(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 104142803 B
(45)授权公告日 2019.12.24

(21)申请号 201410192711.3

(22)申请日 2014.05.08

(65)同一申请的已公布的文献号
申请公布号 CN 104142803 A

(43)申请公布日 2014.11.12

(30)优先权数据
102013104735.1 2013.05.08 DE

(73)专利权人 德国福维克控股公司
地址 德国伍伯塔尔

(72)发明人 V.格雷弗

(74)专利代理机构 北京市柳沈律师事务所 11105
代理人 侯宇

(51)Int.Cl.
G06F 3/06(2006.01)

(56)对比文件
CN 101084482 A,2007.12.05,
CN 101084482 A,2007.12.05,
WO 2009004508 A1,2009.01.08,

审查员 刘念

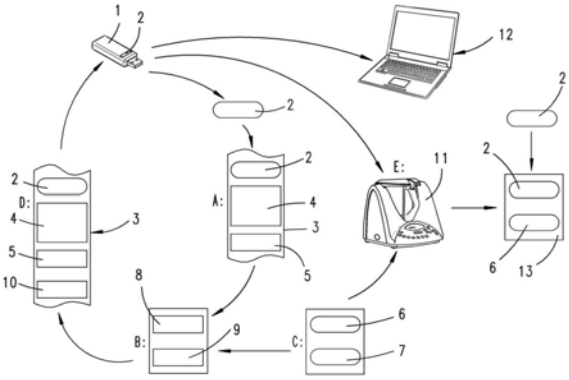
权利要求书2页 说明书4页 附图1页

(54)发明名称

用于将信息防复制地存储在数据载体上的方法

(57)摘要

本发明涉及一种用于将由数字数据组成的信息存储在数据载体上并从数据载体读取信息的方法，其中数据载体具有单独的数字标志，其中形成签名，其中信息具有至少第一信息组成部分，所述第一信息组成部分仅当单独的数字标志和签名彼此存在预定的关系时才能由第一电子数据处理装置来处理。为了向电动家用设备提供过程控制数据，其中同时应当确保，仅使用原始数据，建议，即使当签名和标志彼此不存在预定的关系时，也能由第二电子数据处理装置来处理信息组成部分。本发明还涉及一种具有电子数据处理装置的可电动运行的家用设备，特别是厨房设备，一种系统和一种集成的半导体电路，也实现了用于存储由数字数据组成的信息的特征。



CN 104142803 B

1.一种用于将由数字数据组成的信息(4,5)存储在数据载体(1)上并且从所述数据载体(1)读取所述信息的方法,其中所述数据载体(1)具有单独的数字标志(2),其中形成包括所述单独的标志(2)的签名(10),其中,所述信息(4,5)具有设备控制数据(5),其中仅当所述单独的数字标志(2)和所述签名(10)彼此存在预定的关系时,所述设备控制数据(5)才能由第一电子数据处理装置(11)来处理,其特征在于,所述第一电子数据处理装置(11)是能够电动运行的用于食品准备的家用设备的部件并且所述信息具有能够以文本形式和/或图像形式复述的食品准备食谱,当所述签名(10)和所述标志(2)彼此不存在预定的关系时,所述食品准备食谱也能由第二电子数据处理装置(12)利用人机界面来复述,并且所述设备控制数据(5)与所述食品准备食谱对应,所述设备控制数据(5)包括处理参数。

2.根据权利要求1所述的方法,其特征在于,所述处理参数包括温度、搅拌器转速以及相继跟随的处理步骤的时间。

3.根据权利要求1所述的方法,其特征在于,所述第一电子数据处理装置(11)是能够电动运行的家用设备的部件和/或所述设备控制数据(5)是用于能够电动运行的家用设备的运行程序。

4.根据权利要求1所述的方法,其特征在于,当所述签名(10)和所述单独的数字标志(2)彼此存在预定的关系时,所述设备控制数据(5)能够用于控制设备。

5.根据权利要求1所述的方法,其特征在于,为了产生所述签名(10),使用不对称的密钥对,该密钥对由私有密钥和公有密钥组成,其中在使用私有密钥的条件下产生所述签名,并且在使用公有密钥的条件下由第一电子数据处理装置(11)进行验证,和/或,为了产生所述签名(10),利用私有密钥来加密补充了单独的标志(2)的信息(4,5)或者利用私有密钥来加密由此形成的哈希值,和/或,所述签名(10)是在数据载体(1)上存储的具有信息(4,5)和单独的标志(2)的文件的组成部分,或者是在数据载体(1)上存储的分开的文件。

