[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 29/06 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200580040302.0

[43] 公开日 2007 年 10 月 31 日

[11] 公开号 CN 101065944A

[22] 申请日 2005.11.21
[21] 申请号 200580040302.0
[30] 优先权
[32] 2004.11.24 [33] US [31] 60/630,670
[86] 国际申请 PCT/IB2005/053847 2005.11.21
[87] 国际公布 WO2006/056938 英 2006.6.1
[85] 进入国家阶段日期 2007.5.24
[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 S·V·R·古塔 M·巴比里
[74] 专利代理机构 中国专利代理(香港)有限公司
代理人 龚海军 刘 红

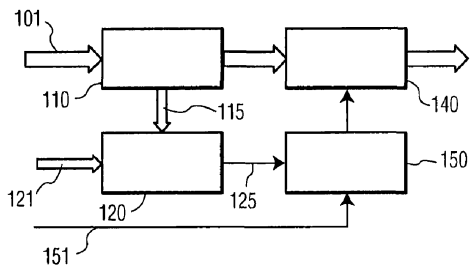
权利要求书 4 页 说明书 9 页 附图 1 页

[54] 发明名称

基于安全得分的译码/解密

[57] 摘要

一种安全系统，提供相应于接收的内容资料(101)被授权交付的可能性的安全得分(125)，并基于该安全得分(125)控制(250)资料的交付。 该安全得分(125)可以和与将被交付的资料相关联的安全标准(151)进行比较(240)，以便不同的资料实行不同的约束。 该安全得分(125)也可以控制(320)资料的交付的质量/保真度等级，以便，例如，仅在建立了提供复制认证的高等级信用度时，才提供资料的高保真度复制。



1、一种用于控制内容资料（101）的交付的方法，包括:

确定（230）与内容资料（101）相关联的安全得分（125），

确定（210）与内容资料（101）相关联的安全标准（151），以及

基于该安全得分（125）和该安全标准（151）控制（250）该内容资料（101）的交付。

2、根据权利要求 1 所述方法，其中

该安全标准（151）基于如下至少之一:

该内容资料（101）的使用年限，

该内容资料（101）的评价，

与该内容资料（101）相关联的人，以及

该内容资料（101）的提纲。

3、根据权利要求 1 所述方法，其中

该安全得分(125)基于该内容资料(101)中包含的安全信息(115)和与该内容资料（101）的已授权备份相关联的认证信息（121）之间的一致性。

4、根据权利要求 3 所述方法，其中

该认证信息（121）相应于生物特征识别。

5、根据权利要求 3 所述方法，其中

该认证信息（121）相应于与包含该内容资料（101）的介质相关联的信息。

6、根据权利要求 1 所述方法，其中

控制（250）交付包括控制该内容资料（101）的交付的质量。

7、根据权利要求 1 所述方法，进一步包括

确定（220-230）随后的安全得分（125）和

基于该随后的安全得分（125）和该安全标准(151)控制交付。

8、根据权利要求 1 所述方法，其中

该安全标准(151)被提供有该内容资料（101）。

9、根据权利要求 1 所述方法，其中

确定（210）安全标准（151）包括确定该交付的预计使用。

10、一种控制内容资料（101）的交付的方法，包括:

确定（230）与该内容资料（101）相关联的安全得分（125），和

基于该安全得分（125）控制该内容资料（101）的交付的质量。

11、根据权利要求10所述方法，其中

该安全得分(125)基于该内容资料(101)中包含的安全信息(115)和与该内容资料（101）的已授权备份相关联的认证信息（121）之间的一致性。

12、根据权利要求11所述方法，其中

该认证信息（121）相应于生物特征识别。

13、根据权利要求11所述方法，其中

该认证信息（121）相应于与包含该内容资料（101）的介质相关联的信息。

14、根据权利要求10所述方法，进一步包括

确定（220-230）随后的安全得分（125）和

基于该随后的安全得分（125）控制（250）质量。

15、根据权利要求10所述方法，其中

控制（250）质量进一步基于该交付的预计的使用。

16、根据权利要求10所述方法，其中

控制（250）质量进一步基于与该内容资料（101）相关联的安全标准（151）。

17、根据权利要求16所述方法，其中

该安全标准（151）基于如下因素的至少之一:

