[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04K 1/02
H04N 5/00

[12] 发明专利申请公开说明书

[21] 申请号 01804971.0

[43] 公开日 2003 年 3 月 5 日

[11] 公开号 CN 1401169A

[22] 申请日 2001.1.17 [21] 申请号 01804971.0
[30] 优先权
[32] 2000. 2.17 [33] US [31] 09/507,478
[86] 国际申请 PCT/US01/01683 2001.1.17
[87] 国际公布 WO01/61904 英 2001.8.23
[85] 进入国家阶段日期 2002.8.13
[71] 申请人 微软公司
地址 美国华盛顿
[72] 发明人 汉里克·马尔法 保罗·英格兰德

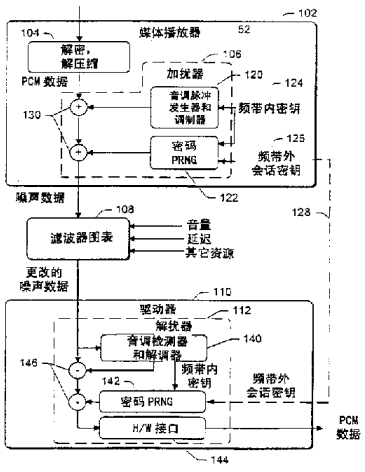
[74] 专利代理机构 中国国际贸易促进委员会专利商标事务所
代理人 付建军

权利要求书 10 页 说明书 13 页 附图 8 页

[54] 发明名称 用于保护在硬件部分中的数据流的系统和方法

[57] 摘要

一种加扰体系结构通过在由操作系统处理数据之前对原始数据进行加扰而保护在计算机的操作系统和硬件组件中的数据流。 该体系结构具有在客户机或服务器上实现的把噪声添加到内容中的加扰器。 具体来说，加扰器根据第一密钥产生具有变化幅度的周期性音调模式的集合。 加扰器还根据第一密钥和第二密钥产生随机信号。 音调模式和随机信号被添加到内容中以对内容加扰。 加扰内容然后被传送到滤波器图表。 解扰器检测在内容中的音调模式，并且从音调模式的变化幅度中恢复第一密钥。解扰器还通过分离的信道(例如，密码保护的路径)接收第二密钥，并且使用该恢复的第一密钥和该第二密钥产生相同的随机信号。 解扰器从加扰内容中减去音调模式和随机信号。



ISSN1008-4274

知识产权出版社出版

1. 一种客户机，其中包括：

处理器；

存储器；

一个或多个输出设备；

内容播放器，其存储在该存储器中并且在处理器上执行，以播放在一个或多个输出设备中的内容；

一个操作系统，其存储在该存储器中，并且在处理器上执行，该操作系统具有用于处理该内容播放器所支持的内容的处理工具；以及

加扰系统，其在该内容被操作系统的处理工具所处理之前对该内容加扰，并且在该内容被操作系统的处理工具所处理之后对该内容解扰。

2. 根据权利要求 0 所述的客户机，其中该处理工具包括具有一个或多个处理该内容的滤波器的滤波器图表。

3. 根据权利要求 0 所述的客户机，其中该内容播放器接收采用加密和压缩格式的内容，该内容播放器对该内容进行解密和解压缩。

4. 根据权利要求 0 所述的客户机，其中该加扰系统把噪声添加到该内容中。

5. 根据权利要求 0 所述的客户机，其中该加扰系统把至少该内容的一个子集与一个随机位流进行异或运算。

6. 根据权利要求 0 所述的客户机，其中该加扰系统使用时域或频域加扰方法中的一种来对该内容执行变换。

7. 根据权利要求 0 所述的客户机，其中该操作系统具有至少一个用于该输出设备的驱动器，并且该加扰系统包括:

加扰器，其驻留在内容播放器上对该内容加扰，以产生加扰的内容；以及

解扰器，其驻留在该驱动器上，对该加扰的内容解扰，以恢复该内容。

8. 根据权利要求 0 所述的客户机，其中该加扰系统把随机信号添加到内容中，以产生加扰的内容，以及把该随机信号从该加扰的内容中减去，以恢复该内容。

9. 根据权利要求 0 所述的客户机，其中该加扰系统把周期性的同步音调和随机信号添加到该内容中，以产生加扰内容，以及从该加扰内容中减去该同步音调和随机信号，以恢复该内容。

10. 根据权利要求 0 所述的客户机，其中该加扰系统利用至少一个密钥来对该内容加扰。

11. 根据权利要求 0 所述的客户机，其中该加扰系统包括:

音调发生器，用于根据第一密钥产生具有变化的幅度的周期性音调模式的集合;

第一随机数发生器，用于根据第一密钥和第二密钥创建一个随机信号;

加法器，其把音调模式和随机信号添加到该内容中，以产生加扰内容;

音调检测器，其检测在加扰内容中的音调模式，并且从该音调模式的变化幅度中恢复第一密钥;

第二随机数发生器，其根据该所恢复第一密钥和该第二密钥来创建随机信号；以及

减法器，其从加扰内容中减去音调模式和随机信号以恢复该内容。

12. 根据权利要求 11 所述的客户机，其中该第二密钥通过与加扰内容相分离的信道传输。

13. 根据权利要求 11 所述的客户机，其中该第二密钥通过安全路径在第一和第二随机数发生器之间交换。

14. 根据权利要求 0 所述的客户机，其中该加扰系统在存储于存储器中的软件中实现，并且在该处理器上执行。

15. 一种用于对内容加扰的内容加扰器，其中包括:

音调发生器和解调器，其根据第一密钥创建周期性音调模式的集合，以及对该集合的幅度进行调制;

随机数发生器，其根据第一密钥和第二密钥创建一个随机信号;以及

加法器，其把音调模式的集合与随机信号添加到该内容中，以产生加扰内容。

16. 根据权利要求 15 所述的内容加扰器，其中该音调发生器和调制器对该幅度进行调制，以把第一密钥嵌入到音调模式的集合中。

17. 根据权利要求 15 所述的内容加扰器，其中该音调发生器和调制器用两个幅度之一产生音调模式，其中具有第一幅度的音调模式表示第一二进制数值，以及具有第二幅度的音调模式表示第二二进制数值，第一密钥被编码为音调模式的集合，作为第一和第二二进制数值的集合。

18. 根据权利要求 15 所述的内容加扰器，其中第二密钥被加密，

用于安全传输到该解扰器。

19. 一种用于播放多媒体内容的媒体播放器，其中包括权利要求15中的内容加扰器。

20. 一种操作系统，其中包括权利要求15的内容加扰器。

21. 一种内容解扰器，用于对加扰内容进行解扰，其中包括:

音调检测器和解调器，用于检测在加扰内容中的周期性音调模式的集合，以及解调该集合的幅度，以恢复第一密钥;

随机数发生器，其根据该所恢复第一密钥和该第二密钥创建随机信号；以及

减法器，其从加扰内容中减去音调模式和随机信号，以恢复该内容。

22. 根据权利要求21所述的内容解扰器，其中音调模式具有两个幅度中的一种，从而具有第一幅度的音调模式表示第一二进制数值，以及具有第二幅度的音调模式表示第二二进制数值，该音调检测器和解调器使用来自该变化幅度的第一和第二二进制数值来恢复第一密钥。

23. 根据权利要求21所述的内容解扰器，其中第二密钥被与该加扰内容相分离地接收。

24. 一种操作系统，其中包括权利要求21的内容加扰器。

25. 一种加扰体系结构，用于保护由内容提供方通过网络发布给客户机的内容，其中包括:

内容加扰器，用于使用第一和第二密钥来对该内容加扰，以产生

加扰的内容，该加扰器把第一密钥嵌入到加扰内容中，并且把第二密钥与该加扰内容相分离地传输；

内容解扰器，用于从加扰内容中恢复第一密钥并且接收第二密钥，该解扰器利用第一和第二密钥对该加扰内容进行解扰，以恢复该内容。

26. 根据权利要求 25 所述的加扰体系结构，其中内容加扰器和内容解扰器用软件来实现。

27. 根据权利要求 25 所述的加扰体系结构，其中内容加扰器在内容提供方应用，使得该内容在通过网络发布到客户机之前被加扰。

28. 根据权利要求 25 所述的加扰体系结构，其中该内容加扰器在客户机上应用，使得该内容在通过网络从内容提供方发布之后，在该客户机上被加扰。

29. 根据权利要求 25 所述的加扰体系结构，其中该内容解扰器在客户机的操作系统上应用。

30. 根据权利要求 25 所述的加扰体系结构，其中该内容解扰器在该客户机的一个驱动器中应用。

31. 根据权利要求 25 所述的加扰体系结构，其中该内容加扰器把第二密钥通过密码保护的路径传送到内容解扰器。

32. 根据权利要求 25 所述的加扰体系结构，其中该内容加扰器包括：

音调发生器和调制器，其创建周期性音调模式的集合，以及根据第一密钥对该组合的幅度进行调制；

随机数发生器，其根据第一和第二密钥创建随机信号；以及

加法器，其把音调模式的集合以及随机信号加到该内容上，以产生加扰内容。

33. 根据权利要求 32 所述的加扰体系结构，其中该音调发生器和解调器对该幅度进行解调，使得第一密钥嵌入到音调模式的集合中。

34. 根据权利要求 32 所述的加扰体系结构，其中音调发生器和调制器产生具有两个幅度中的一个幅度的音调模式，其中具有第一幅度的单调模式表示第一二进制数值，以及具有第二幅度的音调模式表示第二二进制数值，第一密钥被编码到音调模式的集合中，作为第一和第二二进制数值的集合。

35. 根据权利要求 32 所述的加扰体系结构，其中该内容解扰器包括:

音调检测器和解调器，其检测在该加扰内容中的周期性音调模式的集合，以及解调该集合的幅度，以恢复第一密钥;

随机数发生器，其根据该所恢复第一密钥和该第二密钥创建随机信号；以及

减法器，其从加扰内容中减去音调模式和随机信号，以恢复该内容。

36. 一种用于保护内容的客户机-服务器系统，其中包括:

客户机;

服务器，其把内容提供给客户机，该服务器具有一个编码器，用于对该内容加密和压缩，以产生编码内容;

该客户机从该服务器接收该编码内容，并且具有一个解码器，用于对该编码内容进行解密和解压缩，以恢复该内容;

该客户机具有一个加扰器，用于对解密和解压缩之后的内容加扰，该内容在被客户机所处理时保持被加扰状态；以及

该客户机进一步具有一个解扰器，用于对处理之后的内容解扰，以用于播放。

37. 根据权利要求 36 所述的客户机-服务器系统，其中该客户机具有播放该内容的媒体播放器、支持该媒体播放器的处理工具，以及驱动器；该加扰器作为该媒体播放器的一部分而实现，以及该解扰器作为驱动器的一部分而实现。

38. 根据权利要求 36 所述的客户机-服务器系统，其中该客户机运行该操作系统，以及当内容由操作系统所处理时，该内容被加扰。

39. 一种用于保护计算设备中的内容的方法，其中包括：

接收编码的内容；

对该编码的内容解码以恢复该内容；

在解码之后对该内容加扰；

在加扰之后对该内容进行处理；

在处理之后对该内容解扰；以及

播放该内容。

40. 根据权利要求 39 所述的方法，其中该加扰包括把噪声添加到该内容中。

41. 根据权利要求 39 所述的方法，其中该加扰包括把至少该内容的一个子集与一个随机位流执行异或运算。

42. 根据权利要求 39 所述的方法，其中该加扰包括使用时域或频域变换中的一种来对该内容执行变换。

43. 根据权利要求 39 所述的方法，其中该加扰包括：

把同步音调集合周期性地添加到该内容中；以及

把随机信号添加到该内容中。

44. 根据权利要求43所述的方法，其中该解扰包括:

检测在该内容中的同步音调的集合;

从该内容中减去同步音调；以及

从该内容中减去随机信号。

45. 根据权利要求39所述的方法，其中该加扰包括:

根据第一密钥产生具有变化的幅度的周期性音调模式的集合;

根据第一密钥和第二密钥产生一个随机信号；以及

把音调模式和随机信号添加到该内容中。

46. 根据权利要求45所述的方法，其中该解扰包括:

检测在该内容中的音调模式;

从音调模式的变化幅度中恢复第一密钥;

根据该所恢复第一密钥和该第二密钥产生随机信号；以及

从加扰内容中减去音调模式和随机信号，以恢复该内容。

47. 根据权利要求39所述的方法，其中该处理包括通过一个滤波器图表传送该内容。

48. 一种计算机可读介质，其具有用于执行权利要求39的方法的计算可执行指令。

49. 一种用于把内容从服务器通过网络传送到客户机的方法，其中包括:

在该服务器上对该内容解码;

把该内容从服务器提供到客户机;

在该客户机对该内容解码;

在解码之后对该内容加扰;

在加扰之后对该内容执行处理;

在处理之后对该内容解扰;以及

播放该内容。

50. 根据权利要求 49 所述的方法,其中该加扰包括:

把同步音调集合周期性地添加到该内容中;以及

把随机信号添加到该内容中。

51. 根据权利要求 50 所述的方法,其中该解扰包括:

检测在该内容中的同步音调的集合;

从该内容中减去同步音调;以及

从该内容中减去随机信号。

52. 一种用于把内容从服务器通过网络传送到客户机的方法,其中包括:

在服务器对该内容加扰以产生加扰内容;

在服务器对加扰内容执行压缩;

把压缩、加扰后的内容从服务器提供到客户机;

在客户机对该压缩、加扰后的内容解压缩,以恢复该加扰后的内容;

处理该加扰后的内容;

在处理之后对该加扰后的内容解扰,以恢复该内容;以及

播放该内容。

53. 根据权利要求 52 所述的方法,其中该加扰包括:

根据第一密钥产生具有变化幅度的周期性音调模式的集合;

根据第一密钥和第二密钥产生随机信号;以及

把音调模式和随机信号添加到该内容中。

54. 根据权利要求53所述的方法，其中该解扰包括:

检测在该内容中的音调模式;

从该音调模式的变化幅度恢复第一密钥;

根据恢复的第一密钥和第二密钥产生一个随机信号; 以及

从加扰内容中减去音调模式和随机信号，以恢复该内容。

55. 一种计算机可读介质，其具有计算机可执行指令用于:

根据第一密钥产生具有变化幅度的周期性音调模式的集合;

根据第一密钥和第二密钥产生一个随机信号; 以及

把该音调模式和该随机信号添加到该内容中，以对该内容加扰。

56. 根据权利要求55所述的计算机可读介质，其中进一步包括计算机可执行指令用于:

检测在该内容中的音调模式;

从该音调模式的变化幅度恢复第一密钥;

根据该所恢复第一密钥和该第二密钥产生随机信号; 以及

从该加扰内容中减去该音调模式和随机信号，以恢复该内容。

57. 一种计算机可读介质，其具有计算机可执行指令用于:

检测在加扰内容中的周期性音调模式的集合，该音调模式具有根据第一密钥调制的变化幅度;

从音调模式的变化幅度恢复第一密钥;

根据该所恢复第一密钥和该第二密钥产生随机信号; 以及

从加扰内容中减去音调模式和随机信号以产生未加扰的内容。

用于保护在硬件部分中的数据流的系统和方法

技术领域

本发明涉及一种用于保护例如声音和视频数据这样的数据内容系统和方法。更加具体来说，本发明涉及在硬件部分中的数据流的保护。

背景技术

越来越多的内容以数字形式在例如内部网和互联网这样的专用和公用网络上在线传输。对于用户，数据形式可以提供更加复杂的内容，以及在线传输提高及时性和方便性。对于出版商，数字内容还减少传输成本。不幸的是，在损害出版商的利益的情况下，在线信息传输使得获得原始数字内容相对比较容易并且容易盗版该内容，在出版商的头脑中这样的缺点总是超过所获得的优点。

