



(12) 发明专利

(10) 授权公告号 CN 1747033 B

(45) 授权公告日 2011.06.01

(21) 申请号 200510088189.5

EP 0969462 A, 2000.01.05, 全文.

(22) 申请日 2005.07.25

CN 1383643 A, 2002.12.04, 全文.

(30) 优先权数据

审查员 赵承娟

57900/04 2004.07.24 KR

(73) 专利权人 三星电子株式会社

地址 韩国京畿道

(72) 发明人 金以吉

(74) 专利代理机构 北京市柳沈律师事务所

11105

代理人 马莹 邵亚丽

(51) Int. Cl.

G11B 20/10 (2006.01)

H04N 5/913 (2006.01)

H04L 9/28 (2006.01)

(56) 对比文件

CN 1465062 A, 2003.12.31, 全文.

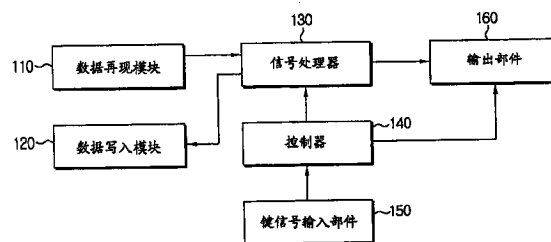
权利要求书 1 页 说明书 4 页 附图 2 页

(54) 发明名称

受密码保护的数据写入和再现装置及方法

(57) 摘要

本发明提供了一种在写入和再现数据时采用密码的数据写入和再现装置。该数据写入和再现装置包括信号处理器,用于利用加密密钥加扰视频数据;数据写入模块,用于将由信号处理器加扰的视频数据写入记录介质;键信号输入部件,用于提供输入密码的功能;以及控制器,用于从该密码中生成加密密钥并将该加密密钥提供给信号处理器。利用数据写入和再现装置存储数据的记录介质只能通过与 CSS 兼容的再现装置再现。因此,可防止数据被第三方非法复制和观看并减小了被窃取的可能性。



1. 一种数据写入装置,包括:
信号处理器,用于利用加密密钥加扰视频数据;
数据写入模块,用于将由信号处理器加扰的视频数据写入记录介质;
键信号输入部件,用于提供输入密码的功能;以及
控制器,用于从该密码中生成加密密钥并将该加密密钥提供给信号处理器。
2. 根据权利要求1所述的数据写入装置,其中,所述控制器控制数据写入模块将由信号处理器加扰的视频数据和密码数据分别写入记录介质的特定部分。
3. 一种数据再现装置,包括:
数据再现模块,用于再现写在记录介质中的视频数据和密码数据;
信号处理器,用于利用加密密钥来解扰由数据再现模块再现的视频数据;
键信号输入部件,用于提供输入用户密码的功能;
控制器,用于当从记录介质再现的密码数据与用户密码比较并匹配时,通过组合该密码数据的数字生成加密密钥并将该加密密钥提供给信号处理器;以及
输出部件,用于将由所述信号处理器解扰的视频数据传送到外部视频显示装置。
4. 根据权利要求3所述的数据再现装置,其中,所述控制器在接收到再现视频数据的命令时,控制所述数据再现模块和输出部件从记录介质中再现要求输入用户密码的消息数据,并将该消息数据传送到视频显示装置。
5. 根据权利要求4所述的数据再现装置,其中,所述控制器在通过键信号输入部件输入的用户密码与写在记录介质上的密码数据比较并匹配时,控制数据再现模块再现视频数据。
6. 根据权利要求5所述的数据再现装置,其中,所述控制器在通过键信号输入部件输入的用户密码与写在记录介质上的密码数据比较并匹配时,通过组合密码数据的数字来生成加密密钥,并控制信号处理器用该加密密钥对视频数据进行解扰。
7. 一种数据写入方法,包括:
利用密码数据生成加密密钥;
利用该加密密钥加扰视频数据;
将该加扰的视频数据写入记录介质;以及
将密码数据写入记录介质的特定部分。
8. 一种数据再现方法,包括:
接收用户密码和存储在记录介质上的存储的密码;
将该用户密码与存储的密码进行比较;
如果该用户密码与存储的密码相匹配,则利用该存储的密码或用户密码生成加密密钥;
利用该加密密钥对存储在记录介质上的数据进行再现和解扰。
9. 根据权利要求8所述的方法,其中,所述接收用户密码和存储的密码包括:
接收数字形式的密码。

