费。提供所述设备和方法, 以用于原始视听流通过多播会话到多个消费者设备的安全分发, 所述方法包括步骤: 通过修改所述原始视听流生成受保护的视听流; 生成包括适合于允许从所述受保护的流重构视听流的数字信息的任何格式的补充流, 其中, 所述方法的特征在于它包括步骤: 根据接收消费者设备或外部安全设备的唯一识别符计算第一标记; 在所述接收消费者设备上根据所述第一标记和所述补充流从所述受保护的流计算第一经标记的视听流; 将所述受保护的流从所述接收设备传送到所述第二设备; 根据第二设备、外部安全设备或使用所述第二设备的消费者的唯一识别符计算第二标记; 在所述第二消费者设备上根据所述第二标记从由所述接收设备所接收的所述受保护的流计算第二经标记的视听流。



1. 一种用于通过多播会话将原始视听流安全分发到多个消费者设备的方法，所述方法包括步骤：

- 生成具有原始视听流的视听内容的经预标记的内容流以及包含用于从经预标记的内容流生成经标记的内容的信息的标记流；

- 通过用不同数据替换所述经预标记的内容流的至少一部分来从所述经预标记的内容流生成受保护的视听流；

- 生成补充流，所述补充流包括适合于允许从所述受保护的视听流重构视听流的数字信息，所述补充流包括所述原始视听流中的被不同数据替换的原始数据和用于生成经标记的内容的信息；

- 把所述受保护的视听流和所述补充流传送给接收消费者设备；

- 根据接收消费者设备或外部安全设备的唯一识别符计算第一标记；

- 在所述接收消费者设备上使用用于生成经标记的内容的所述信息、根据所述第一标记和所述补充流从所述受保护的视听流重构第一经标记的视听流；

- 将所述受保护的视听流和所述补充流从所述接收消费者设备传送到第二消费者设备；

- 根据第二消费者设备、外部安全设备或使用所述第二消费者设备的消费者的唯一识别符计算第二标记；

- 在所述第二消费者设备上使用用于生成经标记的内容的所述信息、根据所述第二标记和所述补充流从经由所述接收消费者设备接收的所述受保护的视听流重构第二经标记的视听流。

2. 如权利要求 1 所述的方法，其中，所述受保护的视听流的生成使用加密算法。

3. 如权利要求 2 所述的方法，其中，所述受保护的视听流的生成使用规范 DVB-CA。

4. 如权利要求 1 所述的方法，其中，所述受保护的视听流与所述原始视听流具有相同的格式。

5. 如权利要求 1 所述的方法，其中，使用直接连接链路将所述补充流从所述接收消费者设备传送到所述第二消费者设备。

6. 如权利要求 1 所述的方法，其中，使用外部安全设备将所述补充流从所述接收消费者设备传送到所述第二消费者设备。

7. 如权利要求 1 所述的方法，其中，使用网络连接将所述补充流从远程服务器传送到所述第二消费者设备。

8. 如权利要求 1 所述的方法，其中，由所述接收消费者设备生成所述第一标记。

9. 如权利要求 1 所述的方法，其中，所述第一标记在外部安全设备上生成，并且被使用直接连接链路传送到所述接收消费者设备。

10. 如权利要求 1 所述的方法，其中，所述第二标记在所述接收消费者设备上生成，并且被使用直接连接链路传送到所述第二消费者设备。

11. 如权利要求 1 所述的方法，其中，所述第二标记在所述接收消费者设备上生成，并且被使用外部安全设备传送到所述第二消费者设备。

12. 如权利要求 1 所述的方法，其中，所述第二标记在外部安全设备上生成，并且被使用直接连接链路传送到所述第二消费者设备。

13. 如权利要求 1 所述的方法,其中,在所述第二消费者设备上生成所述第二标记。
14. 如权利要求 1 所述的方法,其中,通过加密装置保护所述补充流的传输和 / 或存储。
15. 如权利要求 1 所述的方法,其中,通过加密装置保护经标记的补充流的传输和 / 或存储。
16. 一种用于通过多播会话将原始视听流安全分发到多个消费者设备的系统,包括:
 - 用于生成具有原始视听流的视听内容的经预标记的内容流以及包含用于从经预标记的内容流生成经标记的内容的信息的标记流的装置;
 - 用于通过用不同数据替换所述经预标记的内容流的至少一部分来从所述经预标记的内容流生成受保护的视听流的装置;
 - 用于生成补充流的装置,所述补充流包括适合于允许从所述受保护的视听流重构视听流的数字信息,所述补充流包括所述原始视听流中的被不同数据替换的原始数据和用于生成经标记的内容的信息;
 - 用于把所述受保护的视听流和所述补充流传送给接收消费者设备的装置;
 - 用于根据接收消费者设备或外部安全设备的唯一识别符计算第一标记的装置;
 - 用于在所述接收消费者设备上使用用于生成经标记的内容的所述信息、根据所述第一标记和所述补充流从所述受保护的视听流重构第一经标记的视听流的装置;
 - 用于将所述受保护的视听流和所述补充流从所述接收消费者设备传送到第二消费者设备的装置;
 - 用于根据第二消费者设备、外部安全设备或使用所述第二消费者设备的消费者的唯一识别符计算第二标记的装置;
 - 用于在第二消费者设备上使用用于生成经标记的内容的所述信息、根据所述第二标记和所述补充流从经由所述接收消费者设备接收的所述受保护的视听流重构第二经标记的视听流的装置。
17. 如权利要求 16 所述的系统,包括用于生成所述受保护的视听流的加密装置。
18. 如权利要求 16 所述的系统,包括用于将所述补充流从所述接收消费者设备传送到所述第二消费者设备的外部安全设备。
19. 如权利要求 16 所述的系统,包括用于将所述补充流传送到所述第二消费者设备的远程服务器。
20. 如权利要求 16 所述的系统,包括用于生成 / 存储所述第一标记或所述第二标记的外部安全设备 (5, 51)。
21. 如权利要求 16 所述的系统,包括用于将所述第一标记或所述第二标记分别传送 / 存储到所述接收消费者设备或所述第二消费者设备的外部安全设备 (5, 51)。
22. 如权利要求 16 所述的系统,其中,所述接收消费者设备是计算机、机顶盒、媒体中心、移动电话、PDA、便携式媒体播放器、或具有多媒体能力的任何其它硬件设备。
23. 如权利要求 16 所述的系统,其中,所述第二消费者设备是计算机、机顶盒、媒体中心、移动电话、PDA、便携式媒体播放器、或具有多媒体能力的任何其它硬件设备。
24. 如权利要求 16 所述的系统,其中,所述外部安全设备是 SIM 卡、安全 USB 设备、或者能够安全地存储和传送唯一识别符的任何其它安全硬件 / 软件组件。
25. 如权利要求 16 所述的系统,包括 USB 连接、无线网络、有线网络、外部硬盘、闪盘、

