



(21)申请号 201110287678.9

(22)申请日 2011.09.26

(65)同一申请的已公布的文献号

申请公布号 CN 102572309 A

(43)申请公布日 2012.07.11

(30)优先权数据

102010041447.6 2010.09.27 DE

(73)专利权人 罗伯特·博世有限公司

地址 德国斯图加特

(72)发明人 J.肖克罗拉希 C.马丁

(74)专利代理机构 中国专利代理(香港)有限公

司 72001

代理人 胡莉莉 李家麟

(51)Int.Cl.

H04N 17/00(2006.01)

G06K 9/00(2006.01)

H04L 9/32(2006.01)

(56)对比文件

US 2009/0154809 A1,2009.06.18,

US 2010/0194895 A1,2010.08.05,

CN 1012912466 A,2008.10.22,

US 2009/0154809 A1,2009.06.18,

审查员 盛磊

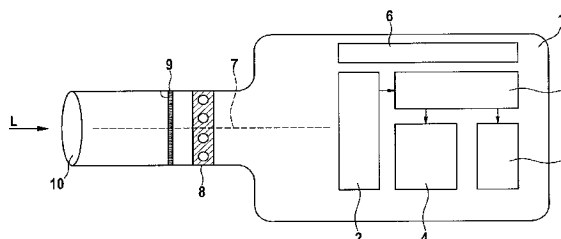
权利要求书1页 说明书5页 附图2页

(54)发明名称

用于验证电荷耦合器件的方法

(57)摘要

本发明涉及用于验证电荷耦合器件的方法。提供了一种用于在使用物理上不可克隆的功能的情况下验证电荷耦合器件(CCD)、尤其是在包括电荷耦合器件的数字摄像机中的电荷耦合器件的方法,其中在电荷耦合器件中存在的像素对所限定的入射光的要测量的响应被用作物理上不可克隆的功能(PUF)。此外,介绍了一种相对应的装置以及一种包括这样的装置的摄像机。



1. 一种用于在使用物理上不可克隆的功能(PUF)的情况下验证电荷耦合器件(CCD)(2)的方法,其中,在电荷耦合器件(2)中存在的像素对所限定的入射光的要测量的响应被用作物理上不可克隆的功能,其中设置有可运动的不透光的盖板(9),借助所述盖板(9)在验证期间阻止不期望的光入射到电荷耦合器件(CCD)(2)上。

2. 根据权利要求1所述的方法,其中,电荷耦合器件(CCD)(2)利用所限定的波长的光被照射。

3. 根据权利要求1或2所述的方法,其中,电荷耦合器件(CCD)(2)在包括电荷耦合器件的数字摄像机(1)中。

4. 根据权利要求3所述的方法,其中,至少一个LED(8)被用作光源。

5. 根据权利要求4所述的方法,其中,多个LED以绕着摄像机(1)的光学轴线(7)环绕的环(8)的形式被布置,使得电荷耦合器件(CCD)(2)大面积覆盖地被照射。

6. 根据权利要求3所述的方法,其中,入射到电荷耦合器件(CCD)(2)上的光由集成到摄像机(1)中的光源来提供。

7. 一种用于验证在包括电荷耦合器件(CCD)的数字摄像机中的电荷耦合器件(CCD)的装置,其具有用于利用光以限定的方式照射电荷耦合器件(CCD)(2)的光源(8)和可运动的不透光的盖板(9),借助所述盖板(9)在验证期间阻止不期望的光入射到电荷耦合器件(CCD)(2)上,其中在验证时,该装置(11)被布置在摄像机(1)上,使得光源(8)以限定的方式照射电荷耦合器件(2),并且能够借助相对应的测量和分析单元(12),在电荷耦合器件(2)中存在的像素对所限定的入射光的响应作为物理上不可克隆的功能(PUF)能被测量和被分析。

8. 根据权利要求7所述的装置,其中,测量和分析单元(12)是该装置的集成的组成部分。

9. 根据权利要求7或8所述的装置,其中,该装置是数字摄像机(1)的集成的组成部分。

10. 一种数字CCD摄像机,其具有根据权利要求7至9之一所述的装置。

用于验证电荷耦合器件的方法

技术领域

[0001] 本发明涉及一种用于验证(Authentifizieren)电荷耦合器件(CCD)、尤其是在数字摄像机中的电荷耦合器件的方法、一种用于验证电荷耦合器件(CCD)的装置以及一种相对应的数字CCD摄像机。

