(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 1658314 B
(45)授权公告日 2010.10.13

(21)申请号 200510052659.2

(22)申请日 2001.05.08

(30)优先权数据
00201951.1 2000.06.02 EP

(62)分案原申请数据
01801572.7 2001.05.08

(73)专利权人 皇家菲利浦电子有限公司
地址 荷兰艾恩德霍芬

(72)发明人 J·P·M·G·林纳茨
A·A·C·M·卡尔克
J·C·塔尔斯特拉

(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 吴立明 陈景俊

(51)Int.Cl.
G11B 20/00(2006.01)
G11B 20/10(2006.01)
G11B 20/12(2006.01)
G06F 12/14(2006.01)

(56)对比文件
US 5982886 A,1999.11.09, 全文.
CN 1248768 A,2003.03.29, 全文.

审查员 李冰

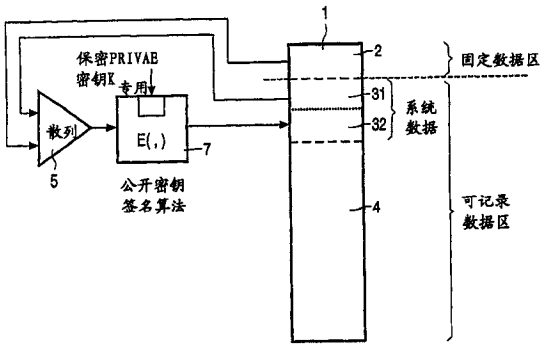
权利要求书 2 页 说明书 4 页 附图 3 页

(54)发明名称

存储数据的方法和记录/重放设备

(57)摘要

本发明涉及一种数据存储方法，该方法将可记录数据存储介质上的数据存储到相应的存储介质，存储到相应的记录装置以及相应的重放装置。复制保护措施要求，在可重写存储介质上必须存储某些数据，而这些数据非用户的终端产品将不能修改或抹掉。实际问题是大量的这类数据要存储在固定数据区。一般其容量限制在几位。同时，需要存储的复制保护数据数量可能大大超出在只读固定数据区能够得到的存储能力。因此，本发明提高把复制保护数据作为系统数据，例如作为介质(1)格式化部分写入可记录数据区(4)。计算密码提要并同时存储在可记录数据区(32)或固定数据区(2)，这样就提供了固定数据区(2)和系统数据区(3)之间的密码关系。重放或重放装置将只接受具有复制保护数据与固定数据有效组合的存储介质。



CN 1658314 B

1. 在可记录数据存储介质 (1) 上存储数据的方法，该存储介质 (1) 包括只读固定数据区 (2) 和可记录数据区 (3,4)，其中系统数据被存储在可记录数据区 (3)，其特征在于，

- 系统数据的密码提要在固定数据区 (2) 中生成并存储，及

- 密码提要被用于在用户数据读出和 / 或记录前系统数据的验证。

2. 在可记录数据存储介质 (1) 上存储数据的方法，该存储介质 (1) 包括固定数据区 (2)，其特征在于 ：

- 固定数据区以角落区的形式包含第一固定数据区和第二固定数据区，

- 系统数据被存储在角落区，

- 系统数据的密码提要在第一固定数据区生成和存储，及

- 密码提要被用于在用户数据读出和 / 或记录前系统数据的验证。

3. 权利要求 1 提出的方法，其特征在于 ：散列函数 (5) 被用于生成密码提要和验证系统数据。

4. 权利要求 1 提出的方法，其特征在于 ：使用信息证实代码算法来生成密码提要和验证系统数据。

5. 权利要求 1 提出的方法，其特征在于 ：使用密匙签名算法来生成密码提要和验证系统数据，并且签名是作为密码提要存储的。

6. 权利要求 1 提出的方法，其特征在于 ：密码提要的生成和系统数据在可记录数据区 (3) 中的存储都是作为存储介质 (1) 格式化的部分进行的。

7. 权利要求 1 提出的方法，其特征在于 ：复制保护信息是作为系统数据来存储的。

8. 权利要求 7 提出的方法，其特征在于 ：所述系统数据包括唯一的存储介质标识符、用一个或多个不同制造厂商特有的或装置特有的密匙加密的密钥，以及用一个或多个清除的装置或清除的存储介质的清单。

