

[19] 中华人民共和国国家知识产权局



[12] 发明专利申请公布说明书

[21] 申请号 200610142490.4

[51] Int. Cl.

H04N 7/16 (2006.01)

H04N 7/26 (2006.01)

[43] 公开日 2007 年 5 月 2 日

[11] 公开号 CN 1956534A

[22] 申请日 2006.10.27

[21] 申请号 200610142490.4

[30] 优先权

[32] 2005.10.27 [33] KR [31] 10 - 2005 - 0101965

[71] 申请人 三星电子株式会社

地址 韩国京畿道水原市灵通区梅滩 3 洞 416

[72] 发明人 申成撤

[74] 专利代理机构 北京铭硕知识产权代理有限公司

代理人 郭鸿禧 常桂珍

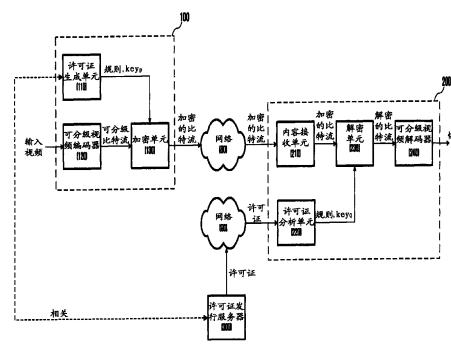
权利要求书 2 页 说明书 11 页 附图 6 页

[54] 发明名称

用于逐层管理多层多媒体流的版权的方法和设备

[57] 摘要

提供一种能够逐层管理多层视频比特流的版权的方法和设备。所述方法包括：根据输入视频生成可分级比特流，所述可分级比特流具有多层数据；生成加密密钥，每一加密密钥相应于所述多个层中的一个；和通过使用相应于所述层的加密密钥对每层数据加密来生成加密的可分级比特流。所述设备包括：可分级视频编码器，使用输入视频生成可分级比特流，所述可分级比特流具有多层数据；许可证生成单元，生成多个加密密钥，每一加密密钥相应于所述多个层中的一个；和加密单元，通过使用相应的加密密钥对相应于各个加密密钥的层数据加密来生成加密的可分级比特流。



1、一种逐层加密多层多媒体数据的方法，包括：

根据输入视频生成可分级比特流，所述可分级比特流具有多层数据；

对所述多个层生成多个加密密钥；和

通过使用相应于所述层的加密密钥对每层数据加密来生成加密的可分级比特流。

2、如权利要求1所述的方法，还包括：生成被应用于全部数据的规则。

3、如权利要求1所述的方法，还包括：生成多个秘密密钥，每一秘密密钥和相应的一个加密密钥形成一对密钥，其中，所述加密密钥是公钥。

4、如权利要求1所述的方法，其中，所述多个层包括基本层和至少一个增强层。

5、如权利要求1所述的方法，其中，所述数据包括运动数据和纹理数据。

6、如权利要求1所述的方法，其中，生成可分级比特流的步骤包括：

通过使用最低分辨率或帧率对输入视频下采样来生成基本层数据；

对下采样的输入视频进行编码；

通过使用比最低分辨率或帧率高的分辨率或帧率对输入视频下采样来生成增强层数据；

去除下采样的输入视频和基本层数据之间的冗余；和

对下采样的输入视频进行编码。

7、如权利要求3所述的方法，还包括：生成包括规则和秘密密钥的许可证，其中，所述许可证包括定义规则的字段、记录装置信息的字段、记录有关秘密密钥的密钥信息的字段。

8、一种逐层解密数据的方法，包括：

接收加密的可分级比特流；

分析许可证以提取包括在所述许可证中的相应于至少一个层的解密密钥；

使用提取的解密密钥，对加密的可分级比特流的属于与提取的解密密钥相应的层的数据进行解密；和

对包括解密的层的解密的比特流进行解码。

9、如权利要求8所述的方法，其中，通过普通公众可以访问的网络接收

所述加密的可分级比特流。

10、如权利要求 8 所述的方法，其中，所述解密密钥与基于公钥的加密算法中的秘密密钥相应。

11、如权利要求 8 所述的方法，其中，所述至少一个层包括基本层和至少一个增强层。

12、如权利要求 8 所述的方法，还包括：通过网络从许可证发行服务器接收许可证。

13、如权利要求 12 所述的方法，其中，所述许可证包括定义规则的字段、记录装置信息的字段、记录有关解密密钥的密钥信息的字段。

14、如权利要求 8 所述的方法，还包括：分析所述许可证以提取包括在所述许可证中的规则，并基于该规则控制对数据的解密。

15、如权利要求 8 所述的方法，其中，对解密的比特流解码的步骤包括：通过使用解密的比特流的基本层数据对相应于基本层级的视频解码；和通过使用与基本层级相应的视频和解密的比特流的增强层数据，对相应于增强层级的视频解码。

16、一种逐层加密数据的设备，包括：

可分级视频编码器，使用输入视频生成可分级比特流，所述可分级比特流具有多层数据；

许可证生成单元，生成多个加密密钥，每一加密密钥相应于所述多个层中的一个；和

加密单元，通过使用相应的加密密钥对与各个加密密钥相应的层数据进行加密来生成加密的可分级比特流。

17、一种逐层解密数据的设备，包括：

内容接收单元，接收加密的可分级比特流；

许可证分析单元，分析许可证以提取包括在所述许可证中的相应于至少一个层的解密密钥；

解密单元，使用提取的解密密钥，对加密的可分级比特流的属于与提取的解密密钥相应的层的数据进行解密；和

可分级视频解码器，对包括解密的层的解密的比特流进行解码。

用于逐层管理多层多媒体流的版权的方法和设备

本申请要求于 2005 年 10 月 27 日在韩国知识产权局提交的第 10-2005-0101965 号韩国专利申请的优先权，本申请完全公开于此，以资参考。

技术领域

与本发明一致的方法和设备涉及管理数字多媒体的版权，更具体地说，涉及逐层管理多层视频比特流的版权。

背景技术

随着包括互联网的信息通信技术的发展，视频通信以及文本和语音通信得到了快速发展。因为传统的文本通信不能满足用户的多种要求，所以对于能够提供诸如文本、画面、和音乐的多种类型的信息的多媒体服务的需求增加了。因为多媒体数据量通常很大，所以多媒体数据需要大容量的存储介质和用于传输的宽的带宽。例如，具有 640×480 分辨率的 24 位真彩色图像每帧需要 $640 \times 480 \times 24$ 比特，即，大约 7.37 M 比特数据的容量。当以每秒 30 帧的速度发送该图像时，需要 221 M 比特/秒的带宽，并且当存储基于该图像的 90 分钟的电影时，需要大约 1200 G 比特的存储空间。因此，对于发送包括文本、视频和音频的多媒体数据来说，压缩编码方法是必不可少的。