背景技术

[0002] 已经公知了不同的方法来识别产品,如例如在Pappu Srinivasa Ravikanth的文献“Physical One-Way Functions”中所描述的那样。在该文献中,作者描述了用算法的所谓单向函数支持加密技术结构的可能性。所谓的单向函数是数值函数并且在其他意义下可以被视为加密方法的物理实现。

[0003] 公知的用于识别和验证产品的方法中的大多数方法都基于将不可克隆的(unklonbar)模块添加到要识别和要验证的产品。通过读取由该不可克隆的模块详细说明的值由此来识别和验证产品。使用所谓的物理上不可克隆的功能以避免克隆的普遍方法在于:生成具有特定的并且不可克隆的随机值模块,或者找到模块的随机分布的要被验证的固有特性。

[0004] 在添加新模块时的三个主要缺点在于:对于新模块形成了额外费用,该模块必须以一种方式被选择来使得考虑要识别的产品或设备的工作条件,并且如果要识别的产品或设备的识别要在产品或设备的工作时间期间进行,则例如每次当起动相对应的系统时,模块的内容也在要识别的产品或设备投入使用期间或者直接在要识别的产品或设备投入运行之前保持可读取。该读取附加地要求会是昂贵的并且必须针对每个要识别的产品或设备被实现的硬件。这样的要求例如在识别和验证数字CCD摄像机或识别该数字CCD摄像机的所实现的CCD芯片时应被满足。

[0005] 因而所希望的是规定一种可替换的可能性,可以毫无问题地、优选地在任何时间并且尽可能成本低廉地识别和验证产品或设备、如尤其是数字CCD摄像机。

发明内容

[0006] 在该背景下,提供了一种根据权利要求1所述的用于验证电荷耦合器件(CCD)、尤其是在包括电荷耦合器件的数字摄像机中的电荷耦合器件(CCD)的方法,以及提供了一种根据权利要求7所述的用于验证在包括电荷耦合器件的数字摄像机中的电荷耦合器件(CCD)的装置和根据权利要求10所述的相对应的数字CCD摄像机。

[0007] 本发明的其他扩展方案由相应的从属权利要求和说明书得到。

[0008] 本发明涉及一种用于验证电荷耦合器件(“Charge-Coupled Device”, CCD)、尤其是在包括电荷耦合器件的数字摄像机中的电荷耦合器件的方法。在此,根据本发明所规定的方法是非常有成本效益的并且是不可克隆的。

[0009] 所谓的电荷耦合器件(CCD)是用于输送电荷的集成电子器件。在此涉及基于内部光电效应的光敏电子部件。最初,CCD芯片针对数据存储被开发,然而快速断定这些部件是

光敏的并且借助这些部件检测二维图像比较容易。二维CCD阵列传感器(CCD-Array-Sensor)在此期间被使用在视频摄像机和数字摄像机、所谓的CCD摄像机中,但是例如也可以被使用在如光谱仪的其他单元中。CCD芯片的主要特征量是相应的像素量和位于该CCD芯片上的像素的数目(掺杂)。

[0010] 为了识别这样的CCD摄像机(或这样的单元)或包含在其中的CCD芯片现在规定,使用物理上不可克隆的功能。在此,作为物理上不可克隆的功能(PUF)使用在电荷耦合器件(CCD芯片)中存在的像素对所限定的入射光的要测量的响应(Antwort)。

[0011] 在此,电荷耦合器件(CCD芯片)优选地用所限定的波长的光来照射。作为光源例如可以采用至少一个发光二极管(LED“Light Emitting Diode”)。在此,有利地采用多个LED并且将这些LED例如以绕着数字CCD摄像机的相应光学轴线环绕的环的形式布置,使得电荷耦合器件(CCD芯片)大面积覆盖地(flaechendeckend)被照射。

[0012] 此外,可以设置有可运动的不透光的盖板(Abdeckung),借助该盖板在验证期间阻止不期望的光入射到该电荷耦合器件上,因为由不同于用于验证的光源的光源入射的光会改变像素对该光的作用或响应,使得不再可能进行验证。

[0013] 可设想的是,入射到电荷耦合器件上的光由集成到摄像机中的光源提供。此外,也可以以合适的方式与集成的光源组合地将要设置的不透光的盖板集成在摄像机内部。接着谈及所谓的在线模式(In-Circuit-Modus),使得所谓的在线测试(In-Circuit-Test)在摄像机内部在不添加其他部件的情况下是可能的。