6.根据权利要求1所述的方法,其特征在于,所述信息(4,5)作为“标记语言”文件以PDF格式、SQLite格式、RTF格式、HTML格式、JPG格式、TIF格式或XML格式存储在数据载体(1)上。

7.根据权利要求1所述的方法,其特征在于,所述单独的标志是仅一次分配的系列编号。

8.一种用于执行按照权利要求1至7中任一项的方法的系统,该系统包括至少一个数据载体(1),在该数据载体上存储由数字数据组成的信息(4,5),其中所述数据载体(1)具有单独的数字标志(2),其中包括所述单独的标志(2)的签名存储在所述数据载体(1)上,其中所述信息(4,5)具有设备控制数据(5),其中仅当所述单独的数字标志(2)和所述签名(10)彼此存在预定的关系时,所述设备控制数据(5)才能由第一电子数据处理装置(11)来处理,其特征在于,所述第一电子数据处理装置(11)是能够电动运行的用于食品准备的家用设备的部件并且所述信息具有能够以文本形式和/或图像形式复述的食品准备食谱,当所述签名(10)和所述标志(2)彼此不存在预定的关系时,所述食品准备食谱也能由第二电子数据处理装置(12)利用人机界面来复述,并且所述设备控制数据(5)与所述食品准备食谱对应,所述设备控制数据(5)包括处理参数。

9.根据权利要求8所述的系统,其特征在于,所述处理参数包括温度、搅拌器转速以及相继跟随的处理步骤的时间。

10.根据权利要求9所述的系统,其特征在于,所述数据载体是USB棒。

11.一种集成半导体电路，具有用于与第一或第二电子数据处理装置(11,12)串行或并行地通信的控制电路以及具有存储装置，该半导体电路具有单独的数字标志(2)，并且在该存储装置上存储了由数字数据组成的信息(4,5)以及包括数字标志(2)的签名(10)，所述信息(4,5)具有设备控制数据(5)，其中所述单独的数字标志(2)和所述签名(10)彼此存在预定的关系，其中仅当所述单独的数字标志(2)和所述签名(10)彼此存在预定的关系时，所述设备控制数据(5)才能由第一电子数据处理装置(11)来处理，其中所述信息还具有与所述设备控制数据(5)对应的能够以文本形式和/或图像形式复述的食品准备食谱，当所述签名(10)和所述标志(2)彼此不存在预定的关系时，所述食品准备食谱也能由第二电子数据处理装置(12)利用人机界面来复述，其特征在于，所述设备控制数据(5)包括用于能够电动运行的用于食品准备的家用设备的处理参数。

12.根据权利要求11所述的集成半导体电路，其特征在于，所述处理参数包括温度、搅拌器转速以及相继跟随的处理步骤的时间。

13.一种能够电动运行的家用设备，其具有电子数据处理装置(11)，所述电子数据处理装置(11)被这样构造/编程，使得该电子数据处理装置从具有能够以文本形式和/或图像形式复述的处理食谱(4)和对应的设备控制数据(5)并且按照权利要求1至7中的任一项存储在具有单独的数字标志(2)的数据载体(1)上的信息(4,5)中仅处理具有所述单独的标志(2)的签名(10)与单独的数字标志(2)彼此存在预定的关系的这样的设备控制数据(5)。

14.一种根据权利要求13所述的能够电动运行的家用设备，其特征在于，仅当单独的数字标志(2)和签名(10)彼此存在预定的关系时，所述电子数据处理装置(11)才能够处理在所述数据载体(1)上存储的设备控制数据(5)。