USB 密钥或 CD/DVD 设备, 用于允许所述受保护的视听流和 / 或所述补充流的传送。

使用加扰和水印技术用于多播视听节目的记录的拷贝的安全共享的方法和装置

技术领域

[0001] 本发明总体上涉及多媒体内容的安全分发 (distribution)。本发明更具体地涉及一种用于在多播视听节目的记录的拷贝的各种个人用户设备之间的安全共享的方法和装置,通过使用加扰 (scramble) 和水印 (watermark) 技术的创造性方法保证再次编码 (recoded) 的视听节目的合法消费。

背景技术

[0002] 增加的数字电视 (卫星、线缆和无线电广播以及更近的 IP 多播) 的部署在客户机侧提供更灵活的内容消费。消费者可以记录电视节目,以在以后观看它们来消磨时间,或者制作可以在任何他们的个人家庭设备上使用的永久私人拷贝。与家人或朋友共享这些拷贝是数字 TV 订户高度需要的另一特征。

[0003] 然而,这些新的服务必须保证内容拥有者或服务提供商批准的权限,并且必须防止任何非法使用和识别 (identify) 成功的剽窃尝试。

[0004] 为了安全地实现这种系统,本领域技术人员已知各种技术。

[0005] DTCP (数字传输内容保护) 是一种用于通过数字接口传递到个人家庭设备的版权内容的拷贝保护的技术规范。在该规范下,数字内容能够在用户的家庭中的设备之间安全地共享,但不能与家庭网络外的第三方共享。通过使用认证方案,DTCP 允许用户指定家庭网络中的设备作为可以将数据传出并且传入的受信目的地。

[0006] 然而,这种技术的缺点是恶意用户可以通过指定“伪装”设备作为他的家庭网络的一部分规避 DTCP 安全性措施,并且使用它不仅违法地消费内容,而且甚至更糟地是,非法地分发内容。

[0007] 另一缺点在于 DTCP 规定应该在传送到其它个人家庭设备之前加密内容。这需要更昂贵的个人家庭设备,因此限制这种系统的部署。

[0008] CPCM (内容保护和拷贝管理) 是 DVB (数字视频广播) 规范的一部分。CPCM 针对在消费者设备已经接收视听内容之后对视听内容的保护。一旦符合 CPCM 的设备接收视听内容,就通过各种加密技术保护它,并且包含消费权限的证书绑定到保护的内容。因此,对于所述内容中存储的使用权限,其它符合 CPCM 的设备能够呈现保护的内容。

[0009] 虽然是两种不同的技术 (CPCM 关注内容保护, DTCP 关注传送链路保护),但 CPCM 具有与 DTCP 相同的缺点:不可能识别成功的剽窃尝试,并且要部署复杂和昂贵的家庭设备。

[0010] 本发明目的在于通过以下方式解决这些缺点:在提出一种需要在服务器侧仅应用一次的内容保护的唯一操作的更简单的保护系统的同时,通过用于每一消费设备的唯一标记对内容进行标记,以允许在以后识别最终的剽窃尝试。

发明内容

[0011] 为了解决这些缺点,提供一种方法,以用于原始视听流通过多播会话到多个消费者设备的安全分发,所述方法包括步骤:

[0012] - 通过修改所述原始视听流生成受保护的视听流;

[0013] - 生成包括适合于允许从所述受保护的流重构视听流的数字信息的任何格式的补充流,

[0014] 其中,所述方法的特征在于它包括步骤:

[0015] - 根据接收消费者设备或外部安全设备的唯一识别符计算第一标记;

[0016] - 在所述接收消费者设备上根据所述第一标记和所述补充流从所述受保护的流计算第一经标记的视听流;

[0017] - 将所述受保护的流从所述接收设备传送到所述第二设备;

[0018] - 根据第二设备、外部安全设备或使用所述第二设备的消费者的唯一识别符计算第二标记;

[0019] - 在所述第二消费者设备上根据所述第二标记从由所述接收设备所接收的所述受保护的流计算第二经标记的视听流。

[0020] 本发明的另一公开是一种设备,包括:

[0021] - 用于通过修改所述原始视听流生成受保护的视听流的装置;

[0022] - 用于生成包括适合于允许从所述受保护的流重构视听流的数字信息的任何格式的补充流的装置,

[0023] - 用于根据接收消费者设备或外部安全设备的唯一识别符计算第一标记的装置;

[0024] - 用于在所述接收消费者设备上根据所述第一标记和所述补充流从所述受保护的流计算第一经标记的视听流的装置;

[0025] - 用于将所述受保护的流从所述接收设备传送到所述第二设备的装置;

[0026] - 用于根据第二设备、外部安全设备或使用所述第二设备的消费者的唯一识别符计算第二标记的装置;

[0027] - 用于在第二消费者设备上根据所述第二标记从由所述接收设备所接收的所述受保护的流计算第二经标记的视听流的装置。

附图说明

[0028] 通过参照附图详细地描述示例性实施例,本发明的以上方面将变得更清楚,其中:

[0029] 图 1A 和图 1B 示出用于安全地传递多媒体内容的多播系统的详细的服务器侧。

[0030] 图 2A、图 2B 和图 2C 示出图 1A 和图 1B 中提出的安全地传递多媒体内容的多播系统的详细的客户机侧。

[0031] 图 3A、图 3B 和图 3C 详细示出位于图 2A、图 2B 和图 2C 中提出的用于多播系统的客户机侧的解扰模块。

具体实施方式

[0032] 下文中,将参照附图详细描述本发明某些示例性实施例。

[0033] 在以下描述中,说明书中定义的内容(例如详细构造和要素)只是被提供用于帮

助本发明的全面理解的东西,而非其他。因此,清楚的是,可以在没有这些限定的内容的情况下执行本发明。此外,由于公知功能和构造将使本发明模糊于不必要的细节中,因此将不详细描述它们。

[0034] 此外,附图内的相同标号针对相似的技术要素,除非清楚地描述不同的含义。

[0035] 图 1A 是保护系统的结构化视图,包括:多播内容分发服务器 11、用于回放服务器 11 分发的内容的接收设备 12、以及用于回放接收设备 12 传送的内容的第二设备 13。