[0014] 通过根据本发明的方法可能的是,直接识别例如视频信号是否确实由相对应的摄像机捕获或者但是通过被伪造的信号源被冒充。此外,可以借助根据本发明的这样的在线模式生成加密密钥,这些加密密钥接着可以被用于将相对应的摄像机软件的部分加密,使得软件被结合到确定的硬件并且不是通过单纯地拷贝相对应的软件而可以运行在其他单元或其他摄像机上。新密钥的产生例如可以借助模糊提取器(Fuzzy Extractor)来执行。这样的方法例如在Yevgeniy Dodis、Jonathan Katz和Leonie Reyzin的“Robust Fuzzy Extractors and Authenticated Key Agreement from Close Secrets”中进行了描述。由此因而得到对寄存在数字摄像机中的软件的相对应的拷贝防护。其他应用例如是使用相对应的CCD芯片的验证信息来检验例如相对应的摄像机或者CCD芯片是否通过特定的硬件制造商来制造。

[0015] 尽管上面所述的应用也可以通过将智能卡插入到相应摄像机中来实现,然而根据本发明的方法提供了一种新的吸引人的并且有成本效益的替换方案。

[0016] 如已在上面已经提及的那样,根据本发明的方法基于在使用物理上不可克隆的功能的情况下进行对象验证。根据本发明,使用相应的CCD芯片的特别的并且独特的(einmalig)特性、即CCD芯片的相应的尺寸和像素的掺杂(Doping)作为明确的识别测量参数。在此,CCD芯片的所谓的“场景噪声(scene noise)”被用作物理上不可克隆的功能。在验证自身时,现在激励和测量物理上不可克隆的功能的相对应的响应。所述响应接着可以被使用,以便识别相对应的摄像机或在摄像机内部的CCD芯片,并且以便生成加密密钥。独特的并且可与CCD芯片明确地关联的特性(在下文中也称作功能、即不可克隆的功能)因而必须被激发并且测量CCD芯片的相应的响应。

[0017] 为了测量在数字摄像机内部的CCD芯片的响应、例如“场景噪声”,可以使用如下方

法:所述方法已经由该出版物公开并且例如在Robert Mendoza的文献“An Analysis of CCD Camera Noise and its Effect on Pressure Sensitive Paint Instrumentation System Signal-to-Noise Ratio”中进行了介绍。这意味着:在数字CCD摄像机内部的要验证的CCD芯片利用一致的光来照射,并且在使用合适的测量方法的情况下读取由每个像素再度发送的信号。根据本发明,所读取的信号被解释为可明确地与相应的CCD芯片关联的值,这些值因而可以被用于验证CCD芯片或集成CCD芯片的数字摄像机。

[0018] 在此,可设想两个测量场景、即所谓的“在线设置(In-Circuit-Setting)”和所谓的“离线设置(Off-Circuit-Setting)”,这两个测量场景在下文中结合附图更为详细地予以描述。

[0019] 此外,本发明提供了一种用于验证在包括电荷耦合器件(CCD)的数字摄像机中的电荷耦合器件(CCD)的装置,其中该装置包括用于以限定的方式用光照射电荷耦合器件的光源和可运动的不透光的盖板,借助该盖板在验证期间可以阻止不期望的光入射到电荷耦合器件,其中在验证时,该装置被布置在摄像机上,使得光源以限定的方式照射电荷耦合器件并且借助相对应的测量和分析单元可将在电荷耦合器件中存在的像素对所限定的光入射的响应作为物理上不可克隆的功能来测量和分析。

[0020] 可设想的是,测量和分析单元是该装置的集成的组成部分。

[0021] 此外,也可设想的是,该装置是相对应的包括电荷耦合器件的数字摄像机的集成的组成部分。

[0022] 此外,本发明提供了一种具有相对应在上面描述的装置的数字CCD摄像机。

[0023] 本发明的其他优点和扩展方案由本说明书和所附的附图得到。

[0024] 应理解的是,前面所述的并且下面还要阐述的特征不仅可以以分别说明的组合而且可以以其他组合或者单独地被使用,而没有离开本发明的范围。

附图说明

[0025] 图1以示意图示出了“在线”模式,在所述“在线”模式下可以执行根据本发明的用于验证在包括CCD芯片的摄像机内部的CCD芯片的方法的实施形式;