数字内容，特别是在线数字内容的盗版还不是一个很大的问题。可以在网络上获得的最有价值的内容也是价值较低的，因此临时性和有组织的盗版者目前还不认为窃取并转售该内容是有利可图的行业。现在可以在网上获得书籍和音像制品，并且随着带宽的增加将开始出现视屏内容。随着在线数字内容的价值增加，对有组织和临时性的偷窃者的吸引力增加。

内容的与众不同的特性在于出版者（或者销售者）把该内容给予或销售给客户，但是即使当该内容完全在客户的实际控制下仍然继续限制使用该内容的权利。例如，出版商一般保留对作品的版权，从而客户在没有得到许可的情况下不能够复制或出版该作品。出版商还根据客户是否要制作永久复本或者仅仅是当该内容被传送之后在线地浏览该内容而调节价格。这些情况揭示了一种特殊的方案。拥有该数字比特的用户通常不具有使用它的全部权利；而是提供者至少保留一些权利。在非常实际的意义下，计算机的合法用户可以是数据或内容提

供者的对方当事人。

因此，如果在线商务继续高速发展，则“数字权管理”很快变为一个中心的需求。内容提供者和计算机工业必需快速地解决用于保证数字内容被根据出版商所授予的权利而适当地处理的技术问题和协议。如果没有采取措施，则传统的内容提供者可能会被广泛地盗版而导致破产，并且很可能完全拒绝在线地传输内容。

传统的安全系统不能完全解决这些问题。现在存在有用于加密在网络上的数据、认证用户、废除证书以及安全地存储数据这样的高度安全的方案。图 1 示出一种代表性的现有系统 20 具有内容制造商/提供者 22，其产生原始内容（例如，声音、视频图像）以及把该内容通过网络 24 发布到客户机 26. 内容制造商/提供者 22 具有存储原始内容的数字数据流的内容存储器 30 以及把该内容通过网络 24（例如，互联网）传输的发布服务器 32. 该发布服务器 32 包括编码器 34，其在通过网络发布之前加密并压缩该数据。按照这种方式，该数据在公共网络 24 上的路径中得到保护。

客户机 26 具有处理器 40、存储器 42 以及一个或多个媒体输出设备 44（例如，监视器、显示器、声卡、扩音器等等）。处理器 40 运行各种工具，以处理数据流，例如对该数据流解压缩、对该数据解密、过滤内容并且进行控制（音调、音量等等）的工具。操作系统 50 存储在存储器 42 中并且在处理器 40 上执行. 操作系统 50 实现媒体播放器 52，其能够播放流媒体内容，包括声音和视频图像数据。媒体播放器 52 具有解码器 54，其提供由处理器 40 所运行的工具，以对该内容解压缩和解码。

一旦该内容存储在该机器上，则存在有被设计为限制购买之后的权利的产品。例如，来自 Liquid Audio (www. liquidaudio. com)的产品使内容提供者能够限制内容仅仅在一台机器上播放。该产品通过在盘上保存内容的加密副本并且在其它地方安全地保存一个解密密钥，从而保证原始材料的安全。

尽管这种体系结构安全地保护从提供者 22 到客户机 26 的内容，

并且在该内容存储于客户机上时提供一些保护，但是它不能够解决在该内容被传送到客户机的操作系统之后保证内容的安全。最终，有用的内容必须在客户机中组装用于显示或音频输出，在这一点该数据会被盗窃。

图 2 示出客户机方的部件，以说明原始数据位如何被盗窃，即使在内容的传输和存储中进行保护。在通信端口 60 从网络接收加密和压缩的数据。该数据被传送到媒体播放器 52，其采用解密和解压缩工具 54 来对该内容流解密和解压缩。媒体播放器 52 输出脉冲编码调制（PCM）数据流，其基本上是没有压缩和加密的数字化样本的原始序列。

该媒体播放器 52 调用操作系统 API（应用程序接口）层 62 来把 PCM 数据提交给混合器 64（或者其它处理部件）。该混合器例如可以使用 ACM（音频压缩管理器）或者来自微软公司的 DirectX 技术来实现。混合器 64 用其它资源处理该 PCM，以产生所需的输出。在这一点，所处理的数据传送到驱动器 66（软件和/或硬件），其把数据输出到媒体输出设备 44，例如声卡和扩音器、或者显示器。

利用这种传统体系结构，在整个客户机设备的操作系统软件和硬件中数据不被保护。与上游加密和压缩无关，该数据最终以能够被盗用的明文（未加密）形式传送到下游软件和硬件。例如，攻击者可以引入一个虚假驱动器 72，以接收来自混合器 64 的数据，并且在存储介质 74 上存储原始数据，用于这不是内容提供者所期望的非法用途（例如，重新发布、多次播放，等等）。例如假设，该媒体播放器是用 DirectX API 层来实现的，DirectX 是一种开放的标准，其使得软件应用程序能够读取声音和视频图像数据。软件包（例如，“整体录音机（Total Recorder）”软件包）可以向声卡驱动器（即，虚假驱动器 72）一样安装，并且流进该虚拟声音驱动器的声音或视频图像可以被捕获到标准声音文件中（例如，以“.wav”格式）。

相应地，需要一种体系结构，其能够在把数据位交给操作系统之后对该数据位提供保护。还需要该体系结构与来自微软公司的运行在

Windows 操作系统上称为"DirectX"的现有的多媒体处理系统相集成。该 DirectX 体系结构确定如何使用称为滤波器的模块部件来控制和处理多媒体数据流。滤波器的例子包括用于音频和视频数据类型的压缩器、解压缩器、渲染器（renderer）、混合器、分析器、分配器以及调谐器。滤波器具有输入或输出端子，或者两者兼有，并且在所谓的滤波器图表（filter graph）的结构中相互连接。应用程序使用称为滤波器图表管理器的对象来组装滤波器图表，并且通过它来移动数据。滤波器图表管理器提供一组组件对象模型（COM）接口，从而应用程序可以访问滤波器图表。应用程序可以直接呼叫滤波器图表管理器接口，以控制媒体流或者检索滤波器事件，或者它们可以使用媒体播放器控制来播放媒体文件。读取器被指向微软的网址 Microsoft.com，以及关于"directx"的文件路径，用于获得更多关于 DirectX 的背景信息、滤波器图表和各个滤波器。

DirectX 体系结构的一个主要吸引人的特征是它是模块化并且可扩展的。不幸的是，这些相同的优越属性可能被用于不正当的用途。例如，窃贼可能把"T"插入到滤波器图表中以把被压缩或未压缩的数据调出到盘中。

一种可能的方法是仅仅使用被认证的组件来保证滤波器表图和设备驱动器的安全。这种方法的缺点是增加为组件获得证书以及在使用过程中对它们进行认证的负担。

另一个方法是保持该数据被加密，直到它到达驱动器层 66 为止。该方法具有一个缺点在于由于当所加密的数据随后被解密时，来自滤波器的一些处理结果不能够通过解密算法而清楚地传输，这可能导致较差质量的输出，通常使得该数据不能够被恢复。例如，考虑一个加密的 MPEG 流。它将会丢失 MPEG 传输层组帧，并且滤波器图表将不能够被处理。另一个例子是 PCM 音频数据。如果加密的音频数据与其它信号（例如，来自邮件程序的"叮"）相混合，则不可能进行解密。作为最后一个例子，把加密的音频位流乘以一个常数的音量控制使得加密的流不能够被恢复。

因此，需要一种体系结构，其能够保护在计算机的操作系统和硬件组件中的数据并且与 DirectX 体系结构相集成，而在播放时不会使信号的质量下降。

发明内容

本发明考虑一种用于保护在计算机的操作系统和硬件组件中的数据流的体系结构。

在一个实施例中，服务器通过网络把加密和压缩的内容提供给客户机。该客户机接收该内容并且对它进行解密和解压缩。在这一点，该内容采用脉冲编码调制（PCM）数据流的形式，其基本上是没有压缩和加密的数字化样本的原始序列。PCM 数据流容易被处理（例如，调节音量、与其它资源混合，等等）。客户机采用一组工具来处理该 PCM 数据，例如在操作系统水平上的滤波器图表技术。

