(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101536514 B
(45)授权公告日 2013.05.15

(21)申请号 200780041236.8
(22)申请日 2007.11.06
(30)优先权数据
06301141.5 2006.11.09 EP
(85)PCT申请进入国家阶段日
2009.05.06
(86)PCT申请的申请数据
PCT/EP2007/061934 2007.11.06
(87)PCT申请的公布数据
WO2008/055900 EN 2008.05.15
(73)专利权人 汤姆森许可贸易公司
地址 法国布洛涅-比郎库尔
(72)发明人 穆罕默德·卡若米 斯蒂芬·昂奴 阿兰·迪朗
(74)专利代理机构 中科专利商标代理有限责任公司 11021
代理人 王波波
(51)Int.Cl.
H04N 21/2343(2011.01)
H04N 21/2347(2011.01)
H04N 21/2662(2011.01)
H04N 21/4405(2011.01)
H04N 21/6334(2011.01)
(56)对比文件
US 2005/0276416 A1,2005.12.15,说明书第20-68,81-128段、图1-4,6.
US 5987124 A,1999.11.16,说明书第5栏第35-67行,第6栏1-15行,第8栏36-48行、图1-2.
CN 1535014 A,2004.10.06,全文.
US 2005/0276416 A1,2005.12.15,说明书第20-68,81-128段、图1-4,6.
US 2005/0182855 A1,2005.08.18,全文.
CN 1535015 A,2004.10.06,全文.
审查员 李慧

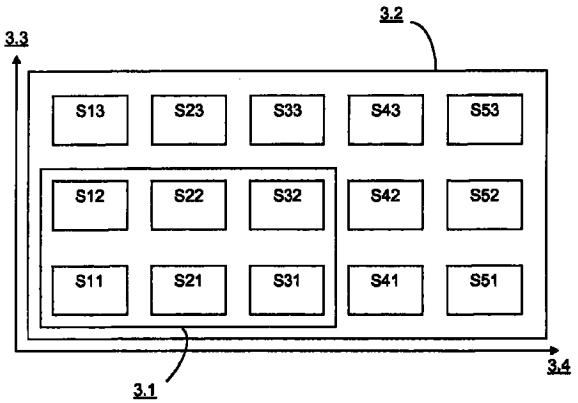
权利要求书2页 说明书8页 附图5页

(54)发明名称

用于管理密钥传输的方法和设备

(57)摘要

本发明涉及一种用于对由发射机(5.1)向接收机(5.2)发送的已编码的可伸缩增强帧(3.2)进行加密的方法和设备,该增强帧包括多个按照质量级别排序的补充流,每个补充流与多于一个可伸缩性类型的组合相对应,其中较低质量级别的补充流与每个可伸缩性类型的较低质量相对应,所述方法在发射机级别包括以下步骤:为每个补充流生成(S1)用于对该补充流进行加密的密钥,使得所有可伸缩性类型可以同时或者单独使用;所述密钥的生成使得仅可以根据补充流的密钥获得低于所述补充流质量级别的质量级别的补充流的密钥;以及向接收机发送(S3)与所需质量级别相对应的补充流的密钥,该密钥允许接收机仅生成较低质量级别的补充流的密钥。本发明还涉及一种用于对接收到的已编码的可伸缩增强帧进行解密的方法和设备。



CN 101536514 B

1. 一种用于对由发射机 (5.1) 向接收机 (5.2) 发送的已编码的可伸缩增强帧 (3.2) 进行加密的方法，所述增强帧包括多个按照质量级别进行排序的补充流，每个补充流与多于一个可伸缩性类型的组合相对应，其中较低质量级别的补充流与每个可伸缩性类型的较低质量相对应，所述方法在发射机 (5.1) 级别包括以下步骤：

生成与最高质量级别的补充流 $S_{M,T}$ 相对应的一个随机密钥 $K_{M,T}$；

通过对随机密钥 $K_{M,T}$ 连续应用单向置换算法 h 来获得较低质量级别的补充流 $S_{I,J}$ 的密钥 $K_{I,J}$；以及

将与质量级别相对应的补充流的密钥 $K_{m,t}$ 发送 (S3) 至接收机，所述密钥使接收机能够仅生成较低质量级别的补充流的密钥，

其特征在于，在获得密钥的步骤中，将随机密钥 $K_{M,T}$ 分为与可伸缩性类型的数量相对应的多个部分 $L_{KM,T}$，$R_{KM,T}$，并且对每个部分连续地使用单向置换算法 $h^{M-I}(L_{KM,T})||h^{T-J}(R_{KM,T})$ 以生成后续密钥 $K_{M-I,T-J}$。

2. 根据权利要求 1 所述的方法，其特征在于，所述方法包括以下步骤：在发送与质量级别相对应的补充流的密钥之前，接收 (S2) 来自接收机的、对于所述质量级别的流接收的请求。

3. 根据权利要求 1 所述的方法，其特征在于，在第一可伸缩性和第二可伸缩性两个可伸缩性类型的组合中，获取针对给定的第一可伸缩性级别的较低质量级别的补充流的密钥的步骤包括以下步骤：

将一级别的密钥划分成左部和右部，

对密钥的右部应用单向置换算法，以及

将密钥的左部与所获得的右部连接以获得较低质量级别的密钥。

4. 根据权利要求 1 所述的方法，其特征在于，在第一可伸缩性以及第二可伸缩性两个可伸缩性类型的组合中，获取针对给定的第二可伸缩性级别的较低质量级别的补充流的密钥的步骤包括以下步骤：

将一级别的密钥划分成左部和右部，

对密钥的左部应用单向置换算法，以及

将所获得的右部与密钥的左部连接以获得较低质量级别的密钥。

5. 一种用于计算解密密钥以对已编码的可伸缩增强帧进行解密的方法，所述增强帧包括多个按照质量级别排序的补充流，每个补充流与多于一个可伸缩性类型的组合相对应，其中较低质量级别的补充流与每个可伸缩性类型的较低质量相对应，所述方法在接收机 (5.2) 级别包括以下步骤：