[0026] 图2示出了“离线”模式,在所述“离线”模式下可以执行根据本发明的用于验证在包括CCD芯片的摄像机内部的CCD芯片的方法的另一实施形式。

具体实施方式

[0027] 本发明依据附图中的实施形式示意性地被示出并且在下文中参照附图被详细地描述。相同的附图标记分别标明相同的单元。

[0028] 图1示出了所谓的“在线”模式,在所述“在线”模式的情况下,根据本发明的用于验证在包括CCD芯片的数字CCD摄像机中的CCD芯片的装置被集成到相对应的摄像机中,即为摄像机的集成的组成部分。图1示出了数字摄像机1,在所述数字摄像机1内部实现不同的功能单元。与此相关联的是CCD芯片2、用于测量像素3的测量单元、成像软件4和要设置用于执行根据本发明的方法的PUF(“物理上不可克隆的功能(Physcial Unclonable Function)”)软件5。此外,设置有控制和检查软件(Steuer- und Kontrollsoftware)6。用附图标记7绘出数字摄像机1的光学轴线。围绕光学轴线7布置LED 8的环,所述环此外还在CCD芯片2之

前。LED本身被示为圆。在下文中,用参考数字“8”不仅表征各个LED而且表征LED的环。环8的LED在验证在数字摄像机1内部的所实现的CCD芯片2时被用作用于照射CCD芯片2的照射源。此外,设置有可运动的盖板9,该盖板9可以与常规的照相机的快门相比较。盖板9被用于阻止除了所述LED之外的其他光源的光在验证过程中到达CCD芯片2。其他光即会相对地使测量结果歪曲,并且对CCD芯片2的明确的验证会不再是可能的。盖板9因而相对地相对于CCD芯片2被布置在LED构成的环8之后,使得在验证过程中,外部光源的光(这在摄像机1中仅从外部、即在这里所示的摄像机1中从左边通过开口10(如通过箭头L绘出)来到)被分离。关于光学轴线7对称布置的LED的环8保证了对CCD芯片2的一致照明。通过照射CCD芯片2来激发在CCD芯片2上所包含的像素并且在其方面发送特定的模拟电信号,所述特定的模拟电信号通过像素测量单元3被记录并且被转换成相对应的数字信号。此后,数字信号被像素测量单元3输送给相对应的分析单元。成像的软件4在验证过程期间是不活动的,而PUF软件5分析像素的相对应的响应,并且断定最终得到的对照射的响应在LED 8方面是否与要期望的响应相一致,使得可以断定通过LED 8所照射的CCD芯片2是否是应在摄像机1中实现的CCD芯片,即CCD芯片2可以根据其像素响应而被验证。

[0029] PUF软件5也可以被使用,以便不是进行检验或验证而是借助模糊提取器方法(如前面已经所提及的那样)产生密钥,该密钥接着可以被用于进行外部验证或者加密。

[0030] 在验证过程之后,数字摄像机接着又被用于正常目的,其中可运动的盖板9被去除或从摄像机的开口10被移开,使得相对应的光可以从外部入射。LED 8在正常工作时被断开并且激活成像的软件4。

[0031] 在此应注意的是:在验证过程时,LED的光量必须足够高,以便通过CCD芯片的所谓的“场景噪声”给出占主导的响应或在正常工作时要表明的噪声,如例如在Donald Robert Mendoza的文献“An Analysis of CCD Camera Noise and its Effect on Pressure Sensitive Paint Instrumentation System Signal-To-Noise Ratio”的图1中所示出的那样。此外,应注意的是,在大多数情况下,商品化的照相机已经具有暗的盖板、例如前面已经提及的快门形式的盖板,该快门同样可以以合适的方式被用于验证目的。

[0032] 图2示出了另一可能的场景,在该场景中能执行根据本发明的用于验证在数字CCD摄像机内部的CCD芯片的方法的另一实施形式。在此,涉及所谓的“离线”模式,由此通过外部装置11激活或激励物理上不可克隆的功能、在这里所选择的情况下为CCD芯片的像素对特定的激发或对特定的光入射的响应。在激发CCD像素时的相对应的响应接着例如也可以在数据库中被调查研究,以便检验例如摄像机或其中实现的CCD芯片是否与特定的组相关联或者是否由特定的制造商来制造。此外,这也可以用于在制造过程期间自动地将固件解密,并且如果这样的操作要是可支配的,则建该固件下载到摄像机的内部的非易失性存储器中。