受密码保护的数据写入和再现装置及方法

技术领域

[0001] 本发明总地涉及一种受密码保护的数据写入和再现装置及方法。具体地说,本发明的实施例涉及在记录介质的特定区域存储密码以生成加扰和解扰数据、在再现数据时如果密码得到验证则再现和解扰数据的加密密钥的数据写入和再现的装置及方法。

背景技术

[0002] 电子技术的发展导致对向一般用户提供各种功能的数据写入和再现装置的广泛使用。近年来,数据写入和再现装置实现了锁定功能,其通过设置密码来限制数据再现。因此,可以防止不知道密码的第三方利用数据写入和再现装置来访问和观看视频数据。

[0003] 但是,如果释放该数据写入和再现装置的锁定功能,或另一个数据写入和再现装置试图再现该记录介质,则很难防止观看该视频数据。此外,如果记录介质存储用户的私人信息,则第三方可以访问和获得该私人信息。

[0004] 为了防止非法观看或复制数字通用盘(DVD),引入了内容加扰系统(CSS)算法。CSS算法利用具有特殊值的加密密钥加扰和记录DVD标题的数据,并解扰该数据以再现相关视频。尽管在DVD标题中包含的内容文件*.VOB可以被复制,但不可能复制加密密钥。因此相关视频不能正确再现,从而防止了非法复制。

[0005] 但是,由于诸如DeCSS的窃取程序是反向设计和发布的,因此现在可以分别生成DVD的加密密钥。由此很难有效防止非法复制或观看。

发明内容

[0006] 为了解决上述和其他与传统设置有关的问题而提出了本发明。本发明的一个方面提供一种通过用组合密码生成的加密密钥加扰视频数据来将数据写入记录介质、并将与该密码有关的数据写入该记录介质的特定部分的数据写入和再现装置及方法。

[0007] 本发明的另一方面是提供一种通过生成作为密码组合的加密密钥来防止第三方窃取数据、并在写入记录介质的密码与用户从该记录介质再现视频数据时输入的密码匹配时解扰再现的视频数据的数据写入和再现装置及方法。

[0008] 为了完成本发明的上述方面提供了一种数据写入和再现装置。该数据写入和再现装置包括信号处理器,用于利用加密密钥加扰视频数据;数据写入模块,用于将由信号处理器加扰的视频数据写入记录介质;键信号输入部件,用于提供输入密码的功能;以及控制器,用于从该密码中生成加密密钥并将该加密密钥提供给信号处理器。

[0009] 控制器控制数据写入模块将由信号处理器加扰的视频数据和密码数据分别写入记录介质的特定部分。

[0010] 所述数据写入和再现装置可以进一步包括用于从记录介质中再现视频数据的数据再现模块;以及输出部件,用于将数据再现模块再现的视频数据传送到外部视频显示装置。

[0011] 在接收到再现视频数据的命令时,所述控制器可以控制数据再现模块和输出部件

从记录介质中再现要求用户输入密码的消息数据,并将该消息数据传送到视频显示装置。

[0012] 当通过键信号输入部件输入的用户密码与写在记录介质上的密码数据比较并匹配时,控制器可以控制数据再现模块再现该视频数据。

[0013] 当通过键信号输入部件输入的用户密码与写在记录介质上的密码数据比较并匹配时,控制器可以通过组合密码数据的数字来生成加密密钥,并可以控制信号处理器用该加密密钥对视频数据进行解扰。

[0014] 与本发明的上述方面一致地,提供了数据再现装置,其包括数据再现模块,用于再现写在记录介质中的视频数据和密码数据,信号处理器,用于利用加密密钥解扰数据再现模块中的视频数据,键信号输入部件,用于提供输入用户密码的功能,以及控制器,用于当从记录介质再现的密码数据与用户密码比较并匹配时,通过组合该密码数据的数字生成加密密钥并将该加密密钥提供给信号处理器。

