



(12) 发明专利

(10) 授权公告号 CN 107102925 B

(45) 授权公告日 2021. 12. 31

(21) 申请号 201710086774.4

(22) 申请日 2017.02.17

(65) 同一申请的已公布的文献号
申请公布号 CN 107102925 A

(43) 申请公布日 2017.08.29

(30) 优先权数据
2016-030171 2016.02.19 JP

(73) 专利权人 佳能株式会社
地址 日本东京都大田区下丸子3丁目30番2号

(72) 发明人 秋庭朋宏

(74) 专利代理机构 北京魏启学律师事务所
11398

代理人 魏启学

(51) Int.Cl.

G06F 11/26 (2006.01)

G06F 11/22 (2006.01)

(56) 对比文件

US 2006259786 A1, 2006.11.16

US 2008098239 A1, 2008.04.24

JP 2012194964 A, 2012.10.11

CN 101118586 A, 2008.02.06

审查员 薛聪帆

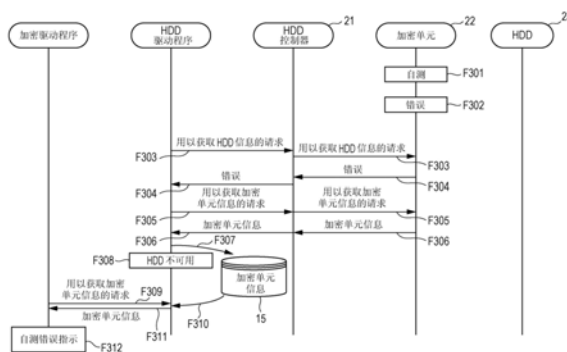
权利要求书2页 说明书12页 附图7页

(54) 发明名称

数据处理装置和数据处理装置的控制方法

(57) 摘要

本发明提供一种数据处理装置和数据处理装置的控制方法。根据一个实施例,在针对加密装置的测试表示加密装置的加密处理中的错误的情况下,数据处理装置将针对加密装置的测试结果保持在保持单元中,并且基于针对加密装置的测试结果来通知加密装置具有错误。



1. 一种数据处理装置,包括:

加密装置,用于对数据进行加密,所述加密装置包括所述加密装置的自测功能;

存储器,用于对所述加密装置加密后的数据进行存储;以及

存储器控制器,用于对在所述存储器中存储数据进行控制,

其中,在通过所述自测功能在测试中检测到所述加密装置的错误的情况下,所述加密装置响应于来自所述存储器控制器的用于获取存储器信息的请求而发送表示错误的信息;以及

其中,在通过所述自测功能在测试中检测到所述加密装置的错误的情况下,所述存储器控制器在接收到表示错误的信息时发送用于获取与所述加密装置有关的信息的请求,以及所述加密装置根据该请求向所述存储器控制器传输表示所述测试的结果是错误的信息。

2. 根据权利要求1所述的数据处理装置,其中,在所述测试中检测到错误的情况下,所述加密装置响应于向所述数据处理装置的电力供给从断开状态向接通状态的转换而传输表示所述测试的结果是错误的信息。

3. 根据权利要求1或2所述的数据处理装置,其中,在所述测试中检测到错误的情况下,所述加密装置响应于所述存储器向所述数据处理装置的连接而传输表示所述测试的结果是错误的信息。

4. 根据权利要求1所述的数据处理装置,其中,

在所述测试中没有检测到错误的情况下,所述数据处理装置向所述存储器发送所述存储器中的信息的获取请求;以及

在所述测试中检测到错误的情况下,所述数据处理装置不向所述存储器发送所述存储器中的信息的获取请求。

5. 根据权利要求1所述的数据处理装置,其中,还包括接收部件,所述接收部件用于接收用以从所述存储器获取所述存储器中的信息的请求,

其中,在所述测试中检测到错误并且所述接收部件从所述存储器控制器接收到获取请求的情况下,禁止从所述存储器获取所述存储器中的信息,并且所述加密装置响应于该获取请求而向所述存储器控制器发送表示错误的信息。

6. 根据权利要求1所述的数据处理装置,其中,所述测试是响应于向所述数据处理装置的电力供给从断开状态向接通状态的转换而进行的。

7. 根据权利要求1所述的数据处理装置,其中,所述测试是响应于所述存储器向所述数据处理装置的连接而进行的。

8. 根据权利要求1所述的数据处理装置,其中,所述测试包括以下测试至少之一:针对加密/解密功能的测试、针对随机数生成功能的测试、针对哈希计算功能的测试和针对固件区域中的篡改检测的测试。