[0033] 在离线模式下,不仅可运动的盖板9而且围绕光学轴线7布置的LED 8的环彼此组合并且被布置在外部装置11内部。装置11接着被布置在相对应的摄像机1'的开口10之前,使得LED 8的光根据光入射(如在图1中在将LED芯片集成在摄像机1内部所示出的那样)射到CCD芯片2上。在装置11的相对应的布局中,因此在此处也以绕着数字摄像机1'的光学轴线7的环的形式布置LED 8,并且因而相对地照明CCD芯片2的表面。这里,CCD芯片2的像素的响应也被测量、被分析并且作为标准被用于验证CCD芯片2或相对应的实现CCD芯片的摄

像机1'。要执行的方法步骤的序列类似于结合图1所描述的在线模式。在这里所示的离线模式下,要验证的摄像机1'被保持得更小和更紧凑,因为装置11被设置在外部用于验证并且此外也可以将相对应的测量和分析单元设置为外部元件12。在验证过程期间,因而外部装置11必须以合适的方式被放置在摄像机1'之前,使得相对应的光可以以合适的方式落到CCD芯片2上。此外,必要时被设置在外部的测量和分析单元12接着也必须与摄像机1'或其中所实现的CCD芯片2相耦合并且相应地被激活。然而,在执行验证之后,不仅外部装置11与LED 8和可运动的盖板9的装置一起可以被去除,而且分析和测量单元12也可以被去除。通过设置不仅用于分析和测量而且用于在验证过程期间照射CCD芯片2的外部装置可以确保要验证的摄像机1'被客观地评价并且必要时在摄像机1'内部也不存在会输出被伪造的图像或被伪造的值的单元。借助该方法和数字签名也可以断定:确定的摄像机实际上是否也由特定的制造商制造。

[0034] 总之可以断定的是,根据本发明的方法以及根据本发明所设置的装置和摄像机适于在将CCD的像素噪声(“场景噪声”)用作物理上不可克隆的功能时来验证相对应的CCD芯片或相对应的实现CCD芯片的摄像机。根据特定的应用,在线模式或者离线模式可以被选择。根据本发明的方法示出了用于明确地识别针对不同应用的摄像机的有效途径,所述不同应用诸如用于检验媒体源或者用于加密或解密摄像机的固件的针对相对应的专用技术(Know-How)保护的部分。

