



(12) 发明专利

(10) 授权公告号 CN 103189874 B

(45) 授权公告日 2016. 06. 22

(21) 申请号 201180052132. 3

(22) 申请日 2011. 10. 28

(30) 优先权数据

10-2010-0107317 2010. 10. 29 KR

(85) PCT国际申请进入国家阶段日

2013. 04. 27

(86) PCT国际申请的申请数据

PCT/KR2011/008160 2011. 10. 28

(87) PCT国际申请的公布数据

W02012/057577 EN 2012. 05. 03

(73) 专利权人 三星电子株式会社

地址 韩国京畿道

(72) 发明人 姜甫暻 李炳来

(74) 专利代理机构 北京市柳沈律师事务所

11105

代理人 钱大勇

(51) Int. Cl.

G06F 21/10(2013. 01)

G06F 21/78(2013. 01)

(56) 对比文件

CN 101315796 A, 2008. 12. 03,

CN 1512360 A, 2004. 07. 14,

CN 101441603 A, 2009. 05. 27,

US 2008163364 A1, 2008. 07. 03,

审查员 王慧敏

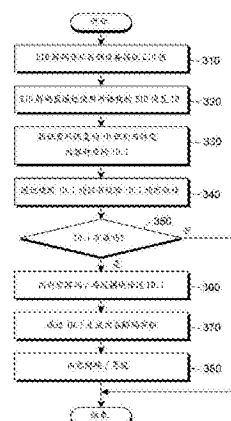
权利要求书2页 说明书4页 附图2页

(54) 发明名称

存储设备及存储设备的验证方法和验证设备

(57) 摘要

一种存储设备的验证方法,包括:由用于验证存储设备的验证设备向存储设备请求EID(经编码的标识符);由验证设备接收EID;通过解码所接收的EID恢复原始的ID信息;以及通过使用从存储设备接收的ID验证信息,校验包括在ID信息中的、与存储设备的使用对应的单个ID信息,其中ID信息包括与存储设备的使用对应的多条单个ID信息。



1. 一种存储设备的验证方法,该验证方法包括:

从所述存储设备接收与从存储设备的多个使用当中选择的所述存储设备的使用相应的经编码的单个ID,其中所述存储设备存储通过对多个单个ID编码获得的多个经编码的单个ID,所述多个单个ID标识所述存储设备并且分别与所述存储设备的多个使用相应;

通过解码接收到的经编码的单个ID来恢复与所述存储设备的所选择的使用相应的多个单个ID其中之一的单个ID;以及

使用与所恢复的单个ID对应的ID验证信息,来校验所恢复的单个ID。

2. 如权利要求1中所要求的验证方法,还包括:当所恢复的单个ID的校验失败时,确定是否丢弃所恢复的单个ID。

3. 如权利要求1中所要求的存储设备的验证方法,进一步包括:

从存储设备接收与所恢复的单个ID对应的ID验证信息。

4. 如权利要求1中所要求的存储设备的验证方法,其中,所述存储设备的多个使用包括内容的使用、私有信息的使用、加密数据的使用和证书信息的使用中的至少两个。

5. 如权利要求1中所要求的存储设备的验证方法,其中通过使用根据公钥基础设施的证书信息,来校验所恢复的单个ID。

6. 如权利要求1中所要求的存储设备的验证方法,其中通过根据广播密钥管理使用一组密钥,来校验所恢复的单个ID。

7. 一种用于验证存储设备的验证设备,该验证设备包括:

ID解码器,用于从所述存储设备接收与从存储设备的多个使用当中选择的所述存储设备的使用相应的经编码的单个ID,其中所述存储设备存储通过对多个单个ID编码获得的多个经编码的单个ID,所述多个单个ID标识所述存储设备并且分别与所述存储设备的多个使用相应,以及通过解码接收到的经编码的单个ID恢复与所述存储设备的所选择的使用相应的多个单个ID其中之一的单个ID;及