为了防止原始数位在处理时被盗用，该客户机对 PCM 数据加扰。一种技术是通过把随机信号添加到该内容中而增加噪声。更加具体来说，客户机具有一个加扰器，以产生周期性的确定的声音模式组。该加扰器基于第一密钥对该声音模式的振幅进行调制，从而把第一密钥嵌入到调制的声音模式中。该加扰器还根据第一密钥和第二密钥产生随机信号。该声音模式和随机信号被添加到 PCM 数据中，以对该内容加扰。

加扰后的内容被传送到滤波器图表或者其它处理系统。该内容被在加扰的状态下处理。尝试在滤波器图表中进行处理时调出该数位的任何攻击者将仅仅获得噪声数据，这对于重新发布或者复制目的来说是无用的。

在处理之后，该加扰的数据被传送到驱动器用于输出。该驱动器实现一个解扰器，以通过除去噪声而对该内容解扰。该解扰器检测在该内容中的声音模式并且从声音模式的变化的振幅中恢复第一密钥。该解扰器也通过一个分离的信道（例如，用密码保护的路径）接收第二密钥，并且根据该所恢复第一密钥和该第二密钥产生相同的随机信

号。该解扰器从加扰的内容中减去声音模式和随机信号，以把 PCM 数据恢复到未加扰的状态，但是具有由于处理所获得的更改。

在另一个实施例中，该服务器在把内容通过网络发布之前对该内容加扰。基于服务器的加扰器与压缩该内容的压缩单元协作或相集成，从而该压缩算法不会使得该加扰内容不可恢复。

附图简述

在图中相同的标号表示相同的部件和特征。

图 1 为一种现有的客户机-服务器网络的方框图，其中服务器把加密和压缩的内容通过网络（例如互联网）提供给客户机。

图 2 为在客户机上实现的用于解密、解压缩和播放该内容的现有硬件和软件组件的方框图。

图 3 为采用加扰技术来保护在操作系统和硬件组件中的数据的客户机体系结构的方框图。

图 4 为示出图 3 的加扰技术的一个实现方式的方框图。

图 5 为通过图 3 和 4 的加扰技术实现的加扰处理的流程图。

图 6 为作为加扰处理的一部分添加到数据中的调制声音信号的时域表示。

图 7 为作为加扰处理的一部分添加到数据中的随机样本的时域表示。

图 8 为在图 4 的加扰技术中采用的声音检测器和解调器的方框图。

图 9 为在网络级上实现加扰技术的客户机-服务器网络系统的方框图，其中在内容提供方执行加扰，以及在客户机方执行解扰。

具体实施方式

基于客户机的体系结构

图 3 示出一种客户机方的体系结构 100，其保护在客户计算机中的数据流（例如，声音和视频数据）。为了讨论的目的，客户机可以被用作为具有处理器、易失性存储器、非易失性存储器以及操作系统

的通用计算单元（例如，台式机、便携机等等）。它还可以被用作为其它设备，例如同轴电缆调制解调器、机顶盒、声频/视频应用程序等等。

图 3 示出在客户计算机上实现的软件/硬件体系结构 100。假设客户机采用防窜改软件应用程序来购买、存储和播放内容，该应用程序使用 SSL（加密套接字协议层）或者其它保密和被认证的连接来连接到内容提供商的服务器。该防窜改软件防止攻击者容易地更改该组件或提取密钥。但是，在一些时段中，该音频数据必须交给操作系统来播放。

该体系结构 100 包括通过网络接收来自服务器的加密和压缩数据的通信层或端口 60。该数据一般使用公知的算法（例如，RSA）来加密并且使用公知的加缩技术（例如，AVI, MPEG, ASF, WMA, MP3）来压缩。该数据被传送到媒体播放器 102，其最好是来自微软公司的 "Windows 媒体播放器"。该 "Windows 媒体播放器"使用 DirectX API（应用程序接口）层来实现，该 DirectX API 是由微软公司所设计的一组技术，以使得基于 Windows 的计算机成为一个用于运行和显示例如真彩图像、视频图像、三维动画和环绕声这样的丰富的多媒体元素的适合平台。

媒体播放器 102 采用解密/解压缩工具 104 来对该内容流进行解密和解压缩。在这一阶段，该内容采用脉冲编码调制（PCM）数据流的形式，该数据流基本上是没有压缩和加密的数字化样本的原始序列。为了防止在滤波器进行处理时该原始数位被盗窃，媒体播放器 102 还采用加扰器 106 来对 PCM 数据进行加扰。该加扰器 106 把该数据改变到这样的程度，使得该数位即使被盗窃也基本上是没有用的。例如，加密的音频数据可能具有使声音变差并且不能够被消除的大量噪声，从而使得被盗的数据没有任何价值。然而同时，声音或视频数据的加扰版本对于在滤波器图表中的滤波器来说基本上与真实的声音或视频数据相同，使得通常未更改的解码器或信号处理组件工作良好。因此，该加扰内容 "看起来"与未更改的内容相同，但是却能够防止盗窃。

加扰的PCM数据通过操作系统API层62传送到滤波器图表108，其通过添加一个或多个其它信号、调节音量或音调等等来处理PCM数据。该滤波器图表108处理该加扰PCM数据，就好象该数据是原始未加扰的PCM数据那样。该滤波器图表108具有一个或多个滤波器，例如处理PCM数据的混合器、音量、音调、编码器、渲染器等等。请注意，滤波器图表108被示出用于讨论的目的，但是其它类型的信号处理技术可以代替该滤波器图表。

所处理的数据被传送到可以用软件和/或硬件实现的驱动器110。该驱动器110实现一个解扰器112，用于对加扰的PCM数据解扰，并且把该PCM数据恢复到加扰之前的状态，作为滤波器图表处理的结果而进行更改。该解扰器112把解扰的更改后的PCM数据输出到媒体输出设备44。

加扰器106和解扰器112利用一个或多个密钥114来产生添加到PCM数据中的加扰信号。密钥114可以在媒体播放器102和驱动器110之间通过频带内信道与加扰数据一同传输，和/或通过与数据路径相分离的频带外信道（例如，在DirectX中的IOCTL设备I/O控制信道）传输。媒体播放器102和驱动器110的一个实施例以及用于加扰和解扰PCM数据的密钥在下文中参照图4更加详细地描述。

加扰体系结构在内容被操作系统和低级别硬件组件所处理时保护该内容。希望使用虚假驱动器72从滤波器图表108中调出原始数位的攻击者会接收到从记录或重新发布方面来看没有价值的加扰数据，从而消除了窃贼在经济方面的动机。另外，如果不知道该密钥114则非常难以对该数据解扰。

加扰技术

存在有不同的方式来在客户机实现加扰体系结构，来对PCM数据加扰。一个方式是把噪声添加到该信道中。在音频数据的情况下，一种噪声添加方案是使用会话密钥来产生一组语音、音乐或类似噪声的函数，并且在时域或者频域或子波域中直接把这些函数添加到该信

号中。根据密钥发生器选择函数、幅度、相位和放大因子。每秒钟添加几十个噪声脉冲使得该信号对于攻击者来说没有价值，并且即使攻击者知道噪声的主要成份，该攻击者必须执行“搜索”以消除噪声的空间是相当大的。但是，给定该密钥（并且假设没过载），则该噪声信号能够被完全地消除，以返回未加扰状态。

另一种用于现有技术中的方法是采用时域和频域加扰。在时域加扰中，时间被分为帧（例如，2 或 3 秒），并且每一帧被分为几个片段。在每个帧中，片段被改变序列和重新组合。一般来说，每个帧使用不同的排列。密钥控制排列的次序。在频域加扰中，信号被分为重叠帧（例如，50 毫秒）然后它被通过 FFT 滤波器组映射到频域上。该频带被重新排列并且通过合成滤波器组而发送。在此，密钥控制排列的次序。频域加扰比时域加扰更加难以破解，但是其优点是增加用于分析和合成滤波器组的额外计算。