9. 权利要求 1 提出的方法，其特征在于 ：系统数据原来被存储在可记录数据区 (3) 的角落区而在首次使用记录装置的存储介质 (1) 的过程中，系统数据被复制到可记录数据区 (3,4) 的用户数据区 (4)。

10. 将数据存储在可记录数据存储介质 (1) 上的记录装置，该记录装置包括记录设备，它把系统数据存储在介质的可记录数据区 (3)，其特征在于，包括生成设备 (5)，它生成系统数据的密码提要，并且该记录设备适合用于把密码提要存储在介质 (1) 的只读固定数据区 (2)，提供密码提要以在用户数据读出和 / 或记录前对系统数据进行验证。

11. 将数据存储在可记录数据存储介质 (1) 上的记录装置，该可记录数据存储介质 (1) 包含固定数据区 (2)，其特征在于，

- 该固定数据区以角落区的形式包含第一固定数据区和第二固定数据区，

- 包括记录设备，它把系统数据存储在角落区，并把系统数据的密码提要存储在第一固定数据区，提供密码提要以在用户数据读出和 / 或记录前对系统数据进行验证，

- 包括生成设备 (5)，它生成系统数据的密码提要。

12. 重放存储在可记录数据存储介质 (1) 上的用户数据的重放装置，该重放装置包括读出设备，它读出存储在介质 (1) 的可记录数据区 (3,4) 中的系统数据，其特征在于，该读出设备还适合用于读出存储在介质 (1) 的只读固定数据区 (2) 中的系统数据的密码提要，及包括验证设备 (5,6)，它用于生成从介质 (1) 读出的系统数据的密码提要并利用所生成

的密码提要对系统数据进行验证。

13. 重放存储在可记录数据存储介质 (1) 上的用户数据的重放装置，该可记录数据存储介质 (1) 包含固定数据区 (2)，其特征在于：该固定数据区以角落区的形式包含第一固定数据区和第二固定数据区，该重放装置包括

- 读出设备，它读出被存储在角落区的系统数据以及被存储在第一固定数据区 (2) 中的系统数据的密码提要，及

- 验证设备 (5,6)，它生成从介质 (1) 读出的系统数据的密码提要并利用所生成的密码提要对系统数据进行验证。

存储数据的方法和记录 / 重放设备

[0001] 本申请是已于 2001 年 5 月 8 日提交的国际申请 :发明名称“有数据保护区的可记录存储介质”、国际申请号 PCT/EP0/05195、国家申请号 01801572.7 的分案申请。

[0002] 本发明涉及一种数据存储方法。该方法将可记录数据存储介质上的数据存储到存储介质,存储到将数据存储在可记录数据存储介质上的记录装置,存储到将存储在可记录数据存储介质上的用户数据重放的重放装置。

[0003] 本发明阐述的存储介质,用户可在其上面存储有版权的和任意复制 (copy-free) 的材料。通常用户有权存储和复制存储信息,但是他能复制 (生成) 的数目存在限制。使用加密来确保享有版权的存储信息只能由遵守复制保护限制的“服从 (compliant)”装置进行翻译。需要进一步的保护以避免非服从装置能够按位复制加密数据。把重要信息,例如解密密匙以不可能被复制的方式存储起来常常能避免加密数据的复制。

[0004] 更一般地结论是复制保护措施要求,在可记录盘上必须存储一些数据,这些数据靠用户的终端产品将不能修改或抹掉。这些数据在下面将称为“系统数据”。“系统数据”的实例是 :

[0005] - 特有的盘标识号码,它用来对用户在该盘上存储的数据加密,

[0006] - 由单个密匙组成的清单,该密匙已用几个不同制造厂商特有的或装置特有的密匙加过密,

[0007] - 被清除装置或被清除盘的电子序号清单。把这样的清单存储到所有的空盘上,清除指令就能传播给用户装置。一旦收到这样的清除指令,服从装置就拒绝与被清除装置联络。

[0008] 用户记录的内容或数据在下面将称为“用户数据”。此外,术语“固定数据区”将用于这样的存储介质区,在该区中存储的任何信息都是只读的而且不能由用户装置进行修改。相反地,在“可记录数据区”存储的信息能够由用户装置修改。同样,在恶意用户已对用户装置做了某些修改 (“黑客”) 后只能由该装置写入数据将存储在可记录数据区。这样的修改可能成为控制记录器的固件或软件中的变化。