用于多媒体的不同类型的发送媒介具有不同的性能。当前使用的发送媒介具有多种发送率。例如，超高速通信网络每秒钟能够发送数十 M 比特的数据，而移动通信网络具有每秒 384 K 比特的发送率。而且，能够接收和播放多媒体数据的终端装置包括具有不同发送率的多种装置，例如大型计算机、个人计算机、DVD 播放器、PDA、移动电话、或其它装置，它们的性能彼此明显不同。

因此，当前正在发展一种可分级视频编码技术，以相应于变化的环境和发送率的需要，容易地从一个视频比特流获得分辨率、帧率或图像质量可调整的多种比特流。更具体地说，基于 H.264 编解码器的可分级视频编码正在被联合视频组(JVT)标准化，所述 JVT 是运动图像专家组(MPEG)和国际电信

联盟(ITU)之间的联合工作组。

另一方面，在保护创建多媒体内容的生产商的知识产权上，用于多媒体的数字版权管理(下文中称为“DRM”)技术正在变得普及。因为 DRM 技术在保护受版权保护的多媒体内容(例如音乐或电影、或其它相似媒体)上扮演重要的角色，所以市场上对 DRM 服务的需要大大增加。

理论上，多媒体加密算法具有高安全性、低复杂性、低压缩费用、错误适应性、和随机播放能力。安全性是多媒体加密所必需的。多媒体加密的特点在于，例如，和用于军事和金融应用的其它类型的加密相比较，将被加密的视频数据的量相对较大以及加密的信息的值通常较低。

预定的加密处理和解密处理需要不必要的处理费用，并且因此，低复杂性成为重要的问题。因为多媒体流具有相对大的数据量，所以低复杂性是优点，并且一些应用甚至要求低复杂性。

而且，因为加密降低了压缩算法的编码效率，或者通过将字节添加到已经压缩的文件而不可避免地影响了压缩效率，所以加密费用也是个问题。这时，如果多媒体加密算法的压缩费用被减少将是理想化的。

近年来，已经提出了许多考虑多媒体加密的特点的算法。然而，考虑到对一个内容的多种权利(例如，读取、复制、或转发)来应用这些算法。然而，如上所述，可分级比特流的特点在于：具有高质量的图像更靠近多个层的上层。因此，有必要逐层加密可分级比特流，并且根据终端装置的许可证权利，给予仅能解密相应层的权利。

发明内容

本发明的一方面提供一种通过将独立许可证授予多层多媒体流的每一层来控制多媒体内容的方法和设备。

然而，本发明的方面不局限于上述方面，通过下面的描述本领域的技术人员将会理解本发明的其它方面。

为了实现上述和其它方面，提供一种逐层加密数据的方法，该方法包括：从输入视频生成可分级比特流，该可分级比特流具有多层数据；生成多个加密密钥，每一加密密钥都相应于所述多个层之一；和通过使用相应于所述层的加密密钥对每层数据加密来生成加密的可分级比特流。

而且，根据本发明的另一方面，提供一种逐层解密数据的方法，该方法

包括：接收加密的可分级比特流；分析许可证以提取包括在该许可证中的与至少一个层相应的解密密钥；使用提取的解密密钥对加密的可分级比特流的属于与提取的解密密钥相应的层的数据解密；和对包括解密的层的解密的比特流解码。

而且，根据本发明的另一方面，提供一种用于逐层加密数据的设备，该设备包括：可分级视频编码器，通过使用输入视频生成可分级比特流，该可分级比特流具有多层数据；许可证生成单元，生成多个加密密钥，每一加密密钥都相应与所述多个层之一；和加密单元，通过使用相应的加密密钥对相应于各个加密密钥的层数据进行加密来生成加密的可分级比特流。

此外，根据本发明的另一方面，提供一种用于逐层解密数据的设备，该设备包括：内容接收单元，接收加密的可分级比特流；许可证分析单元，分析许可证以提取包括在该许可证中的与至少一个层相应的解密密钥；解密单元，使用提取的解密密钥对加密的可分级比特流的属于与提取的解密密钥相应的层的数据解密；和可分级视频解码器，对包括解密的层的解密的比特流解码。

附图说明

通过下面结合附图对特定示例性实施例进行的详细描述，本发明的上述和其它方面将会变得更加清楚，其中：

图 1 是示出根据本发明示例性实施例的数字版权管理系统的结构的示图；

图 2 是示出根据本发明示例性实施例的可分级视频编码器的结构的示图；

图 3 是示出根据本发明示例性实施例的可分级比特流的结构的示图；

图 4 是示出了图 3 中示出的可分级比特流的每一层数据的结构的示图；

图 5 是示意性地示出通过多种内容播放装置将加密的比特流解密的过程的示图；

图 6 是示出可分级视频解码器的结构的示图；和

图 7 是示出了本发明示例性实施例的全部操作的流程图。

具体实施方式

通过参照下面对示例性实施例和附图的详细描述，本发明的优点和特征以及实现本发明的优点和特征的方法将会更加容易理解。然而，可以以多种不同的形式来实现本发明的构思，而不是将本发明的构思解释为限于这里阐述的示例性实施例。而且，提供这些示例性实施例以便本公开是完整和全面的，并将本发明的构思完全传达给本领域技术人员，本发明仅由权利要求限定。在整个说明书中，相同的附图标记表示相同的部件。

下面将参照附图对本发明的构思做更完全的描述，在附图中示出了本发明的示例性实施例。

图 1 是示出了根据本发明示例性实施例的数字版权管理系统的整体结构的示图。所述数字版权管理系统包括：内容生成装置 100、内容播放装置 200、和许可证发行服务器 300。