验证器,用于使用与所恢复的单个ID对应的ID验证信息,来校验所恢复的单个ID。

8. 如权利要求7中所要求的验证设备,其中当所恢复的单个ID的校验失败时,验证设备确定是否丢弃所恢复的单个ID信息。

9. 如权利要求7中所要求的验证设备,其中从存储设备接收与所恢复的单个ID对应的ID验证信息。

10. 如权利要求7中所要求的验证设备,其中,所述存储设备的多个使用包括内容的使用、私有信息的使用、加密数据的使用和证书信息的使用中的至少两个。

11. 如权利要求7中所要求的验证设备,其中验证器通过使用根据公密基础设施的证书信息,来校验所恢复的单个ID。

12. 如权利要求7中所要求的验证设备,其中验证器通过根据广播密钥管理使用一组密钥,来校验所恢复的单个ID。

13. 一种存储设备,包括:

经编码的标识符EID区域,其位于存储设备的特定区域,并且存储通过对多个单个ID编码获得的多个经编码的单个ID,所述多个单个ID标识所述存储设备并且分别相应于所述存储设备的多个使用;及

控制器,用于传送与从所述存储设备的多个使用当中选择的所述存储设备的使用相应

的经编码的单个ID到验证设备,和传送与所恢复的、与所述存储设备的所选择的使用相应的多个单个ID其中之一的单个ID相应的ID验证信息到所述验证设备以供验证所述存储设备。

14.如权利要求13中所要求的存储设备,其中ID验证信息包括根据公密基础设施的证书信息。

15.如权利要求13中所要求的存储设备,其中ID验证信息包括能够根据广播密钥管理进行密钥管理的一组密钥。

存储设备及存储设备的验证方法和验证设备

技术领域

[0001] 本发明大致涉及一种非易失性存储设备,并且更具体地,涉及非易失性存储设备的验证方法和验证设备。

背景技术

[0002] 在DRM(数字版权管理)技术中,通过使用诸如PKI(公钥基础设施)的密码技术来执行用于SD(安全数字)卡的CPRM(可记录介质内容保护)技术、用于蓝光盘的AACS(高级存取内容系统)技术、存储设备的验证。

[0003] 存储设备使用无关使用的特定标识符用于它自身的安全。当通过如上述的验证过程将存储设备认作不合适的存储介质时,通过单独的过程丢弃对应的存储设备。

[0004] 在用于SD卡的CPRM技术和用于蓝光盘的AACS技术的设备验证方法中,当生产存储介质时在被指定为只读区域的位置处存储标识符,并且采用密码方案用于设备验证和内容保护。

发明内容

[0005] 技术问题

[0006] 然而,生产出来后,如果由于存储设备的任何非法使用而丢弃标识符,则存储设备(即SD卡、蓝光盘)可能不再用于任何用途。

[0007] 因此,本领域需要一种用于根据存储设备的各种使用而提供标识符的方法。

[0008] 解决方案

[0009] 因此,本发明的一方面是解决现有技术中出现的上述问题,并且提供一种存储设备及存储设备的验证方法和验证设备,其中根据存储设备的使用来提供标识符使得可以针对每个标识符单独地执行验证。

[0010] 根据本发明,提供了一种存储设备的验证方法,包括:由用于验证存储设备的验证设备向存储设备请求EID(经编码的标识符);由验证设备根据请求从存储设备接收EID;通过解码所接收的EID而恢复原始的ID信息;以及通过使用从存储设备接收的ID验证信息,校验包括在ID信息中的、与存储设备的使用对应的单个ID信息,其中ID信息包括与存储设备的使用对应的多条单个ID信息。

[0011] 根据本发明,提供了一种用于验证存储设备的验证设备,该验证设备包括:ID解码器,用于向存储设备请求EID,根据请求从存储设备接收EID,并通过解码所接收的EID而恢复原始的ID信息;及验证器,用于通过使用从存储设备接收的ID验证信息,来校验包括在ID信息中的、与存储设备的使用对应的单个ID信息,其中ID信息包括与存储设备的使用对应的多条单个ID信息。