[0009] 在固定数据区存储数据要求使用一些部件,这些部件一般在用户装置中是无法得到的。存储这种数据的一个技术实例就是“波动法 (wobble)”,它是使槽位或预留纹道自完善的螺旋纹产生径向偏离的方法。物理学和力学定律都禁止把这样的波动像光盘用户可记录器中可用的那样匆忙地用激光写入。在固定数据区存储的其他数据实例有推荐给 DVD-ROM 的 BCA 代码或数据,代码是用大功率激光在盘材料上有选择烧制的一些破损点,数据是存储在含只读材料的盘特别区中的数据。

[0010] 实际问题是在固定数据区存储大量数据的问题。通常其容量限制在几 (几百) 位。另一方面,需要存储的系统数据可能会大大超过固定数据区中具备的存储能力。

[0011] 因此,本发明的目的就是提供一种在可记录数据存储介质上存储数据的方法,依照此法上述问题被克服了,此法还使大量系统数据的存储能以抗窜改的方式进行。另外,将提供相应的存储介质,相应的可记录装置以及相应的记录装置。

[0012] 按照本发明,使用权利要求 1 或 2 中提出的方法,权利要求 9 或 10 提出的存储介

质，权利要求 12 或 13 中提出的记录装置以及权利要求 14 或 15 提出的重放装置，这些目的都达到了。

[0013] 本发明主要是基于这样一种思想，即在固定数据区中存储的数据与系统数据之间存在某种密码关系。这种关系是通过密码提要 (cryptographic summary) 形成的，而密码提要根据本发明则是由系统数据单独或系统数据与标识数据一起生成的，标识数据可以是存储在固定数据区的一个随机数。记录或重放装置使用此密码提要探测系统数据是否已被窜改，例如被抹掉或修改，以便控制存储介质的复制保护。因而密码提要也用来验证系统数据，这就意味着一旦验证失败，存储介质之存储信息的读出或记录就能够停止。

[0014] 按照第一种解决办法，系统数据被写入可记录数据区，例如作为存储介质格式化部分被写入。密码提要例如密码散列 (cryptographichash) 是在系统数据范围内计算的，而该密码提要的结果，例如该散列的结果则被存储在固定数据区。这样记录装置将只接受具有系统数据与固定数据如密码提要有效组合的存储介质。

[0015] 按照另一种解决办法，标识数据，例如随机数，生成并存储在固定数据区。因而可记录数据区已含用户数据，系统数据，以及系统数据与标识数据例如其电子签名的密码提要。记录或重放装置将使用验证器（例如公开密匙）检验密码提要，系统数据以及标识数据的有效性，亦即将检验签名的有效性。取代使用电子签名，可以使用信息证实代码 (MAC) 进行验证，它比较便宜但安全性较差。

[0016] 本发明的其他优选实施方案均公开于相关的权利要求中。

[0017] 本发明及其优选实施方案在下文中将参照附图进行更详细的说明，附图中

[0018] 图 1 示出依照第一实施方案的记录方法，

[0019] 图 2 示出依照第一实施方案的重放方法，

[0020] 图 3 示出依照第二实施方案的记录方法，

[0021] 图 4 示出依照第一实施方案的重放方法，

[0022] 图 5 示出依照第三实施方案的记录方法，及

[0023] 图 6 示出依照第三实施方案的重放方法。

[0024] 图 1 示出示意图，它说明了依照本发明第一实施方案将数据存储在可记录数据存储介质上的方法。存储介质 1，它可以是数据光学记录盘例如 DVD 或 CD，被分成为只读固定数据区 2 和可记录数据区 3、4，可记录数据区又再细分成系统数据区 3 和用户数据区 4。存储在固定数据区 2 中的数据，用户不能修改。固定数据区 2 的典型执行过程是将槽压入可重写盘，即是，部分可重写盘用作为 CD-ROM 或 DVD-ROM 介质。另一种执行过程是 BCA（脉冲串切割区 (Burst Cut Area)），一种处在极其靠近盘中心的条码图，该条码图在盘生产厂家用 YAG 激光器写入。第三种执行过程是把固定数据存储在预压槽（“槽 - 波动”）以径向位移或预留纹道（“预留纹道波动”）的径向位移中。

[0025] 存储在可记录数据区 3、4 的数据能够由用户修改。尽管如此，系统数据区还是保留给系统数据，如像开头概述过的复制保护信息。可记录数据区最大部分 4 可以用来存储用户数据，例如音频或视频数据。