接收 (S3) 与所需质量级别相对应的补充流 $S_{m,t}$ 的密钥 $K_{m,t}$；以及

通过对接收到的密钥连续应用与发射机所用的单向置换算法相同的单向置换算法 h 来根据接收到的密钥仅生成 (S4) 与较低质量级别相对应的补充流的后续密钥，

其特征在于，将随机密钥 $K_{M,T}$ 分为与可伸缩性类型的数量相对应的多个部分 $L_{KM,T}$，$R_{KM,T}$，并且对每个部分连续地使用单向置换算法 $h^{M-I}(L_{KM,T})||h^{T-J}(R_{KM,T})$ 以生成后续密钥 $K_{M-I,T-J}$。

6. 根据前一权利要求所述的方法，其特征在于，所述方法包括以下步骤：在接收 (S3) 补充流的密钥的步骤之前，指示 (S2) 所述所需质量级别的流接收。

7. 一种用于对已编码的可伸缩增强帧 (3.2) 进行加密的设备，所述增强帧包括多个按

照质量级别进行排序的补充流，每个补充流与多于一个可伸缩性类型的组合相对应，其中较低质量级别的补充流与每个可伸缩性类型的较低质量相对应，所述设备包括：加密装置，用于生成与最高质量级别的补充流 $S_{M,T}$ 相对应的一个随机密钥 $K_{M,T}$，并通过对所述随机密钥 $K_{M,T}$ 连续应用单向置换算法 h 来生成较低质量级别的补充流的密钥，

其特征在于，将随机密钥 $K_{M,T}$ 分为与可伸缩性类型的数量相对应的多个部分 $L_{KM,T}$，$R_{KM,T}$，并且对每个部分连续地使用单向置换算法 $h^{M-I}(L_{KM,T})||h^{T-J}(R_{KM,T})$ 以生成后续密钥 $K_{M-I,T-J}$。

8. 一种用于对已编码的可伸缩增强帧进行解密的设备，所述增强帧包括多个按照质量级别排序的补充流，每个补充流与多于一个可伸缩性类型的组合相对应，其中较低质量级别的补充流与每个可伸缩性类型的较低质量相对应，所述设备包括：解密装置，用于通过对接收到的密钥 $K_{m,t}$ 连续应用与发射机所用的单向置换算法相同的单向置换算法 h 来根据接收到的密钥 $K_{m,t}$ 仅生成与较低质量级别相对应的补充流的后续密钥，

其特征在于，将接收到的随机密钥 $K_{M,T}$ 分为与可伸缩性类型的数量相对应的多个部分 $L_{KM,T}$，$R_{KM,T}$，并且对每个部分连续地使用单向置换算法 $h^{M-I}(L_{KM,T})||h^{T-J}(R_{KM,T})$ 以生成后续密钥 $K_{M-I,T-J}$。

用于管理密钥传输的方法和设备

技术领域

[0001] 本发明涉及一种用于管理密钥传输的方法。

背景技术

[0002] 在MPEG4-第2部分以及MPEG2-第10部分中定义了细粒度可伸缩性(Fine Grain Scalability)技术。以下将其表示为MPEG-4 FGS。MPEG-4 FGS定义了一种方法,其中数据流被压缩为两个层:基本层(非可伸缩部分),以及增强层(可伸缩部分)。压缩流的接收机可以仅仅对基本层进行解码或者对基本层以及增强层进行解码。如果仅对基本层进行解码,这将导致低质量版本的原始内容。如果对增强层的一部分进行解码并且将其与基本层组合,这将生成改善质量的内容,所改善的质量与经解码的增强部分成正比。此外,增强层支持峰值信噪比(下文记为PSNR)可伸缩性,以及时间可伸缩性。因此MPEG-4FGS提供了一定的灵活性,或者通过仅增加比特率来支持时间可伸缩性,或者支持PSNR可伸缩性而保持相同的比特率,或者同时支持PSNR以及瞬时可伸缩性。细粒度可伸缩性是由增强层提供的。峰值信噪比是用于比较两幅图像的客观视频质量度量,其可以由视频的接收机自动计算。比特率是在用于接收视频的接收机处的可用比特率。

[0003] 可伸缩多层FGS加密(记为SMLFE)是针对MPEG-4 FGS编码同时支持PSNR和比特率可伸缩性的分层访问控制方案。在SMLFE中,增强层被加密成为具有多个质量级别的单个流,其中多个质量级别是依照于PSNR以及比特率值划分的。较低质量级别可以被相同可伸缩性类型的较高质量级别访问以及重用。此时,增强层由若干不同片段组成。对每个片段生成一个密钥,以对每个片段进行加密。

[0004] 为了访问MPEG-4 FGS的压缩内容,消费者需要密钥以对全部所需片段进行解密。密钥的数量可以很大。因此,将所有密钥发送至消 费者是很麻烦的,并且向所传输的内容加入了大量的开销。那么就需要提供一种高效的密钥管理方案。

发明内容

[0005] 本发明涉及一种用于管理加密密钥并使接收机能够将与所需质量相对应的增强层中的全部片段解密,同时使消费者依旧无法访问所有其它片段的方法。本发明集中研究以对补充流进行高效加密和解密为目标的密钥管理系统。

[0006] 其特别适用于MPEG4 FGS领域,但是更一般地也适用于传输加密编码帧的其它领域。

[0007] 为了达到该目的,本发明涉及一种用于对由发射机向接收机发送的已编码的可伸缩增强帧的加密的方法,该增强帧包括多个按照质量级别排序的补充流,每个补充流与多于一个可伸缩性类型的组合相对应,其中较低质量级别的补充流与每个可伸缩性类型的较低质量相对应,所述方法在发射机级别包括以下步骤:为每个补充流生成用于对该补充流进行加密的密钥,使得所有可伸缩性类型可以同时或者单独使用;所述密钥的生成使得仅可以根据补充流的密钥获得低于所述补充流质量级别的质量级别的补充流的密钥;以及向

接收机发送与质量级别相对应的补充流的密钥，该密钥允许接收机仅生成较低质量级别的补充流的密钥。

[0008] 本发明提供了期望特性，如高安全性、低复杂度、以及低数据开销。对于加密方案及其相关的密钥管理系统，具有高安全性是最基本的；尽管如此这一般是以复杂度和数据开销为代价而实现的。低复杂度方法是使用尽可能少的密钥，短密钥尺寸并且甚至可以与计算能力有限的设备一同工作的方法。低数据开销意味着不以“加扰流”增加巨大开销的方法。密钥生成过程允许根据单个密钥生成全部后续的密钥。服务器仅需要向接收机发送一个密钥，使得接收机推断出允许的密钥。这要求极少的数据开销。