内容生成装置 100 通过使用输入的原始视频生成可分级比特流，并根据图中“规则”指示的规则通过使用加密密钥集 key_p 逐数据层地对可分级比特流加密，从而生成加密的比特流，所述各个数据层形成可分级比特流，所述规则可以是预定的。为了实现这一目的，内容生成装置 100 包括许可证生成单元 110、可分级视频编码器 120、和加密单元 130。

许可证生成单元 110 生成将被应用于整个视频内容的规则和将被应用于各层数据的加密密钥集 key_p 。该规则指示应用于内容的权利。所述内容可以是预定的。在视频内容的情况下，所述规则指示根据多种操作而授予的权利，例如读取内容、在某一时间段内读取内容、读取内容一定的次数、和转发内容。所述时间段和次数都可以是预定的。例如，被授予了能够读取内容一次的权利的加密密钥可以使得相应内容仅被播放一次，并且被授予了两个小时内能够读取内容一次的权利的加密密钥可以在两个小时内使得相应内容被播放一次。因此，根据本发明示例性实施例，因为对于形成一个内容的每一层来说加密密钥独立存在，所以相应于层数的加密密钥(即，加密密钥集)关于一个规则独立存在，尽管通常是对一个规则存在一个相应的加密密钥。

此外，许可证生成单元 110 生成相应于加密密钥的解密密钥。在通常使用的公钥基础结构(PKI)算法中，创建包括公钥类型的加密密钥和私钥类型的解密密钥的一对密钥，通过使用加密密钥将数据加密，然后通过使用私钥将加密的数据解密。这种类型的算法被称为非对称加密，该算法基于如下原理：根据两个大的素数的乘积反过来计算这两个大的素数是很困难的。因此，即

使用公钥加密的数据被发送给的第三方根据该数据找出公钥，使用该公钥将该数据解密的可能性也很小。即，在非对称加密方法中，用公钥加密的数据只能通过秘密密钥解密，所述秘密密钥和公钥形成一对密钥。

然而，本发明的密钥创建方法不局限于非对称方法。例如，可以使用对称加密方法。在使用对称密钥时，加密密钥和解密密钥彼此相同。因此，如果第三方从加密的数据发现加密密钥，则可以通过该加密密钥将加密的数据解密。因此，在安全性方面，对称加密方法不如非对称加密方法。

可分级视频编码器 120 通过使用输入的视频(即，原始视频)生成可分级比特流。图 2 中示出了可分级视频编码器 120 的详细结构。

可分级视频编码器 120 包括多个(N 个)编码器 121、122、123、124 和熵编码单元 125，所述多个编码器 121、122、123、124 通过使用输入的视频创建各层数据，熵编码单元 125 对各层数据进行无损编码。编码器的数量可以是预定的。

首先，对基本层编码器 121 执行的操作进行描述。

以空间和/或时间方式对输入的视频画面进行下采样。然后，对下采样的视频画面执行运动估计处理。运动估计处理是通过参考相邻的参考画面而发现与当前画面相关的运动矢量的处理。通常，为了执行运动估计，块匹配算法被广泛使用。然而，也可以使用其它相似算法。

此后，通过使用获得的运动矢量对参考画面执行运动补偿，从而生成与当前画面相关的估计的画面。然后，通过使用当前画面和估计画面之间的差获得残差信号。

通过离散余弦变换(DCT)处理、小波变换处理、或相似处理将所述残差信号空间转化，然后将其转换以生成系数。然后，转换的系数被量化以具有量化步长的预定间隔。通过控制量化步长的大小，可以调整输出层数据的压缩率和图像质量。在量化步长的大小和图像质量之间进行平衡。通常，当量化步长的大小变大时，压缩率变大，图像质量降低。量化的结果，即，量化的系数和运动矢量从基本层编码器 121 输出。

第一增强层编码器 122 的基本操作和基本层编码器 121 的基本操作相同。然而，第一增强层编码器 122 在如下方面不同于基本层编码器 121：第一增强层编码器 122 通过使用较低层中的信息能够提高压缩效率，第一增强层编码器 122 中使用的量化步长略微小于基本层编码器 121 中使用的量化步长。

以同样的方式，第二增强层编码器 123 和第(N-1)增强层编码器 124 通过使用较低层(第一增强层)中的信息也能够提高数据压缩效率。

熵编码单元 125 对由相应编码器为每一层创建的各层数据进行无损编码以便创建比特流。诸如哈夫曼编码、算术编码、可变长度编码或其它相似方法的多种编码方法可以被用作无损编码方法。

图 3 是示出了根据本发明示例性实施例的可分级比特流 10 的结构的示图。可分级比特流 10 具有由多个层组成的数据结构。假定总共存在“N”个层，则可分级比特流 10 具有一个基本层数据和“N-1”个增强层数据。基本层可以被表示为 0(层 0)。通常，独立地创建(编码)基本层数据而无需参照其它层，而在参照另一层(通常是最接近的较低层)去除冗余后创建增强层。

在图 3 中，各层数据可以包括图 4 所示的运动数据和纹理数据。运动数据至少包括在运动估计处理期间创建的运动矢量，还可以包括宏块模式、参考画面的数量等。纹理数据是通过对从相应于各个层的编码器输出的量化系数进行无损编码而获得的结果。

换句话说，参照图 1，加密单元 130 通过使用许可证生成单元 110 基于特定加密算法而创建的加密密钥集对可分级比特流加密。所述特定加密算法可以是预定的。作为加密算法，可以使用任何一种通过使用公钥执行加密处理的传统算法。

由许可证生成单元 110 创建的加密密钥集包括“N”个加密密钥(P_0 到 P_{N-1})。因此，加密单元 130 通过使用“N”个加密密钥对图 2 中示出的可分级比特流 10 的各层数据进行加密。这里，加密密钥 P_k (k 为整数，可以是预定的)用于对相应于层 k 的层数据进行加密。

在加密单元 130 中被加密的比特流通过网络 80 被分发给多个终端装置 200。网络 80 优选为能够被普通公众容易地访问的因特网，但并不局限于此。

许可证发行服务器 300 响应终端装置而发行许可证，然后对许可证收取费用，所述许可证包括由许可证生成单元 110 创建的规则和加密密钥集。许可证发行服务器 300 通常和内容生成装置 100 相分离。然而，许可证发行服务器 300 可以和内容生成装置 100 的许可证生成单元 110 形成整体。