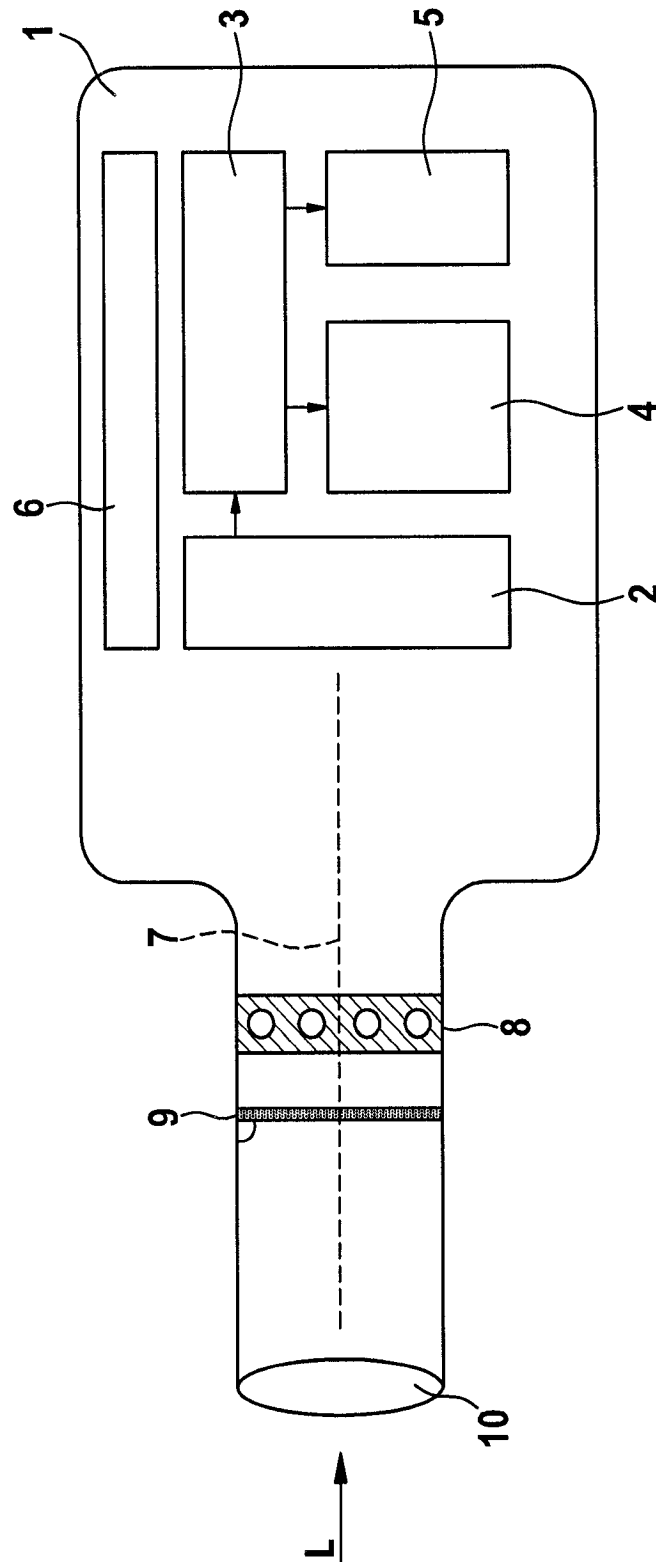


图 1

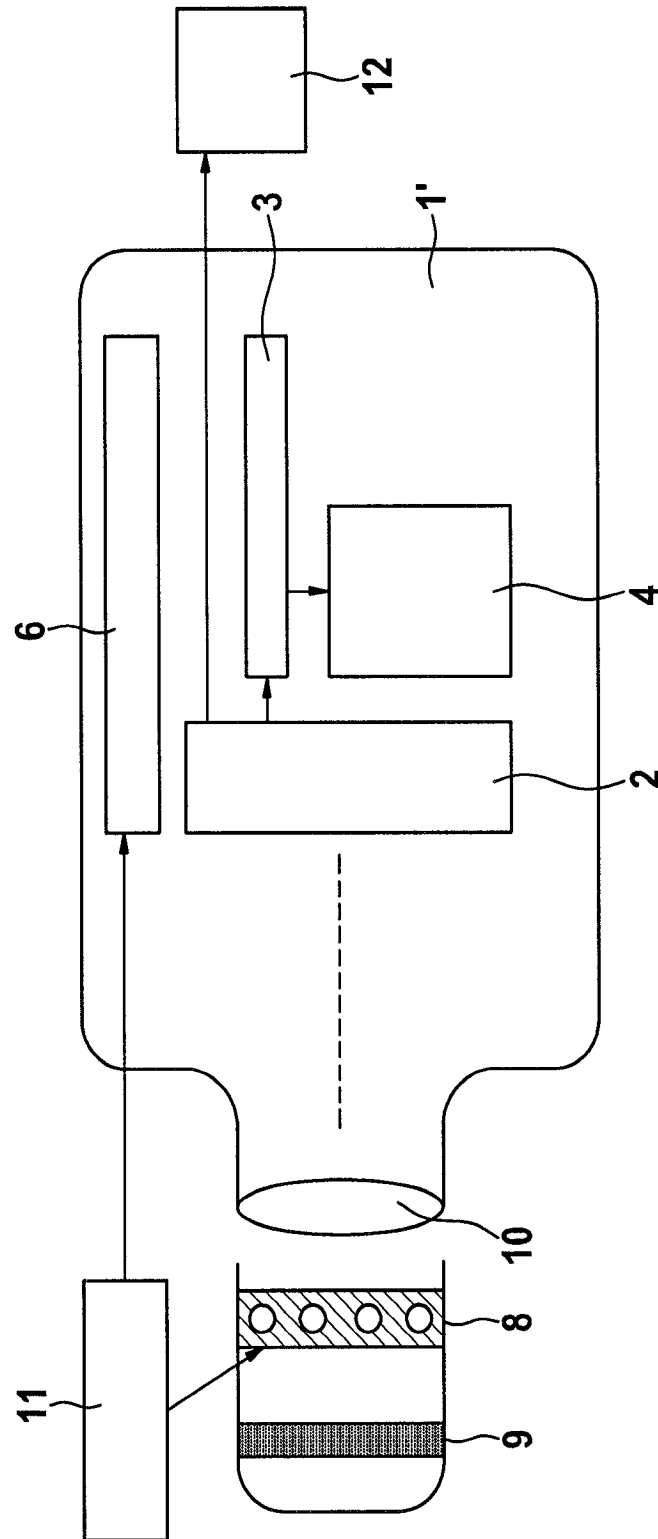


图 2