[0009] 根据一实施例，该方法包括以下步骤：在发送与质量级别相对应的补充流的密钥之前，接收来自接收机的、对所述质量级别的流接收 的请求。

[0010] 根据一实施例，为每个补充流生成密钥的步骤包括以下步骤：生成较高质量级别的补充流的随机密钥；以及通过对该随机密钥连续地应用至少单向置换算法，来获得较低质量级别的补充流的密钥。

[0011] 单个函数允许生成全部的后续密钥。这要求极少的计算资源。

[0012] 特别地，在第一可伸缩性以及第二可伸缩性两个可伸缩性类型的组合中，获取针对给定的第一可伸缩性级别的较低质量级别的补充流的密钥的步骤包括以下步骤：将一级别的密钥划分成左部和右部；对密钥的右部应用单向置换算法；以及将密钥的左部与获取到的右部连接 (concatenating)，以获得较低质量级别的密钥。

[0013] 类似地，在第一可伸缩性以及第二可伸缩性两个可伸缩性类型的组合中，获取针对给定的第二伸缩性级别的较低质量级别的补充流的密钥的步骤包括以下步骤：将一级别的密钥划分成左部和右部；对密钥的左部应用单向置换算法；以及将获取到的右部与密钥的左部连接，以获得较低质量级别的密钥。

[0014] 本发明还涉及一种用于计算解密密钥以对已编码的可伸缩增强帧进行解密的方法，其中增强帧包括多个按照质量级别排序的补充流，每个补充流与多于一个可伸缩性类型的组合相对应，其中较低质量级别的补充流与每个可伸缩性类型的较低质量相对应，所述方法在接收机级别包括以下步骤：接收与所需质量级别相对应的补充流的密钥；以及根据接收到的密钥仅生成与较低质量级别相对应的补充流的后续密钥。

[0015] 接收机不需要接收针对全部补充流的全部密钥。其仅接收允许生成授权密钥的唯一密钥。

[0016] 根据一实施例，该方法包括接收补充流的密钥的步骤，该方法包括：指示所述所需质量级别的流接收的步骤。

[0017] 根据一实施例，生成后续密钥的步骤包括：连续地对接收到的密钥应用单向置换算法的步骤。

[0018] 本发明还涉及一种用于对已编码的可伸缩增强帧进行加密的设备，其中增强帧包括多个按照质量级别排序的补充流，每个补充流与 多于一个可伸缩性类型的组合相对应，其中较低质量级别的补充流与每个可伸缩性类型的较低质量相对应，该设备包括：加密装置，用于生成较高质量级别的补充流的随机密钥，并通过对该随机密钥连续应用至少单向置换算法来生成较低质量级别的补充流的密钥。

[0019] 本发明还涉及一种用于对已编码的可伸缩增强帧进行解密的设备，其中增强帧包

括多个按照质量级别进行排序的补充流，每个补充流与多于一个可伸缩性类型的组合相对应，其中较低质量级别的补充流与每个可伸缩性类型的较低质量相对应，该设备包括：解密装置，用于根据接收到的密钥仅生成与较低质量级别相对应的补充流的后续密钥。

[0020] 本发明的另一个目的是一种计算机程序产品，该计算机程序产品包括：程序代码指令，用于当在计算机上执行该程序时，执行根据本发明的过程的步骤。此处的“计算机程序产品”意味着计算机程序支持，其可以不仅存在于包含程序的存储空间中，还存在于信号（例如电或者光信号）中。

附图说明

[0021] 通过下面的以非限制方式参考附图的实施例和执行示例，本发明将得到更好的理解以及说明，附图中：

[0022] 图 1 示出了被划分为基本流和两个补充流的流；

[0023] 图 2 示出了对可伸缩的已编码补充流的加密；

[0024] 图 3 示出了可伸缩增强层；

[0025] 图 4 示出了在增强层中使用可伸缩性的不同模式；

[0026] 图 5 示出了用于加密和解密的方法的流程图；以及

[0027] 图 6 示出了实施例的系统。

[0028] 在图 6 中，所示出的块是纯功能实体，其不必对应于物理上分离的实体。即，它们可以以软件的形式进行开发，或者用一个或几个集成电路来实现。

[0029] 具体实施方式

[0030] 示例实施例属于 MPEG-4 FGS 的框架，但是本发明并不限于这个特定环境，并且可以应用于其它传输加密编码帧集合的框架中。

[0031] 存在多种将所传输的数字服务分离为不同组件的方法；这些组件借助于客户端特定流予以传输。例如，可以使用增量编码器，增量编码器对服务或者后者的组件（例如视频）以小带宽“第一”流（又称基本流）以及补充流的形式进行编码。在级别降低了的传输模式下，基本流一般足以实现服务的还原。基本流始终可以独立地进行解码。就视频而言，该基本服务可以包含低分辨率版本的视频。对于音频来说也是一样的。补充流发送基本流中缺失的信息，使得能够以非降级模式恢复服务。补充流仅可以与较低的流一起进行解码。

[0032] 图 1 中示出了这样的服务，或者至少其视频组件。完整视频 1 被分解为第一基本流 1.1 以及可伸缩增强层，可伸缩增强层包括两个被标记为 1.2 和 1.3 的补充流。基本流使得可以将视频以第一低分辨率进行复原。基本流以及补充流 1 的解码使得可以将视频恢复至中间分辨率。三个流的解码使得可以以完整视频的最佳分辨率来恢复完整视频。

[0033] 实际上，补充流编码是可伸缩的，反之基本流编码一般是不可伸缩的。在加密方面，一个密钥足以对基本层进行加密并且不需要针对基本流的密钥管理方案。需要几个密钥以对补充流进行加密，并且通常需要密钥管理方案。图 2 示出了可伸缩编码补充流的加密。实施例提出了一种方案，该方案允许将可伸缩的编码补充流 2.1 加密为加密补充流 2.2，其中这些经加密的流保持可伸缩性。对明码视频部分 2.1 应用加密 2.3 以提供加密视频部分。