该内容资料（101）的使用年限，

该内容资料（101）的评价，

与该内容资料（101）相关联的人，以及

该内容资料（101）的提纲。

18、一种系统包括:

被配置来接收内容资料（101）的接收机（110），

被配置来译码该内容资料（101）以提供可交付的内容资料的译码器（140）；

可操作地耦合到接收机（110）的安全鉴别器（120），其被配置来确定与该内容资料（101）相关联的安全得分（125），

可操作地耦合到安全鉴别器（120）的安全控制器（150），其被配置来:

接收与该内容资料（101）相关联的安全标准（151），和

基于安全得分(125)与安全标准(151)的比较控制译码器(140)。

19、根据权利要求 18 所述系统，其中

该安全标准（151）基于如下至少之一:

该内容资料（101）的使用年限，

该内容资料（101）的评价，

与该内容资料（101）相关联的人，以及

该内容资料（101）的提纲。

20、根据权利要求 18 所述系统，其中

安全鉴别器（120）被配置来基于该内容资料（101）中包含的安全信息（115）和与该内容资料（101）的已授权备份相关联的认证信息（121）之间的一致性来确定安全得分（125）。

21、根据权利要求 18 所述系统，其中

译码器（140）是可控制的，以改变可交付的内容资料的质量，和

安全控制器（150）被配置来基于该安全得分（125）控制在译码器（140）的质量。

22、一种系统包括:

被配置来接收内容资料（101）并提供可交付的内容资料的译码器（140），和

被配置来确定与该内容资料（101）相关联的安全得分（125）的安全控制器（150），

其中

该译码器（140）是可控制的，以改变可交付的内容资料的质量，和

该安全控制器（150）被配置来基于该安全得分（125）控制在译码器（140）的质量。

23、根据权利要求 22 所述系统，其中

可交付的内容资料的质量包括该可交付的内容资料的分辨率。

24、根据权利要求 22 所述系统，其中

安全鉴别器（120）被配置来基于该内容资料（101）中包含的安全信息（115）和与该内容资料（101）的已授权备份相关联的认证信息（121）之间的一致性来确定安全得分（125）。

25、根据权利要求 22 所述系统，其中

安全控制器（150）进一步被配置来基于与内容资料（101）相关联的安全标准（151）来控制在译码器（140）的质量。

基于安全得分的译码/解密

技术领域

本发明涉及电子安全系统领域，并具体涉及基于由保护的内容资料的接收机确定的安全得分控制译码或解密过程的复制/重放保护系统。

背景技术

对保护版权资料免于非法复制和发布的保护系统的需求在继续增长。同时，对这样的保护系统的可靠性的不满意已经妨碍了这些系统的实施。

特别关心的是“漏报”的问题，其中保护系统拒绝运行内容资料的经授权的复制。用户对拒绝运行已授权资料的产品非常不满意，同时具有获得了阻止已授权资料运行的名声的产品的销售商很可能失去真正的销售额，包括今后产品的销售额。同样地，获得了在允许已授权资料被运行之前需花费长时间的名声的产品将对销售商的销售额产生影响。

相反地，“误报”的问题，其中保护系统允许未被授权的资料运行，影响经授权的内容资料的销售额，并且表现出高比率的误报的系统可能接收不到内容提供商的认可。

常见的安全技术的示例和它们的局限性的示例如下。

水印是常被用于保护内容资料。水印被设计来以至它的去除将不利地影响保护的资料的质量，然而它的存在将不会不利地影响该资料的质量。在大多数保护系统中，水印包含必须被译码来确定资料的即时复制是否是合法复制的信息。因为水印必定是基本上“看不见的”，水印信号的幅值必定基本上小于资料的幅值，而且包含在水印内的信息的译码易发生错误，尤其是当资料源与水印检测器之间的资料的处理引入了处于或者接近水印信号的幅值电平的噪声时。

为了增强水印信号的潜在的信噪比，一些保护系统基本上降低该水印信号的带宽；然而，这样的降低限制了在该水印中可以包含的信息量和/或增加了接收该水印并确定资料是否被授权所需的时间。可替