9. 根据权利要求1所述的数据处理装置,其中,所述存储器信息包括以下内容至少之一:所述存储器的存储容量、所述存储器的型号和所述存储器的使用时间。

10. 一种数据处理装置的控制方法,所述控制方法包括以下步骤:

通过加密装置对数据进行加密,所述加密装置包括所述加密装置的自测功能;

通过存储器对所述加密装置加密后的数据进行存储;

通过存储器控制器对在所述存储器中存储数据进行控制,

其中,在通过所述自测功能在测试中检测到所述加密装置的错误的情况下,通过所述加密装置响应于来自所述存储器控制器的用于获取存储器信息请求而发送表示错误的信息;以及

其中,在通过所述自测功能在测试中检测到所述加密装置的错误的情况下,通过所述存储器控制器在接收到表示错误的信息时发送用于获取与所述加密装置有关的信息的请求,以及通过所述加密装置根据该请求向所述存储器控制器传输表示所述测试的结果是错误的信息。

数据处理装置和数据处理装置的控制方法

技术领域

[0001] 本发明涉及一种数据处理装置和数据处理装置的控制方法。

背景技术

[0002] 数据处理装置可以包括硬盘驱动器 (HDD) 作为存储装置。已经提出了如下技术：在 HDD 控制器和这种 HDD 之间连接有加密单元，以使得可以对 HDD 中所存储的数据进行加密/解密。

[0003] 例如，存在定义了与加密单元有关的安全要求的联邦信息处理标准 (FIPS) 140-2 以及用于多功能外围设备和打印机的国际标准 IEEE Std 2600TM-2008 (以下称为 IEEE2600)。在这些标准中所设置的要求之一是针对加密单元的自测，以判断该加密单元的安全功能是否正常地运行在该加密单元上。

[0004] 为了满足该要求，加密单元可以具有内部自测功能。数据处理装置可以通过对加密单元所进行的自测的结果进行检查，来确认加密处理是否依据各规格而运行以及加密处理是否已被篡改等。

[0005] 日本特开 2012-194964 公开了如下的信息处理装置，其中该信息处理装置进行对 HDD 加密功能的自测，以判断加密处理的安全功能是否正常地运行在信息处理装置中。如果运行对 HDD 加密功能的自测产生了表示加密功能正成功运行的结果，则信息处理装置启动 HDD 加密功能。另一方面，如果运行对 HDD 加密功能的自测产生了表示加密功能失败的结果，则信息处理装置停止启动与该 HDD 加密功能相关联的功能。

[0006] 这是因为，如果运行对加密单元的自测产生了表示加密功能失败的结果，则存在 HDD 中所存储的数据可能没有被加密单元正确地加密的可能性。在 HDD 中所存储的数据没有被正确地加密的情况下，如果第三方可以利用 HDD 中所存储的数据，则存在 HDD 中所存储的数据可能在未许可的情况下被访问的风险。为了避免该结果，加密单元可能在对加密单元的自测返回表示加密功能失败的结果的情况下阻止 HDD 中所存储的数据的获取请求。

[0007] 另一方面，当启动数据处理装置或者连接至 HDD 时，数据处理装置通常基于与 HDD 有关的基本信息 (包括存储容量、型号以及使用时间) 来判断连接至数据处理装置的 HDD 针对数据获取请求是否可用。然而，在上述系统中，如果针对加密单元的自测产生了表示加密单元失败的结果，则如上所述，可以阻止 HDD 中所存储的数据的获取请求。因而，即使在数据处理装置可以获取连接至该装置的 HDD 的基本信息 (包括存储容量、型号以及使用时间) 的情况下，加密功能的自测也可能具有不成功的结果。因此，可能难以判断连接至装置的 HDD 针对数据获取请求是否可用。在无法获取与 HDD 有关的基本信息的情况下，数据处理装置识别为该 HDD 没有连接至该装置。因而，在该情况发生的情况下，数据处理装置将不发出针对与 HDD 有关的信息或者与加密单元有关的信息的获取请求。由于数据处理装置没有获取到与加密单元有关的信息 (包括与运行自测是否得到加密单元失败指示的结果有关的信息)，因此用户可能无法判断出 HDD 中所存储的数据无法被获取到的原因是由于加密单元处于错误状态。

发明内容

[0008] 各种实施例提供如下的装置和方法：通过该装置和方法，在针对加密装置所进行的测试生成了表示加密装置的加密处理中的错误的结果的情况下，用户可以判断出存储装置中所存储的数据无法被获取到的原因是由于加密装置处于错误状态。