用于将信息防复制地存储在数据载体上的方法

技术领域

[0001] 本发明涉及一种用于将由数字数据组成的信息存储在数据载体上并且从数据载体读取信息的方法，其中数据载体具有单独的数字标志(Kennung)，其中形成包括单独的标志的签名(Signatur)，其中信息至少具有信息组成部分，所述信息组成部分仅当单独的数字标志和签名彼此存在预定的关系时才能由第一电子数据处理装置来处理。

背景技术

[0002] 在DE102009018941A1中描述了一种前述种类的方法。为了对存储媒介的加密的文件系统进行访问，在那里应当使用存储元件的单独的标志。每个制造的存储元件具有与存储元件单独对应的并且因此仅一次分配的系列编号。在现有技术中由该系列编号和对密钥组的密钥的参考构成子密钥。应当仅当标志具有与密钥的正确关系时才允许借助安全媒介访问站(Secure Media Access-Station)对文件系统进行访问。将密钥复制到另外的存储媒介由此具有如下结果，即，访问被拒绝。应当利用个人密钥对子密钥或由此借助哈希函数(Hash-Funktion)获得的标志进行签名，例如基于不对称密码系统(asymmetrisch Krypto-System)，例如基于RSA-2048。

[0003] 从DE102007059236A1中，以及从商业标记“福维克美善品(Vorwerk-Thermomix)”公知电动家用设备，特别是厨房设备。属于现有技术的可电动运行的家用设备能够根据在程序存储器中存储的程序来工作，其中程序包含时间上相继的程序步骤并且程序步骤通过不同类型的处理参数，诸如处理温度或搅拌器的转速或过程步骤的持续时间来区别。所属的过程控制数据被存储在集成的半导体电路的存储装置中。

发明内容

[0004] 本发明要解决的技术问题是，提供措施，利用这些措施可以向电动家用设备提供过程控制数据和/或可利用人机界面复述的数据，其中应当同时确保，仅应用原始数据。

[0005] 上述技术问题通过在权利要求中给出的发明来解决。

[0006] 通过按照本发明的方法将由数字数据组成的信息提供到数据载体上。该数字信息在使用单独的、已签名的标志的情况下可以对可信度进行检查。仅当可以是独一无二的系列编号的单独的数字标志和在制造数据载体时或在将数字数据存储到数据载体上时产生的签名彼此存在预定的关系时，才由电子数据处理装置来处理、即读取和识别该信息。该关系可以构造为代码(Chiffrierung)。其可以是数据载体的单独的标志和签名的校验和数关系(Prüfsummenbeziehung)。可以以公知的方式在使用哈希函数的条件下产生数字签名，其中事先给出单独的数字标志，即数据载体(特别是USB棒)的系列编号，在其中写入了携带信息的文件或写入到额外的、但属于同一个文件系统的文件中。该以公知的方式利用私有密钥签名的文件然后被存储在数据载体上。在此例如考虑开头提到的不对称密码系统。在电动家用设备中布置的电子数据处理装置被这样编程，使得仅当签名通过验证时该电子数据处理装置才接受数据载体或在其上存储的信息。如果采用由私有和公有密钥组成的密码系

统，则允许借助公有密钥验证签名。在该优选的方案中通过使用公有密钥以及将在文件中存储的系列编号与数据载体的实际系列编号相比较来建立关系。在此在成功验证的情况下将在文件中存储的单独的数字标志(也就是特别是系列编号)与数据载体本身的系列编号相比较并且检查，两个编号是否一致。如果系列编号不一致或者作为篡改数据载体上存储的信息的结果的签名不能被验证，则拒绝处理在数字数据载体上存储的信息。然而按照本发明在签名的情况下不进行这样的加密，即，仅在使用合适的密钥的条件下才能够读取信息。而是按照本发明设置，信息至少具有信息组成部分，该信息组成部分能够由第二电子数据处理装置(即例如商业通用的PC或另外的数据显示设备)来处理，即读取或分析，特别是在人机界面上复述，即使签名和标志彼此不存在前面描述的关系，也就是验证失败或在文件中存储的系列编号与数据载体的系列编号不一致。在数据载体上存储的信息可以具有性质彼此不同的信息组成部分。由此信息可以具有以文本文件、音频文件、视频文件或图像文件形式的信息组成部分。这些可由使用者有意义地理解的数据可以经由不同的人机界面输出；例如可以在PC的显示器上显示文本文件和图像文件。与之相关的文件可以以PDF格式、RTF格式、HTML格式、XML格式、SQLite格式或另外的格式存储，特别是在使用“标记语言方案(mark-up-language-Konzept)”的条件下存储，其中系列编号可以存储在文件的不可显示的组成部分中。但系列编号也可以存储在额外的、同样在数据载体上存储的文件中。至少该文件被签名。此外，信息可以包含设备控制数据。设备控制数据优选是在合适的协议中包含过程参数的过程控制数据，其中过程参数可以是过程的持续时间、过程步骤的温度和/或搅拌器的转速等。该过程控制数据也可以加密地存储在数据载体上，从而该过程控制数据不能由第二电子数据处理装置来处理。