时域和频域加扰的主要特点是被加扰的信号不能通过混合器（例如，图 3 中的 108 这样的滤波器图表混合器），由于在解扰之后，混合的信号将仍然被加扰。下面描述基于噪声添加的加扰解决该问题：混合到加扰的音频信号中的信号的音频信号在解扰之后保持不变。

基于噪声添加的加扰的例子

图 4 示出当内容被在客户计算机的操作系统和硬件组件中处理时采用基于噪声添加的加扰处理来保护内容的客户机方组件。更加具体来说，图 4 示出在媒体播放器 102 中的加扰器 100 以及在驱动器 110 的解扰器 112 的实现例子。另外参照图 5 的流程图来描述加扰处理。这些步骤由图 4 中所示的各种软件和/或硬件组件所执行。

该处理以在媒体播放器 102 接收加密和被压缩数据流（例如，音频、视频数据）为开始。该媒体播放器利用工具 104 来对该数据流解密和解压缩，得到 PCM 数据流（步骤 204）。加扰器 106 通过把噪声添加到数据中而对 PCM 数据加扰（步骤 206）。该加扰器 106 具有用于产生同步音调的音调脉冲发生器和调制器 120 以及用于产生随机信

号的密码伪随机数发生器（PRNG）122。同步音调和随机信号都被添加到 PCM 数据中，以产生噪声或加扰的 PCM 数据。

音调脉冲发生器 120 和 PRNG 122 使用两级密钥来创建同步音调和随机信号：（1）“频带内”密钥 124，以及（2）“频带外”或“会话”密钥 126。音调脉冲发生器 120 和 PRNG 122 都使用频带内密钥 124，而仅仅 PRNG 122 使用频带外密钥 126。该密钥例如可以具有较大的数位长度，例如 56 位或者 128 位密钥。

音调脉冲发生器和调制器 120 使用频带内密钥来产生可以容易在解扰器处识别的音调脉冲组合（在图 5 的步骤 S208）。音调模式被周期性地添加到 PCM 数据信号，例如每隔 100 毫秒。

图 6 示出具有交替正/负数值的脉冲的确定模式的示例同步音调 300。该脉冲可以具有两个不同的幅度中的一个幅度，例如+0.5/-0.5 或+1/-1。调制每个脉冲模式的幅度使得加扰器在每个脉冲序列解码一个数位或一块信息。例如，一个音调脉冲 302 的序列利用+1/-1 来表示第一二进制数值（例如，1），以及音调脉冲 304 的一个不同序列利用+0.5/-0.5 来表示第二二进制数值（例如，0）。该频带内密钥 124 被嵌入到声调脉冲序列的组合中，作为数位集合，以把该密钥与数据一同传送到该驱动器。该频带内密钥可以随着每个音频/视频剪辑、剪辑组、或者甚至在剪辑内而改变。

同步音调 300 具有为原始信号的采样频率的一半的频率。对于具有 44.1kHz 的采样频率的音频数据，该音高脉冲发生器 120 产生 22.05kHz 的同步音调。该音调容易被解扰器所检测和除去。另外，即使该解扰器没有完全除去该同步音调，用于该驱动器或声卡中的模-数转换器将除去该音调频率。

再次参见图 4 和 5，该密码 PRNG 122 使用频带内密钥和频带外会话密钥产生伪随机信号（在图 5 中的步骤 210）。图 7 示出具有+1 或-1 幅度的数据值的随机模式的示例随机序列 400. PRNG 122 被使用以提供相等机率的+1 或-1 输出，总体平均年龄，以避免把直流偏移导入该原始数据信号。

当把频带内密钥 124 嵌入到音调同步信号中时，会话密钥 126 保持数据的独立并且在与数据路径相分离的信道 128 上传送。会话密钥 126 使用密码密钥交换（例如，Diffie-Hellman 交换和认证）来保护，以保证密钥 126 安全地从媒体播放器 102 通过信道 128（其例如可以是在 DirectX 中的 IOCTL 设备控制器）传输到驱动器 110。相应地，加扰器 106 或媒体播放器 102 具有加密和发信功能，与加密和发送用于安全传输的会话密钥到驱动器 110 和解扰器 112。

加扰器 106 通过加法器 130 添加同步音调脉冲和随机信号到该 PCM 数据，以对该数据加扰（在图 5 中的步骤 212）。如果需要的话，原始信号（即，PCM 数据）和随机信号可以被标准化，以把复合信号返回到该滤波器图表 108 所预期的范围。例如，该 PCM 数据可以乘以因子 0.75，并且该随机信号可以在加上两个信号之前乘以因子 0.25，以对所获得的复合信号标准化。

加扰的 PCM 数据被传送到滤波器图表 108，在此被处理并且与其它资源混合（在图 5 中的步骤 214）。该滤波器图表可以具有一个或多个处理该数据的滤波器。作为一个例子，该滤波器图表可以调节信号的音量，或者可以增加任意延迟，这作为一个处理步骤的一部分。滤波器对噪声数据进行操作，就好象该数据是原始 PCM 数据那样。该滤波器图表把更改的噪声数据输出到驱动器 110。

在图 5 的步骤 216 中，在驱动器 110 的解扰器 112 通过从该数据中除去噪声成份而对该更改的噪声 PCM 数据解扰。该解扰器 112 具有音调检测器和解调器 140、密码 PRNG 142 以及硬件接口 144。音调检测器和解调器 140 检测在复合信号中的同步音调，测量任何音量和由滤波器图表 108 所导入的延迟，并且对该音调解调以恢复频带内密钥 124（在图 5 中的步骤 218）。音调检测器 140 把所恢复的频带内密钥 124 传送到 PRNG 142。

解扰器 112 还接收来自频带外信道 128 的会话密钥 126，对它进行解密和认证，并且把该密钥 126 给予 PRNG 142。该解扰器具有解密和认证装置，用于对来自媒体播放器 102 的会话密钥进行解密和认

证。PRNG 142 采用与媒体驱动器 PRNG 122 中所用相同的算法。给定相同的频带内密钥 124 和会话密钥 126，PRNG 142 重新创建与以前添加到媒体播放器的 PCM 数据中的随机信号相同的随机信号（在图 5 中的步骤 220）。

解扰器 112 通过减法器 146 从该噪声 PCM 数据中减去同步音调和随机信号，以除去噪声（在图 5 中的步骤 222）。PCM 数据通过硬件接口 144 传送到输出设备（例如声卡、显示器），该处理结束（步骤 224 和 226）。

图 8 示出在解扰器 112 中采用的音调检测器和解调器 140 的一个例子。音调检测器和解调器具有匹配滤波器 500，用于检测在噪声 PCM 数据中的同步音调。该匹配滤波器 500 具有该纯同步音调的一个有限长度的时间逆转副本，作为脉冲响应 h(n)。因此匹配滤波器的输出 y(n) 由下式给出：

$$y(n) = \sum_{l=-L}^{L} h(l)x(n-l)$$

其中 x(n)是更改的噪声数据信号，以及 2L+1 是音调脉冲的长度。当音调模式 h(n)的位置与信号中的音调成份相对齐时，y(n)具有最大值。第一最大值的位置确定延迟 506，通过该延迟应当及时地移动该音调和 PRNG 噪声模式，使其适当地与更改的噪声数据相对齐。

延迟量和噪声数据被传送到峰值搜索模块 502，估计由滤波器图表 108 所作的任何音量改变。该模块估计通过搜索处理的适当增益 508（在减法 146 之前应当把该增益乘以恢复的音调脉冲和 PRGN 噪声），其中增益估计被迭代地细化，直到在音调减法之后的信号能量最小。恢复的同步音调与正确的增益和延迟一同在模块 510 中产生。