[0015] 数据再现装置还可以包括输出部件,用于将数据处理器解扰的视频数据传送到外部视频显示装置。

[0016] 在接收到再现视频数据的命令时,所述控制器可以控制数据再现模块和输出部件从记录介质中再现要求用户输入密码的消息数据,并将该消息数据传送到视频显示装置。

[0017] 与本发明的上述方面一致地,提供了一种数据写入和再现方法,其包括利用密码数据生成加密密钥,利用加密密钥加扰视频数据,将加扰的视频数据写入记录介质,将密码数据写入记录介质的特定部分。

[0018] 所述数据写入和再现方法还可以包括在接收到再现视频数据的命令时显示要求输入用户密码的消息,在输入用户密码时通过比较用户密码和密码数据验证该用户密码,当用户密码和密码数据相互匹配时通过组合该密码的数字生成加密密钥,从记录介质中再现视频数据并用加密密钥解扰该视频数据。

[0019] 所述数据写入和再现方法还可以包括在用户密码和密码数据相互不匹配时显示表明密码错误的消息。

[0020] 与本发明的上述方面一致地,提供了一种数据再现方法,包括:接收用户密码和存储在记录介质上的存储的密码;将该用户密码与存储的密码进行比较;如果该用户密码与存储的密码相匹配,则利用该存储的密码或用户密码生成加密密钥;利用该加密密钥对存储在记录介质上的数据进行再现和解扰。

[0021] 本发明的其他方面和/或优点将部分在下面的描述中提出,并由于该描述而变得明显或通过实现本发明获得。

[0022] 附图说明

[0023] 下面,通过结合附图描述示例实施例,本发明的上述和/或其它方面和优点将变得更容易理解:

[0024] 图1是根据本发明实施例的数据写入和再现装置的结构框图;

[0025] 图2是根据本发明实施例的数据写入方法的流程图;

[0026] 图3是根据本发明实施例的数据再现方法的流程图。

[0027] 具体实施方式

[0028] 现在详细参考本发明的实施例,这些例子在附图中示出,其中全篇中相似的附图标记指相似的元件。为了参照附图解释本发明而在下面描述实施例。

[0029] 图 1 示出根据本发明的数据写入和再现装置的结构。参考图 1, 数据写入和再现装置包括数据再现模块 110、数据写入模块 120、信号处理器 130、控制器 140、键信号输入部件 150、输出部件 160。

[0030] 键信号输入部件 150 提供可以使用户输入再现命令、写入命令等的功能。当用户利用提供给数据写入和再现装置或远程控制器的按钮键输入再现命令或写入命令时, 键信号输入部件 150 识别并向控制器 140 通知输入命令。

[0031] 在通过键信号输入部件 150 接收数据写入命令时, 控制器 140 控制数据写入模块 110 写入数据。可以从通过接口连接的诸如可携式摄像机等等的外部视频显示装置接收视频数据并记录在记录介质上。在实施例中, 采用内容加扰系统 (CSS) 算法来加扰和写入视频数据。也就是说, 利用特定加密密钥按照特殊顺序混合视频数据, 由此即使在视频数据再现时也能防止被正确显示。

[0032] 信号处理器 130 采用特定加密密钥加扰视频数据。可以由控制器 140 利用密码生成该加密密钥。当例如密码包括 4 个数字时, 可以通过组合该 4 个数字生成加密密钥。

[0033] 用户可以用键信号输入部件 150 在写入数据的同时设置密码。所设置的密码可以存储在记录介质的特定部分中, 如上所述, 还可以用于生成再现该数据所需的加密密钥。为了防止窃取该密码, 可能对该密码加密并存储。也就是说, 可以加扰并存储密码数据。密码的每个数字或字母可以分别存储在记录介质的不同部分。

[0034] 当数据写入和再现装置是数字通用盘播放器 (DVDP) 时, 数据写入模块 110 将加扰的视频数据以 VOD 文件的格式存储在 DVD 上。此外, 涉及该 DVD 的信息可以按照 IFO (信息) 文件的格式记录。因此, 关于密码的数据也可以按照 IFO 文件的格式记录。