[0036] 多播内容分发服务器 11 具有两个主要功能:保护输入内容,以及通过广播技术将其传送到动态用户组。

[0037] 原始内容流 1 是包含视频和音频流以及富媒体流的多媒体流。

[0038] 视听压缩方法是本领域技术人员公知的方法,例如标准方法:MPEG-2、MPEG-4 部分 2、MPEG-4AVC/H. 264、MPEG-4SVC 等,或产业中大量使用的方法:Windows Media Audio and Video、VP6 等。

[0039] 原始内容流 1 的结构,以及允许混合各种音频和视频流的所有其它机制与编解码器类型、流类型和私有数据的信令(signaling)为标准的 MPEG-2TS、MP4 文件格式等,或专用的 FLV(Flash 视频文件格式)、ASF(先进系统格式)文件格式等。

[0040] 加扰模块 2 加扰原始内容流 1,生成受保护的流 121 和补充流 122 作为输出,补充流 122 包括解扰组件 21 分别根据第一标记 511、第二标记 512 从受保护的流 121 生成经标记的内容 124 和 127 所需的信息。

[0041] 补充流 122 的格式可以是专用的或标准的,例如与受保护的流 121 的格式相同的标准。

[0042] 根据一方面,加扰模块 2 通过使用本领域技术人员已知的各种加密机制(例如规范 DVB-CA,见 ETR 289)生成受保护的流 121 和补充流 122。

[0043] 根据一方面,允许受保护的流具有与原始流相同格式的技术是利用将强加给解码器的视听标准的不同参数来跳过(因此不解码)受保护的流内包含的修改的数据。例如,对于进一步编码为 H. 264 标准的视频数据,如果 NALU 类型字段的值被设置为 0 或以 24 至 31 开始,则标准解码器跳过作为受保护的流的一部分的修改的 NALU。跳过受保护的流的修改的 NALU 允许用户具有对受保护的内容的降级的表示的访问(因为仅未修改的 NALU 被解码),这将不允许他消费它,但这将提示他购买该内容而以适当的质量显现。

[0044] 根据另一方面,加扰模块 2 通过以不同数据替换原始内容流 1 的一些部分并且因此生成与原始内容流 1 的格式符合的受保护的流内容、以及在补充流 122 内存储原始的被替换的部分,生成受保护的流 121 和补充流 122。

[0045] 在各种文献(例如文献 WO 2005/032135)中描述了这种方法。

[0046] 根据一方面,传输模块 4 使用用于两个流的一个多播会话将生成的流 121 和 122 分发到接收机的动态组。

[0047] 根据一方面,传输模块 4 集成 DVB MUX 功能以复用和/或传送生成的流 121 和 122。

[0048] 根据另一方面,传输模块 42 和 43 分别使用用于每个流的单独的多播会话将生成的流 121 和 122 分发到接收机的动态组。

[0049] 根据一方面,传输模块 43 和 / 或 42 集成 DVB MUX 功能以复用和 / 或传送生成的流 121 和 122。

[0050] 根据一方面,本领域技术人员公知的各种加密装置保护补充流 122 的传输。例如,通过执行规范 DVB-CA(见 ETR 289) 保护补充流 122。

[0051] 在客户机侧,接收设备 12 通过网络接口 41 得到受保护的流 121 和补充流 122。

[0052] 接收设备 12 是计算机、机顶盒、媒体中心、移动电话、PDA、便携式媒体播放器或具有多媒体能力的任何其它硬件设备。

[0053] 取决于传送两个流的网络的种类,网络接口 41 是 IP(互联网协议)、线缆、地面、卫星或移动网络接口。

[0054] 解扰模块 22 然后处理两个流,以根据第一标记 511 生成第一经标记的内容 124。稍后(图 3A) 将描述解扰模块 21 的功能。

[0055] 然后第一经标记的内容 124 被传送到多媒体解码接口 6,以供解码和呈现。

[0056] 多媒体解码接口 6 是执行视听解码的软件 / 硬件模块、多媒体播放器或具有关于多媒体解码和呈现的各种能力的外部设备。

[0057] 受保护的内容 121 通过直接连接(例如 USB 连接)、网络传送(例如无线或有线)或外部存储介质(例如外部硬盘、闪盘、USB 密钥或 CD/DVD)从接收设备 12 传送到第二设备 13。

[0058] 第二设备 13 是计算机、机顶盒、媒体中心、移动电话、PDA、便携式媒体播放器或具有多媒体能力的任何其它硬件设备。

[0059] 在第二设备 13 上,解扰模块 21 然后处理受保护的内容 121 和补充流 122,以根据第二标记 512 生成第二经标记的内容 127。

[0060] 然后第二经标记的内容 127 被传送到多媒体解码接口 61,以供解码和呈现。

[0061] 多媒体解码接口 61 是执行视听解码的软件 / 硬件模块、多媒体播放器或具有关于多媒体 5 解码和呈现的各种能力的外部设备。

[0062] 图 1B 是替选的保护系统的结构化视图。与图 1A 内提出的保护系统的不同在于,预标记模块 3 而不是加扰模块 2 处理原始内容流 1。

[0063] 预标记模块 3 分析原始内容流 1 并且生成 2 个流:经预标记的内容流 131 以及标记元数据流 132,所述经预标记的内容流 131 具有与原始内容流 1 相同的视听表示,所述标记元数据流 132 包括分别根据第一标记 511、第二标记 512 从经预标记的内容流 131 生成经标记的内容 124 和 127 所需的信息。

[0064] 根据本发明一方面,如文献 WO 9965241 中描述的那样生成经预标记的内容流 131 和标记元数据流 132。

[0065] 加扰模块 2 处理经预标记的内容流 131 和标记元数据流 132,以生成受保护的流 121 和补充流 122,补充流 122 包括解扰组件 21 分别根据第一标记 511、第二标记 512 从受保护的流 121 生成经标记的内容 124 和 127 所需的信息。

[0066] 然后,解扰模块 21 在接收设备 12 上处理受保护的流 121 以及补充流 122,以根据第一标记 511 生成第一经标记的内容 124。稍后(图 3B) 将描述解扰模块 21 的功能。

[0067] 图 2A 详细示出在处理如图 1A 和图 1B 描述的那样生成的受保护的内容 121 和补充流 122 时接收设备 12 和第二设备 13 的功能。