频带内密钥的检测由幅度解调模块 512 所执行。对于每个音调脉冲，该模块把脉冲幅度与以前几个时间间隔上的平均音调脉冲幅度测量值相比较。如果该幅度大于该平均值（例如，所述幅度等于 1.0 并且该平均值等于 0 75），则该密钥的数值被解调为具有一个二进制数值（例如，“1”）。如果该幅度小于该平均值（例如，该幅度等于

0.5，并且该平均值等于 0.75），然后该密钥的一个数值被解调为具有另一个二进制数值（例如，“0”）。该处理对后续的音调脉冲重复执行，直到频带内密钥 124 的所有数位被恢复。然后，该频带内密钥 124 可以由密码 PRNG 142 所使用，以恢复要从该加扰信号中减去的随机噪声序列。

在上述实施例中，通过添加同步音调和随机信号而把噪声导入到该内容中。另外，可以通过把至少一部分内容与由 PRNG 122 所产生的随机位流之间执行异或运算而对该内容加扰。例如，对于 16 个音频数据，13 个最低有效位与由 PRNG 122 所产生的数位进行异或运算。这样有效地对该内容加扰，并且具有不会使表示声音的整数“溢出”的额外特性。为了对该内容解扰，再次把较低数位与相同的随机位流进行异或运算。

结论

该加扰体系结构的优点在于保护在计算机的操作系统和硬件组件中的数据内容。另一个优点是该体系结构与现有的 DirectX 技术良好地集成。尽管本发明已经用具体结构特征和/或方法步骤进行描述，但是应当知道在权利要求书中所限定的本发明不一定限于所述的具体特征或步骤。而是，该具体特征和步骤被公开作为实现所要求保护的发明的优选形式。

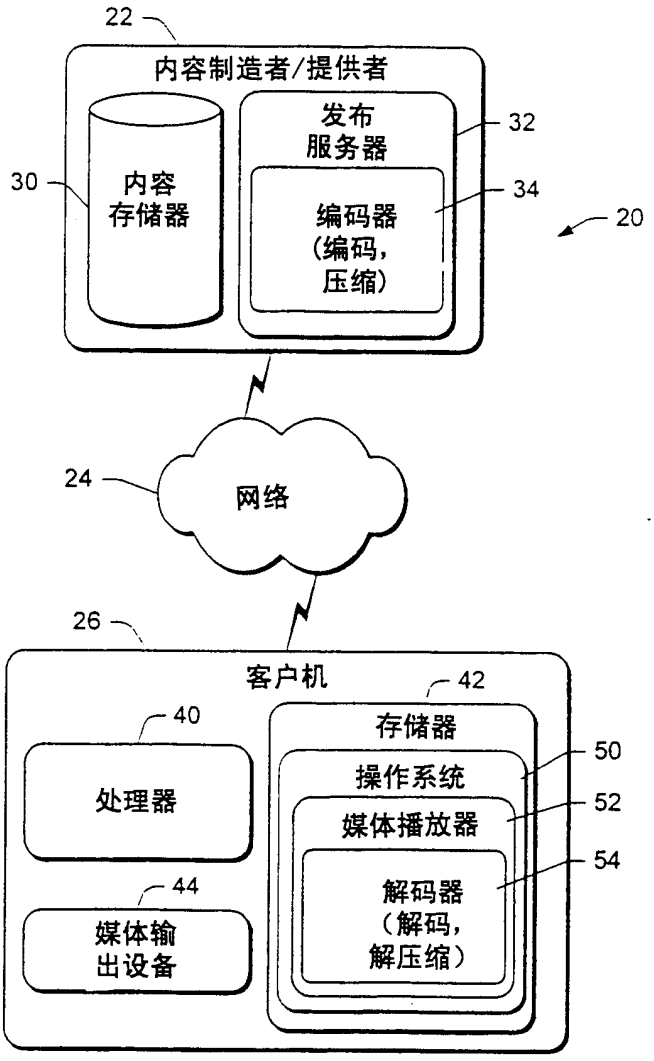

22
内容制造者/提供者
发布
服务器
32
30
内容
存储器
34
编码器
(编码,
压缩)
20
24
网络
26
客户机
42
40
存储器
处理器
操作系统
50
媒体播放器
52
54
解码器
(解码,
解压缩)
44
媒体输
出设备

图 1
现有技术

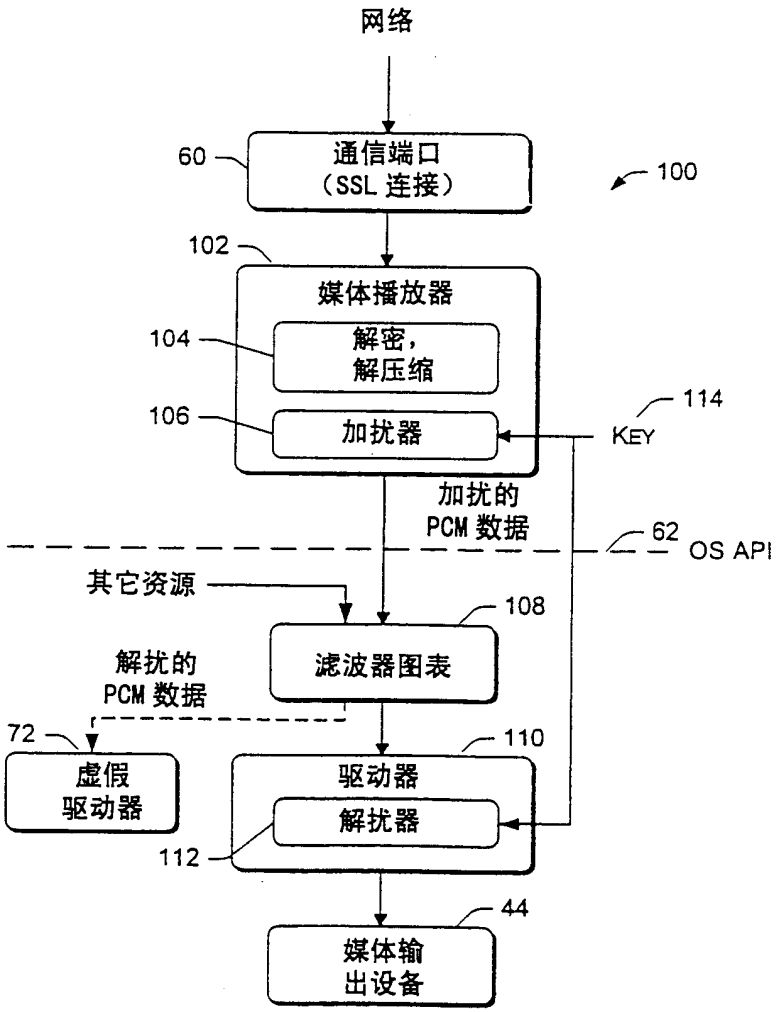

网络
60
通信端口
（SSL 连接）
100
102
媒体播放器
104
解密，
解压缩
106
加扰器
114
KEY
加扰的
PCM 数据
62
OS API
其它资源
108
滤波器图表
解扰的
PCM 数据
72
虚假
驱动器
110
驱动器
解扰器
112
44
媒体输
出设备