[0026] 既然固定数据 2 区的容量有限，而数量不断增长的系统数据又要存储并且不予修改，本发明提出将系统数据存储在记录数据区 3，并且在系统数据和存储在固定数据区 2 且在随后的记录或重放过程中又不能修改的特殊信息之间建立密码关系。因此，系统数据的

密码提要使用生成设备 5 计算，它计算出本实施方案中系统数据的散列。然后，该散列的加密可靠结果存储在固定数据区 2。

[0027] 图 1 所述方法最好在这样的记录装置上实施，该装置使用同样的或分立的记录设备把系统数据和密码提要存储在空白介质上。

[0028] 在如图 2 所示的重放装置中，存储在系统数据区 3 中的系统数据散列使用重放装置中包含类似的生成设备 5 进行计算。计算结果传送给重放装置中的验证设备 6，验证设备 6 同时也收到从介质 1 的固定数据区读出的密码提要。如果该数密码提要与散列计算结果相等，验证就是成功的，用户数据的重放可以开始或继续，相反在验证失败后，播放就可以停止，因为系统数据已被操纵的概率很高。从介质中读出系统数据和密码提要的读出设备来示出。

[0029] 在实际认识中，介质 1 可以想象成为是（最初是空白的）DVD-RAM 或 CD-RW 或某些其他可重写介质，这些介质有卖并含有已知盗版记录器，以下称为“顽皮 (naughty)”记录器的在盘生产厂家已经写好的序号清单。DVD-RAM/CD-RW 或其他介质的诚实用户使用此请单来拒绝重放这些记录器的记录，因为人们已经知道它们卷入了非法复制之中。这样的清单通常太长（一般多于 1MB），不能存储在固定数据区（一般为几百位）。因此，该清单如同正规文件一样在生产厂中写在可重写介质上。为防止有人要抹掉或修改此清单，对清单的散列进行了计算。此散列比系统数据短得多，因此在介质生产过程中就能很容易地写进固定数据区。这样，可靠的播放器在插入介质时就会首先计算系统数据的散列并用固定数据区中存储的散列对结果进行检查。若它们不相一致，系统数据就已被窜改过了。

[0030] 在这种基本形式中，系统中的任何地方都不必使用密码保密（例如密码密匙）。但缺点是缺乏灵活性。这就意味着可重写介质上固定数据区的实际位数内容在工厂的生产盘的时候就永久地固定了。因而，应该保护的系统数据的散列在盘生产之前就必须计算。如果系统数据要改变，例如将更多的顽皮记录器加到清单上，那么散列改变。这样工厂就必须生产新介质，因为旧介质对新的系统数据不再有正确的散列。还存在其他一些原因说明为什么系统数据在盘生产和散列固定后应该改变或校正。

[0031] 在图 3 和 4 所示的本发明第二实施方案中得到了更大的灵活性。按照这一实施方案，标识数据例如随机数，在介质生产过程中就存储在固定数据区。系统数据区再细分为用于实际系统数据的第一区 31 和用于存储密码提要的第二区 32。此密码提要使用生成设备 7 算出的公开密匙签名算法来生成。其中标识数据和系统数据的数字签名使用保密专有密匙 $K_{专有}$ 进行计算，向系统数据是通过生成设备厂先用散列编过码的。这一计算还可以写成为

[0032] ED = E（散列（系统数据，标识数据），专有密匙）其中 ED 表示额外数据（= 密码提要），E 表示公开密匙密码。算出的数字签名再作为密码提要存储在第二系统数据区 32。

[0033] 在如图 4 所示的重放装置或记录装置中，系统数据是首先通过在标识数据和系统数据范围内计算散列，然后使用验证设备 8 中公开密匙签名验证算法和公开密匙 $K_{公开}$ 来进行验证，以检验数据区 32 中存储的签名的有效性。用来生产图 3 中数字签名的专有密匙必须保持保密，而用于图 4 所示重放或记录装置中验证工作的公开密匙可以自由分配，因为这种公开密匙在如图 3 所示的加密步骤中是毫无用处的。

[0034] 第三实施方案图 5 和 6 予以说明。如同在第二实施方案中一样，标识数据存储在

固定数据区 2，实际系统数据存储在系统数据区 31。为了加密，用生成设备 9 来生成密码提要，密码提要应存储在系统数据区 32，而生成设备 9 则使用信息证实代码算法（MAC 算法）和保密 MAC 密匙根据标识数据和系统数据来生成密码提要。这种 MAC- 密码可以简单地写成为