[0007] 此外，本发明涉及一种用于执行本方法的系统，该系统由数据载体组成，在该数据载体上存储由数字数据组成的信息，其中数据载体具有单独的数字标志，该数字标志与信息一样存储在数据载体上，但是其中对单独的标志进行签名。此外，系统具有电子数据处理装置，该电子数据处理装置被这样编程，使得当单独的数字标志和签名彼此不存在预定的关系时，也就是当签名不能被验证或者在数据载体上存储的数字标志与数据载体的实际的数字标志不一致时，该电子数据处理装置拒绝处理在数据载体上存储的数字数据。按照本发明，电子数据处理装置是可电动运行的家用设备的组成部分，特别是厨房设备的组成部分，并且特别优选地是用于根据预定的食谱准备食品的装置的部件，其中食谱作为信息存储在数据载体上。

[0008] 此外，本发明涉及一种可电动运行的家用设备，特别是厨房设备，其具有电子数据处理装置，该电子数据处理装置被这样编程，使得其能够从经由接口与电子数据处理装置相连的数据载体中读取数据，其中电子数据处理装置被这样编程，使得其验证在数字的数据载体上存储的数字数据的签名并且在成功验证的情况下将在数据载体上存储的、对于单独的数字标志的、由签名所一起包括的值与数据载体的实际的数字标志相比较。家用设备还被这样构造，使得当签名验证失败或者存储的单独的数字标志与数据载体的实际的单独的数字标志不一致时，拒绝处理信息。按照本发明的家用设备优选还能够执行由多个相继跟随的步骤组成的处理过程，特别是食品准备过程，其中过程数据是在数字的数据载体上存储的过程控制数据。

[0009] 此外，本发明涉及一种集成电路，特别是以具有集成的存储器和集成的控制器的

存储媒介的形式，其中在集成的存储器上存储了数字数据并且存储媒介具有单独的数字标志。重要的是，在存储媒介上存储的信息是处理食谱，该处理食谱可以在人机界面上，例如在显示器上以文本形式和/或图像形式显示，和/或包括可由家用设备执行的过程控制数据。在集成的存储器中以数字数据的形式存储签名，该签名可由前述种类的电子数据处理装置来验证。

[0010] 前面描述的独立权利要求的特征既是本身重要的，也可以彼此组合，其中独立权利要求1、12、15、16的另外的特征也可以仅与每个另外的独立权利要求的各个特征组合。

附图说明

[0011] 下面结合所附的附图对实施例作进一步说明。

[0012] 图1以方框图的形式示出了用于存储由数字数据组成的信息并且读取该信息的方法的流程以及一种按照该方法工作的系统。

具体实施方式

[0013] 在图1的位置E处示出了一种电运行的厨房设备，如其在DE102007059236A1中描述的那样。DE102007059236A1的内容就此完全地包含在本发明的公开中，为此目的，也包含在本发明的权利要求的特征中。

[0014] 附图标记11表征集成在电子厨房设备中的电子数据处理装置。该第一电子数据处理装置11可以由微控制器构成。厨房设备具有未示出的接口，利用该接口可以将外部存储媒介与电子数据处理装置11有效连接。

[0015] 以附图标记1表示商业通用的USB棒，该USB棒具有通用的串行接口，利用该串行接口可以将USB棒1与厨房设备的电子数据处理装置11或与以商业通用的PC形式的第二电子数据处理装置12进行数据传输连接。