根据请求和付费情况，许可证可以包括不同的规则或者只提供与加密密钥集相应的解密密钥集中的一部分密钥。表 1 中示出了根据本发明示例性实施例的许可证。

在表 1 所示出的许可证中，规则是“播放一次”，还可以包括用于识别装置是否是能够使用许可证的特定装置的装置 ID，并且可以包括诸如所有者、标题、和长度的内容信息。具体地说，所述许可证包括至少一个用于将加密的比特流的相应层数据解密的解密密钥。在表 1 中，包括三个解密密钥 Q_0 、 Q_1 、 Q_2 ，这三个解密密钥 Q_0 、 Q_1 、 Q_2 分别是能够将基本层编码器、第一增强层编码器、第二增强层编码器中的数据解密的解密密钥。

表 1

规则	播放 1 次
装置信息	装置 ID
密钥信息	Q_0
	Q_1
	Q_2
内容信息	所有者、标题、长度等

内容播放装置 200 是通过网络 80 连接到内容生成装置 100 并通过网络 90 连接到许可证发行服务器 300 的终端装置。所述内容播放装置 200 表示能够被连接到网络和播放视频的装置，例如数字电视(TV)、计算机、个人数字助理(PDA)、移动电话、或便携式多媒体播放器(PMP)。所述装置可以是预定的。网络 90 可以是和网络 80 相同种类的网络。然而，和网络 80 可以被普通公众访问不同，因为在发送许可证时网络 90 要求比网络 80 更高的安全性，所以优选的，网络 90 是可以在安全性方面得到保证的网络。

内容播放装置 200 包括内容接收单元 210、许可证分析单元 220、解密单元 230 和可分级视频解码器 240。

内容接收单元 210 通过网络 80 接收编码的比特流并将接收的加密的比特流存储在存储单元中。所述存储单元可以是预定的。内容接收单元 210 具有相应于网络 80 的类型的接收调制解调器，所述调制解调器可以通过 IEEE 802.3 以太网卡、IEEE 802.11 串行接收卡、IEEE 802.15.3 串行接收卡或相似的调制解调器实现。所述存储单元可以通过 RAM 14、闪存、硬盘、或多种其它存储介质实现。

许可证分析单元 220 分析许可证发行服务器 300 提供的诸如表 1 中所示许可证的许可证，并提取图中“规则”表示的规则和解密密钥集 Key_Q 作为分析结果，并将其提供给解密单元 230。

解密单元 230 只将加密的比特流的层中与解密密钥集中包括的密钥相应的层解密，并将解密的比特流提供给可分级视频解码器 240。在使用非对称密钥方法的情况下，解密密钥是与内容生成装置 100 创建的加密密钥形成一对密钥的秘密密钥。另一方面，在使用对称密钥方法的情况下，解密密钥与内容生成装置 100 创建的加密密钥相同。

根据解密密钥集，解密的比特流可以是整个比特流或比特流的一部分。而且，解密单元 230 周期性地检查规则“规则”以确定相应的规则是否到期。如果相应规则到期，则解密单元 230 停止为可分级视频解码器 240 提供比特流。

图 5 是示出了在内容生成装置 100 中被用于各层的加密密钥 P_0 到 P_{N-1} 加密的比特流 150 如何被多个内容播放装置 200a、200b、200c 解密的示图。因为包括在许可证中的解密密钥为 Q_0 ，所以接收到各个层都被加密的比特流 150 的内容播放装置 200a 将基本层(层 0)中的视频数据解密。在内容播放装置 200a 是在处理能力、资源或显示能力方面不足的装置，例如，移动电话的情况下，有时候只有能够通过其仅将基本层解密的许可证就足够。

而且，在内容播放装置 200b 的情况下，因为包括在许可证中的解密密钥是 Q_0 和 Q_1 ，所以内容播放装置 200b 通过使用解密密钥 Q_0 和 Q_1 可以将基本层(层 0)和第一增强层(层 1)中的视频数据解密。通过将已经解密的基本层数据和第一增强层数据组合，内容播放装置 200b 能够获得具有与第一增强层级相应的质量的视频。

而且，在内容播放装置 200c 的情况下，可以获得与所有层数据相关的解密密钥 Q_0 到 Q_{N-1} ，然后可以通过使用解密密钥 Q_0 到 Q_{N-1} 将全部加密的比特流 150 解密。通过组合对各个层已经解密的全部数据，可以获得具有(N-1)增强层级，即，最高质量的视频。在内容播放装置 200c 是在处理能力、资源、或显示能力方面足够的装置，例如，数字电视或计算机的情况下，可以提供通过其将所有层解密的许可证。

被解密单元 230 解密的全部比特流或比特流的一部分被提供给可分级视频解码器 240，然后通过可分级视频解码器 240，将所述全部比特流或比特流的一部分作为解码的视频输出。

图 6 中示出了可分级视频解码器 240 的详细结构。

熵解码单元 241 对解密的比特流执行无损解码处理以便提取各层数据，

然后将提取的数据提供给相应的解码器 242 到 245。各层数据包括图 4 中示出的运动数据和纹理数据。

下面将对基本层解码器 242 执行的操作进行描述。

首先，通过逆量化处理将纹理数据逆量化。所述逆量化处理是与由编码器执行的量化处理相反的处理。即，所述逆量化处理是从指数类型的量化系数(量化级)将可用的系数解码的处理。

通过诸如逆 DCT 处理或逆小波变换处理的逆变换处理将解码的系数逆变换。作为逆变换的结果，与当前画面相关的残差信号被解码。

通过使用包括在运动数据中的运动矢量，对已经被解码的参考画面进行运动补偿，从而生成估计画面。最后，通过将估计画面和残差信号相加，相应于基本层级的画面被解码。这些画面聚集在一起形成一个视频。

在基本操作方面，第一增强层解码器 243 和基本层解码器 242 相同。然而，在如下方面第一增强层解码器 243 和基本层解码器 242 不同：与基本层解码器 242 不同，第一增强层解码器 243 通过使用较低层中的信息将相应于第一增强层级的视频解码。以同样的方式，第二增强层解码器 244 通过使用较低层(第一增强层)中的信息能够恢复相应于第二增强层级的视频。

如表 1 的例子所示，假定内容播放装置 200 具有三个解密密钥 Q_0 、 Q_1 、 Q_2 ，输入到可分级视频解码器 240 的加密比特流具有基本层、第一增强层、第二增强层。因此，这时，第二增强层解码器 244 的输出将成为最终视频输出。