换地，在资料中可以编码多个水印，并且基于被成功地认证的水印的比例来对访问资料授权。

生物识别度量也已经被提出来控制对受保护的内容资料的访问。典型地，生物识别特征由感测设备检测或采样，并且与样本相关联的参数被存储用于与与生物识别特征的其它样本相关联的参数进行比较。为了简化参考，术语生物识别或生物识别度量在下文中被用来指与感测的或者采样的生物度量的特征相关联的参数。因而，例如，术语“指纹”包括典型地从一个人的指尖的图像中得到的任意参数。

在生物识别安全系统的一个示例中，购买者的指纹被用于生成一个密钥来加密购买时的内容资料。在这样一个系统中，类似地接收设备被配置来生成一个密钥来基于用户的指纹解密该内容资料。如果使用相同的手指来创建该加密密钥和该解密密钥，那么该加密的资料将在接收设备处被正确地解密。

在生物识别安全系统的另一个示例中，购买者的指纹（或其它生物识别特征）被编码到水印中，该水印被嵌入在被购买的内容资料的备份中。接收系统解码该水印并比较购买者的指纹和用户的指纹，且此后只有指纹匹配才交付保护的资料。

然而，众所周知生物特征随时间而变化，而且基于具体使用的设备、生物识别特征相对于感测设备的方位、生物识别特征与感测设备之间的干扰的电平、生物识别特征的清晰度等等，生物特征的每次读取是不同的。如在犯罪辩论术领域公知的，例如，在一个人的指纹的不同实例中存在的差异需要专家分析来判断匹配。

用于控制对保护的资料的访问的其它技术也是可用的，已经示出的没有一个是确实可靠的。每个已知的技术呈现某种具有两个分量的错误的可能性：误报的可能性（允许呈现未经授权的资料）和漏报的可能性（妨碍经授权的资料被呈现）。错误的可能性可以通过修改与检测相关联的参数（诸如前述的降低水印带宽来增加信噪比）来控制，但是典型地带有负面效应（诸如前述的更长的水印处理时间和/或减小的水印信息内容）。另外，如所属领域公知的，一个错误分量的减小（误报或漏报）通常导致另一个错误分量的增加。

如果所有已知的安全系统均呈现错误的可能性，则存在用于控制这样的错误的影响的需要。

发明内容

本发明的一个目的是动态地控制漏报和误报的可能性。本发明的进一步目的是基于资料是已授权资料的信用度的度量动态地控制内容资料的交付。本发明的进一步目的是基于与被交付的资料相关的因子动态地控制内容资料的交付。

这些目的和其它的目的由一种方法和系统来实现，该方法和系统提供一种相应于所接收内容资料被授权交付的可能性的安全得分，并且基于该安全得分控制资料的交付。该安全得分可以和与正被交付的资料相关联的安全基准进行比较，以便不同的资料强制执行不同的约束。安全得分也可以控制资料交付的质量/保真度的等级，以便例如当建立提供已授权备份的高级信用度时才提供资料的高保真备份。

附图说明

以下将参考附图并以示例的方式进一步详细说明本发明，其中：

图 1 举例说明根据本发明的一种安全系统的示例性框图。

图 2 举例说明根据本发明动态地控制受保护内容资料的交付的安全系统的示例性流程图。

图 3 举例说明根据本发明动态地控制受保护内容资料的交付的质量等级的安全系统的示例性流程图。

所有附图中，相同的附图标记表示相同的元件，或执行实质上相同功能的元件。包括的附图是用于说明的目的，而不是意欲限制本发明的范围。

具体实施方式

图 1 举例说明根据本发明的一种安全系统的示例性框图。该安全系统包括用于接收受保护内容资料 101 的接收机 110，将该受保护资料转换成可交付格式的译码器 140，确定与内容资料 101 相关联的安全度量 125 的安全鉴别器 120，以及基于安全度量 125 控制译码器 140 的安全控制器 150。

译码器 140 包括被用于提供资料 101 的可控交付的任意的各种设备。在使用内容资料 101 的加密格式的实施例中，例如，译码器 140

包括被配置来基于由控制器 150 提供的信息解密资料的解密器。在一个可替换的或者补充的实施例中，译码器 140 可以被配置来由控制器 150 激活或禁用，或者可以被配置来基于来自控制器 150 的控制信号提供变化等级的输出保真度/质量，如以下进一步讨论的。