[0016] 数字的数据载体1包括具有集成的存储器和集成的控制器的存储媒介。在其中存储了以普遍、即独一无二的系列编号的形式的单独的标志2。在图1中象征性地以附图标记2表征了该系列编号。

[0017] 附图标记3表示具有数字信息4和5的文件。数字信息4可以是可在PC12的数据显示设备上显示的信息，例如文本或图像，但也可以是音频或视频文件。这样的文件，例如PDF、RTF、HTML、XML、SQLite文件不仅包含纯信息，而且包含在那里作为附加标签或元数据存储的补充信息。同样作为不可见或不可有意义地理解的信息，在相同的文件3中或在属于同一个文件系统的文件中存储与数据载体1的系列编号2相应的值。此外，也可以由多个文件的群(Ensemble)组成的文件3可以携带设备控制数据5，该设备控制数据是过程控制数据，利用该过程控制数据，厨房设备的电子数据处理装置11可以在那里运行食品准备程序，其中过程控制数据5至少包含单个的处理步骤的持续时间、处理步骤的温度和搅拌器转速。

[0018] 由此在流程图的用A表示的位置处建立文件或多个文件3的群，其包括含单独的标志2、按照明文的处理食谱4和最优对应的设备控制数据5。

[0019] 在用B表示的位置处利用哈希函数8建立多位的校验数字，该校验数字表征文件或多个文件3的群的独一性。例如可以在使用信息摘要算法(Message Digest Algorythm)2(MD2)或类似算法，例如MD4、MD5或SHA256等的条件下产生哈希值。优选地使用算法SHA256，

因为该哈希值从安全性和处理速度来看被视为最好折衷。

[0020] 在流程规划的位置C处示出了不对称的密钥对，该密钥对包含公有密钥6和私有密钥7。两个密钥6、7具有如下特征，即，利用公有密钥6加密的文件仅能以对应的私有密钥7解密或者(按照本发明需要)将文件利用私有密钥来签名，其中签名仅能在使用公有密钥6的条件下被验证。可以以公知的方式根据RSA算法以足够的比特数产生与此相关的密钥对。

[0021] 在使用公有密钥7的条件下对在位置B处产生的哈希值8签名。在此形成的签名9至少包含单独的系列编号2的值。但在实施例中签名9延伸到包括信息4、5和单独的数字标志2的整个文件3。

[0022] 位置D表示，将作为证书10的数字签名9添加到文件3或由多个文件3组成的群中。

[0023] 该文件3或文件系统3现在被存储到数字的数据载体1，从该数据载体已经获得了单独的数字标志2。

[0024] 如果信息4、5也应当被存储到一个、特别是多个另外的数据载体上，则必须产生与此相关的单独的签名9，该签名与信息4、5一起被存储在各自的数据载体1上。

[0025] 如果改变在数据载体1上存储的信息4、5，则不能由第一电子数据处理装置11验证签名9或证书10。该验证在使用公有密钥6的情况下进行，该公有密钥被在厨房设备中的第一电子数据处理装置11中实施的程序所使用。验证13首先通过借助公有密钥6检查签名9、然后检查在文件3中存储的系列编号2与数据载体1中实际的系列编号2来进行。如果文件3或属于文件3的群的信息被复制到具有另外的系列编号2的另外的数据载体上，则第一电子数据处理装置11拒绝处理信息4、5，因为系列编号2不一致。对于篡改的数据同样适用，因为签名9不能被验证。

[0026] 但是同样地，可有意义地感知的信息4也可以由作为电子数据处理装置12的商业通用的PC来处理，即显示或使得可被有意义地理解。

[0027] 通过这种方式例如可以任意频繁地复制用于准备食品的可读的食谱。然后可以由任意的PC 12读取和显示该副本。但不能借助具有第一电子数据处理装置11的厨房设备使用该副本来准备食品。