通过使用被设计用来执行在本说明书中描述的功能的通用处理器、数字信号处理器(DSP)、专用集成电路(ASIC)、现场可编程门阵列(FPGA)、可编程逻辑单元、离散门或晶体管逻辑单元、离散硬件组件、或相似组件、或其任意组合，可以实现或执行参照示例性实施例描述的示例性逻辑块。所述通用处理器可以是微处理器。然而，选择性地，所述通用处理器可以是任意传统处理器、控制器、微控制器、或状态机。而且，可以通过计算装置的组合，例如，DSP 和微处理器、多个微处理器、至少一个与 DSP 核相关的微处理器的组合或任意其它组合来实现通用处理器。

图 7 是示出本发明示例性实施例的全部操作的流程图。首先，将对内容生成装置 100 执行的操作 S400 进行描述。

首先，可分级视频编码器 120 通过使用输入视频生成可分级比特流

(S410)，所述可分级比特流具有多层数据。所述多个层可以包括基本层和至少一个增强层，并且一个层中的数据可以包括运动数据和纹理数据。

操作 S410 可以被划分为如下处理：通过使用最低分辨率和/或帧率对输入视频下采样然后对下采样的输入视频进行编码来生成基本层数据的处理；和通过使用比最低分辨率和/或帧率高的分辨率和/或帧率对输入视频下采样然后在去除下采样的输入视频和基本层数据之间的冗余之后对下采样的输入视频编码来生成增强层数据的处理。

许可证生成单元 110 生成与层数相同数量的加密密钥(S420)。当加密方法基于非对称密钥时，加密密钥可以是公钥。还应该创建每一个都与相应加密密钥形成一对密钥的秘密密钥。

加密单元 130 通过用相应加密密钥对相应于每一加密密钥的层数据进行加密来生成加密的可分级比特流(S430)。操作 S400 还可以包括许可证生成单元 110 生成将被应用于全部多媒体数据的规则的处理。可通过可以被普通公众访问的网络来分发加密的可分级比特流(S440)。

许可证发行服务器 300 生成包括规则和秘密密钥的许可证(S500)，并响应内容播放装置的请求和随后的付费来提供所述许可证。所述许可证包括定义规则的字段、记录装置信息的字段、记录有关秘密密钥的密钥信息的字段。

现在对内容播放装置 200 执行的操作 S600 进行描述。

内容接收单元 210 接收并存储加密的可分级比特流(S610)。通过可以被普通公众访问的网络来进行所述接收操作。

许可证分析单元 220 分析由许可证发行服务器 300 发行的许可证(S620)，然后提取包括在许可证中的与至少一个层相应的解密密钥(S630)。所述许可证可以是预定的。当使用基于公钥的加密算法时，解密密钥相应于秘密密钥。

解密单元 230 通过使用提取的解密密钥对加密的可分级比特流的属于与提取的解密密钥相应的层的数据进行解密(S640)。

可分级视频解码器 240 对包括解密的层的解密的比特流进行解码(S650)。操作 S650 可以被划分为：通过使用属于基本层的数据来恢复解密的比特流的与基本层级相应的视频的处理；和通过使用与基本层级相应的视频和属于增强层的数据，来恢复解密的比特流的与增强层级相应的视频的处理。

上述操作 S600 还可以包括通过分析许可证提取包括在许可证中的规则的处理和基于所述规则控制解密处理的处理。

尽管参照多层视频流描述了本发明的示例性实施例，但是只要流包括多个层并且多个层之间的冗余被去除，则本发明的构思还可以应用于音频流、数据流或各种多媒体流。

如上所述，根据本发明示例性实施例，通过应用适合于可分级比特流的特性的加密方法，可以多种方式来使用多媒体内容。

尽管已参照本发明的示例性实施例描述了本发明的构思，但本领域技术人员应该理解，在不脱离本发明的精神和范围的情况下，可以对这些实施例进行各种修改和改变。因此，应该理解，上述示例性实施例在各方面是示例性的，而不是限制性的。

