[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04L 9/32
H04N 7/16
G06K 9/00

[12] 发明专利申请公开说明书

[21] 申请号 02827002.9

[43] 公开日 2005 年 5 月 4 日

[11] 公开号 CN 1613228A

[22] 申请日 2002.12.9 [21] 申请号 02827002.9
[30] 优先权
[32] 2002. 1.11 [33] EP [31] 02075093.1
[86] 国际申请 PCT/IB2002/005273 2002.12.9
[87] 国际公布 WO2003/058876 英 2003.7.17
[85] 进入国家阶段日期 2004.7.9
[71] 申请人 皇家飞利浦电子股份有限公司
地址 荷兰艾恩德霍芬
[72] 发明人 M·范德费恩

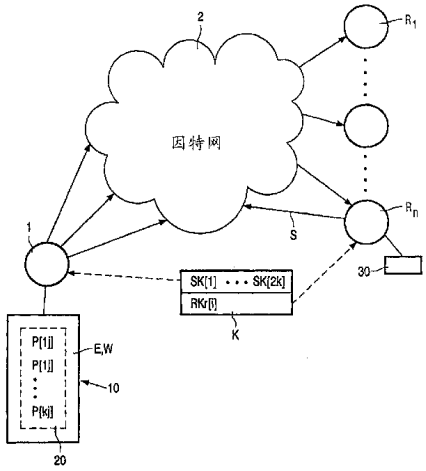
[74] 专利代理机构 中国专利代理(香港)有限公司
代理人 程天正 王 勇

权利要求书 3 页 说明书 8 页 附图 2 页

[54] 发明名称 对多媒体的多播传输的接收机唯一的水印的产生

[57] 摘要

一种通过使用多播传输以有效的方式来分布多媒体数据的方法、装置以及系统，为此每一接收机配备有它自己的以水印形式的唯一的标识符以及附加信息，在相同的水印中，所述附加信息典型地为例如符合 DRM 规则的全局信息。



ISSN1008-4274

1.一种产生一个对于数据分组形式的多媒体数据多播传输的接收机唯一的水印的方法，所述方法包括以下步骤：

－从源（1）传输具有不同水印的每一数据分组（P[1]，P[2]，…P[k]）的至少两个不同拷贝（V_0[i]，V_1[i]），至少分别是第一水印（w_0）和第二水印（w_1），

－对所述拷贝（V_0[i]，V_1[i]）不同地加密，最好是借助不同的加密密钥SK[1],SK[2],…SK[2k]，

－给每一接收机（R_1，R_2…R_n）提供对所述两个加密的拷贝中仅一个拷贝的访问，由此给每一接收机（R_1，R_2…R_n）提供唯一的所合成数据流（S），所述数据流包括具有第一和第二水印（w_0，w_1）的数据分组，其中该第一和第二水印（w_0，w_1）在所合成流（S）中存在的顺序提供该唯一的水印，

－给该数据流（S）提供在单层中的多位容量以用于存储附加的信息。

2.根据权利要求1的方法，其中该附加信息是全局信息。

3.根据权利要求2的方法，其中该附加信息是版权信息、生产者信息以及所有者信息中的至少一个。

4.根据权利要求1的方法，其中源（1）和接收机（R_1，R_2…R_n）通过诸如因特网的分布式网络（2）而链接在一起。

5.根据权利要求1的方法，其中通过一个随机加密密钥序列（SK[1],SK[2],…SK[2k]）来确定接收机可访问的拷贝（V_0[i]，V_1[i]），所述随机加密密钥序列先于传输而被发送。

6.根据权利要求5的方法，其中由源（1）先于传输而产生该密钥（SK[1],SK[2],…SK[2k]）并且将该密钥存储在文件中。

7.根据权利要求1的方法，其中只要水印不同，所述产生的水印就随时间而改变，并且源追踪它们。

8.根据权利要求1的方法，其中所产生的水印多于两个。

9.根据权利要求1的方法，其中也产生由源根据给予接收机的密钥和所合成流而导出的一个身份串。

10.根据权利要求1的方法，其中例如通过不对所有分组加水印、

例如通过对一部电影的最后十分钟加水印，而通过优化来减少带宽的使用率。

11.一种用于传输多媒体数据到多播传输的接收机（R_1，R_2…R_n）的源（1），所述源包括运算装置（10），该运算装置进一步包括或者可连接到传输和加密装置（20），它们一起：