[0009] 根据各种实施例，提供一种数据处理装置，包括：存储器，用于存储数据；加密部件，用于对所述存储器中所存储的数据进行加密；获取部件，用于经由所述加密部件从所述存储器获取所述存储器中的信息；控制部件，用于进行控制，以在所述加密部件所进行的测试产生了表示加密处理失败的结果的情况下获取所述存储器中所存储的信息；保持部件，用于在所述加密部件所进行的测试产生了表示加密处理失败的结果的情况下，保持所述加密部件所进行的测试的结果；以及通知部件，用于基于所述加密部件所进行的测试的结果，来通知用于表示所述加密部件所进行的测试表示加密处理失败的信息。

[0010] 根据各种实施例，提供一种数据处理装置的控制方法，所述控制方法包括以下步骤：将数据存储存储在存储器中；通过加密部件对所述存储器中所存储的数据进行加密；经由所述加密部件从所述存储器获取所述存储器中所存储的信息；进行控制，以在所述加密部件所进行的测试表示加密处理失败的情况下从所述存储器获取所述存储器中的信息；在所述加密部件所进行的测试表示加密处理失败的情况下，保持所述加密部件所进行的测试的结果；以及基于所述加密部件所进行的测试的结果，来通知所述加密部件所进行的测试表示加密处理失败的信息，其中所述结果保持在保持部件中。

[0011] 通过以下参考附图对典型实施例的说明，本发明的其它特征将变得明显。

附图说明

[0012] 图1是示出根据第一实施例的MFP的结构框图。

[0013] 图2是示出根据第一实施例的加密单元的结构框图。

[0014] 图3是示出根据第一实施例的处理的流程的序列图。

[0015] 图4是示出根据第一实施例的画面的结构的序列图。

[0016] 图5是示出根据第二实施例的处理的流程的序列图。

[0017] 图6是示出根据第三实施例的处理的流程的序列图。

[0018] 图7是示出根据第四实施例的处理的流程的序列图。

具体实施方式

[0019] 以下将参考附图来详细说明实施例。然而，以下说明的实施例并不意图限制要求保护的发明。根据所说明的实施例的特征的全部组合并不是实现本发明的其它实施例所必需的。

[0020] 第一实施例

[0021] 将参考图1所示的框图来说明根据第一实施例的MFP(多功能外围设备)的结构。

[0022] 作为根据第一实施例的数据处理装置的示例的MFP 1包括作为图像输入装置的扫描器装置2、作为图像输出装置的打印机装置4、图像处理单元5、非易失性存储器20、作为存储装置的硬盘驱动器(HDD) 23以及控制器单元3。

[0023] 扫描器装置2具有原稿进给单元11和扫描器单元12。这些单元以电气方式连接，并

且相互交换控制命令和数据。

[0024] 原稿进给单元11具有原稿托盘,其中,要在原稿托盘上载置原稿,以输送该原稿托盘上所载置的原稿。为了读取原稿进给单元11所输送的原稿,扫描器单元12可以在固定光学系统的位置处光学地读取所输送的原稿上所打印的图像信息。另一方面,为了读取载置在原稿台玻璃上的原稿,扫描器单元12可以针对载置在原稿台玻璃上的原稿、在副扫描方向上扫描光学系统,以光学地读取原稿台玻璃上所载置的原稿上所打印的图像信息。对通过诸如CCD传感器等的光学系统所读取的图像信息进行光电转换,并且作为图像数据而输入至控制器单元3。

[0025] 打印机装置4基于传输至打印机装置4的图像数据来进行用于将图像输出至薄片的操作(打印操作)。打印机装置4具有进给单元18、标记单元16和排出单元17。这些单元以电气方式连接,并且相互交换控制命令和数据。

[0026] 进给单元18具有用于储存打印所要使用的薄片的多个盒和手动进给托盘,并且将多个盒其中之一或手动进给托盘中所储存的薄片输送至标记单元16。标记单元16被配置为将基于图像数据所形成的调色剂(显影剂)图像转印并定影至进给单元18输送来的薄片,并且将对应图像形成(打印)至薄片。排出单元17被配置为向外排出通过标记单元16形成有图像的薄片。

[0027] 控制器单元3具有CPU 13、RAM 15、HDD控制器21、加密单元22和操作单元24。这些单元经由系统总线25以电气方式连接,并且相互交换控制命令和数据。尽管以下将说明根据本实施例的由硬件芯片来实现加密单元22的示例,但是其它实施例可以不包括该特征。加密单元22可以通过CPU 13所执行的程序来实现。换句话说,加密单元22还可以通过软件来实现。