[0012] 根据本发明,提供了一种存储设备,其包括:EID区域,其位于存储设备的特定区域,并且存储用于特定地识别存储设备的EID;及ID验证信息,包括用于校验ID信息的信息,其中ID信息包括与存储设备的使用对应的多条单个ID信息。

[0013] 有益效果

[0014] 在本发明中,根据存储设备的使用提供多个标识符,并且单独验证每个标识符。因此,当对于用于存储设备的特定使用的标识符的验证失败时,可以单独地放弃仅仅验证失败的特定使用的功能,而不是整个存储设备。因此,即使放弃用于存储设备的特定使用的功能,存储设备仍可以继续用于其它用途,从而改善了存储设备的适用性。此外,本发明的存储设备可以按相同方式通过使用同一验证设备(ID解码器)来执行对于多个标识符的验证过程。

附图说明

[0015] 从下面结合附图的详细描述中,本发明的上述和其他方面、特征和优点将变得更加清楚,其中:

[0016] 图1示出根据本发明的标识符的结构和存储设备的配置;

[0017] 图2示出根据本发明的执行存储设备的验证的验证设备的配置;以及

[0018] 图3示出根据本发明的存储设备的验证过程。

具体实施方式

[0019] 以下将参照附图详细描述本发明的设备和操作。在下面的描述中,阐述诸如配置元件的具体细节以便提供对本发明的彻底理解。对本领域技术人员来说,显然可以在不脱离本发明的精神的情况下进行各种改变和修改。此外,为了清楚和简明,在此将不详细描述公知技术。

[0020] 本发明公开了根据非易失性存储设备的使用的单独的验证方法及其设备,其可以改善存储设备的适用性。为此,本发明的存储设备包括与存储设备在特定领域的各个功能对应的多个ID,其中ID被编码。当使用存储设备时,用于验证存储设备的验证设备通过使用ID解码器恢复原始ID,并通过校验(verify)与使用对应的ID而执行验证。当由于存储设备的特定的非法使用而验证存储设备失败时,仅丢弃与该ID的特定非法使用对应的ID以便禁止非法使用。因此,存储设备可以继续用于其它目的。

[0021] 图1示出根据本发明的标识符的结构和存储设备的配置。

[0022] 在图1中,用于标识存储设备130的ID110包括多个单独的ID(ID_i)和校验和。使用标识符的单个ID来标识存储设备的各个使用。存储设备可以用于各种目的,诸如私有信息存储、使用诸如DRM的文件加密技术的数据存储、证书信息存储和内容存储。可以根据每种使用来生成单个ID。

[0023] 参照图1,ID编码器120通过使用用于标识存储设备130的ID110来生成EID。

[0024] 存储设备130包括EID131和与ID110的各自单独的ID对应的证书132。证书132与用于校验由验证存储设备的验证设备恢复的ID的适合性的信息对应。

[0025] 在存储设备130的生产步骤或测试步骤中通过ID编码器120对用于标识存储设备130的ID110编码,并将其转换成EID131,并且EID131被编程到存储设备130中。在存储设备130的记录或再现期间,执行记录或再现的主机设备通过使用EID来执行存储设备的验证。

[0026] 图2示出根据本发明的执行存储设备的验证的验证设备的配置。

[0027] 参照图2,存储设备130包括用于存储经编码的ID信息的EID131,及用于校验各个

ID的多个证书132,并且可以存储诸如图像内容133(诸如电影)和私有信息134的数据。存储设备130还包括用于控制存储设备的输入/输出及读/写的控制器(未示出)。控制器控制向验证设备传送EID和ID验证信息,用于验证存储设备。

[0028] 在图2中,用于验证存储设备130的验证设备(主机设备)140包括EID解码器141、验证器142和内容解码/再现模块143。

[0029] EID解码器141从存储设备130接收EID,并且从EID恢复原始ID。

[0030] 验证器142接收从EID解码器141输出的存储设备130的ID,并且通过执行密码校验来执行存储设备的验证。验证设备140,即主机设备,根据主机设备要使用的存储设备的用途,通过使用对应的存储设备的单个ID_i和证书132来确定存储设备130的合法性。