在图 1 的示例中，安全鉴别器 120 被配置来接收包含在来自接收机 110 的内容资料中的安全信息 115，如同将在例如基于水印的安全系统中被使用的。另外，安全鉴别器 120 接收认证信息 121，其被用来基于安全信息 115 验证内容资料 101 的认证。例如，包括经授权的盘的序列号的水印可以被嵌入到资料 101 中。接收机 110 被配置来将这一水印作为安全信息 115 提供给安全鉴别器 120，以及提供该内容资料 101 的盘驱动器（未示出）提供其中资料 101 从该盘被获取的盘的序列号作为认证信息 121。

安全鉴别器 120 利用所属领域的常用技术应用适当的检测来确定内容资料 101 是否是经授权的/有效的。然而，与常规的安全系统相比，本发明的安全鉴别器 120 提供定量的得分 125，而不是常规的二进制的通过/失败确定。例如，如果认证是基于比较序列号的，得分 125 可以是基于该序列号的匹配比特的数量，考虑到从水印中译码序列号可能是一个容易错的过程。同样地，如果认证是基于比较生物特征，则得分 125 可以是基于生物特征之间的匹配程度，诸如在一对指纹中匹配特征点的数量。

因为上述的典型地与水印相关联的低信噪比，和/或因为上述的生物特征的高可变性，常常使用安全信息 115 对保护的内容资料 101 进行冗余编码。以及，在许多安全系统中，多个（但不必是冗余的）安全标识符被用来提供一种用于不断地检查资料 101 的有效性的手段。在提供定量得分的另一个示例中，尽管具体的检测仅仅提供二进制结果，安全鉴别器 120 可以被配置来提供安全得分 125，其基于通过的或者失败的检测的比例，和/或基于多个检测的平均得分。由于该公开，对所属领域的普通技术人员来说，用于基于与保护的资料相关联的安全信息提供安全得分的这些和其它技术是显而易见的。

按照本发明的第一方面，安全控制器 150 使用来自安全鉴别器 120 的安全得分 125 和安全标准 151 来控制译码器 140。该安全标准 151 可以呈现各种各样的形式，如下面进一步详细描述的，但是该标准 151

的主要目的是允许安全控制器 150 基于与内容资料 101 相关联的信息动态地控制译码器 140。为了本发明的目的，术语动态的控制包括在不同的时间提供不同的控制。在正在处理相同的内容资料 101 的同时，可以应用不同的控制，或者可以将不同的控制应用到内容资料 101 的不同实例中。

在安全标准 151 的第一示例中，内容资料 101 的提供者可以将最小所需安全等级与该内容资料 101 相关联，其中等级越高，对该资料 101 的交付的控制越严格。如果安全得分 125 大于最小所需安全等级，那么安全控制器 150 允许译码器 140 继续内容资料 101 的交付；否则，交付被终止。

如果例如基于重复检测或者连续检测来配置安全鉴别器 120 以提供与资料 101 相关联的正在进行的得分，那么可以配置安全控制器 150 以便只要安全得分下降到低于与该内容资料 101 相关联的最小等级就终止该交付。可替换地，提供者可以将一套标准 151 与给内容资料 101 相关联，诸如在特定点之上，启动交付所需的一个初始的等级和继续交付所需的更高的等级。以这种方式，开始该资料的交付的延时时间可以被降低，同时仍然保证高等级的安全来交付该内容资料的真实的部分。

在另一个实施例中，正规的统计检测可以由安全控制器 150 应用，并且提供者可以关联通过/失败标准，诸如在检测结果中所需的信用等级用于终止交付。在由安全鉴别器 120 执行的多个继续评估的情况下，序列检测的使用，诸如序列概率比检测（SPRT），尤其好地适合于确定是否允许交付，继续检测，或者阻止交付。

特别注意，按照本发明，不同的标准 151 可以与不同的内容资料 101 相关联。以这种方式，内容资料 101 的提供者可以有效地控制上述的漏报和误报差错率。如果提供者考虑非法复制的代价超过了使用严格的控制潜在地打扰客户和潜在的漏报的代价，提供者可以将安全标准 151 设置为高。另一方面，如果提供者关注获得销售难于播放的资料 101 的声誉，那么提供者可以选择降低标准 151 以降低漏报的可能性，尽管允许未经授权的资料的播放的可能性被增加。