－读取数据分组 i P[i]，

－创建数据分组 i 的至少两个加水印的拷贝 $V_0[i]$，$V_1[i]$，

－得到两个加密密钥 SK[2i-1]和 SK[2i]，

－加密数据分组 i 的加水印的拷贝 $V_0[i]$，$V_1[i]$ 为 $C_0[i]=E(V_0[i],SK[2i-1])$和 $C_1[i]=E(V_1[i],SK[2i])$，

－使用数据分组添加附加信息，典型的为诸如版权的全局信息，

－经由网络传输 $C_0[i]$和 $C_1[i]$连同 i 到接收机（R_1，R_2…R_n），其中 i＝1，2，…k。

12.根据权利要求 11 的源，其中运算装置（10）、传输装置以及加密装置（20）被实施为软件。

13.一种用于接收多媒体数据的接收机，该接收机包括接收和解密装置（30），它们一起：

－接收至少两个数据分组： $C_0[i]$和 $C_1[i]$，

－得到用于数据分组 i 的解密密钥：RKr[i]，

－试图用密钥 RKr[i]来解密两个数据分组，

－接收全局信息，

由此仅有一个数据分组将被解密成一个合适的数据分组：$Vji[i]=D(Cj[i],RKr[i])$，$ji \varepsilon \{0,1\}$，

－解码并且再现 Vji[i]。

14.一种包括源（1）、接收机（R_1，R_2…R_n）以及介于其间的分布式网络（2）的系统，用于实现一种产生对数据分组形式的多媒体数据多播传输的接收机（R_1，R_2…R_n）唯一的水印的方法，所述方法包括以下步骤：

－从源（1）传输具有不同水印的每一数据分组（P[1]，P[2]，…P[k]）的至少两个不同的拷贝（$V_0[i]$，$V_1[i]$），至少分别是第一水印（w_0）和第二水印（w_1），

－对所述拷贝进行不同地加密，最好是借助不同的加密密钥SK[1],SK[2],…SK[2k]，

－给每一接收机(R_1,R_2…R_n)提供对所述两个拷贝(V_0[i],V_1[i])中仅一个拷贝的访问，由此给每一接收机提供唯一的所合成数据流（S），所述数据流包括具有第一和第二水印（w_0，w_1）的数据分组，其中第一和第二水印在所合成流（S）中存在的顺序提供该唯一的水印，

－给该数据流（S）提供在单层中的多位容量以用于存储附加信息。

15.根据权利要求14的系统，其中源是服务器而接收机是客户。

对多媒体的多播传输的接收机唯一的水印的产生

发明领域

本发明涉及将多媒体传输到多个接收机的领域，并且特别涉及用于产生水印的方法和装置，该水印对于所述媒体的多播传输的接收机来说是唯一的。当在此使用时，术语“多媒体”可以是以数据分组流的形式典型分布的任一类型媒体，诸如视频、声音等等。

背景技术

多播传输在分布式网络中，典型地在因特网环境中提供有效的一对多或多对多的多媒体传输。源将数据分组形式的多媒体传输到典型地可以被单个 IP 目的地址识别的接收机组。由于有可缩放性，所以多播传输很适合于多媒体的大规模传输；不管接收机的数量如何，分布式网络中的每一网络链接仅必须传送每一数据分组的一个拷贝。

通过数据的加密能够解决验证和机密性问题；然而，关于接收机仍存在一个问题，即重传未加密的数据到其他接收机。基本的加密不足以保护信息。检测非法拷贝源自何人的一种方法是指纹识别，也就是将唯一信息（典型为水印）嵌入原始数据的每一拷贝中，由该唯一信息来识别接收该拷贝的接收机。

在单播传输中，所需拷贝的数量是接收机数量的倍数，这对于大规模传输来说当然隐含着缺陷。然而，这样很容易追踪非法拷贝源自何人，因为能将稍有不同的拷贝传输到每一个接收机。