[0035] 下面解释数据如何由数据写入和再现装置再现。在通过键信号输入部件 150 接收到数据再现命令时, 控制器 140 控制数据再现模块 110 产生密码数据。在 DVDP 的情况下, 可以通过打开 IFO 文件从 DVD 的 IFO 文件中提取出密码数据。

[0036] 控制器 140 控制发送要求输入密码的消息数据并在视频显示装置的屏幕上显示该消息数据。该消息数据可以利用存储在记录介质的特定部分的消息数据。具体地说, 在 DVDP 的情况下, 当 DVD 标题插入 DVDP 中时, 显示介绍视频 (如运动图像预览) 和菜单屏幕。菜单屏幕可以显示出一个菜单, 包括诸如播放和场景选择的选项。当用户用远程控制器或其它输入装置选择播放时再现该视频。关于该菜单屏幕的数据存储为 IFO 文件。密码输入菜单添加到该菜单屏幕中, 从而只在输入密码并得到验证的时候才再现该视频数据。为了理解起见, 由用户输入的要再现数据的密码称为用户密码。

[0037] 控制器 140 判定通过消息窗口输入的用户密码是否与存储在记录介质中的密码匹配。如果匹配, 则控制器 140 用该密码生成加密密钥。所生成的加密密钥提供给信号处理器 130。控制器 140 控制数据再现模块 110 再现该视频数据。

[0038] 信号处理器 130 利用控制器 140 提供的加密密钥对数据再现模块 110 再现的数据进行解扰。解扰后的数据由输出部件 160 传送到外部视频显示装置。

[0039] 如果用户密码与记录介质上存储的密码不匹配, 则控制器 140 控制发送表明密码不正确的消息数据并显示在视频显示装置的屏幕上。表明密码不正确的消息数据可以存储在记录介质中。

[0040] 只具有再现功能的数据再现装置可以通过利用存储在记录介质中的加密密钥解

扰视频数据来实现锁定功能或复制防止功能。在这样的实施例中,数据再现装置包括如图 1 所示的相同部件,除了数据写入模块 120。

[0041] 图 2 是根据本发明实施例的数据写入方法的流程图。参考图 2,当用户输入数据写入命令时,控制器 140 识别数据写入命令 (S210)。存储在记录介质上的特定消息数据被发送到视频显示装置上以显示密码输入消息 (S220)。

[0042] 当用户输入密码时 (S230),控制器 140 通过组合该密码的数字或字母生成加密密钥 (S240)。用生成的加密密钥加扰待写入的视频数据 (S250)。

[0043] 加扰的视频数据被写入记录介质中。用于生成加密密钥的关于密码的数据写在记录介质的特定部分 (S260)。由此,可以为再现而解扰视频数据。

[0044] 图 3 是根据本发明实施例的数据再现方法的流程图。参考图 3,当用户输入数据再现命令时 (S310),要求输入密码的消息显示在视频显示装置的屏幕上 (S320)。控制器 140 可以从记录介质的特定部分再现涉及密码输入菜单的数据,并将该数据发送到视频显示装置。

[0045] 在从用户接收到密码时 (S330),再现记录介质中的密码并将其与所接收的密码进行比较 (S340)。

[0046] 如果密码相互匹配,则通过组合该密码的数字或字母生成加密密钥 (S350)。从记录介质再现视频数据并利用该加密密钥进行解扰 (S360)。

[0047] 如果密码不匹配,则产生密码错误的消息并发送到视频显示装置 (S370)。

[0048] 根据本发明的实施例,不知道密码的第三人无法正确再现视频数据。

[0049] 根据上述说明,为记录介质设置和记录不同的密码。由此,不知道密码的第三人无法正确解扰和再现视频数据,因为加密密钥不是用密码来生成的。如果记录介质被非法复制,则由于密码的存在而不可能再现数据,从而防止了非法复制和观看。特别是,由于密码对每个记录介质都不同,因此现有窃取方法无法获得加密密钥。由此大大减小了被窃取的可能性。