图 3

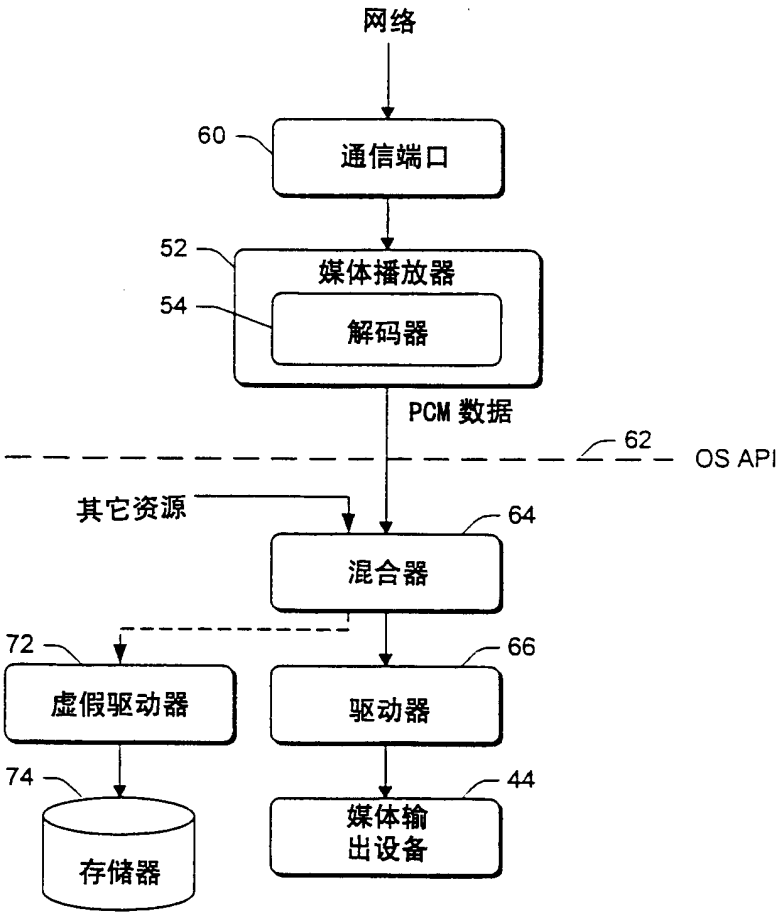

网络
60
通信端口
52
媒体播放器
54
解码器
PCM 数据
62
OS API
其它资源
64
混合器
72
虚假驱动器
66
驱动器
74
存储器
44
媒体输出设备

图 2
现有技术

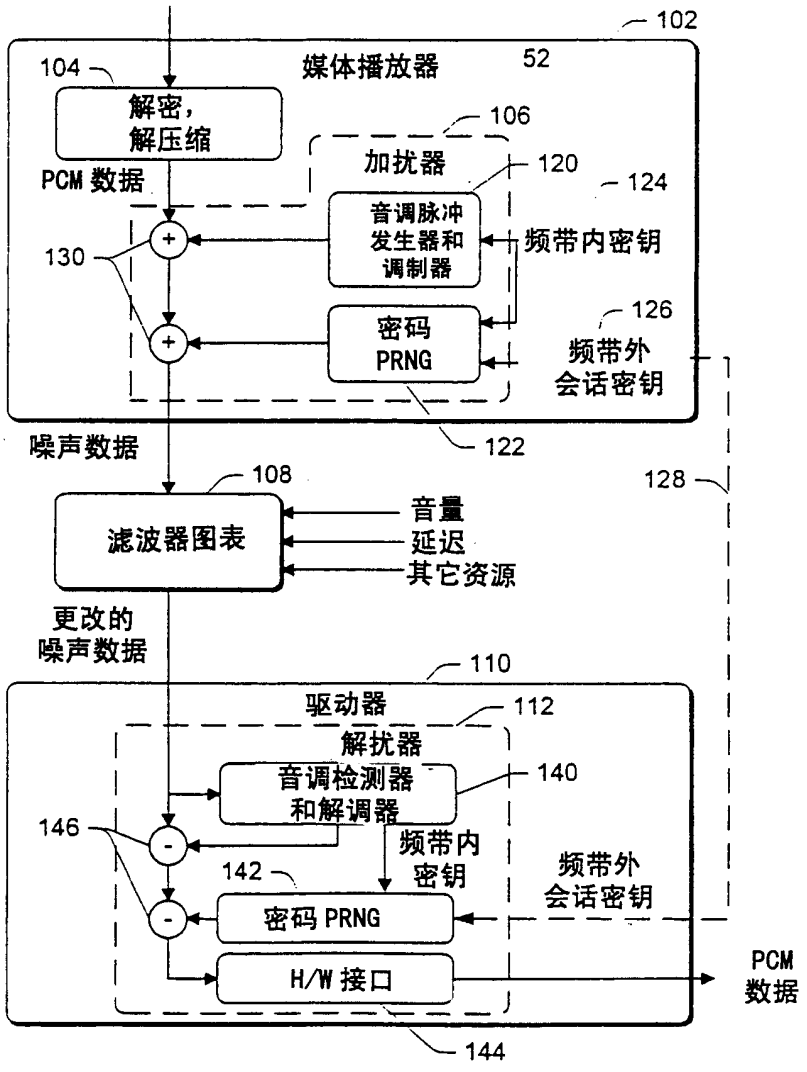

102
媒体播放器
52
104
解密，
解压缩
106
加扰器
120
124
PCM 数据
音调脉冲
发生器和
调制器
频带内密钥
130
126
密码
PRNG
频带外
会话密钥
噪声数据
122
128
108
滤波器图表
音量
延迟
其它资源
更改的
噪声数据
110
驱动器
112
解扰器
音调检测器
和解调器
140
146
频带内
密钥
频带外
会话密钥
142
密码 PRNG
H/W 接口
PCM
数据
144

图 4

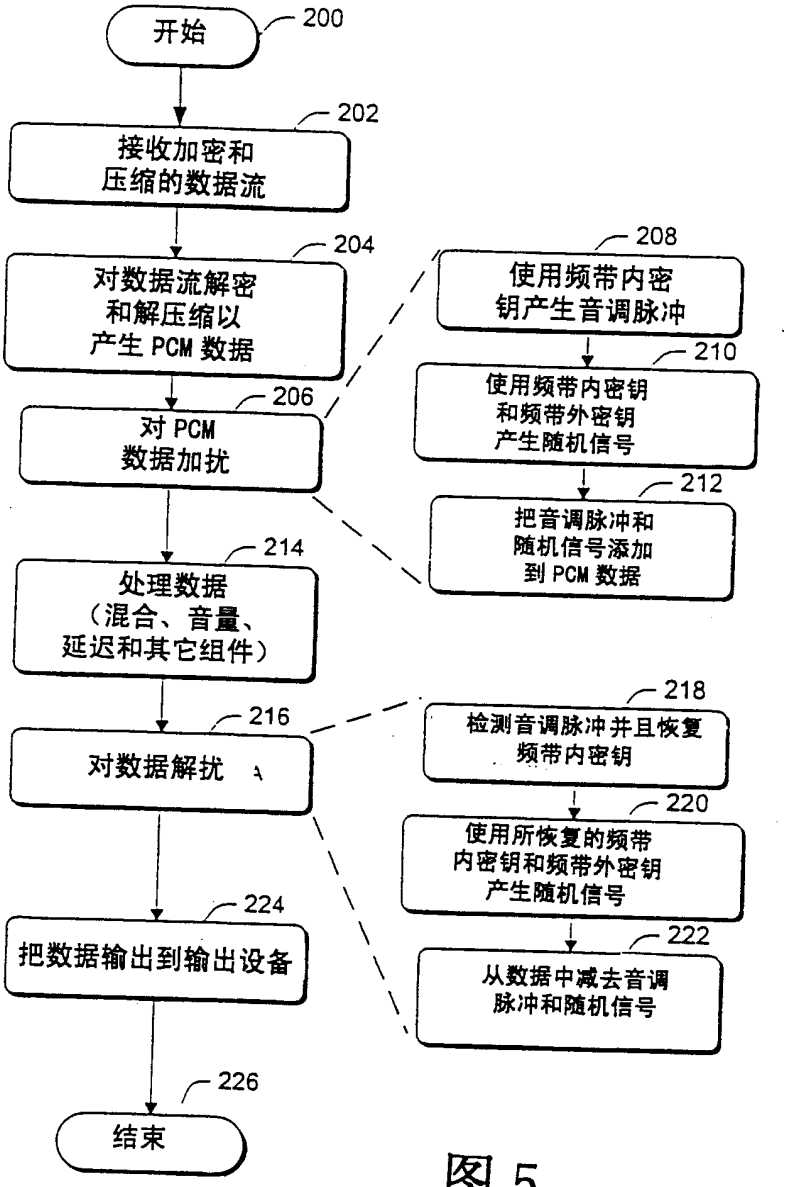

开始
200
接收加密和
压缩的数据流
202
对数据流解密
和解压缩以
产生 PCM 数据
204
对 PCM
数据加扰
206
处理数据
（混合、音量、
延迟和其它组件）
214
对数据解扰
216
把数据输出到输出设备
224
结束
226
使用频带内密
钥产生音调脉冲
208
使用频带内密钥
和频带外密钥
产生随机信号
210
把音调脉冲和
随机信号添加
到 PCM 数据
212
检测音调脉冲并且恢复
频带内密钥
218
使用所恢复的频带
内密钥和频带外密钥
产生随机信号
220
从数据中减去音调
脉冲和随机信号
222