[0034] MPEG-4 FGS 编码定义于 MPEG4- 第 2 部分 ISO/IEC 14496-2 :2003 标准。在 FGS 中，数据流被编码以及压缩为两层 :基本层（非可伸缩部分）以及增强层（可伸缩部分）。如果仅对基本层进行解码，这将导致原始内容的低质量版本。尽管如此，如果对增强层的部分进行解码并且将其与基本层组合，这将生成改善质量的内容，所改善的质量与经解码的增强部分成正比。此外，增强层同时支持 PSNR 以及时间可伸缩性。图 3 是示出了这样的服务的框图，其中完整视频被分解成图中未示出的基本层以及可伸缩增强层 3.2，可伸缩增强层 3.2 基于两个可伸 缩性 (PSNR 3.3 以及比特率 3.4) 包括多个补充流。每个增强层被独立地划分为 T 个 PSNR 级别以及 M 个比特率级别。那么增强层由 M*T 个不同的片段（或者补充流）构成。在图 3 中，T ＝ 3，M ＝ 5，并且每个片段 $S_{m,t}$ 位于一个 PSNR 级别和一个比特率级别的交叉位置，其中 m 属于 {1，...，M}，t 属于 {1，...，T}。

[0035] MPEG-4FGS 内容质量可以同时依赖于时间可伸缩性比特率以及 PSNR 可伸缩性。针对所请求的质量，内容提供方可以仅使用比特率，仅使用 PSNR 层而针对比特率保持相同级别，或者通过同时使用 PSNR 以及比特率层来允许对特定级别层进行访问。所以，存在可以获得相同内容质量的三种模式。图 4 示出这点，其中图 4 示出了与图 3 中所示的框图类型相同的框图类型。在 4.1 中，仅使用了比特率可伸缩性而针对 PSNR 保持相同级别。在 4.2 中，仅使用了 PSNR 可伸缩性而针对比特率保持相同级别。在 4.3 中，同时使用了两种可伸缩性。对两种可伸缩性的使用允许仅向用户提供对于行或者列中的一些片段的访问，而不需要允许对行或者列中的全部片段进行访问。实际上，内容提供方可以向消费者提供对片段 S1，1、S2，1、S3，1、S1，2、S2，2、S3，2 的访问，同时保持使消费者无法访问例如 S4，1、S5，1、S4，2、S5，2。在 4.1 和 4.2 中，当仅使用一种类型的可伸缩性，如果消费者有权访问给定质量类型的层中的一个片段，那么他有权访问该层中全部片段。在 4.1 中，消费者有权访问第 2 级别的比特率，因此如 4.1.1 所示有权访问在比特率为第 2 级别以及第 2 级别以下的层中的任意片段。在 4.2 中，消费者有权访问第 2 级别的 PSNR，因此如 4.2.1 所示有权访问在 PSNR 为第 2 级别以及第 2 级别以下的层中的任意片段。

[0036] 实施例的加密方案允许使用这三种模式来访问经加密的增强层。该加密方案允许以加密片段维持可伸缩性。为了能够使用可伸缩性，不需要对增强层的任意片段进行解密。此时，密钥管理是灵活的，并且可以用经加密的内容完全利用 MPEG4 FGS 的可伸缩性。所有可伸缩性类型可以同时或者单独使用。

[0037] 可伸缩多层 FGS 加密分层访问控制方案（记为 SMLFE）针对 MPEG-4 FGS 编码支持 PSNR 以及比特率可伸缩性。SMLFE 定义于文献 C.Yuan，B.B.Zhu，M.Su，X.Wang，S.Li，以及 Y.Zhong 的“Layered AccessControl for MPEG-4 FGS Video”，IEEE 国际会议，图像处理，巴塞罗那，西班牙，2003 年 9 月，Vol.1，pp.517-520 中。在 SMLFE 中，增强层被加密为单个流，其中多个质量级别是依照于 PSNR 以及比特率值划分的。较低质量级别可以被相同可伸缩性类型的较高质量级别所访问以及重用，但是反之则不行。两种不同可伸缩性类型的保护是正交的，即，对一个可伸缩类型的级别进行访问的权利并不能使得可以对其它可伸缩性类型的级别进行访问。

[0038] 图 3 的每个片段用相应片段密钥 $K_{m,t}$（图中未示出）进行加密。在这样的情况下，随机生成 M*T 个密钥使得视频的发射机对全部片段进行加密。为了访问 MPEG-4 FGS 的压缩内容，不得不对这些密钥进行管理，并将它们发送至视频的接收机。

[0039] 下面描述根据实施例的对片段加密和解密的方法以及生成加密密钥的方法。在服务器或者发射机处执行编码和加密。在客户端或者视频的接收机处执行解码以及解密。

[0040] 如 SMLFE 的环境中那样，增强层由 M*T 个不同的片段构成。使用每个不同的密钥 $K_{m,t}$ 以对片段 $S_{m,t}$ 进行加密，其中 m 属于 {1,...,M} 并且 t 属于 {1,...,T}。$S_{M,T}$ 是针对两种可伸缩类型的较高质量的片段。

[0041] 在服务器中，首先随机生成密钥。该密钥对应于最高质量片段 $S_{M,T}$ 的密钥 $K_{M,T}$。该密钥被分成两半，左侧以及右侧。因此，与较低 PSNR 质量片段相关联的密钥是通过将密钥 $K_{M,T}$ 的左侧与密钥 $K_{M,T}$ 右侧的单向置换结果相连接来获得的。并且与较低比特率质量片段相关联的密钥是通过将左侧密钥 $K_{M,T}$ 的单向置换结果与右侧密钥 $K_{M,T}$ 相连接来获得的。以相同的方法重复执行该过程，直到计算出最低质量片段 $S_{1,1}$ 的加密密钥 $K_{1,1}$，从而获得全部密钥 $K_{m,t}$，其中 m = 1,...,M 并且 t = 1,...,T。