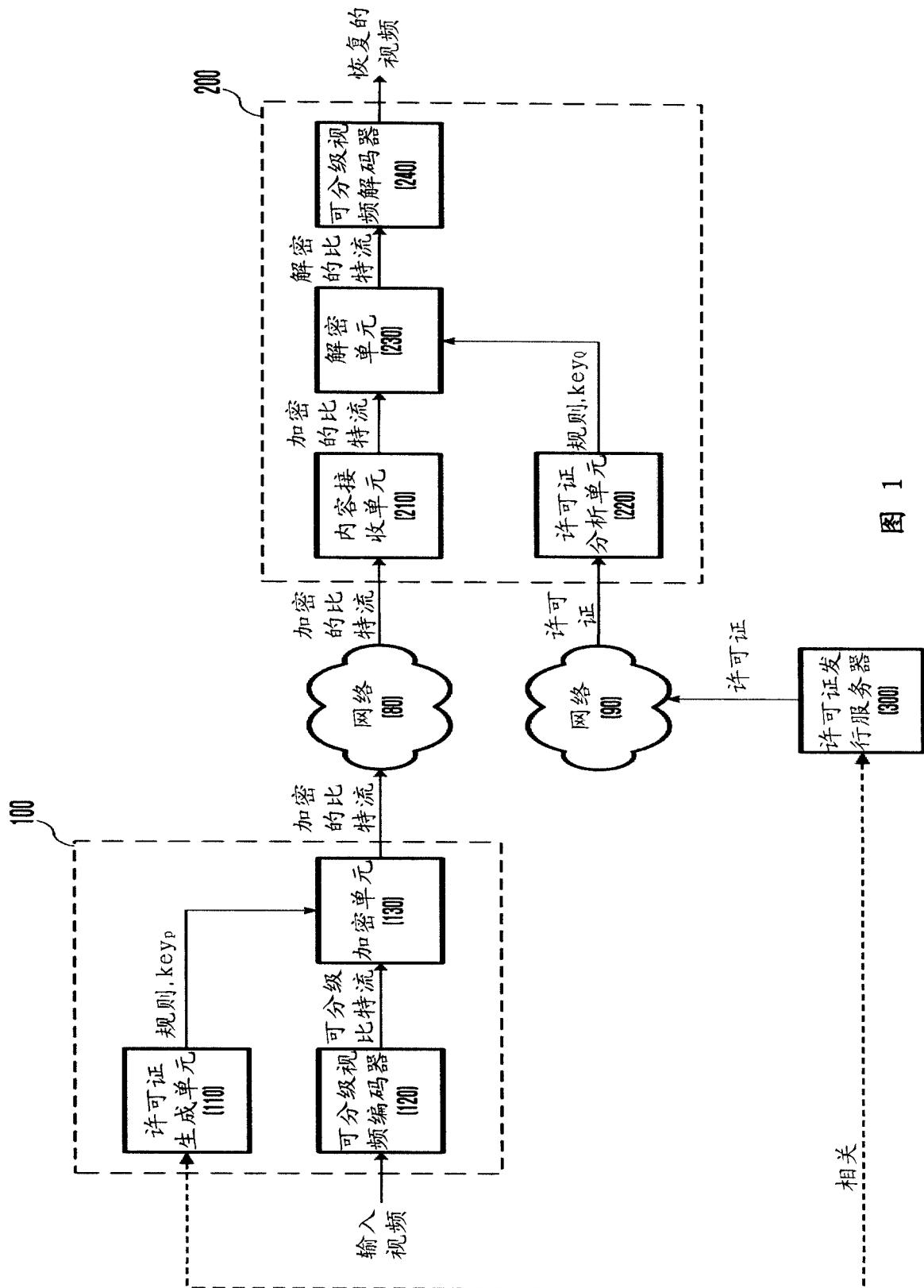


图 1

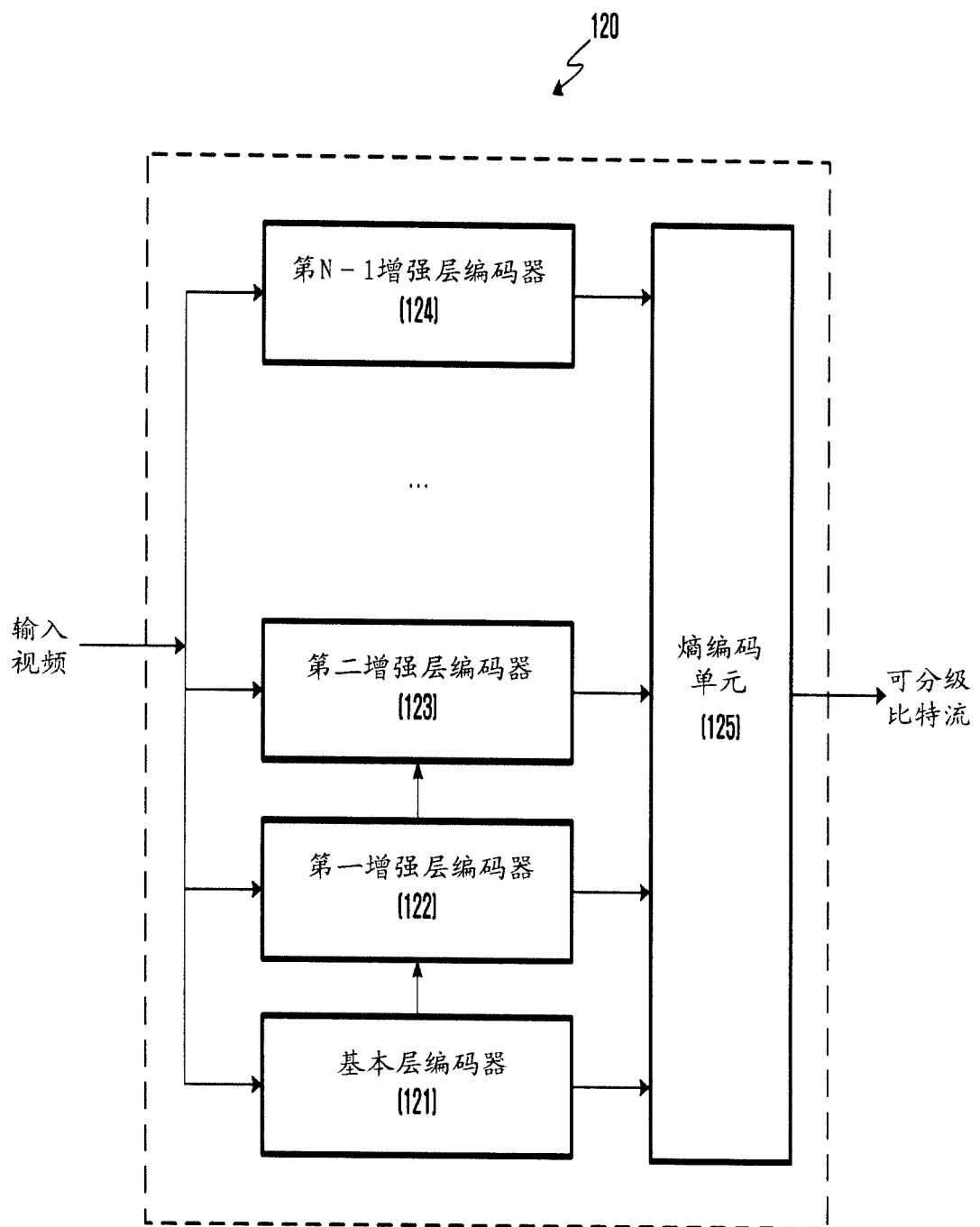


图 2