图 5

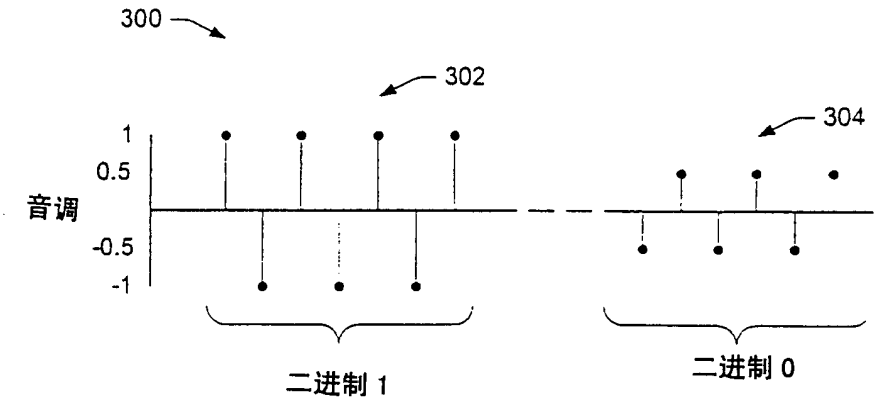


图 6

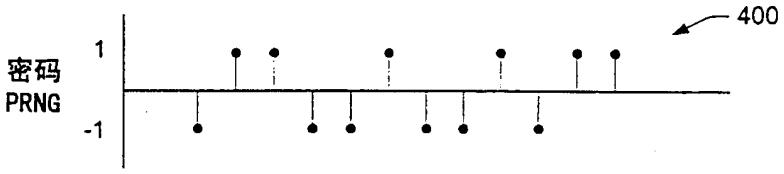


图 7

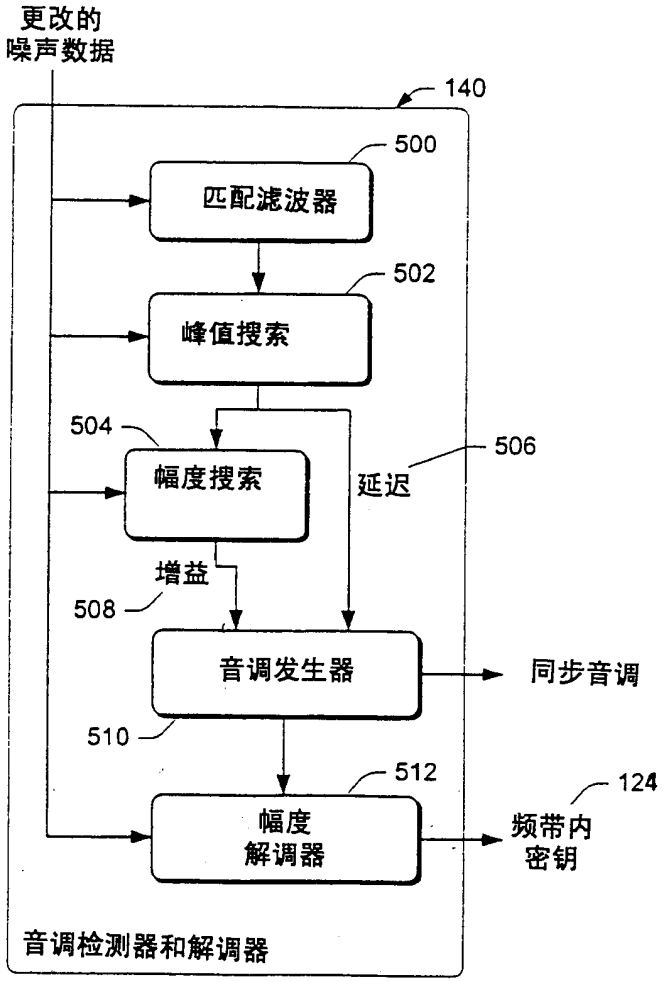

更改的
噪声数据
140
500
匹配滤波器
502
峰值搜索
504
幅度搜索
506
延迟
增益
508
音调发生器
同步音调
510
512
124
幅度
解调器
频带内
密钥
音调检测器和解调器

图 8

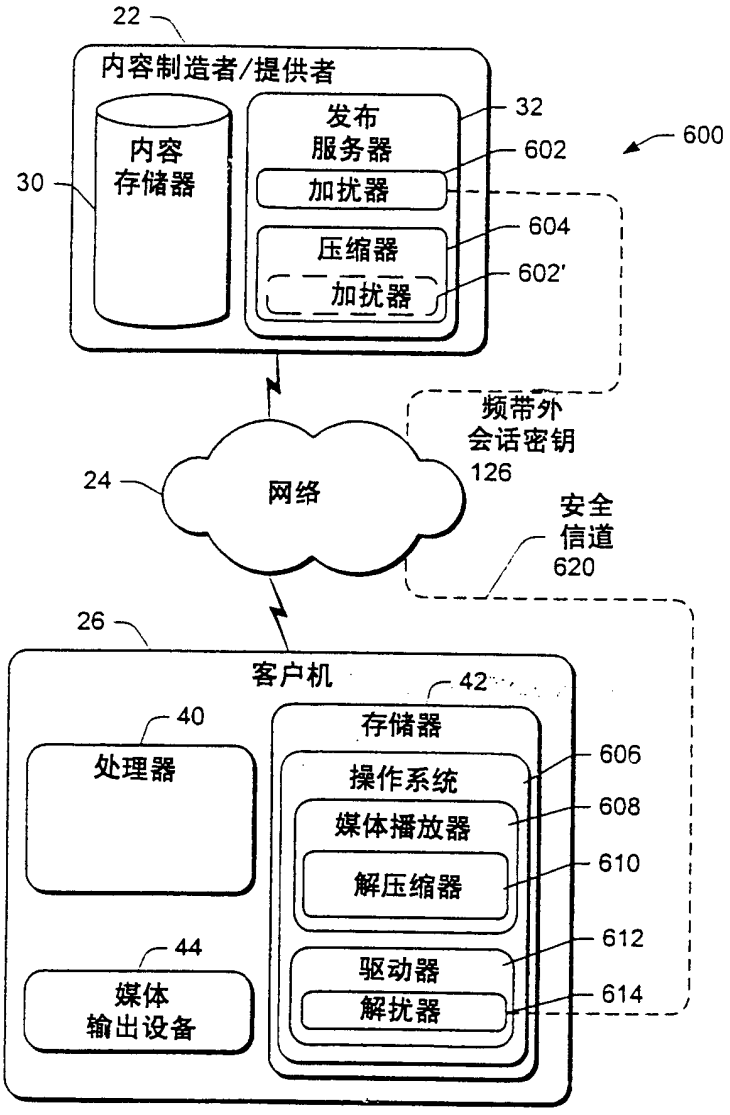

22
内容制造者/提供者
内容
存储器
30
发布
服务器
32
600
602
加扰器
604
压缩器
602'
加扰器
频带外
会话密钥
126
24
网络
安全
信道
620
26
客户机
42
40
处理器
存储器
606
操作系统
608
媒体播放器
610
解压缩器
612
驱动器
614
解扰器
44
媒体
输出设备

图 9