[0050] 尽管示出和描述了本发明的一些实施例,本领域的技术人员可以理解可以 对这些实施例进行修改而不偏离本发明的原理和精神。本发明的范围由权利要求及其等价物限定。

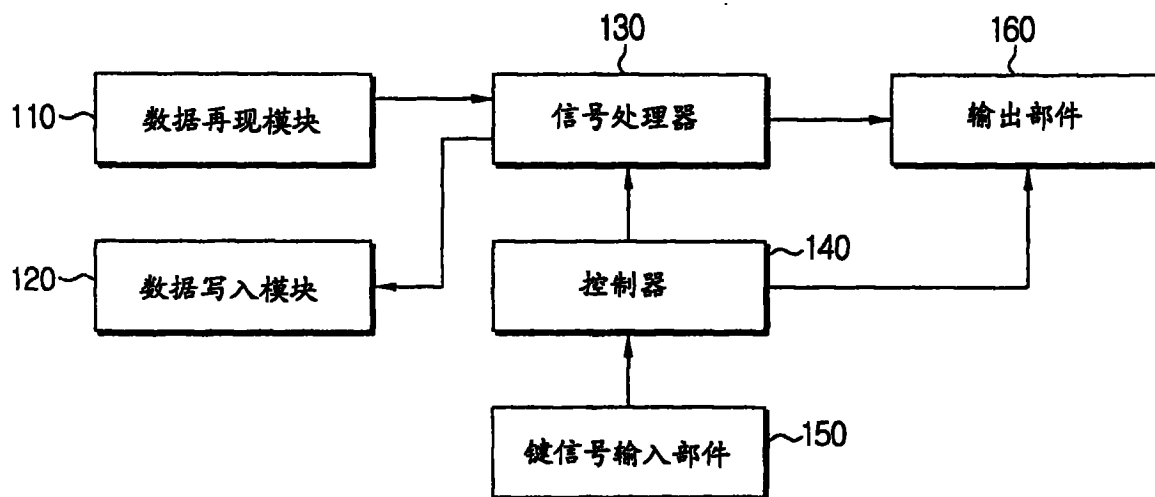