[0028] 通常,CPU 13可以基于RAM 15中所存储的控制程序来控制MFP 1。CPU 13可以读出RAM 15中所存储的控制程序,并且执行诸如针对扫描器装置2所进行的读取的控制、针对打印机装置4所进行的打印的控制以及针对固件程序的更新的控制等的控制处理。

[0029] CPU 13可以将从扫描器装置2所接收到的图像数据暂时存储在RAM 15中。CPU 13可以将RAM 15中所暂时存储的图像数据存储至HDD 23。

[0030] CPU 13可以读出HDD 23中所存储的图像数据,并且将这些图像数据暂时存储在RAM 15中。然后,CPU 13可以将RAM 15中所暂时存储的图像数据传输至打印机装置4。

[0031] 图像处理装置5具有通用图像处理单元19并且被配置为进行诸如图像的放大、缩小和旋转等的图像处理。通用图像处理单元19可以对RAM 15中所存储的图像数据进行诸如缩小等的处理,并且可以将缩小之后的图像数据存储回至RAM 15。

[0032] 非易失性存储器20是保持单元的示例。非易失性存储器20被配置为存储控制器单元3进行操作所需的设置信息。即使在MFP 1的电源被断开的情况下,非易失性存储器20也能够保持数据。

[0033] RAM 15是保持单元的示例。RAM 15是数据可以被写入和读出的存储器。RAM 15被配置为存储从扫描器装置2传输来的图像数据、程序以及设置信息。

[0034] HDD 23是存储装置的示例。HDD 23被配置为存储控制程序、图像数据、用以存储诸如用户ID和密码等的用户信息的用户数据库、用以存储例如个人文档的文档数据的文档数据库、以及所保持的作业。HDD 23可以存储用于存储打印所要使用的薄片的诸如名称、表面

特性和克重等的介质信息的介质库。HDD 23经由HDD控制器21和加密单元22连接至控制器单元3。

[0035] HDD控制器21是存储控制装置的示例。HDD控制器21将从CPU 13接收到的命令转换成能够被HDD 23解译的电信号,并且将该命令传输至加密单元22。HDD控制器21将从HDD 23接收到的电信号转换成能够被CPU 13解译的命令,并且将该命令传输至CPU 13。例如,HDD控制器21可以将HDD 23中所存储的数据传输至加密单元22。例如,HDD控制器21将与HDD 23有关的基本信息(包括存储容量、型号和使用时间)的获取请求(以下称为HDD信息获取请求)传输至加密单元22。

[0036] 加密单元22是可连接在HDD控制器21和HDD 23之间的加密芯片。加密单元22被配置为对从HDD控制器21传输来的数据进行加密,并将加密后的数据传输至HDD 23。因而,将被加密单元22加密后的数据存储存储在HDD 23中。加密单元22还被配置为对HDD 23中所存储的数据进行解密,并且将解密后的数据传输至HDD控制器21。

[0037] 操作单元24是用户接口单元的示例,并且具有显示单元和键输入单元。操作单元24被配置为经由显示单元和键输入单元接收来自用户的设置。操作单元24被配置为使显示单元显示要向用户通知的信息。显示单元可以被配置为显示MFP 1所用的操作画面、加密单元22的状态和HDD 23的状态等。

[0038] 接着,将参考图2的框图来说明加密单元22的结构。

[0039] 加密单元22包括CPU 101、ROM 102、RAM 103、NVRAM 104、盘控制器1 (DISKC1) 106、数据传输单元107、加密处理单元108以及盘控制器2 (DISKC2) 109。这些单元经由系统总线105以电气方式连接,并且相互交换控制命令和数据。

[0040] 通常,CPU 101可以基于ROM 102或RAM 103中所存储的控制程序来控制加密单元22。例如,CPU 101将用于基于ROM 102或RAM 103中所存储的控制程序来指示针对HDD 23的预定处理(诸如HDD 23的存储容量、型号和使用时间的获取请求等)的命令发送至HDD控制器21。例如,CPU 101基于ROM 102或RAM 103中所存储的控制程序来进行对加密单元22的自测。对加密单元22的自测是与IEEE2600相关的功能,并且包括与HDD 23中的加密处理相关的测试。以下将参考图3来说明对加密单元22的自测的详情。

[0041] ROM 102或RAM 103保持作为用于控制加密单元22的程序的加密驱动程序。ROM 102或RAM 103保持作为用于控制HDD控制器21的程序的HDD驱动程序。