[0035] ED ＝ E（系统数据，固定数据，MAC- 密匙）其中 ED 表示额外数据（＝密码提要），E 表示 MAC- 密码。

[0036] 在如图 6 所示的记录或重放装置中，设置相应的生成设备 9 来计算信息证实代码，后者是使用同样的保密 MAC- 密匙根据标识数据和系统数据进行计算的。出于验证原因，算出的 MAC 要在验证设备 6 中与存储在系统数据区 32 中的密码提要 (MAC) 进行比较。

[0037] 与示于图 3 和 4 中的第二实施方案相比，使用 MAC 要比使用公开密匙签名的安全性差。用于计算 MAC 的密匙留存在系统中的每个重放装置，如果有人闯开任何一个单个播放器并掌握了这把密匙，此人便可以继续前进并用其他的能证明 MAC 的系统数据来代替该系统数据。相反，在第二实施方案的公开密匙系统中，加密方法中使用保密专有密匙，而公开的公开密匙则用检验证。

[0038] 使用本发明可以防止系统数据受到操纵。在固定数据区存储特殊数据就能防止恶意记录器把旧的有效系统数据复制到新介质上，例如用旧的短的清单来代替顽皮记录器的新的大清单。由于系统数据本身存储在可记录数据区，固定数据区容量有限的问题就克服了。

[0039] 一般，系统数据存储或隐蔽在用户进不去的区域或介质区，在此区中系统数据不会影响盘的一般用途，即不会影响用户数据存储。对 DVD 和 CD 来说，一个实例就是所谓的盘‘引入 (lead in)’和‘引出 (leadout)’区。下文中这样的区域将统称为‘角落区’。其优点是它不麻烦用户，而且通常还使生产过程便宜得多，因为角落区能极快地压印，而可记录数据则不得不以常规速度记录。一般来说，播放器比记录器便宜得多也简单得多，所以播放介质角落区中的系统数据，对播放器来说比之于记录器是个相当大的负担。因此，首次使用介质时，拥有记录器读出系统数据并将其信息复制到记录数据区中的主用户数据区是有意义的。这样读出器就能找到主用户数据区中的系统数据信息，而重放器无论以何种方式都能重放此信息。问题是播放器不能信任可记录器，因为后者可能没有如实地复制系统数据。然而，如果按照本发明第一实施方案那样，把系统数据的散列存储在固定数据区，那么读出器就能确定主用户数据区中体现的系统数据与固定数据区中的散列相符合。显然记录器不可能操纵固定数据区。

[0040] 应当指出，本发明的任何细节每次都是重放装置说明的，但重放装置也可以用可记录装置取代。两种装置可能包括适当的读出和 / 或记录设备把数据从介质中读出或记录进介质。另外，应当了解，权利要求中提出的存储介质，记录装置以及重放装置可以按照上述和附属权利要求中提出的同样或相应方法并参照数据存储方法进行了进一步的开发。