在“Large Scale Distributed Watermarking of multicast media through encryption”Parvianninen Roland, Parnes Peter, Department of Computer Science/Centre for Distance Spanning Technology, 2001 中公开了一种方法，其中多播会话的每一接收机接收具有不同的唯一水印的数据流，同时仍旧保持多播传输的可缩放性。该加水印的流能够用于追踪那些制作该流的未授权拷贝的接收机。然而，该文献并未公开如何在数据流中提供附加的信息，所述附加信息是被要求来例如符合数字权限管理规则（DRM）。附加信息的实现必须满足许多基本的要求，诸如不能显著地影响图像、视频序列和声音的感知质量；其对于能够应用于图像、视频序列或声音的变换和/或运算必须是健壮

的，所述变换和/或运算是诸如彩色变换、几何变换、平移或旋转、诸如 JPEG/MPEG 的数据压缩、噪声、D/A、A/D 转换、图像平滑等等。

发明概要

本发明的一个目的是提供一种用于产生对于多媒体多播传输的接收机唯一的水印的方法，该方法也提供附加的信息以便例如符合 DRM 规则，而不会在媒体中引起有影响的视觉和/或听觉的人工产物。

根据本发明，这一目的在产生对于数据分组形式的多媒体数据多播传输的接收机来说唯一的水印的方法中实现，所述数据分组包括在单层中具有多位容量以用于存储附加信息的多媒体流。主要优点在于：通过水印的一个单层，可以以最小的信号降级来嵌入诸如版权信息的全局信息和用户所特定的信息。这样，便能够避免典型情况下在多层中进行多个水印的嵌入。这是重要的，因为例如通过将水印相互堆叠起来而嵌入多个水印是一个潜在的、在媒体的内容中引入可察觉到的人工产物的源。

在非多播环境中，可以使用一种不同的解决方案，它是通过简单地将其中的一部分水印位分配给附加信息，而将一部分位分配给用户所特定的信息来进行的，所述用户所特定的信息典型为指纹信息。然而，由于本发明是在多播环境中得到应用，所以这样的解决方案将不在本文档中进一步讨论。

本发明也提供用于执行上述公开的方法的装置和系统。

在其一些优选实施例的第一方面中，本发明提供一种在多播环境中借助于一单个水印算法而将指纹和版权水印相组合的有效方法。在本发明的另一方面中，同样也可能使用更多的水印。例如，不同的数据分组可以嵌有来自不同算法的水印。这仍是单层水印，但是是通过不同的水印算法。

在其一些优选实施例的第二方面中，本发明提供通过一随机加密密钥序列确定的、接收机已经访问的每一数据分组的拷贝，所述随机加密密钥序列先于传输而被发送。

在其一些实施例的第三方面中，本发明提供每一数据分组的两个以上的拷贝。

根据本发明的优选实施例，提供一种产生一个对于数据分组形式的多媒体数据多播传输的接收机唯一的水印的方法，所述方法包括以下步

骤:

-从源传输具有不同水印的每一数据分组的至少两个不同拷贝，至少分别是第一水印和第二水印，

-对所述拷贝不同地加密，最好是借助不同的加密密钥，

-给每一接收机提供对所述两个拷贝中仅一个拷贝的访问，由此给每一接收机提供唯一的所合成的数据流，该数据流包括具有第一和第二水印的数据分组，其中第一和第二水印在所合成流中存在的顺序提供了该唯一水印，

-给该数据流提供在单层中的多位容量以用于存储附加信息。

优选地，附加信息是全局信息，诸如版权信息、生产者信息以及所有者信息。

优选地，源与接收机是借助分布式网络诸如因特网而链接在一起。

在其一些优选实施例的第四方面中，本发明提供通过基于无线电的分布式网络而链接在一起的源和接收机，所述基于无线电的分布式网络典型为移动电话网络，诸如 GPRS 网络或 3G 网络。

根据本发明的优选实施例，进一步提供一种用于传输多媒体数据到多播传输的接收机的源，所述源包括运算装置，所述运算装置进一步包括或可连接到传输和加密装置，它们一起:

-读取数据分组 i ，

-创建数据分组 i 的两个加水印的拷贝 $V_0[i]$，$V_1[i]$，

-得到两个加密密钥 SK[2i-1]和 SK[2i]，

-加密数据分组 i 的加水印拷贝，$C_0[i]=E(V_0[i],SK[2i-1])$和 $C_1[i]=E(V_1[i],SK[2i])$，

-使用数据分组添加附加信息，典型地为诸如版权的全局信息，

-经由网络传输 $C_0[i]$和 $C_1[i]$连同 i 到接收机，其中 i = 1，2，...k。

借助于该方法，通过使用一单个水印算法而能够提供指纹和全局水印，或者当仍旧嵌有单层水印时，也可使用多个水印算法。

在其一些优选实施例的第五方面，本发明体提供作为软件实现的运算装置、传输装置以及加密装置。

根据本发明的优选实施例，进一步提供一种用于接收多媒体数据的接收机，该接收机包括接收和解密装置，它们一起:

-接收两个分组: $C_0[i]$和 $C_1[i]$，

-得到用于分组 i 的解密密钥: RKr[i],

-试图用密钥 RKr[i]来解密两个分组,

-接收全局信息,

由此仅有一个分组将被解密成一个合适的数据分组: Vji[i]=D(Cj[i],RKr[i]),ji ε {0,1},

-解码并且再现 Vji[i]。

根据本发明的另一优选实施例,接收装置被安排来接收两个以上数据分组和/或解密装置被安排来解密两个以上的数据分组。

根据本发明的优选实施例,进一步提供一个包括源、接收机以及介于其间的分布式网络的系统,以实现一种产生一个对于数据分组形式的多媒体数据多播传输的接收机唯一的水印的方法,所述方法包括以下步骤:

-从源传输具有不同水印的每一数据分组的至少两个不同拷贝,至少分别是第一水印和第二水印,

-对所述拷贝进行不同地加密,最好是借助于不同的加密密钥,

-给接收机提供对所述两个拷贝中仅一个拷贝的访问,由此给每一接收机提供唯一的所合成数据流,该数据流包括具有第一和第二水印的数据分组,其中该第一和第二水印在所合成流中存在的顺序提供该唯一的水印,

-给该数据流提供在单层中的多位容量以用于存储附加信息。

一个加指纹的媒体数据流可减少媒体内容的非法复制,因为该媒体流的来源或购买者能够被识别。对于不可能实施抗篡改硬件的纯软件解决方案,这可以成为唯一的选项。

本发明的主要方面是提供一单个水印,所述水印提供用于跟踪的两个标识符并且包括附加的信息。参考下文中所述的实施例,本发明的这个和其他的方面将变得很明显。

附图的简要描述

图 1 是根据本发明的最优实施例的系统的示意性表示。

图 2 说明从源传输的数据分组的媒体流的实例。

图 3 说明可从多媒体多播传输的接收机传输的加指纹的媒体流的实例。

优选实施例的描述

图 1 示出了一个用于 IP 多播的系统，该系统包括源 1，例如服务器，以及仅示出了三个客户，例如接收机 R_1，R_2 ... R_n。在典型的因特网多播环境中，接收机的数量典型的大于 100000，但并非限制于此。源 1 和接收机 R_1，R_2 ... R_n 借助于分布式网络 2（诸如因特网）而链接在一起。当然其他类型的网络也是可能的，但是将不随同该实施例一起进一步地公开。

源 1 必须访问运算装置 10 所提供的 k 个数据分组：P[1]，P[2]，...P[k]和加密算法 E，所述运算装置进一步包括或可连接到传输和加密装置 20，以致于得到一个覆盖对象（cover object） P=D(E(P,K),K)。也就是说，E(P,K)用加密/解密密钥库 k 来加密第 k 个数据分组 P[K]，并且 D(P,K)借助于解密装置 30 来解密该覆盖对象 P。也要求有一个加水印算法 W：P_w=W(P,w)，w = U(P_w)和至少两个不同的水印，第一水印 w_0 和第二水印 w_1（图 2 所示）。水印的数量不限于两个，而能够是任何合适的数量。然而，为简单起见，这里只描述两个水印。此外，水印不必是恒定的并且根据本发明的优选实施例，只要水印不相同，它们便能够随时间而改变，并且源跟踪它们。

源 1 发送每一数据分组 P[1]，P[2]，...P[k]的至少两个不同的拷贝 V_0[i]，V_1[i]，每一拷贝具有不同的水印 w_0，w_1。数据分组 P[1]，P[2]，...P[k]的两个拷贝 V_0[i]，V_1[i]用两个不同的随机的加密密钥 SK[1],SK[2]...SK[2k]来加密。然后，借助于多播传输、经由分布式网络 2 而将加密数据分组发送到所有的接收机 R_1，R_2 ... R_n，优选地是在下文中称为“IP 多播”的因特网环境中。任一给定的接收机 R_1，R_2 ... R_k 可访问一个数据分组的仅一个加密密钥。