通过本发明的使用，最受版权实施的影响的一方被提供该实施的控制，带着其伴随的优势和缺陷，以及重放设备的销售商被解除了用

于确定漏报和误报差错之间的一个适当的平衡的责任。可替换地，如果提供者不愿意接收该责任并设置安全标准，那么设备的销售商可以利用该能力来基于实际领域的经验和用户反馈调整安全等级以便获得一个可接受等级的漏报。同样地，假设内容资料 101 的不同提供者可能针对安全信息 115 展现不同等级的可靠性，诸如不同电平的信噪比，交付设备的销售商可以根据资料 101 的提供者选择实施不同等级的安全，以避免被加到销售商的交付设备的安全信息 115 的缺乏。

另外，通过本发明的使用，当允许未经授权资料的交付的预期损失被降低时，内容信息 101 的提供者被提供降低防止交付已授权资料的可能性的能力。例如，如果可以获得非法的复制，那么当电影第一次发行时，来自高度评价的电影的经授权备份的销售收入的损失是相当大的。另一方面，发行后一年或两年的预期收入基本上更少，并且因此对于非法复制，预期的收入损失相应更少。同样地，来自非常较差评价的电影的预期收入基本上少于来自高度平均的电影的预期的收入，并且因此对于较差评价的电影的非法复制的预期收入损失将基本上少于对于高度评价的电影的非法复制的损失。通过本发明的利用，内容资料 101 的提供者可以针对具体的内容资料 101 基于预期的收入损失修改标准 151。同样地，在资料 101 的提供者不提供安全标准 151 的情况下，接收设备的销售商可以基于资料 101 的时间性、资料 101 的评价等级等等来选择实现不同的标准 151。

任何各种各样的方法可被用于将安全标准 151 传递到安全控制器 150。在一个简单的实施例中，安全标准 151 可被包含在被提供有内容资料 101 的元信息（meta-information）。例如，安全标准 151 可被包含在典型地提供在 CD 和 DVD 上的目录中，或者包括在广播传输的提纲中。在一个可替换的实施例中，安全标准 151 可通过在线连接到与资料 101 的提供者、接收设备的销售商、或诸如视频或音频制作者的协会的第三方相关联的网站来获得。

在销售商确定安全标准 151 或者产品确定安全标准 151 的示例性情况下，安全标准 151 可以当前日期为基础，并且安全控制器 150 被配置来基于当前日期与诸如在资料 101 相关联的元数据（meta-data）发现的版权日的与内容资料 101 相关联的日期之间的差值来控制译码器 140。例如，如果资料 101 不足一年时间，那么安全控制器 150 可

被配置来防止资料 101 的交付，除非获得了一个非常高的安全得分 125。另一方面，如果资料 101 已经有 10 年时间了，控制器 150 可以允许资料 101 的交付，尽管安全得分 125 是低值。同样地，安全控制器 150 可包括存储器，该存储器包括“流行（popular）”项，诸如当前流行的男演员和女演员、当前流行的制作者和导演等等的名字。在这样的实施例中，安全标准 151 可以是与资料 101 相关联的元数据，以及如果控制器 150 检测元数据与“流行”项之间的匹配，那么将需要更高等级的安全得分 125 来允许资料 101 的交付。

在另一个示例的实施例中，安全标准 151 可以取决于由译码器 140 提供的功能。即，例如用于制作资料 101 的备份的安全标准可以被设置为充分地高于用于只重放资料 101 的安全标准。如此，利用译码器 140 来重放保护的资料 101 的用户很可能比利用译码器 140 来制作资料 101 的备份的用户更少地受漏报决定的影响。

考虑到本发明，根据基于安全得分 125 的交付控制的确定来定义和确定安全标准 151 的这些和其它方法对所属领域普通技术人员来说将是显而易见的。

图 2 举例说明根据本发明动态地控制保护的内容资料的交付的安全系统的示例性流程图，如在图 1 的安全系统中一样被使用。

在 210，利用如上述详细描述的方法之一确定安全标准。无需说明，如果没有安全标准，图 1 的控制器 150 被配置来允许内容资料 101 的不受限制的交付，并且避免了随后详细的过程。