[0042] 明确地，令 h 代表单向置换。给定密钥 K，$h^n(K)$ 代表对 K 应用了 n 次单向置换 h 的结果。令 $K_{m,t}$ 表示增强层中的给定片段 $S_{m,t}$ 的加密密钥，该密钥由下列过程生成：

[0043] - 随机地生成 $K_{M,T} = (LK_{M,T}||RK_{M,T})$，其中 $LK_{M,T}$ 代表左侧密钥值，$RK_{M,T}$ 代表右侧密钥值，符号 || 代表连接。

[0044] - 计算差 M-m = x，以及 T-t = y。

[0045] - 使用下列密钥生成公式来产生密钥 $K_{m,t}$：

[0046] $K_{m,t} = (h^x(LK_{M,T})||h^y(RK_{M,T}))$

[0047] 在实施例中，密钥 $K_{m,t}$ 为 128 比特长，且 $h^x(LK_{M,T})$ 以及 $h^y(RK_{M,T})$ 为 64 比特长。

[0048] 为了避免针对不同的片段具有相同的片段密钥，$K_{M,T}$ 的右半部分的值应该与左半部分的值不同。否则就需要重新生成密钥 $K_{M,T}$ 直到得到合适的密钥。

[0049] 回到图 3 中所示的片段，$S_{5,3}$ 是同时针对 PSNR 以及比特率可伸缩性的最高质量的片段。

[0050] 首先，随机地生成相关联的片段密钥 $K_{5,3}$。

[0051] 其次，将该密钥划分为两半 $K_{5,3} = (LK_{5,3}||RK_{5,3})$，并且使用单向置换 h 对其进行处理，以获得全部其它密钥。

[0052] 表 1 示出了如何用上面定义的密钥生成公式获得全部其它片段密钥。

[0053]

级 别	t = 1	t = 2	t = 3
m = 1	$K_{1,1} = (h^4(L_{K5.3}) \| h^2(R_{K5.3}))$	$K_{1,2} = (h^4(L_{K5.3}) \| h(R_{K5.3}))$	$K_{1,3} = (h^4(L_{K5.3}) \| R_{K5.3})$
m = 2	$K_{2,1} = (h^3(L_{K5.3}) \| h^2(R_{K5.3}))$	$K_{2,2} = (h^3(L_{K5.3}) \| h(R_{K5.3}))$	$K_{2,3} = (h^3(L_{K5.3}) \| R_{K5.3})$
m = 3	$K_{3,1} = (h^2(L_{K5.3}) \| h^2(R_{K5.3}))$	$K_{3,2} = (h^2(L_{K5.3}) \| h(R_{K5.3}))$	$K_{3,3} = (h^2(L_{K5.3}) \| R_{K5.3})$
m = 4	$K_{4,1} = (h(L_{K5.3}) \| h^2(R_{K5.3}))$	$K_{4,2} = (h(L_{K5.3}) \| h(R_{K5.3}))$	$K_{4,3} = (h(L_{K5.3}) \| R_{K5.3})$
m = 5	$K_{5,1} = (L_{K5.3} \| h^2(R_{K5.3}))$	$K_{5,2} = (L_{K5.3} \| h(R_{K5.3}))$	$K_{5,3} = (L_{K5.3} \| R_{K5.3})$

[0054] 表 1

[0055] 当接收机获得了对于具有特定质量的内容的权利时，发射机计算与所请求质量的最高质量片段相关联的密钥并且将其发送至接收机。 假定该最高质量片段是具有与其相关联的密钥 $K_{3,2}$ 的 $S_{3,2}$。差 M-m = 5-3 以及 T-t = 3-2 分别等于 2 和 1。片段密钥 $K_{3,2} = (h^2(LK_{5,3})||h(RK_{5,3}))$ 是由发射机使用上述定义的密钥生成公式以及单向置换算法根据 $K_{5,3}$ 计算得出的片段密钥。$K_{3,2}$ 被发送至接收机。在接收机处，可访问片段是图 3 中 3.1 所示的 $S_{3,2}$、$S_{3,1}$、$S_{2,2}$、$S_{2,1}$、$S_{1,2}$ 以及 $S_{1,1}$。即，如果最高质量片段是 $S_{m,t}$，则可访问片段是 $S_{u,v}$，其中 $1 \leqslant u \leqslant m$ 并且 $1 \leqslant v \leqslant t$。

[0056] 接收机接收到 $K_{3,2}$ 并且 $K_{3,2}$ 被分为两半 $LK_{3,2}$ 以及 $RK_{3,2}$。然后，通过对 $LK_{3,2}$ 以及 $RK_{3,2}$ 进行散列以及连接获得片段密钥 $K_{3,1}$、$K_{2,2}$、$K_{2,1}$、$K_{1,2}$ 以及 $K_{1,1}$。这可以通过使用与发射机所用的单向置换算法相同的单向置换算法来完成。重复执行该过程直到计算出所有片段密钥位置。根据 $K_{3,2}$ 获得的计算出的密钥如表 2 所示。

[0057]

级别	t = 1	t = 2
m = 1	$K_{1,1} = (h(LK_{2,2})\|\|h(RK_{2,2})) = (h^2(LK_{3,2})\|\|h(RK_{3,2}))$	$K_{1,2} = (h(LK_{2,2})\|\|RK_{2,2}) = (h^2(LK_{3,2})\|\|h(RK_{3,2}))$
m = 2	$K_{2,1} = (h(LK_{3,2})\|\|h(RK_{3,2}))$	$K_{2,2} = (h(LK_{3,2})\|\|RK_{3,2})$
m = 3	$K_{3,1} = (LK_{3,2}\|\|h(RK_{3,2}))$	$K_{3,2}$

[0058] 表 2

[0059] 通过分别对片段密钥的右侧或者左侧进行散列，访问一质量级别的权利还提供了访问针对不同 PSNR 或者比特率可伸缩性的低质量级别的权利。由于散列函数的单向标准，以及散列函数并非单射的事实，较高质量级别是不可访问的。如果最高质量片段是 $S_{m,t}$，则片段 $S_{u,v}$，其中 $m < u$ 或者 $t < v$ 不可访问。密钥管理方案的安全性基本上依赖于散列函数的选择以及健壮性。