[0068] 标记生成器 5 生成第一标记 511。

[0069] 标记生成器 5 是 SIM 卡、安全 USB 设备、或者能够安全地存储唯一识别符以生成第

一标记 511 的任何其它安全硬件 / 软件组件。

[0070] 第一标记 511 包括允许接收设备 12、接收设备 12 的硬件 / 软件组件中的一个的唯一识别的值（对于接收设备 12 例如为 SIM 卡 ID，对于接收设备 12 的硬件 / 软件组件例如为芯片组中的内建值）。此外，第一标记 511 可以包括与受保护的内容 121 有关的操作中的一个的识别符（例如受保护的内容流 121 的获取 / 接收、受保护的内容流 121 的消费的日期 / 时间等等）。

[0071] 为了允许第二设备 13 上受保护的内容流 121 的消费，补充流 122 从接收设备 12 传送到第二设备 13。

[0072] 补充流 122 通过直接连接（例如 USB 连接）、网络传送（例如无线或有线）或通过任何其它外部存储介质（例如外部硬盘、闪盘、USB 密钥或 CD/DVD）从接收设备 12 传送到第二设备 13。

[0073] 根据一方面，本领域技术人员公知的各种加密装置保护补充流 122 从接收设备 12 到第二设备 13 的传输。

[0074] 标记生成器 51 生成第二标记 512。

[0075] 标记生成器 51 是 SIM 卡、安全 USB 设备、或者能够安全地存储唯一识别符以生成第一标记 512 的任何其它安全硬件 / 软件组件。

[0076] 第二标记 512 包括允许第二设备 13、第二设备 13 的硬件 / 软件组件中的一个的唯一识别的值（对于第二设备 13 例如为 SIM 卡 ID，对于第二设备 13 的硬件 / 软件组件中的一个例如为芯片组中的内建值）。此外，第二标记 512 可以包括与受保护的内容 121 有关的操作中的一个的识别符（例如受保护的内容流 121 的获取 / 接收、受保护的内容流 121 的消费的日期 / 时间等等）。

[0077] 图 2B 详细示出在处理如图 1A 和图 1B 描述的那样生成的受保护的内容 121 和补充流 122 时接收设备 12 和第二设备 13 的替换的功能。该实施例与图 2A 中提出的实施例之间的不同在于，同一标记生成器 5 生成两个标记：第一标记 511 和第二标记 512。

[0078] 根据一方面，使用标记生成器 5，将补充流 122 从接收设备 12 传送到第二设备 13。在此情况下，标记生成器 51 是 SIM 卡、安全 USB 设备、或能够安全地读取 / 写入 / 存储二进制数据的任何其它安全硬件 / 软件组件。

[0079] 根据一方面，标记生成器 5 包括用于认证 (authentify) 接收设备 12 和 / 或第二设备 13 以确保补充流 122 从接收设备 12 到第二设备 13 的安全传输的装置。

[0080] 图 2C 详细示出在处理如图 1A 和图 1B 描述的那样生成的受保护的内容 121 和补充流 122 时接收设备 12 和第二设备 13 的替换的功能。该实施例与图 2A 和图 2C 中提出的实施例之间的不同在于，补充流 122 或补充的经标记的流 123 从远程服务器 7 传送到第二设备 13。

[0081] 补充的经标记的流 123 是从补充流 122 和第二标记 512 生成的，并且它包括从受保护的内容流 121 生成第二经标记的流 127 所需的信息。稍后（图 3C）将描述补充的经标记的流 123 的生成。

[0082] 根据一方面，如文献 WO 2008081113 中描述的那样生成补充的经标记的流 123。

[0083] 根据一方面，第二设备 13 和远程服务器 7 包括本领域技术人员公知的加密装置来确保补充流 122 从远程服务器 7 到第二设备 13 的安全传输。

[0084] 根据另一方面,标记生成器 5 或 51 参与补充流 122 或补充的经标记的流 123 从远程服务器 7 到第二设备 13 的传输的保护的处理。在该处理中起的作用是:安全地存储第二设备 13 与远程服务器 7 之间的认证处理所使用的信息(例如 SIM 卡 ID),以及 / 或者,加密 / 解密第二设备 13 与远程服务器 7 之间交换的消息。

[0085] 图 3A 高亮显示解扰设备 21 执行的用于根据第一标记 511 或第二标记 512 从受保护的内容流 121 和补充流 122 生成经标记的内容 124 或 127 的不同步骤。

[0086] 解扰设备 21 执行以下步骤:

[0087] - 通过生成具有与原始内容 1 相似的视觉和听觉表示的干净的内容流 125, 使用补充流 122 中包含的信息解扰(211)受保护的内容流 121;

[0088] - 通过分别根据第一标记 511、第二标记 512 生成经标记的内容 124 或 127, 标记(311)所述干净的内容流 125。

[0089] 根据一方面,解扰步骤 211 使用补充流 122 中包含的解密密钥将受保护的内容流 121 解密为干净的内容流 125, 其中,解密算法是本领域技术人员公知的算法。

[0090] 根据另一方面,解扰步骤 211 使用补充流 122 中包含的原始内容流 1 的原始部分,将其插回到受保护的内容流 121 中,以获得干净的内容流 125。

[0091] 根据另一方面,插回到受保护的内容流 121 的原始部分替换加扰模块 2 插入的伪(dummy)部分。

[0092] 根据一方面,干净的内容流 125 的标记步骤 311 使用补充流 122 中包括的信息。

[0093] 根据一方面,使用本领域技术人员公知的标记技术,在干净的内容流 125 的编码或解码的形式上完成干净的内容流 125 的标记步骤 311。

[0094] 根据另一方面,如文献 WO 9965241 中描述的那样完成干净的内容流 125 的标记步骤 311。

[0095] 图 3B 高亮显示替选的解扰设备 21 执行的用于根据第一标记 511 或第二标记 512 从受保护的内容流 121 和补充流 122 生成经标记的内容 124 或 127 的不同步骤。

[0096] 解扰设备 21 执行以下步骤:

[0097] - 通过生成经标记的补充流 126, 使用第一标记 511 或第二标记 512 来标记(312)补充流 122;

[0098] - 通过生成经标记的内容 124 或 127, 使用 25 经标记的补充流 126 中包含的信息,解扰 212 受保护的内容流 121。

[0099] 根据一方面,如 30 文献 WO 2008081113 中描述的那样在标记步骤 312 期间生成经标记的补充流 126。

[0100] 根据另一方面,如例如在文献 WO 2005/032135 中描述的那样,补充流 122 包含加扰模块 2 所提取的并且用受保护的内容流 121 中的伪数据替换的原始部分形式的原始内容流 1。如图 1B 中公开的那样,补充流 122 包含来自标记元数据流 132 的数据。如在文献 WO 9965241 中描述的那样生成标记元数据流 132。标记步骤 312 如下生成经标记的补充流 126:

[0101] - 如在文献 WO 9965241 中描述的那样,根据第一标记 511 或第二标记 512 选取标记元数据流 132 的一些标记的部分以插入视听内容。

[0102] - 通过将来自标记元数据流 132 的所述选取的经标记的部分与补充流 122 中包括

的原始内容流 1 的原始部分混合在一起,生成经标记的补充流 126。

[0103] 经标记的补充流 126 的格式是标记元数据流 132 的格式、补充流 122 的格式、或者专用的或标准的任何其它格式。

[0104] 解扰步骤 212 通过将经标记的补充流 126 中包括的所有内容部分(经标记的和原始的)插入受保护的内容流 121 中,生成标记内容流 124 或 127。例如,如同在文献 WO 2008081113 中那样实现该步骤。

[0105] 图 3C 高亮显示替选的解扰设备 21 执行的用于根据第二标记 512 从受保护的内容流 121 生成经标记的内容 127 的不同步骤。该实施例与图 3B 中提出的实施例之间的不同在于,在远程服务器 7 远程地应用标记步骤 312 的同时,解扰模块 21 在第二设备 13 上仅执行解扰步骤 212。在此情况下,从远程服务器 7 到第二设备 13,在其间仅仅传送经标记的补充流 126。

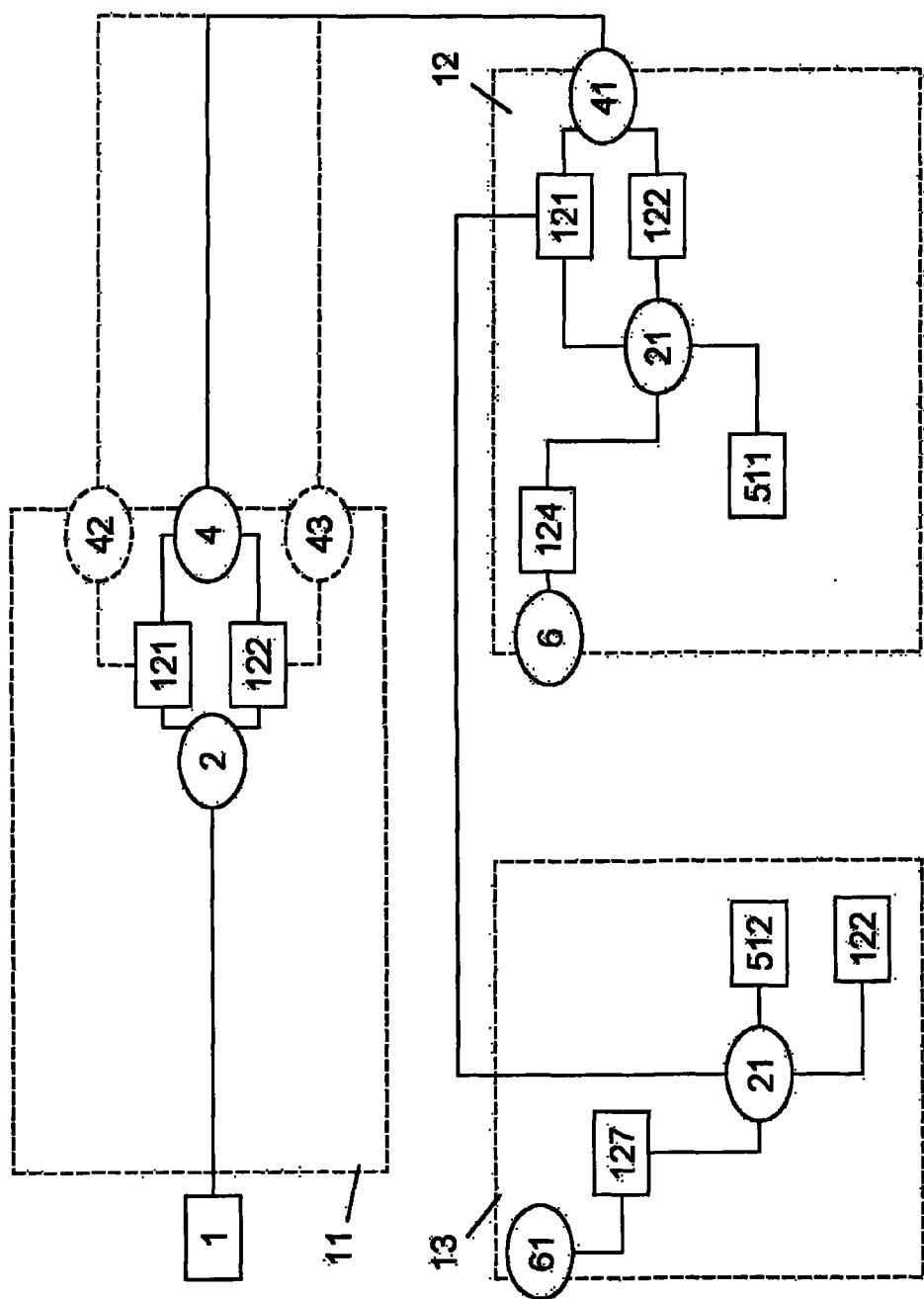


图 1A

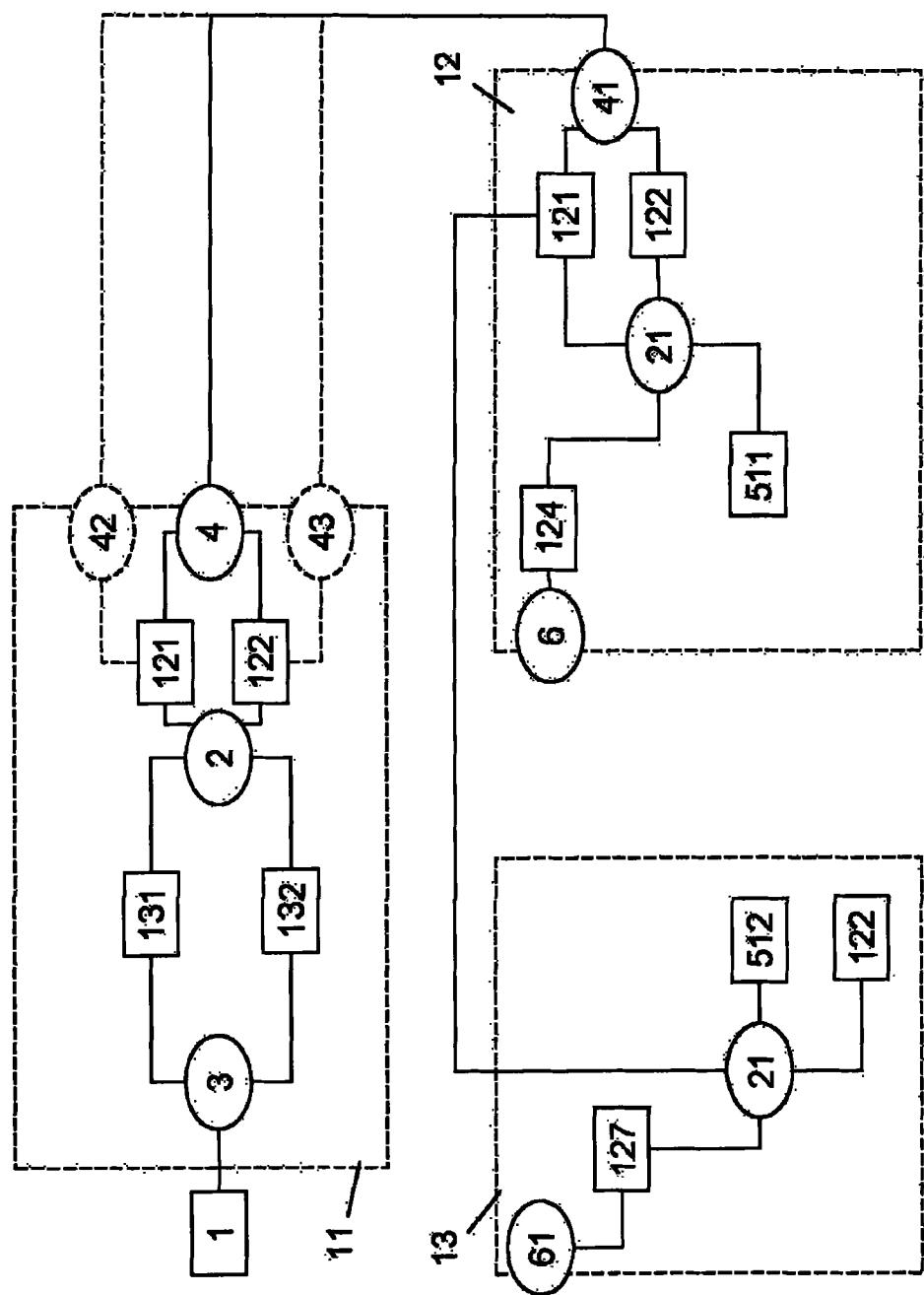


图 1B

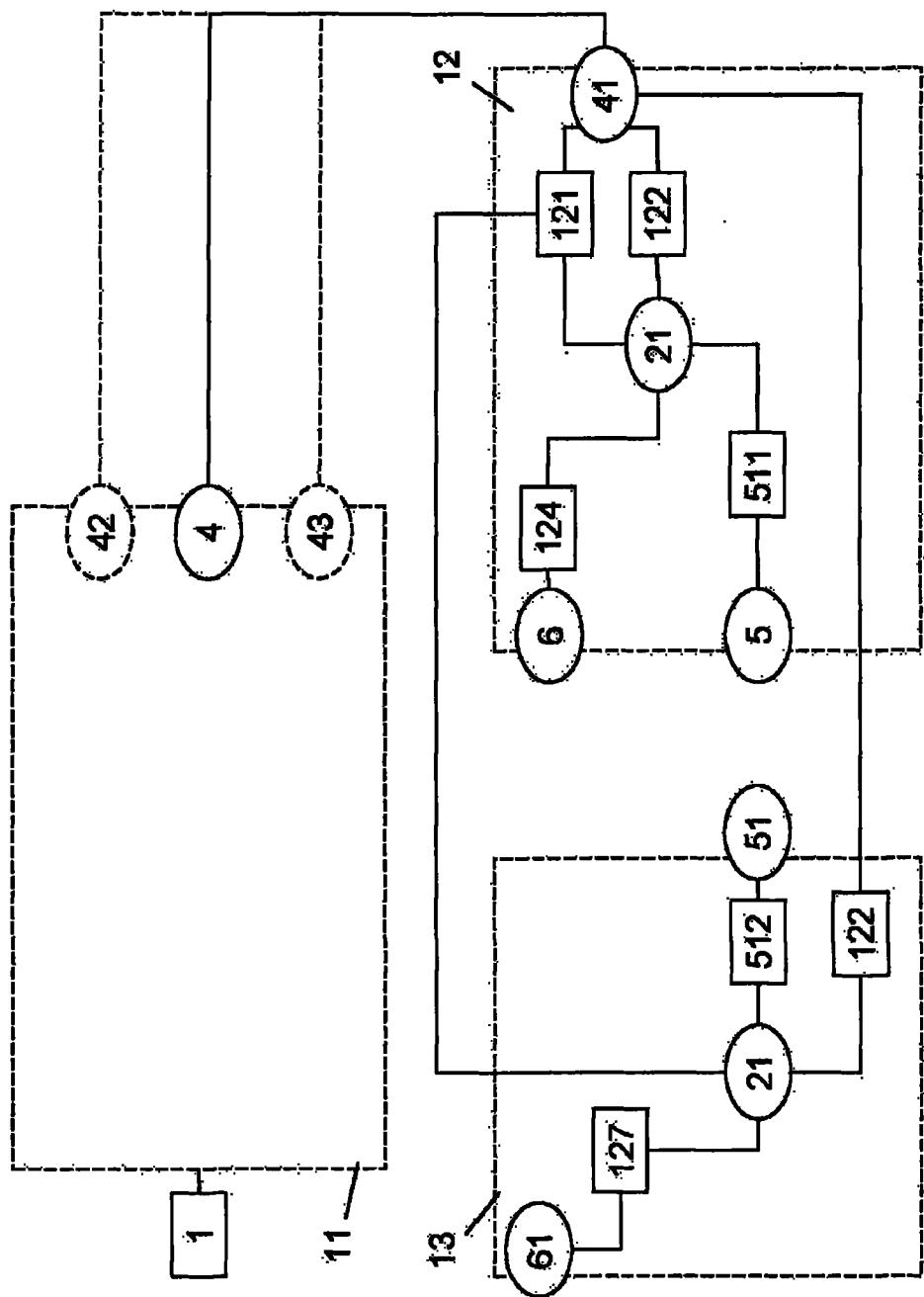


图 2A