[0028] 附图标记列表

[0029] 1 USB棒

[0030] 2 标志

[0031] 3 文件

[0032] 4 信息

[0033] 5 信息

[0034] 6 公有密钥

[0035] 7 私有密钥

[0036] 8 哈希值

[0037] 9 数字签名

[0038] 10 厨房设备

[0039] 11 第一电子数据处理装置

[0040] 12 第二电子数据处理装置

[0041] 13 验证

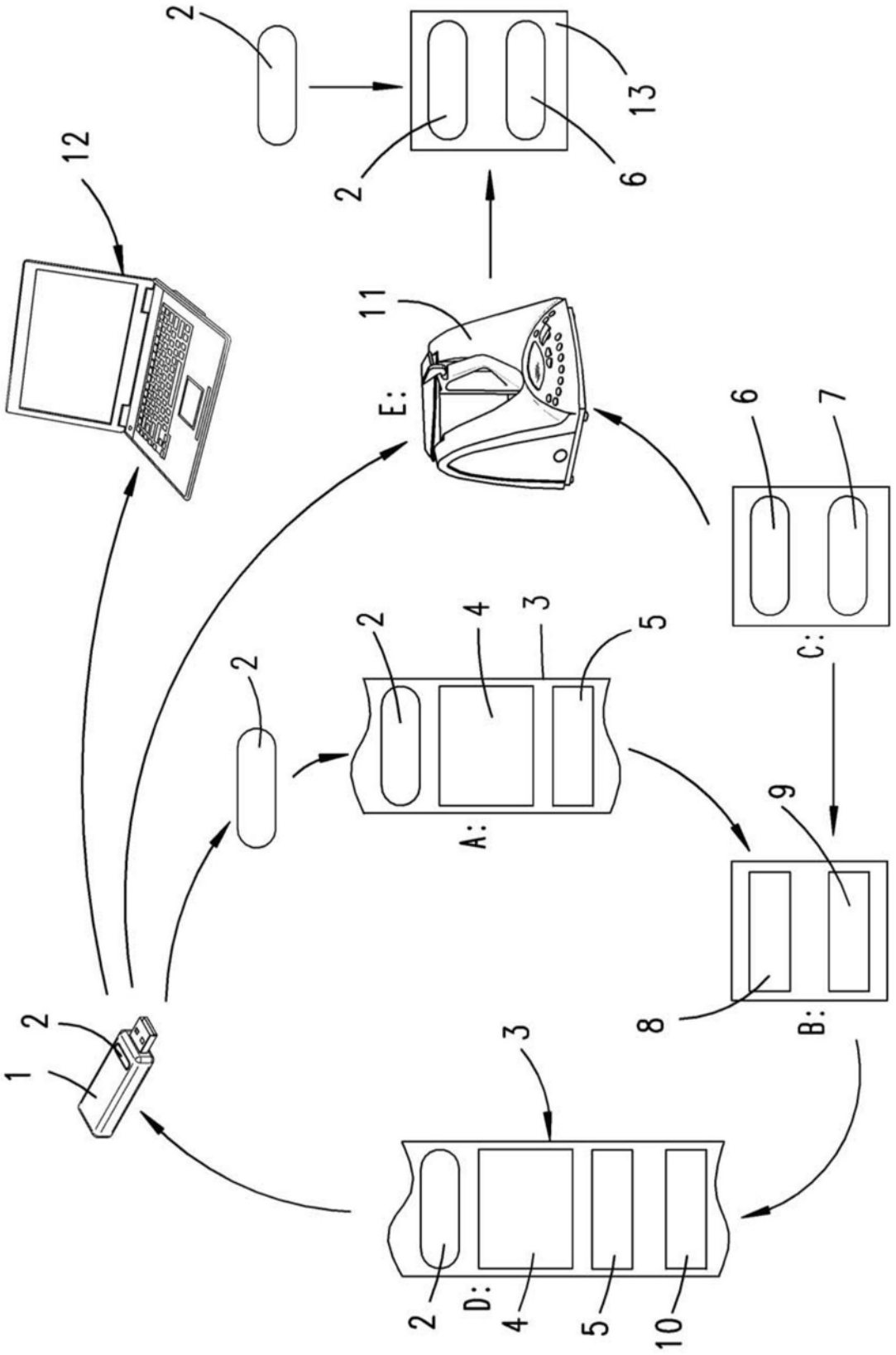


图1