水印算法 W 将水印 w 嵌入覆盖对象 P 中，并且检测算法 U 从被标记的对象 P 中提取水印（w）。代替地能够使用检测水印（w）是否仍然存在的检测算法：U(Pw,w)=B,B ε {真，假}。源需要 2k 个随机加密密钥 SK[1],SK[2]...SK[2k]以便能够传输媒体流的数据分组。接收机 R_1，R_2 ... R_n 可访问这些密钥 SK[1],SK[2]...SK[2k]中的 k 个密钥：接收机密钥 RK_r 是 RK_r[i]=SK[2i-1]或 RK_r[i]=SK[2i]，i={1,2,...k}。

在图 1 中，没有详细地示出加密密钥的传输。为此可使用不同的策略。例如，如果信道能被鉴权，那么可能经由因特网来传输密钥。

根据本发明优选的实施例，为传输数据分组 k，源 1 执行以下的方法步骤：

-读取数据分组 i P[i]，

-创建数据分组 i 的两个加水印的拷贝 $V_0[i]$，$V_1[i]$，

-得到两个加密密钥 SK[2i-1]和 SK[2i]，

-加密数据分组 i 的加水印的拷贝 $V_0[i]$，$V_1[i]$ 为 $C_0[i]=E(V_0[i],SK[2i-1])$和 $C_1[i]=E(V1[i],SK[2i])$，

-使用数据分组添加附加的全局信息，诸如版权，

-将 $C_0[i]$和 $C_1[i]$连同 i 一起传输。

图 2 说明了从源传输的数据分组的媒体流的实例。示出了第一分组 P[1]和第 k 个分组 P[k]；以便说明每一分组如何包括两个不同的被加密分组 $V_0[i]$，$V_1[i]$，上述不同的被加密数据分组分别具有两个不同的水印 w_0，w_1。

现在再一次参考图 1。

在接收机侧，根据本发明的优选实施例，每一接收机 R_1，R_2 ... R_k 接收这两个分组并且借助于以下方法步骤试图以随后的方式对它们进行解密：

-接收两个分组 $C_0[i]$和 $C_1[i]$，

-得到用于分组 i 的解密密钥：RKr[i]，

-试图用解密密钥 RKr[i]来解密这两个分组，

-接收全局信息，

由此仅有一个分组将被解密成一个适当的数据分组：$Vji[i]=D(Cj[i],RKr[i])$，$ji \varepsilon \{0,1\}$，

-解码并且再现 Vji[i]。

对于每一数据分组，接收机将能够解码加水印的数据分组中的恰恰一个数据分组。是这两个数据分组中的哪一个，则由源已经指配给接收机的密钥来决定。

图 3 说明了可从多媒体多播传输的接收机所传输的加指纹的媒体流 S 的实例。该媒体流包括具有不同水印的数据分组。来自于第一接收机 R_1 的流与来自于另一接收机的流不一致。所以，每一接收机将具有它自己的加指纹的所合成的流。

如果一个接收机可访问的密钥在所有的接收机间是唯一的并且被源所知道，那么能够定义用于那个用户的一个唯一的身份串（identity string）：

Idr = Br[1], Br[2], …Br[k], Br[i] ε (0, 1)。

所述身份串能够通过源根据接收机被给定的两个密钥和来自于接收机的所合成流而导出。根据该密钥，源向接收机发送：

Br[i]=0 ，如果 RKr[i]=SK[2i-1]

Br[i]=1 ，如果 RKr[i]=SK[2i]

根据用于用户的所合成流：

Br[i]=0 ，如果 U(Vji)=w_0

Br[i]=1 ，如果 U(Vji) = w_1

Br[i]=未定义，如果 C_0[i]和 C_1[i]都没有被接收或解密

如果接收机没有接收所有的分组，则由于例如数据分组丢失或迟后调谐接收机，那么身份串将不会完全地匹配。如果 n 足够大，则尽管有一些位未定义，该部分身份串也将足够长，以使得在所有接收机间是唯一的。

由于不得不为每一数据分组发送两个拷贝，因此对于源和接收机来说，带宽的使用率将加倍。优选地，通过优化能够减少带宽。如果发送多于两个拷贝，则当然会出现在本发明的范围内的其他需求。