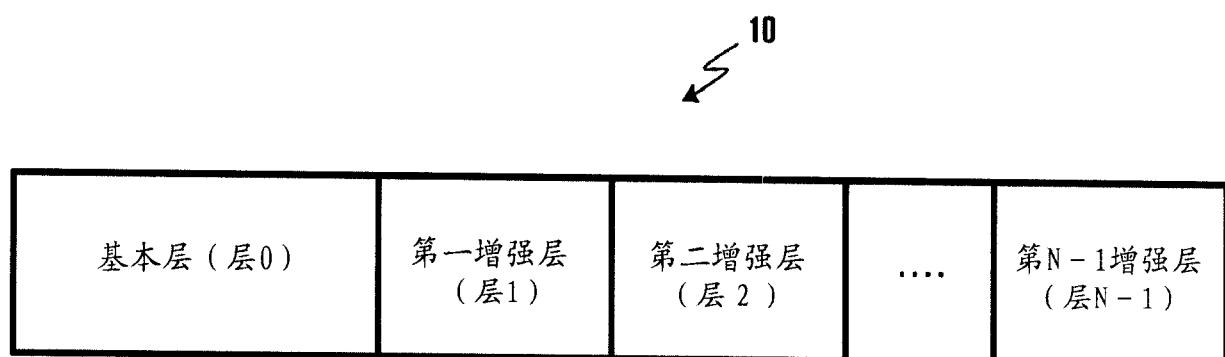


图 3

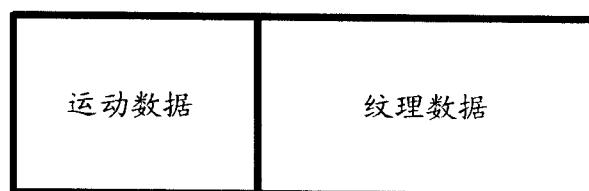


图 4

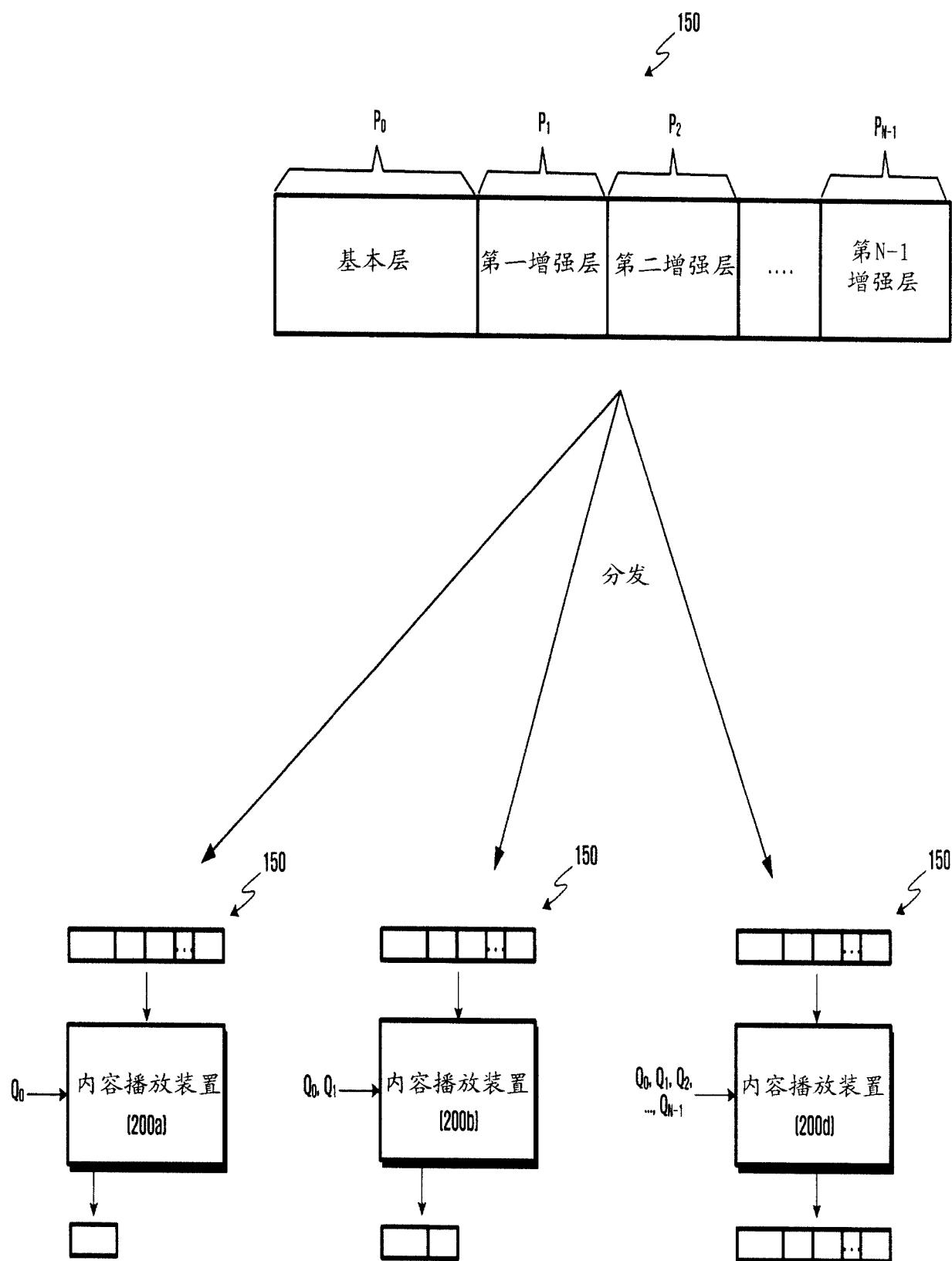