[0031] 当验证器142确定单个ID合法时,内容解码/再现模块143通过使用单个ID的值来生成内容解码密钥,并且通过解码内容来执行内容再现。

[0032] 在存储设备130的验证期间,EID解码器141从存储设备130的EID区域131接收EID,并且验证器142从存储设备接收证书132。

[0033] 为了校验存储设备130的单个ID,使用证书132的公共密钥基础设施(PKI)被使用。然而,本发明不限于此。如果使用广播密钥管理,则代替证书132,可以提供根据各自用途的能够进行密钥管理的一组密钥。此外,可以与广播密钥管理技术组合使用PKI方案。在这种情况下,存储设备130可以包括证书和能够进行密钥管理的一组密钥两者。

[0034] 图3示出根据本发明的存储设备的验证过程。

[0035] 参照图3,当用于执行存储设备130的记录或再现的主机设备接收关于存储设备130的特定内容的存取请求时,包括在主机设备中的用于验证存储设备130的验证设备140在步骤310中通过EID解码器141向存储设备130作出对于EID的请求,并且接收根据请求的来自存储设备130的EID。

[0036] ID解码器141可以被设置为根据存储设备130的使用而仅从存储设备130接收EID当中的、与存储设备130的使用对应的经编码的单个ID ID_i。具体地,当向存储设备130作出对于EID的请求时,ID解码器141传送关于存储设备130的使用的信息。

[0037] 基于关于存储设备的使用的信息,根据控制器的控制,存储设备130从EID131中仅提取与使用对应的经编码的单个ID,并且向ID解码器141传送所提取的经编码的单个ID。

[0038] ID解码器141可以被设置为在步骤310中接收存储设备130的所有EID,并且在更后的步骤中仅使用与存储设备130的使用对应的单个ID。

[0039] 在步骤320中,EID解码器141通过使用所接收的EID恢复原始的ID。

[0040] 在步骤330中,验证器142从所恢复的ID识别与存储设备的使用(特定内容)对应的单个ID_i。验证器142从存储设备接收与单个ID对应的证书132。

[0041] 在步骤340中,验证器142通过使用证书132校验单个ID ID_i的有效性。在此有效性校验中,可以如下使用下面的算法1。

[0042] Hash(ID_i)=?校验和.....算法1

[0043] 在步骤350中,确定是否已校验单个ID的有效性。当已确定单个ID非法时,结束该过程。主机设备可以停止内容的再现,并且可以连接到预定的许可权站点,并且通过发送丢弃的理由来向所连接的站点作出放弃使用对应的存储设备130的请求。

[0044] 在步骤350中,当已确定单个ID合法时,该过程前进到步骤360,其中对内容解码/

再现模块143被调用(page)并且向内容解码/再现模块143传送单个ID ID_i。

[0045] 在步骤370中,当所校验的单个ID被定义为用于图像数据的ID时,内容解码/再现模块143通过使用单个ID生成内容解码密钥。此处,可以通过使用如下定义的算法2来生成内容解码密钥。

[0046] Hash(ID_i,Decryption Key(解密密钥))=ContentsDecryptionKey(内容解密密钥)...算法2

[0047] 在步骤380中,解码并再现内容。

[0048] 在本发明中,根据存储设备的使用提供各种标识符,并且单独验证每个标识符。因此,当对于用于存储设备的特定使用的标识符的验证失败时,可以单独地放弃仅仅验证失败的特定使用的功能,而不是整个存储设备。因此,即使放弃用于存储设备的特定使用的功能,存储设备可以继续用于其它用途,从而改善了存储设备的适用性。此外,本发明的存储设备可以按相同方式通过使用同一验证设备(ID解码器)来执行对于各个标识符的验证过程。

[0049] 虽然详细描述了本发明,但是在本发明的描述中的实施例仅仅是例子,并且本发明不限于此。本领域技术人员将理解,在不脱离如所附权利要求定义的本发明的精神和范围的情况下,可以在其中进行在形式和细节上的各种改变。