[0060] 图 5 中总结了用于加密以及解密的方法。

[0061] 步骤 S1。服务器生成随机密钥以及根据随机密钥生成的后续密钥。

[0062] 步骤 S2。接收机发送接收某质量级别的内容的请求。服务器接收该请求并且推断出最高质量的匹配片段。

[0063] 步骤 S3。服务器向接收机发送与最高质量的匹配片段相对应的密钥。

[0064] 步骤 S4。接收机接收到该密钥，并且生成对应于可访问片段的密钥。

[0065] 如上所述，对每侧使用唯一的单向置换函数。取而代之地，可以针对右侧以及左侧使用不同的单向置换。则用 h1 以及 h2 函数表示，密钥生成的公式将是 :$K_{m,t} = (h1^x(LK_{M,T})||h2^y(RK_{M,T}))$。

[0066] 在实施例中，$K_{M,T}$ 是用 $LK_{M,T}$ 以及 $RK_{M,T}$ 连接起来得到的，其中 $LK_{M,T}$ 代表左侧密钥值，$RK_{M,T}$ 代表右侧密钥值。可选地，$LK_{M,T}$ 可以代表 $K_{M,T}$ 的偶数比特位并且 $RK_{M,T}$ 代表 $K_{M,T}$ 的奇数比特位。

[0067] 单向置换是沿一个方向计算比沿相反方向计算容易得多的函数 ;即，如果输出是通过对输入进行单向置换得到的，那么不容易根据给定的输出得到输入。例如，可以用几秒钟沿前向计算该函数，但是计算其反向则可能要花费数月或者数年（如果可以计算的话）。可以使用多种单向置换算法 :

[0068] - 本领域所熟知的散列函数，诸如 MD5、RIPEMD-160 或者 SHA1。

[0069] - 本领域所熟知的伪随机数发生器（记为 PRNG），诸如马其赛特旋转 (Mersenne Twister)、ISAAC 等。将片段密钥，或者片段密钥的一部分，用作 PRNG 的种子，h(K) = PRNG(K)。可以将输出截断以适应预定义的尺寸。

[0070] - 对称密码：块密码或者流密码，诸如 DES 或者 RC4。对称密码需要两个输入（消息以及密钥），但是当用作单向置换时，两个输入可以是相同的。在本发明中，当对片段密钥 K 应用对称密码时，K 被同时作为所要加密的消息以及用于加密的密钥二者来使用。在该情况下 $h(K) = E_{\{K\}}(K)$。

[0071] - 离散对数或者公钥加密算法 RSA：

[0072] - 关于离散对数，选择乘法群 Z^*_p 的生成元 g，其中 p 是一个大素数。通过用较高质量片段密钥的值对 g 求幂然后（模 p）获得与较低质量片段相关联的片段密钥。在该情况下 $h(K) = g^K \bmod p$。

[0073] - 关于 RSA，生成公共值 (e，n)，其中 n 是两个素数的乘积并且 e 是公共指数（私钥被丢弃）。通过对较高质量片段密钥 K 用公共指数 e 求幂（模 n）来获得与较低质量片段相关联的片段密钥。在该情况下 $h(K) = K^e \bmod n$。

[0074] 置换所需要的属性仅仅是单向标准。例如，对于 MD5，可能存在一些冲突，该现象不会对安全性造成任何后果。

[0075] 实施例涉及同时支持 PSNR 以及比特率可伸缩性的增强层。实际上，其适用于多于两个的可伸缩性。当有 N 个可伸缩性时，被传输的密钥 $K_{M,T}$ 被分为 N 部分，并且对每个部分连续地使用单向置换以生成后续的密钥。

[0076] 图 6 示出了本实施例的系统，包括：服务器 5.1（也称作发送器）、通过网络 5.3 连接至服务器的客户端 5.2（也称作接收机）。服务器向客户端发送加密的视频内容。例如，网络是因特网。服务器是视频的发射机。客户端是视频的接收机。

[0077] 服务器包括用于对流进行压缩并生成根据实施例的基本层和后续增强层的装置 5.1.5。还包括用于生成根据实施例的加密密钥和对片段进行加密的加密装置 5.1.2。包括用于通过网络向客户端发送流的通信装置 5.1.3。服务器包括处理装置 5.1.1 以及用于存储运行压缩算法和加密算法的程序的存储装置 5.1.4。服务器包括用于在内部传输数据的内部总线 5.1.6。

[0078] 客户端包括用于对流进行解压缩的解压缩装置 5.2.5。其包括用于生成根据实施例的加密密钥以及对加密的片段进行解密的解密装置 5.2.2。其包括用于通过网络从服务器接收流的通信装置 5.2.3。客户端包括处理装置 5.2.1 以及用于存储运行解压缩算法和解密算法的程序的存储装置 5.2.4。客户端包括用于在内部传输数据的内部总线 5.2.6。

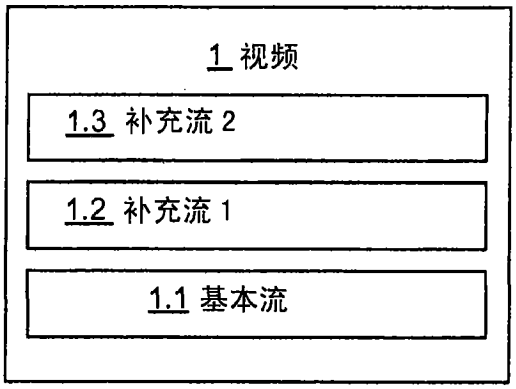

1 视频
1.3 补充流 2
1.2 补充流 1
1.1 基本流

图 1

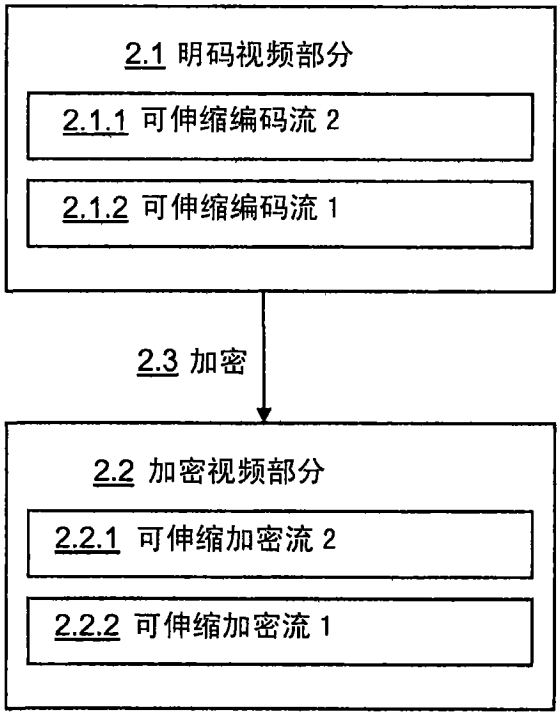

2.1 明码视频部分
2.1.1 可伸缩编码流 2
2.1.2 可伸缩编码流 1
2.3 加密
2.2 加密视频部分
2.2.1 可伸缩加密流 2
2.2.2 可伸缩加密流 1