在任一给定的时间，两个加水印的分组中仅有一个分组对于单个接收机是实际有用的，因为另一个数据分组不能够被解密。如果在不同的多播组上发送两个拷贝，那么随着正确分组被在其上传输的组改变，接收机也可通过加入和离开各组而在组之间进行跳跃。在该方法中，不但有必要将密钥发送到每一接收机，而且要发送接收哪个流；在这样的情况中，对于每一密钥需要一额外的位。同样，这是在本发明的范围内，但将不会进一步公开，因为不幸地是，对于该方法而言，用于 IP 多播传输的加入/离开的等待时间普遍很长。同样，如果一个以上的接收机是在同一网段上，那么大多数的节省都会丧失。

加水印的可选方式能够是对每 x 个分组中的一（1）加水印，从而将带宽需求减少到原始流的带宽的（1 + 1/x）倍。不幸地是，如果 x 很大，则恶意的接收机能够移除这些加水印的分组并且重新发送所合成的降级的流。所以有必要保证降级是足够的大，以便阻止加水印的数据分

组的移除。这样的一个实例是仅对 MPEG 视频流的 I 帧加水印或仅对一部电影的最后十分钟加水印。同样这也是在本发明的范围内。

接收机可被作为在用户登记时由带外装置所分发的长期密钥对待，或者是作为最好受到 SSL/TLS 保护的可下载文件，或者是在磁盘或只读光盘上递送给用户。当考虑撤销访问时，所有这些解决方案都有一些问题。所述密钥也能够连续地流播到用户，这也是在本发明的范围内的。

每一接收机所需要的密钥的量取决于所要求的安全性。用于一个接收机的密钥的总的大小是密钥*密钥大小。一个加密安全随机数字发生器也能够改而产生位屏蔽，以进一步减少在源处的存储需求。

优选的，密钥是 56 位密钥，因为攻击者将不得不破坏足够量的密钥以便得到足够的分组来创建一个不可识别的加水印的流。对于本领域技术人员来说，当然也可使用其他合适数量的位而不脱离本发明。最好由源先于传输而产生该密钥并且将其存储在文件中。

假设在适当的时间内，既不能移除水印也不能破坏加密。同样假设攻击者不能通过闯入服务器而从源窃取没有加水印的流。如果加密算法被破坏，那么攻击者能够选择最终的加水印的流并且使得不可能进行叛逆者跟踪，但是如果慎重选择加密算法且使该加密算法具有足够大的密钥大小，以及适当地产生该密钥，则能够避免这个问题。不再考虑对于接收机取消访问的问题；然而这将需要传输新的密钥。

如果足够大数量 p 的接收机协作，那么总是将保留来自于其中一个数据流的原始位的至少 k/p。这可以被解决，但是在此文档中没有讨论，因为在现有技术中已经对其进行了明确的描述。

例如，本发明能够在一个现有的 Java 应用系统中实现，所述应用系统通过使用 MPEG-1 音频压缩标准的多播来进行音频传输。优选地，选择“Blowfish（河豚）”作为加密算法。

不需要有源网络元件或抗篡改智能卡。组成指纹的水印不被固定为某一数量的位或不在格式上被限制，而能够是水印算法为健壮性而要求的任一格式。为了避免攻击，也可能在一个媒体流中增加水印的数量。