[0042] ROM 102保持如下数据,其中该数据用于计算与作为加密单元22的自测中的计算结果的计算值的比较可使用的已知解、并且用于计算测试检验和。

[0043] NVRAM 104保持诸如加密单元22进行操作所需的设置和加密单元22的状态(包括对加密单元22的自测的执行结果)等的信息。即使在加密单元22的电源被断开的情况下,也保持NVRAM 104中所存储的信息。

[0044] 盘控制器1 (DISKC1) 106经由SATA线缆而以电气方式连接至HDD控制器21,并且与HDD控制器21相互交换控制命令和数据。盘控制器2 (DISKC2) 109经由SATA线缆而以电气方式连接至HDD 23,并且与HDD 23相互交换控制命令和数据。

[0045] 加密处理单元108被配置为对数据进行加密。加密处理单元108还被配置为对加密后的数据进行解密。

[0046] 数据传输单元107以电气方式连接至加密处理单元108、盘控制器1 (DISKC1) 106和

盘控制器2 (DISKC2) 109,并且与这些单元相互交换控制命令和数据。

[0047] 将没有加密并存储在HDD 23中的数据(以下称为非加密数据)经由盘控制器2 (DISKC2) 109输入至加密处理单元108。加密处理单元108对输入至加密处理单元108的非加密数据进行加密。随后,数据传输单元107将加密处理单元108加密后的数据(以下称为加密数据)传输至盘控制器2 (DISKC2) 109。将传输至盘控制器2 (DISKC2) 109的加密数据输入至HDD 23。

[0048] 另一方面,将HDD 23中所存储的加密数据经由盘控制器2 (DISKC2) 109而输入至加密处理单元108。加密处理单元108对输入至加密处理单元108的加密数据进行解密。随后,数据传输单元107将加密处理单元108解密后的数据(以下称为解密数据)传输至盘控制器1 (DISKC1) 106。然后,将传输至盘控制器1 (DISKC1) 106的解密数据输入至HDD控制器21。

[0049] 接着,将参考图3的序列图来说明HDD控制器21、加密单元22和HDD 23中的处理的流程。该控制程序包括加密驱动程序和HDD驱动程序,并且在CPU 13上运行。可以通过CPU 13所执行的程序(加密驱动程序的软件)来实现加密驱动程序的功能。可以通过CPU 13所执行的程序(HDD驱动程序的软件)来实现HDD驱动程序的功能。加密驱动程序属于HDD驱动程序的更高层。因而,加密驱动程序的功能依赖于HDD驱动程序的功能。

[0050] 加密单元22响应于向MFP 1的电力供给的输入(即,对MFP 1的电力供给从OFF(断开)状态向ON(接通)状态的转换)而对加密单元22自身进行自测(F301)。可选地,在F301中,加密单元22响应于传感器检测到HDD 23连接至MFP 1,来对加密单元22自身进行自测。要进行的自测例如可以包括“针对加密/解密功能的使用已知解的测试”、“针对随机数生成功能的使用已知解的测试”、“针对哈希计算功能的使用已知解的测试”和“利用固件区域中的校验和的篡改检测测试”。

[0051] “针对加密/解密功能的使用已知解的测试”用于确认通过加密/解密功能所用的算法针对输入馈送所计算出的值是否与预先存储在ROM 102中的加密/解密功能用的已知解一致。如果一致,则“针对加密/解密功能的使用已知解的测试”产生表示加密成功的结果。如果不一致,则“针对加密/解密功能的使用已知解的测试”产生表示加密失败的结果。

[0052] “针对随机数生成功能的使用已知解的测试”用于确认通过随机数生成功能所用的算法针对输入馈送所计算出的值是否与预先存储在ROM 102中的随机数生成功能用的已知解一致。如果一致,则“针对随机数生成功能的使用已知解的测试”产生表示加密成功的结果。如果不一致,则“针对随机数生成功能的使用已知解的测试”产生表示加密失败的结果。

[0053] “针对哈希计算功能的使用已知解的测试”用于确认通过哈希计算功能所用的算法针对输入馈送所计算出的值是否与预先存储在ROM 102中的哈希计算功能用的已知解一致。如果一致,则“针对哈希计算功能的使用已知解的测试”产生表示加密成功的结果。如果不一致,则“针对哈希计算功能的使用已知解的测试”产生表示加密失败的结果。

[0054] “利用固件区域中的校验和的篡改检测测试”用于确认针对固件区域中的二进制文件所计算出的校验和值是否与预先存储在ROM 102中的校验和值一致。如果一致,则“利用固件区域中的校验和的篡改检测测试”产生表示加密成功的结果。如果不一致,则“利用固件区域中的校验和的篡改检测测试”产生表示加密失败的结果。