图 2

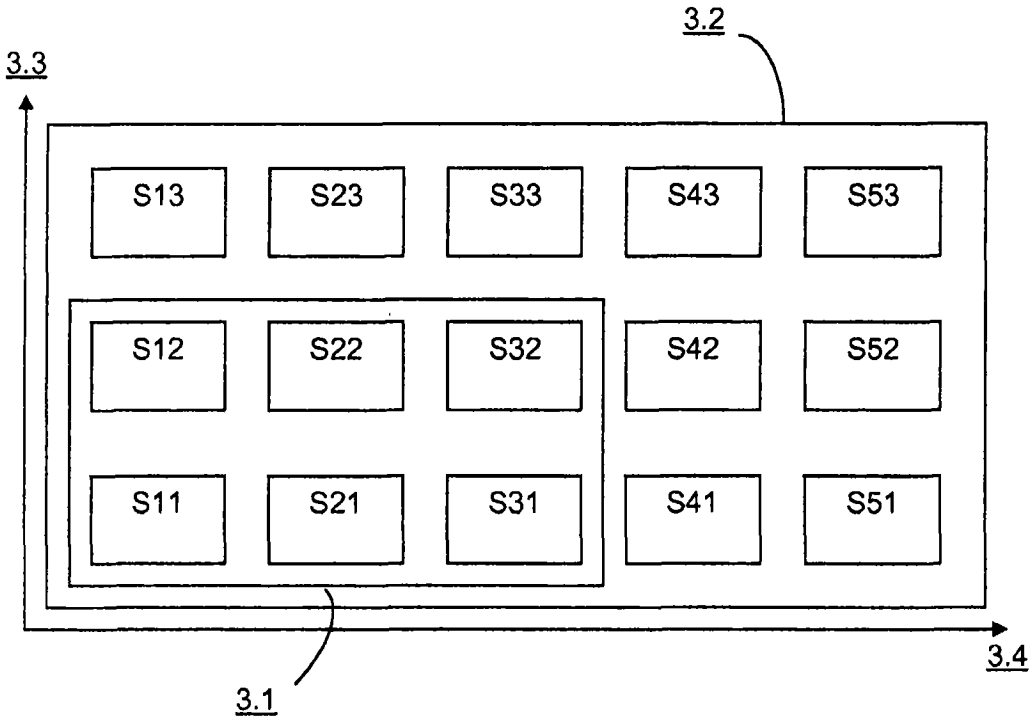

3.2
3.3
S13
S23
S33
S43
S53
S12
S22
S32
S42
S52
S11
S21
S31
S41
S51
3.4
3.1

图 3

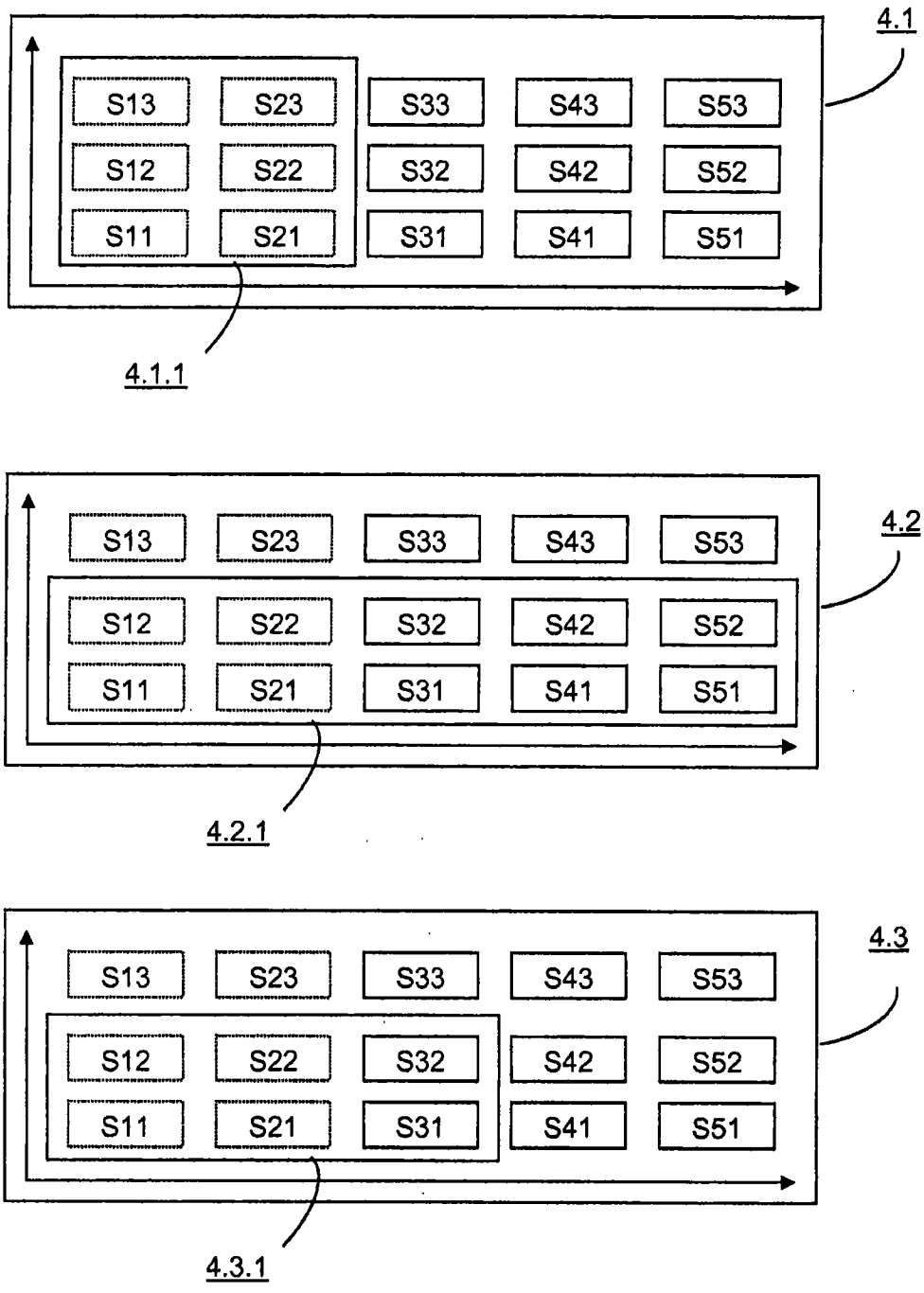

4.1
S13
S23
S33
S43
S53
S12
S22
S32
S42
S52
S11
S21
S31
S41
S51
4.1.1
4.2