图 1

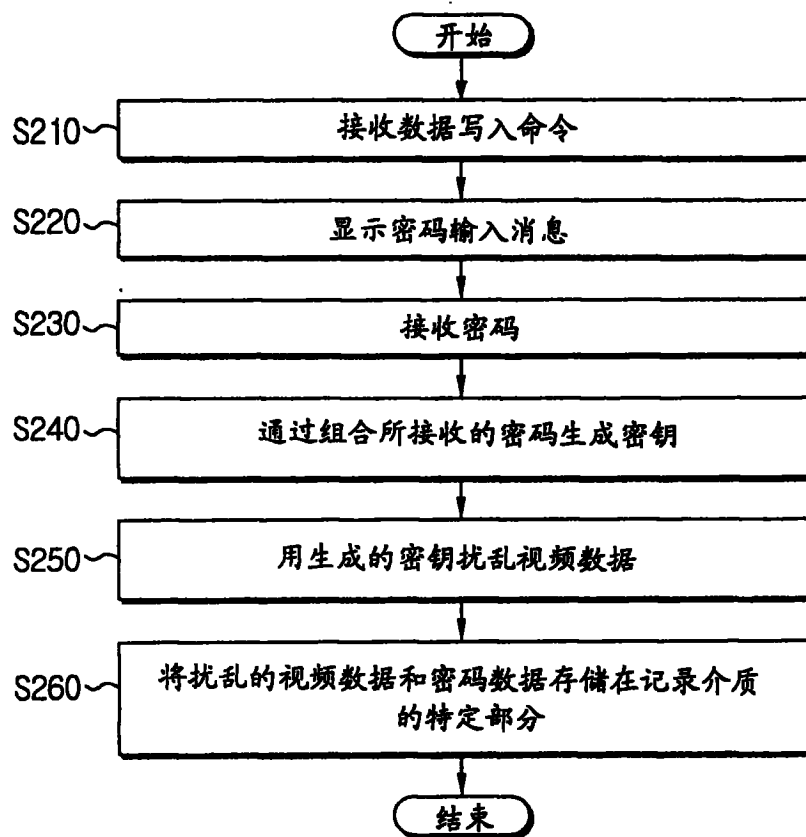


图 2

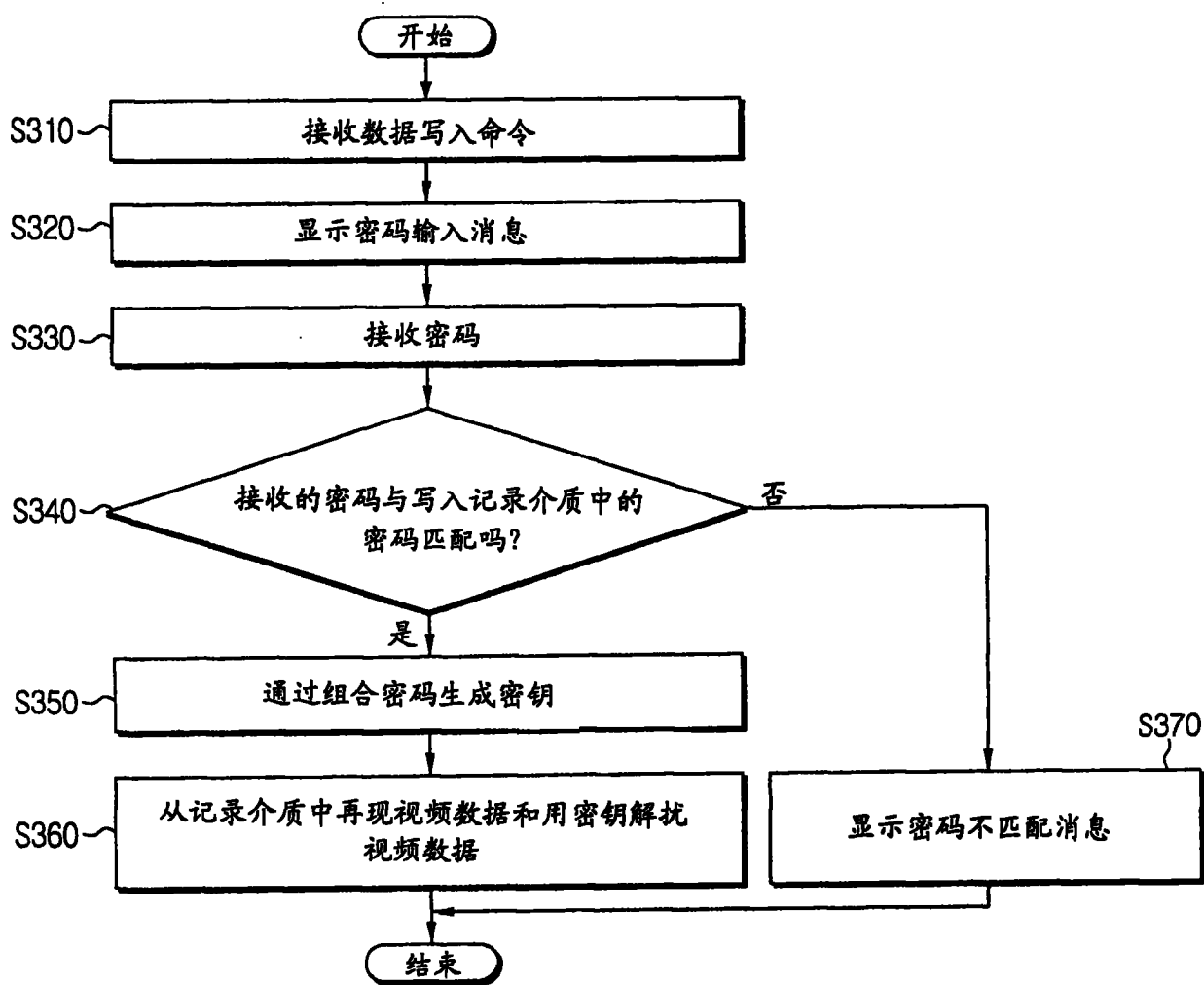


图 3