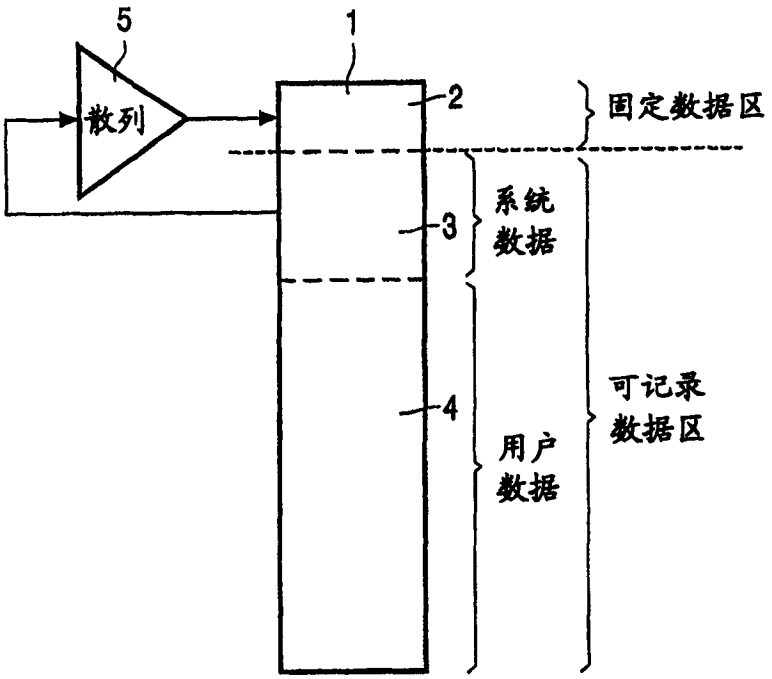

5
1
散列
2
固定数据区
系统
数据
3
可记录
数据区
4
用户
数据

图 1

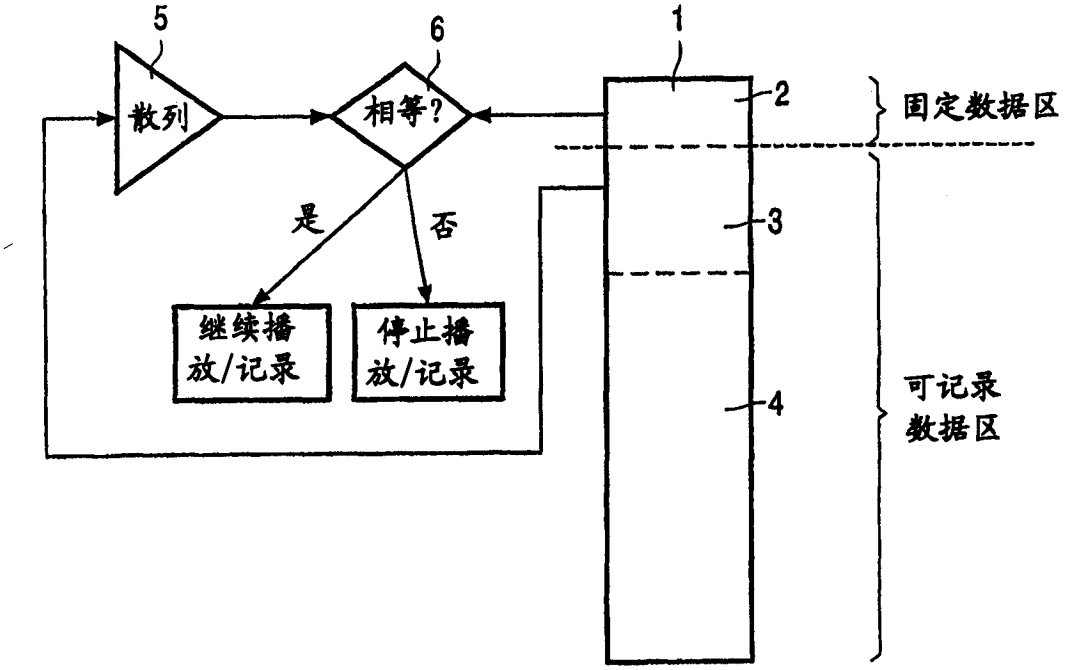

5
6
1
散列
相等?
2
固定数据区
是
否
3
继续播
放/记录
停止播
放/记录
4
可记录
数据区

图 2

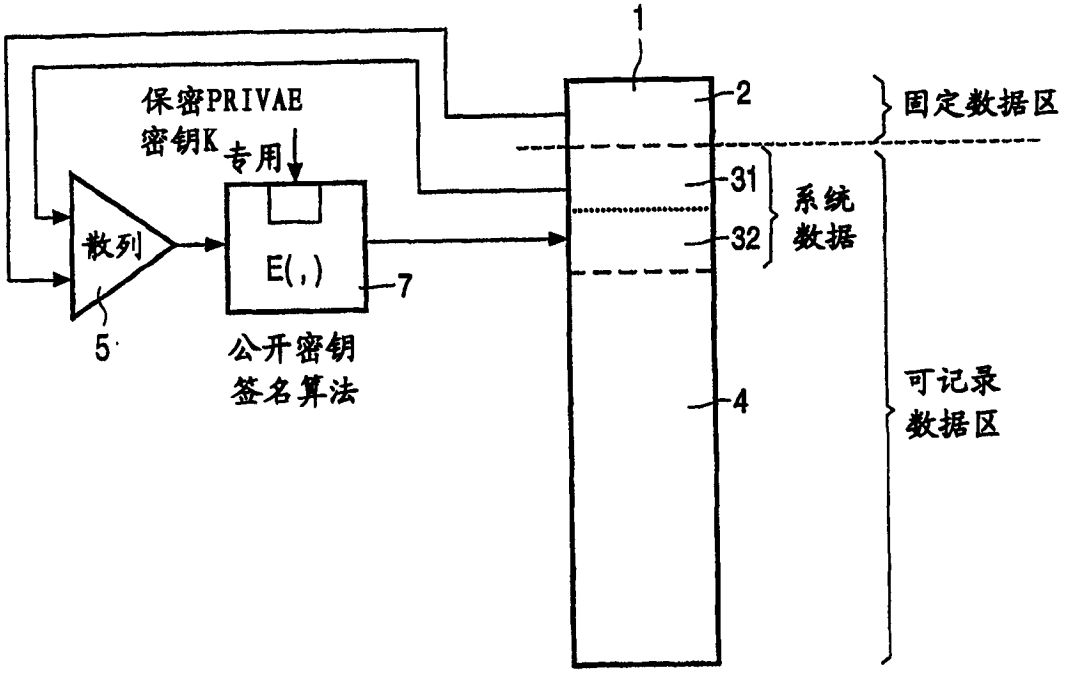