4.2.1
4.3
4.3.1

图 4

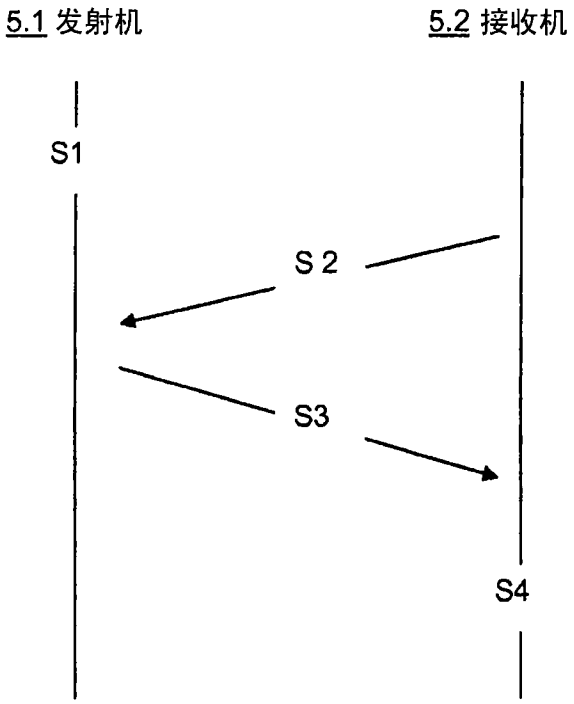


图 5

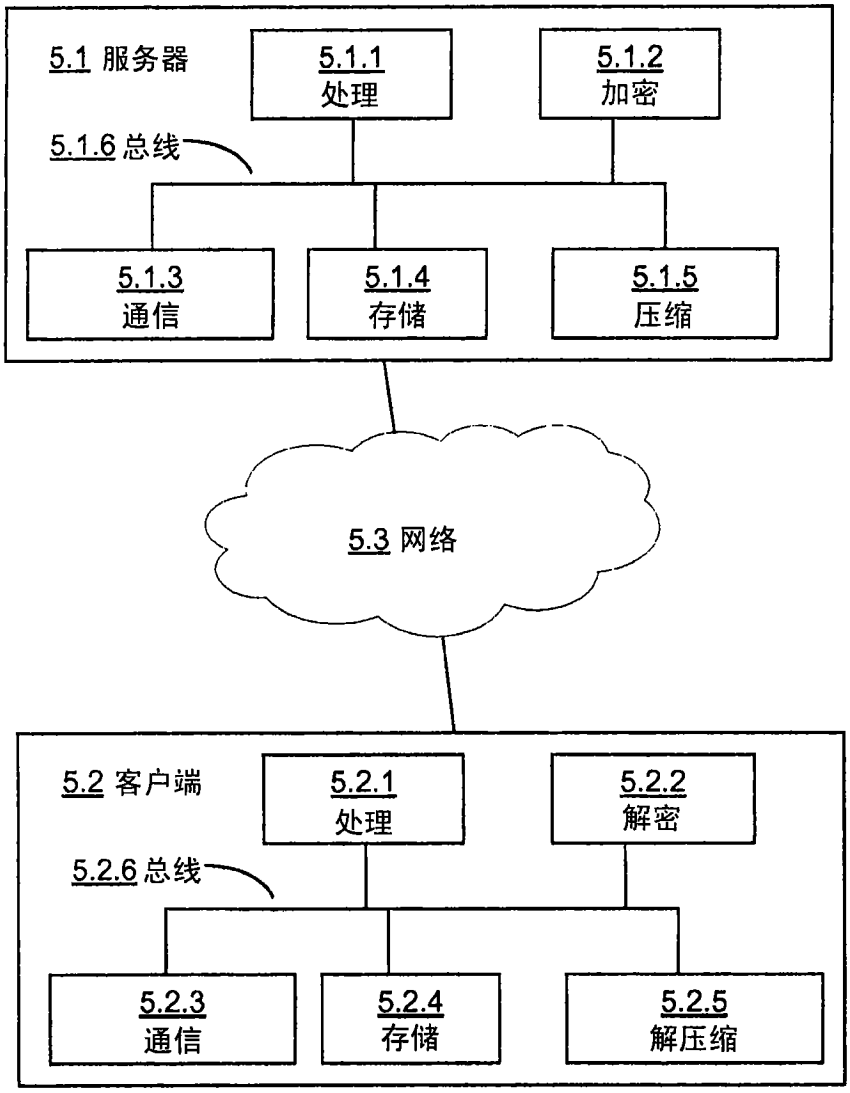

5.1 服务器
5.1.1 处理
5.1.2 加密
5.1.6 总线
5.1.3 通信
5.1.4 存储
5.1.5 压缩
5.3 网络
5.2 客户端
5.2.1 处理
5.2.2 解密
5.2.6 总线
5.2.3 通信
5.2.4 存储
5.2.5 解压缩

图 6