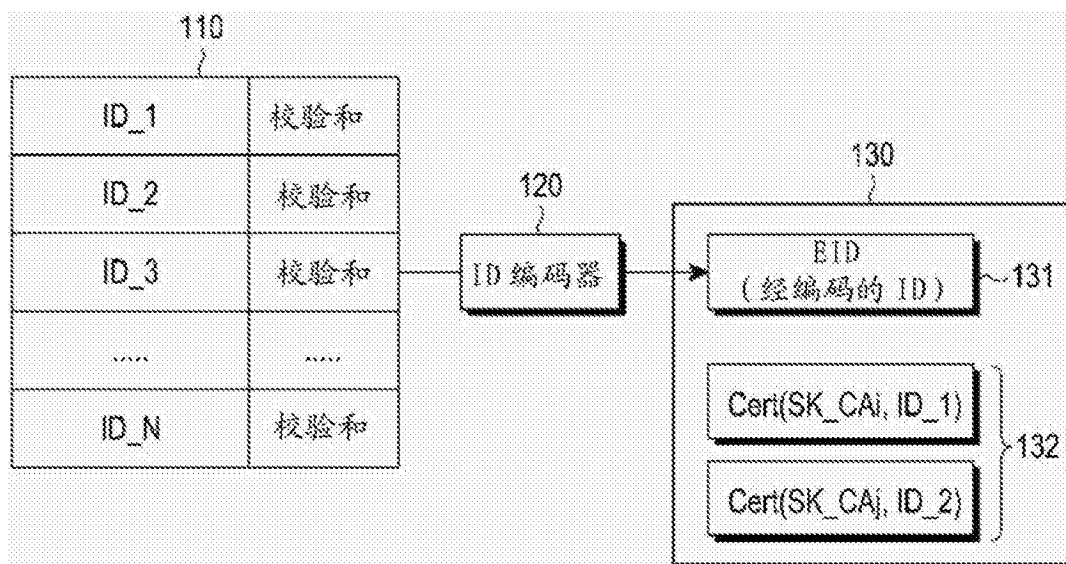


图1

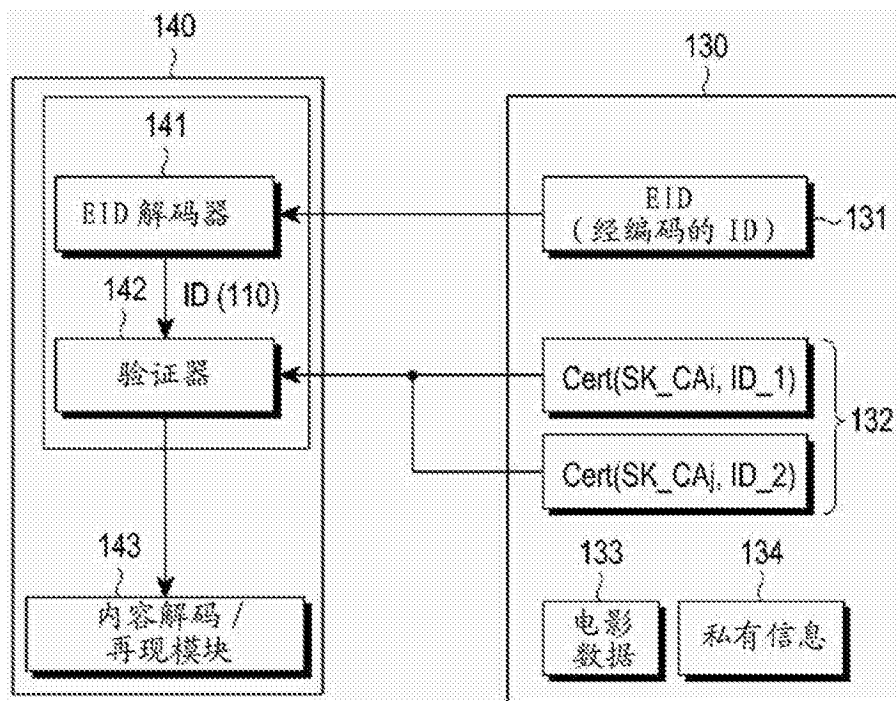