图 5

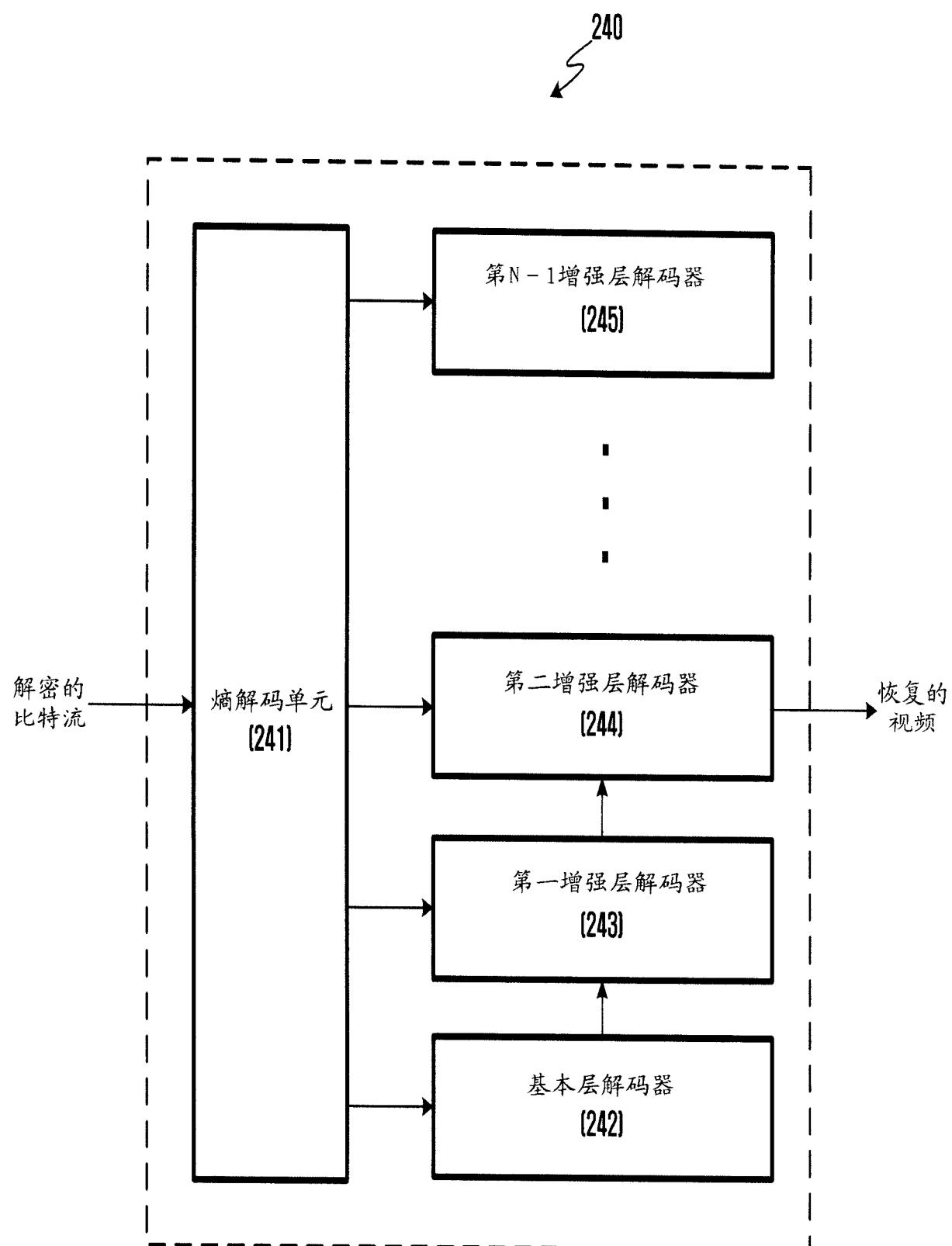


图 6

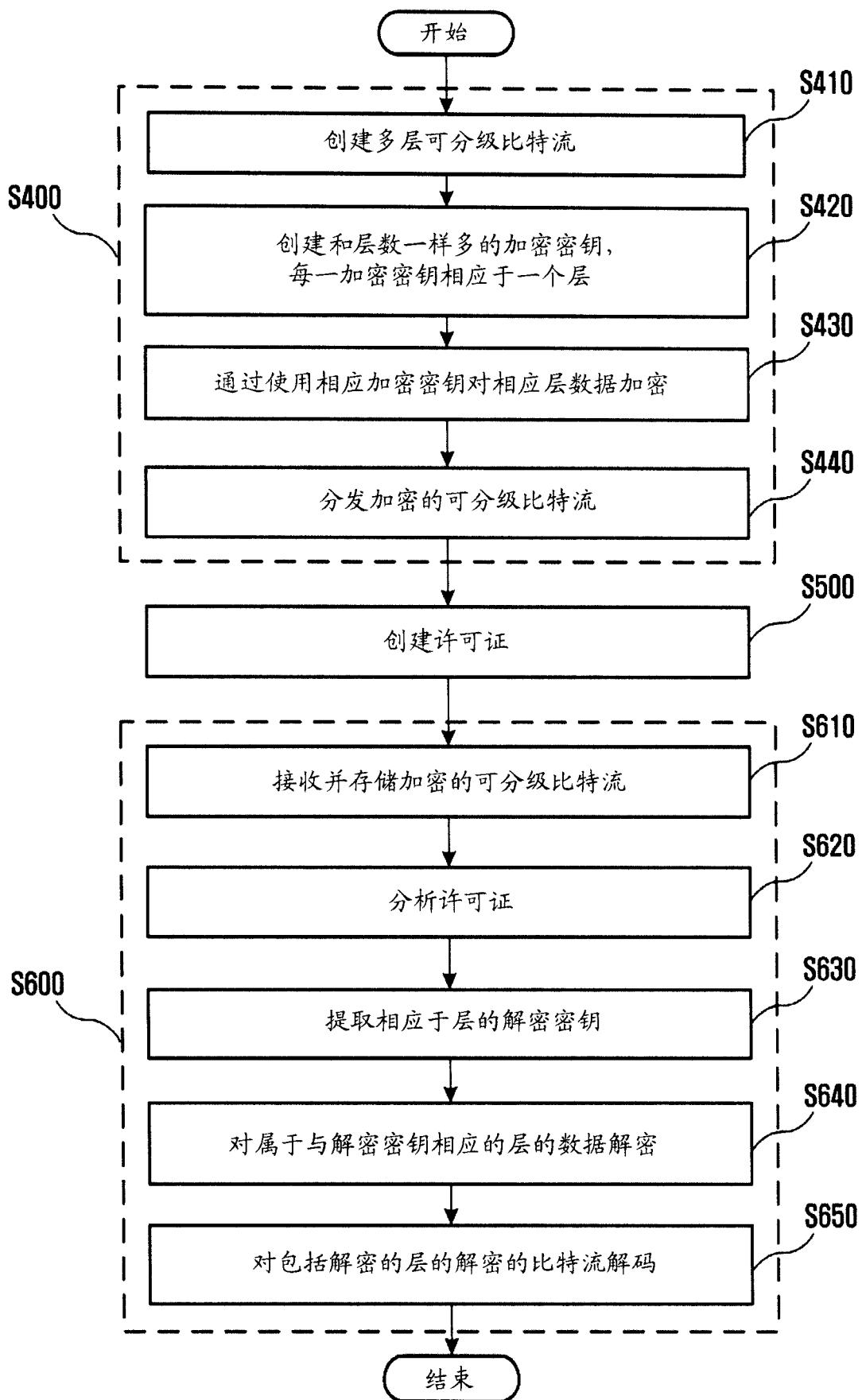


图 7