1
保密PRIVAE
密钥K
专用
散列
E(,)
7
5
公开密钥
签名算法
2
固定数据区
31
32
系统
数据
4
可记录
数据区

图 3

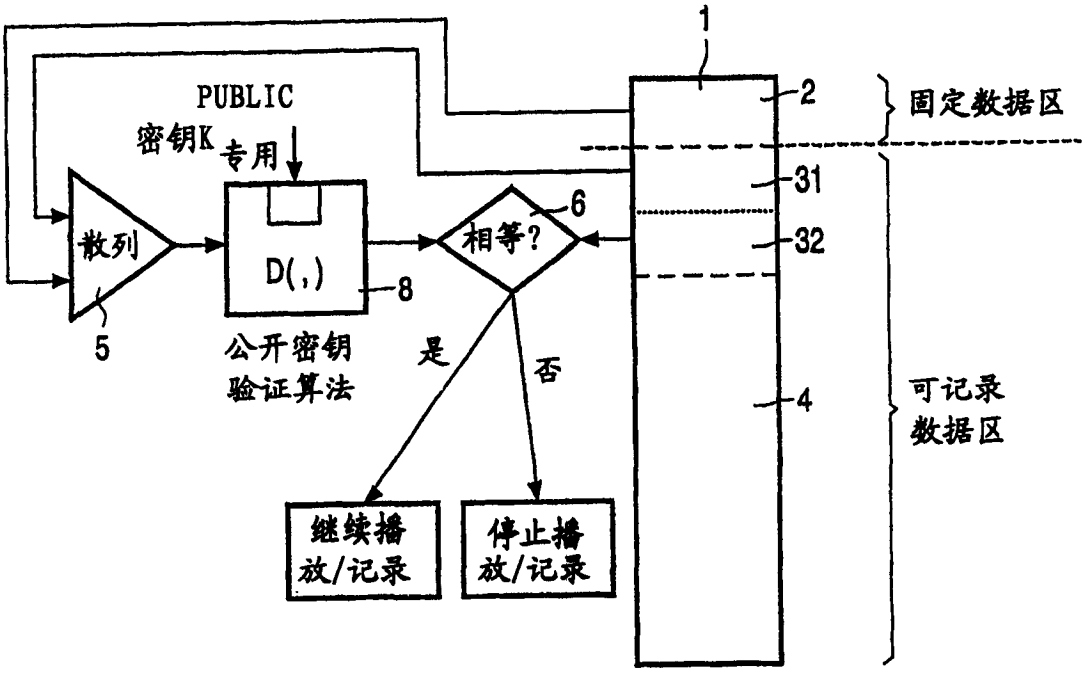

1
PUBLIC
密钥K
专用
散列
D(,)
8
5
公开密钥
验证算法
相等?
6
是
否
继续播
放/记录
停止播
放/记录
2
固定数据区
31
32
4
可记录