在 220，接收内容资料，或者接收内容资料的下一分段，从中推导出安全信息。

在 230，执行安全检验/评估，例如，如上详述的关于图 1 的鉴别器 120，以及确定安全得分。如图 2 的框 230 的虚线说明的，可以不断地重复安全检验/评估。可以连续地提供来自框 230 的安全得分，或者在满足诸如内容资料的最小数量的分段的接收和检验等具体的标准之后，提供来自框 230 的安全得分。

在 240，安全检验框 230 的输出被相对于在 210 确定的安全标准进行评估。基于这一评估，在 250 控制内容资料的译码/解码。该控制可以是简单的开/关控制，或者可变的控制，如以下进一步讨论的。

按照本发明的第二方面，安全控制器 150 和译码器 140 被配置来

在内容资料 101 的交付中提供用于改变质量/保真度的等级。这一方面可以与上述讨论的可控制的安全标准 151 的使用相呼应地，或者独立地实现。

因为定量的得分 125 由安全鉴别器 120 提供，安全控制 150 可以被配置来提供译码器 140 的控制的变化程度。

在本发明的这一方面的一个简单的实施例中，译码器 140 被配置来截短内容资料 101 的可交付的版本的低位比特。在本实施例中截短的程度由安全控制器 150 基于安全得分 125 确定。任选地，安全控制器 150 基于相对于安全标准 151 的安全得分 125 确定截短的程度。

在一个更复杂的实施例中，控制器 150 控制在累进的译码器 140 中的内容资料的译码电平。如所属领域公知的，一些编码策略以分层方式编码或加密内容资料 101。在该分层结构的最上层，只有资料的最显著的特征被编码。在分层结构的每个随后层，清晰度或分辨率的附加等级被编码。

图 3 举例说明动态地控制累进编码的内容资料的交付的质量等级的安全系统的示例性流程图。

在 310，典型地从与内容资料相关联的“头”信息中确定编码电平数。在 320，基于编码电平数和为当前内容资料确定的安全得分来确定译码电平数，基于安全标准选择性地调整译码电平数。例如，相对于安全标准的高安全得分将导致将译码电平数设置为等于编码电平数。另一方面，相对于安全标准的低安全得分将导致译码电平少于编码电平。

在 340，基于与当前内容资料相关联的安全得分，环路 330－350 累进地译码每个编码电平，直到确定数量的译码电平。

通过控制内容资料的交付的质量，内容提供者或者设备销售商通过允许怀疑的非法资料的交付（虽然在较低的质量等级上）可以降低已授权内容资料的用户由于过度地限制安全约束所可能经历的不满意。

同样地，通过基于与内容资料相关联的安全的度量控制交付的质量，非法的复制的扩散可以被减少。例如，如果假设内容资料的非法复制通常展现较低的安全得分，每个随后的复制将具有低于最好质量的质量，它们的市场价值将被降低。

同样地，可以基于交付的预计使用来控制交付的质量。即，例如译码电平数量的确定，或者截短比特的数量的确定可以取决于交付是正在被执行来产生资料的备份还是仅仅重放该资料。

前述仅仅举例说明本发明的原理。可以理解，那些所属领域技术人员能够设计各种各样的装置（虽然没有在此明显地描述或者示出）来具体化本发明的原理，并在随后的权利要求的精神和范围内。

在解释这些权利要求中，应当理解:

a）用语“包括”不排除在给定的权利要求中除了列出的那些之外的其它元件或动作的存在;

b）在元件之前的用语“一”不排除多个这样的元件的存在;

c）在权利要求中的任何附图标记不限制它们的范围;

d）几个“装置”可以由用结构或功能实现的相同的项目或硬件或软件来表示;

e）每个公开的元件可以被包含在硬件部分（例如，包括离散或集成的电子电路），软件部分（例如，计算机程序设计），和它们的任意组合;

f）硬件部分可以由模拟和数字部分之一或者两者组成;