图2

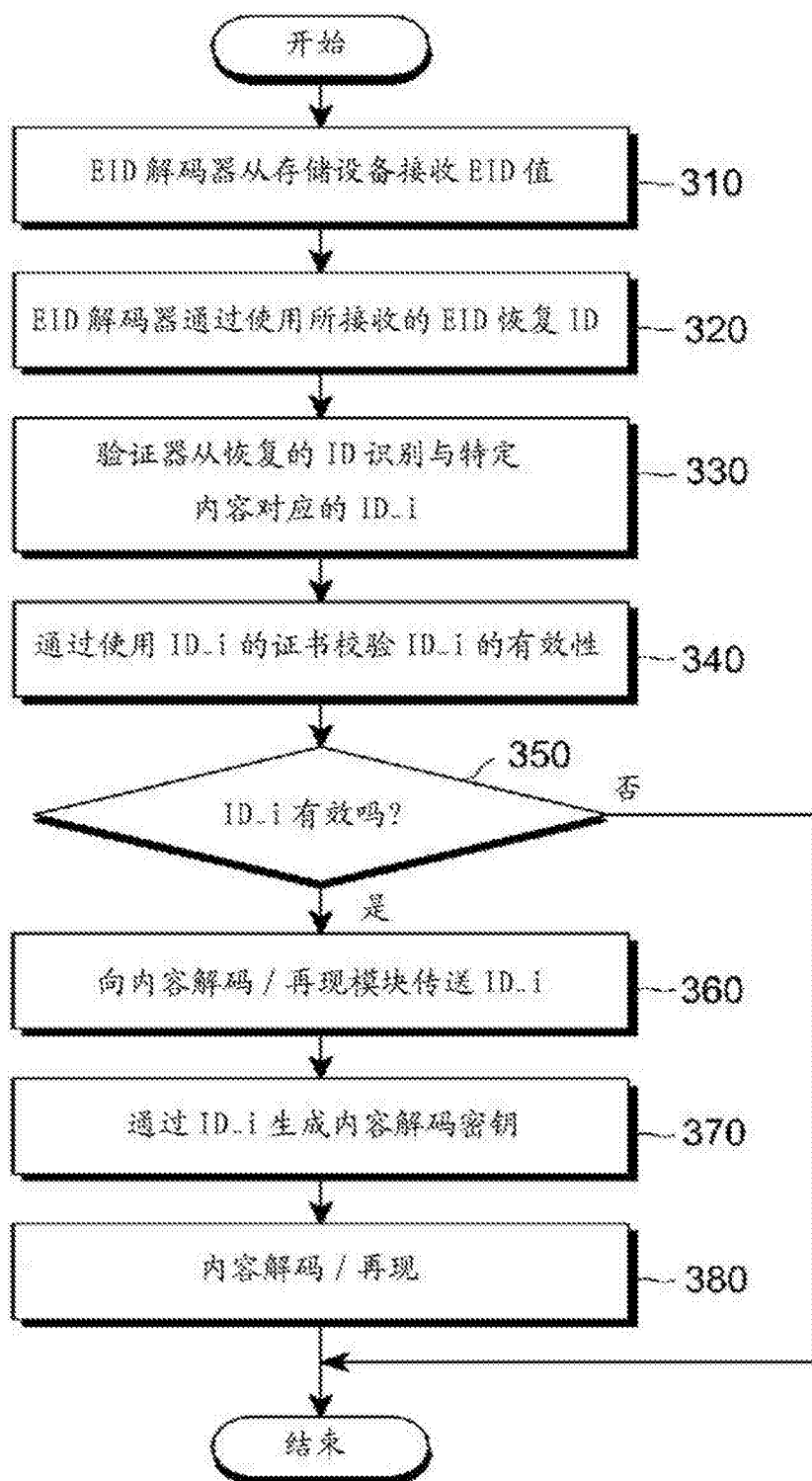


图3