数据区

图 4

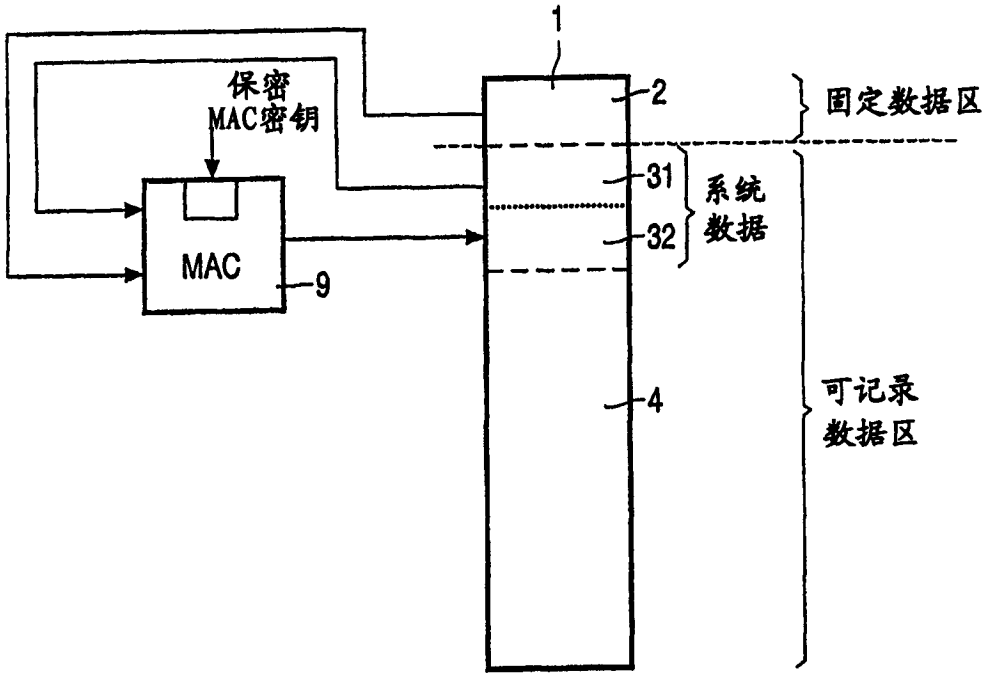

1
保密
MAC密钥
MAC
9
2
固定数据区
31
32
系统
数据
4
可记录
数据区

图 5

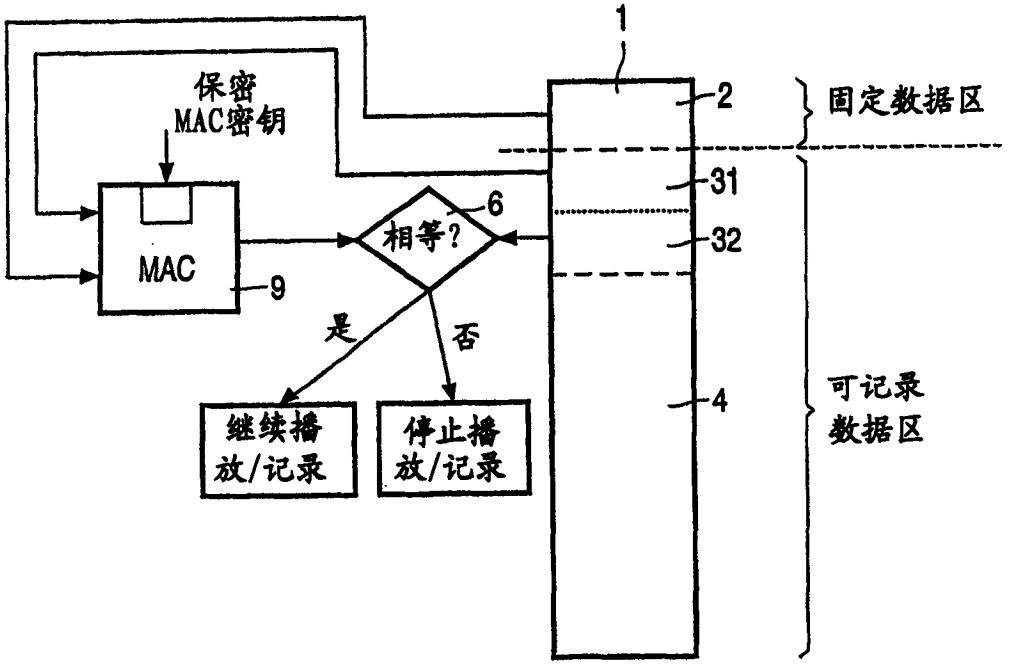

1
保密
MAC密钥
MAC
9
相等?
6
2
固定数据区
31
32
是
否
继续播
放/记录
停止播
放/记录
4
可记录
数据区

图 6