g）其任何公开的设备或部分可以被组合在一起或者进一步分离成各部分，除非有其他特别说明；以及

h）旨在不需要特定的动作顺序，除非特别指出。

i）术语“多个”元件包括两个或以上要求保护的元件，且不意味着任意特定范围的元件数量；即，多个元件可以少到等于两个元件。

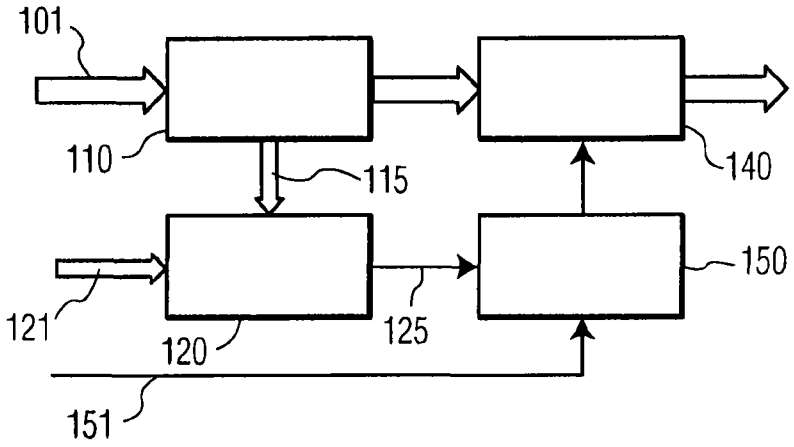

101
110
115
140
150
121
120
125
151

图 1

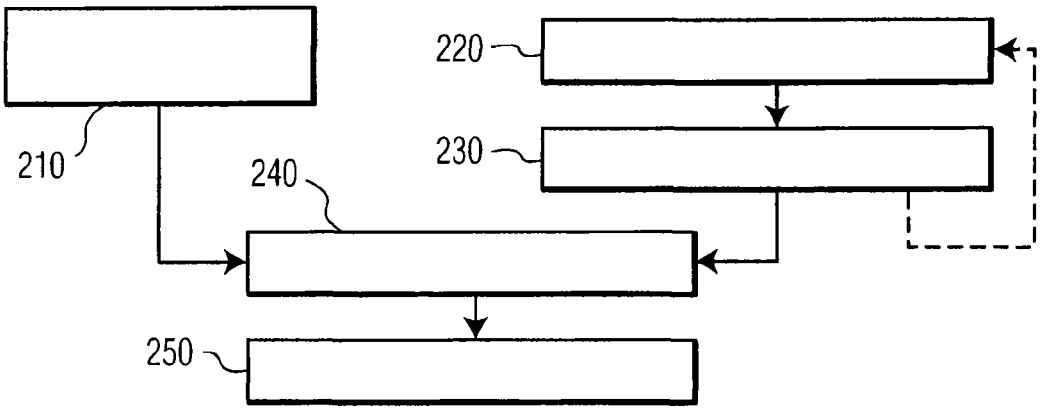

220
210
230
240
250

图 2

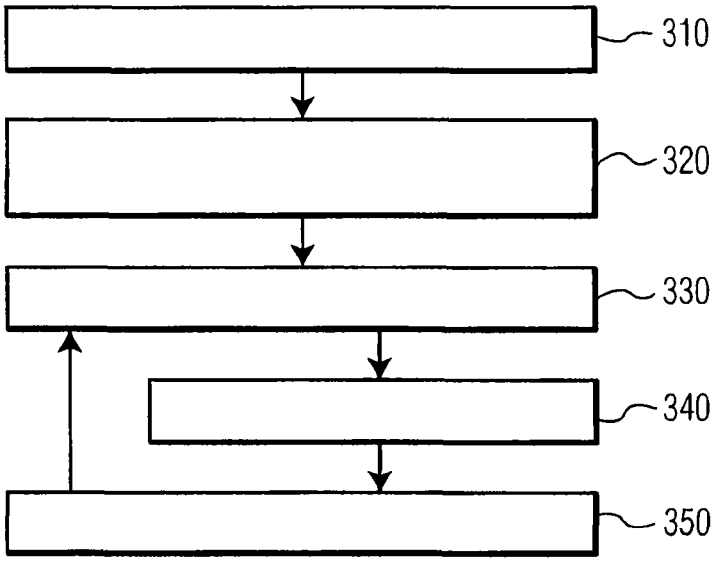

310
320
330
340
350

图 3