[0055] 在针对加密单元22的自测中的多个测试至少之一产生表示加密失败的结果的情

况下,加密单元22判断为自测检测到加密处理中的错误。例如,在从外部使用加密单元22的固件程序被篡改的情况下,运行“利用固件区域中的校验和的篡改检测测试”产生表示加密失败的结果,由此判断为在加密处理中存在错误。

[0056] 如果基于自测检测到加密处理中存在错误,则加密单元22将用于描述自测检测到加密处理中的错误的信息存储在NVRAM 104中(F302)。

[0057] 如果基于自测检测到加密处理中存在错误,则在检测到错误之后,加密单元22针对从HDD控制器21接收到的针对HDD 23的命令,对错误作出响应。如果基于自测检测到加密处理中存在错误,则之后加密单元22可以接收来自HDD控制器21的命令。该命令例如可以包括HDD控制器21和加密单元22之间的相互认证用的命令、用以获取加密单元22的状态的命令、与HDD 23的镜像有关的命令以及针对HDD 23的命令。在针对加密单元22的这些命令中,加密单元22对用于获取加密单元22的状态的命令作出响应,并且发送包括与加密单元的加密功能有关的自测结果的加密单元信息。包括自测结果的加密单元信息例如可以是与包括加密单元22中的自测结果的加密单元22的状态有关的信息或者与HDD 23的镜像有关的信息。

[0058] 如果确认HDD控制器21存在,则HDD驱动程序必须确认HDD 23是否经由HDD控制器21而连接。为此,HDD驱动程序请求HDD控制器21获取与HDD 23有关的基本信息(包括存储容量、型号和使用时间)(F303)。HDD控制器21接收来自HDD驱动程序的HDD信息获取请求,并且将该HDD信息获取请求传输至加密单元22(F303)。加密单元22接收来自HDD控制器21的HDD信息获取请求。

[0059] 另一方面,如果加密单元22根据自测检测到加密处理中已经发生了错误,则存在HDD中所存储的数据没有被加密单元正确地加密的可能性。在HDD中所存储的数据没有被正确地加密的情况下,如果第三方可以利用HDD中所存储的数据,则存在HDD中所存储的数据可能在未许可的情况下被访问的风险。为了避免这种风险,加密单元响应于接收到作为对加密单元运行自测的结果而表示加密处理失败的指示,来阻止HDD中所存储的数据的获取请求。因而,在该情形下,加密单元22响应于HDD信息获取请求而向HDD控制器21返回错误(F304)。HDD控制器21接收从加密单元22返回的错误,并且将所返回的错误传输至HDD驱动程序(F304)。

[0060] 接着,HDD驱动程序请求HDD控制器21获取包括自测结果的加密单元信息(F305)。HDD控制器21从HDD驱动程序接收加密单元信息的获取请求,并且将加密单元信息的获取请求传输至加密单元22(F305)。

[0061] 加密单元22参考NVRAM 104中所保持的自测结果,并且将加密单元信息(包括加密单元22的自测结果为错误的信息)发送至HDD控制器21(F306)。HDD控制器21从加密单元22接收加密单元信息(包括加密单元22的自测结果表示加密处理中的错误的信息),并且将所接收到的加密单元信息传输至HDD驱动程序(F306)。

[0062] HDD驱动程序将从HDD控制器21接收到的加密单元信息(包括加密单元22的自测结果表示加密处理中的错误的信息)存储在非易失性存储器20或RAM 15中(F307)。

[0063] 然后,在将加密单元信息存储在非易失性存储器20或RAM 15中之后,HDD驱动程序将内部状态识别为“HDD 23没有连接至MFP 1的状态”(F308)。换句话说,在将加密单元信息存储在非易失性存储器20或RAM 15中之后,HDD驱动程序阻止针对HDD控制器21的请求。这

是因为,在无法获取到连接至MFP 1的HDD 23的基本信息(包括存储容量、型号和使用时间)的情况下,CPU 13无法判断连接至MFP 1的HDD 23是否可用。

[0064] 在对加密单元22所进行的自测表示加密处理中发生错误的情况下,MFP 1识别为HDD 23没有连接至MFP 1。因而,之后,如上所述,不发出与HDD 23有关的信息或与加密单元22有关的信息的获取请求。换句话说,在针对加密单元22的自测表示加密处理中未发生错误的情况下,MFP 1许可从HDD 23获取与HDD 23有关的信息,或者许可从加密单元22获取与加密单元22有关的信息。另一方面,在针对加密单元22的自测表示加密处理中发生错误的情况下,MFP 1禁止从HDD 23获取与HDD 23有关的信息,或者禁止从加密单元22获取与加密单元22有关的信息。