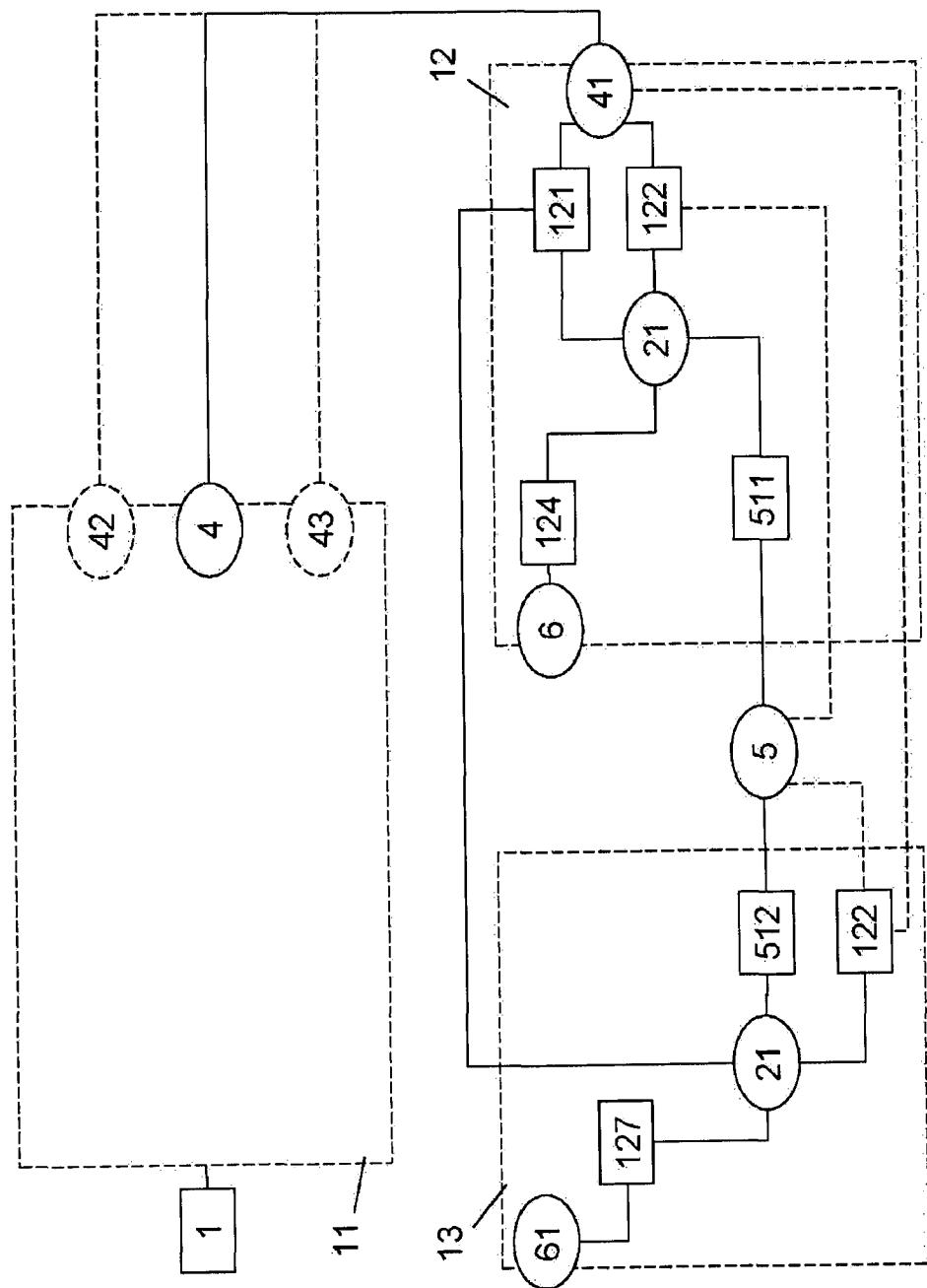


图 2B

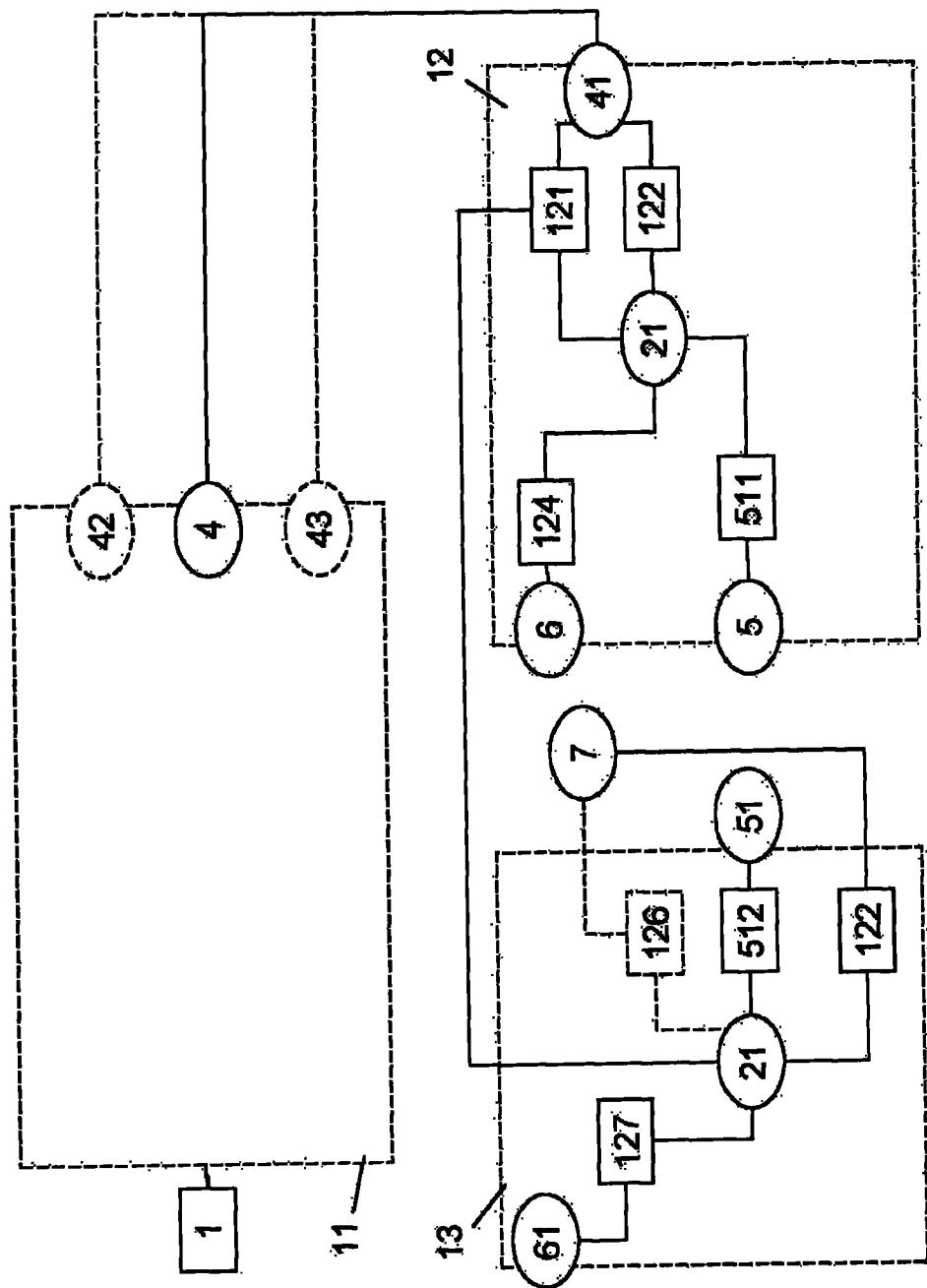


图 2C

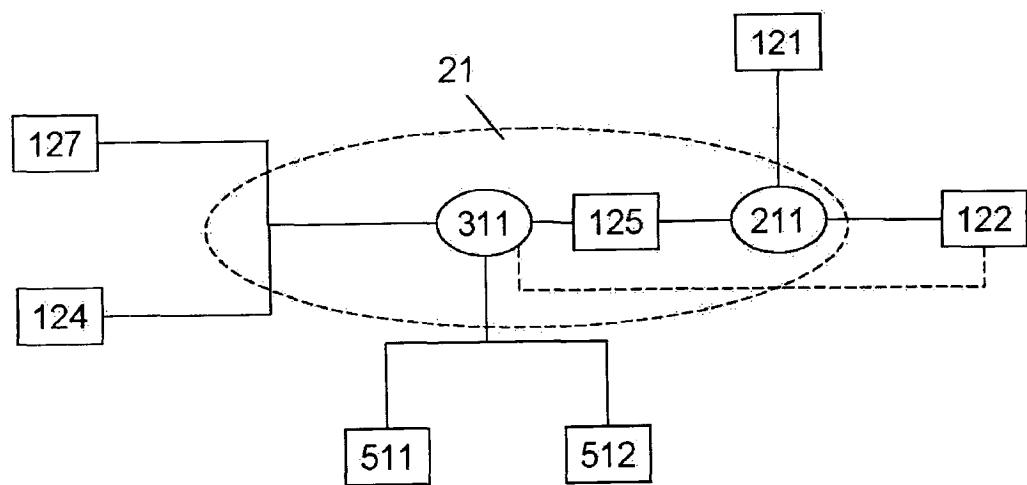


图 3A

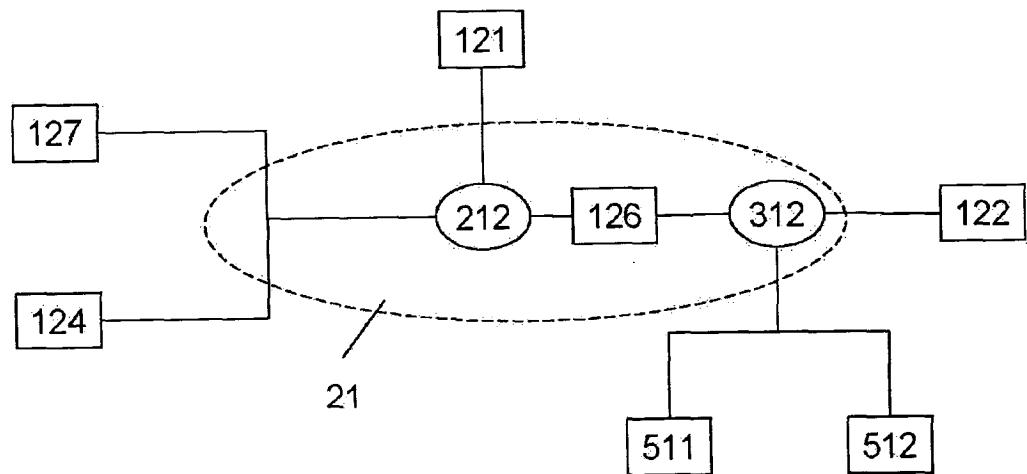


图 3B

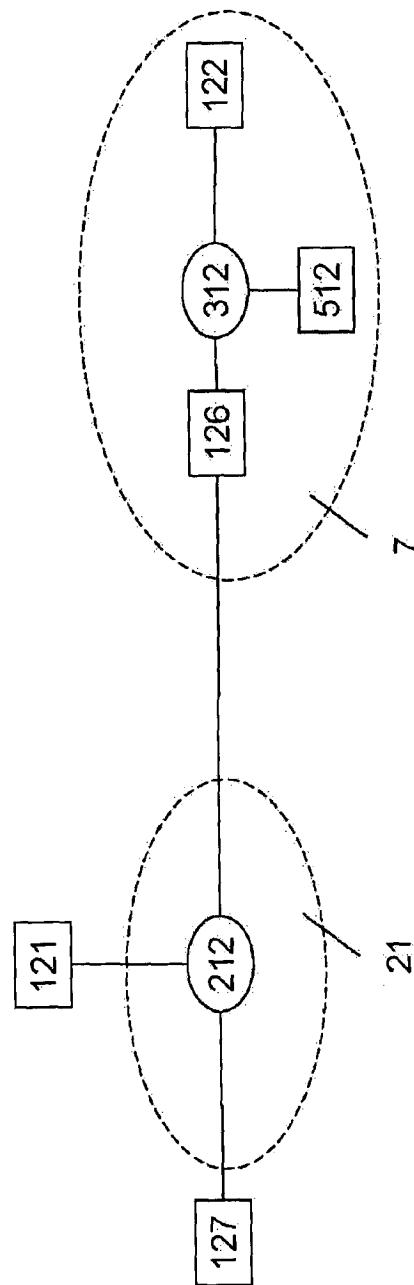


图 3C