如在随后的权利要求中所使用的那样，单词“包含”或“包括”或它们的连接的意思是“包括，但不一定限于”。

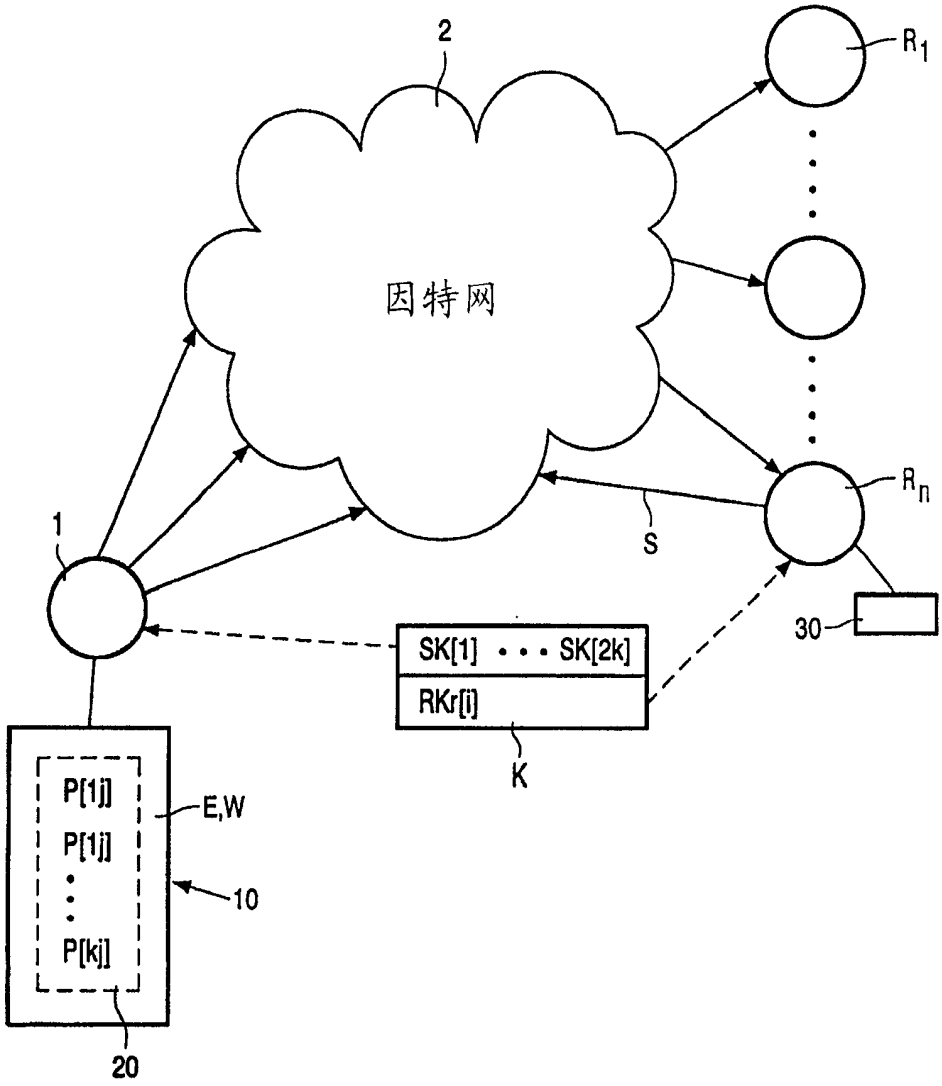


图 1

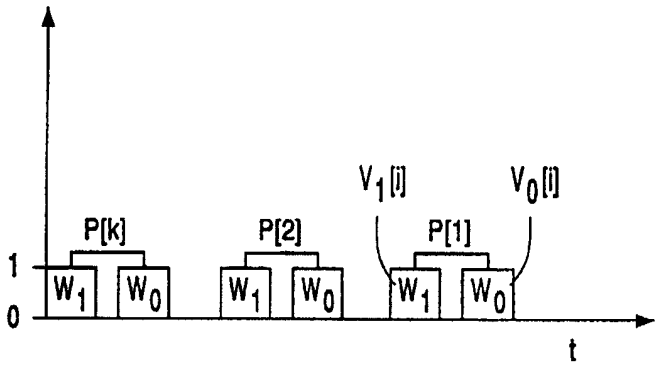


图 2

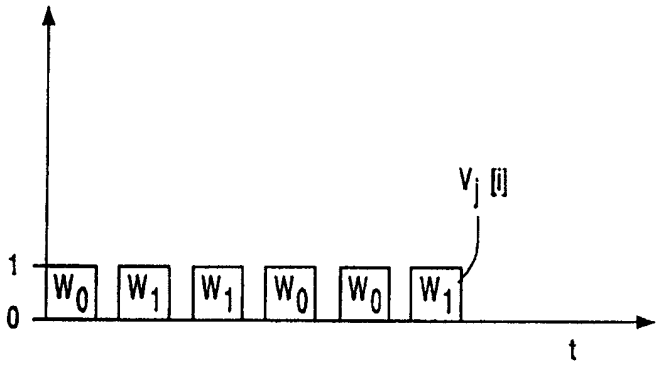


图 3