[0065] 根据第一实施例,在对加密单元22所进行的自测表示加密处理中发生错误并且HDD驱动程序无法获取到HDD 23的基本信息(包括存储容量、型号和使用时间)的情况下,提供了用于通知针对加密单元22的自测表示加密处理中发生错误的机制。更具体地,在自测表示加密处理中发生错误之后加密单元22阻止针对HDD控制器21的请求之前,加密驱动程序向HDD控制器21请求获取加密单元信息。在从HDD控制器21获取到加密单元信息并且将所获取到的加密单元信息存储在非易失性存储器20或RAM 15中之后,HDD驱动程序不发出与HDD 23有关的信息或与加密单元22有关的信息的获取请求。以下将说明其详情。

[0066] 加密驱动程序响应于“HDD 23没有连接至MFP 1的状态”的识别,请求HDD驱动程序获取加密单元信息(F309)。然后,HDD驱动程序响应于从加密驱动程序接收到加密单元信息的获取请求,获取非易失性存储器20或RAM 15中所存储的加密单元信息(F310)。接着,HDD驱动程序将F310中所获取到的加密单元信息传输至加密驱动程序(F311)。

[0067] CPU 101判断从HDD驱动程序所接收到的与加密单元有关的信息是否包括针对加密单元22的自测结果表示加密单元22的加密处理中的错误的信息。由于针对加密单元22的自测结果表示加密处理中发生错误,因此CPU 101经由图4所示的错误画面400来将消息401显示在操作单元24中的显示单元上(F312)。

[0068] 换句话说,在针对加密单元22的自测表示加密处理中发生错误的情况下,响应于MFP 1的电源的接通(或者响应于对MFP 1的电力供给从OFF状态向ON状态的转换),向用户通知加密单元22具有错误这一事实。可选地,在针对加密单元22的自测表示加密处理中发生错误的情况下,响应于传感器检测到HDD 23已连接至MFP 1,向用户通知加密单元22具有错误这一事实。

[0069] 如果用户可以从消息401识别出由于针对加密单元22的自测结果产生加密处理中的错误的指示的结果、因而加密单元22具有错误,则消息401可以是消息“加密功能没有正常地运行”或者消息“针对加密功能的自测已失败”,或者可以是相应的错误代码。消息401的表现形式不限于如上述示例那样显示在操作单元24中的显示单元上,而可以例如显示在经由诸如LAN等的网络而连接至MFP 1的诸如PC等的外部设备中的显示单元上。如果用户可以识别出针对加密单元22的自测结果表示加密处理中发生了错误,则消息401的表现形式不限于如上述示例那样显示在显示单元上,而可以是向用户的音频或光学通知。

[0070] 用户(诸如服务工程师等)可以阅读操作单元24中的显示单元上所显示的消息401,从而识别出MFP 1中所安装的加密功能具有错误。识别出MFP 1中所安装的加密功能具有错误的用户可以将加密功能中具有错误的加密单元22更换成加密功能中不具有错误的

新的加密单元22,并且将该新的加密单元22连接至HDD控制器21和HDD 23。在加密单元22和HDD控制器21安装在一个基板上的情况下,用户可以将具有加密单元22和HDD控制器21的基板更换成加密功能不具有错误的新的基板,并且将该新的基板连接至HDD 23。在对HDD 23的数据访问不被允许的情况下,用户可以通过针对加密单元22的自测结果表示加密处理中发生了错误的通知,识别出连接至HDD 23的加密单元22的加密功能具有错误。因而,在对HDD 23的数据访问不被允许的情况下,用户可以判断为更换加密单元22,而不是更换HDD 23。

[0071] 根据第一实施例,如上所述,进行图3的F305~F307中的处理,以使得可以在加密单元22和HDD控制器21之间无需专用信号线的情况下向加密驱动程序通知针对加密单元22的自测得到了加密处理失败的指示。因而,在针对加密装置的测试得到失败的指示的情况下,用户可以识别出存储装置中所存储的数据无法被获取到的原因是由于加密装置具有错误。

[0072] 第二实施例

[0073] 根据第二实施例,即使在针对加密单元22的自测结果表示加密处理中发生错误的情况下,HDD驱动程序也可以将内部状态识别为“HDD 23连接至MFP 1的状态”。因而,在根据第二实施例的变形例中,即使在加密单元22的自测结果表示加密处理中发生错误的情况下,加密驱动程序也可以从加密单元22获取加密单元信息(包括针对加密单元22的自测结果)。由于第二实施例在部分处理方面与第一实施例不同,因此将参考图5来主要说明与第一实施例的处理不同的处理。

[0074] 由于图5的F301~F306、F309、F311和F312中的流程与图3的F301~F306、F309、F311和F312中的流程相同,因此将省略任何重复的详细说明。

[0075] HDD驱动程序在F306中从HDD控制器21接收加密单元信息(包括针对加密单元22的自测结果表示加密处理中的错误的信息)。之后,HDD驱动程序判断针对加密单元22的自测结果是否表示加密处理中发生错误。基于针对加密单元22的自测结果表示加密处理中发生错误的判断,HDD驱动程序将内部状态识别为“HDD 23连接至MFP 1的状态”(F501)。在这种情况下,HDD驱动程序将内部状态识别为“HDD 23连接至MFP 1的状态”,但不许可访问HDD 23中所存储的实际数据(诸如用户数据库、文档数据库和所保持的作业等)。

[0076] 在针对加密单元22的自测表示加密处理失败的情况下,存在HDD 23中所存储的数据没有被加密单元22正确地加密的可能性。在HDD 23中所存储的数据没有被正确地加密的情况下,如果第三方可能利用HDD 23中所存储的数据,则存在HDD 23中所存储的数据可能在未许可的情况下被访问的风险。为了避免这种风险,加密单元22可以基于针对加密单元22运行自测的结果表示加密处理失败,来阻止HDD 23中所存储的实际数据(诸如用户数据库、文档数据库和所保持的作业等)的获取请求。

[0077] 另一方面,由于HDD驱动程序识别为“HDD 23连接至MFP 1的状态”,因此加密驱动程序可以获取加密单元信息。

[0078] 加密驱动程序请求HDD驱动程序获取加密单元信息(F309)。然后,HDD驱动程序从加密驱动程序接收加密单元信息的获取请求,并且将加密单元信息的获取请求传输至HDD控制器21(F502)。然后,HDD控制器21从HDD驱动程序接收加密单元信息的获取请求,并且将加密单元信息的获取请求传输至加密单元22(F502)。

[0079] 然后,加密单元22从HDD控制器21接收加密单元信息的获取请求。之后,加密单元22参考NVRAM 104中所保持的自测结果,并且将加密单元信息(包括加密单元22的自测结果表示加密处理中的错误的信息)发送至HDD控制器21(F503)。然后,HDD控制器21接收从加密单元22发送来的加密单元信息,并且将所接收到的加密单元信息传输至HDD驱动程序(F503)。

[0080] 然后,HDD驱动程序从HDD控制器21接收加密单元信息(包括加密单元22的自测结果表示加密处理中的错误的信息),并且将所接收到的加密单元信息传输至加密驱动程序(F311)。

[0081] CPU 101判断从HDD驱动程序所接收到的与加密单元有关的信息作为针对加密单元22的自测结果是否包括针对加密单元22的自测结果表示加密处理中的错误的信息。由于针对加密单元22的自测结果表示加密处理中的错误,因此CPU 101经由图4所示的错误画面400将消息401显示在操作单元24中的显示单元上(F312)。

[0082] 根据第二实施例,如上所述,进行图5的F501~F503中的处理,以使得可以在加密单元22和HDD控制器21之间无需专用信号线的情况下向加密驱动程序通知针对加密单元22的自测得到了加密处理失败的指示。因而,在针对加密装置的测试表示加密处理中发生错误的情况下,用户可以识别出存储装置中所存储的数据无法被获取到的原因是由于加密装置没有恰当地运行。

[0083] 第三实施例

[0084] 在根据第三实施例的变形例中,在针对加密单元22的自测结果表示加密处理中的错误的情况下,尽管不允许HDD驱动程序获取HDD 23中所存储的实际数据,但是允许HDD驱动程序获取与HDD 23有关的基本信息。

[0085] 由于第三实施例在部分处理方面与第一实施例不同,因此将参考图6来主要说明与第一实施例的处理不同的处理。由于图6所示的F301~F303、F309、F311和F312中的流程与图3所示的F301~F303、F309、F311和F312中的流程相同,因此将省略任何重复的详细说明。

[0086] 加密单元22从HDD控制器21接收与HDD 23有关的基本信息(包括存储容量、型号和使用时间)的获取请求(F303),并且将与HDD 23有关的基本信息(包括存储容量、型号和使用时间)的获取请求传输至HDD 23(F601)。然后,加密单元22从HDD 23获取与HDD 23有关的基本信息(包括存储容量、型号和使用时间)(F602),并且将所获取到的与HDD 23有关的基本信息(包括存储容量、型号和使用时间)传输至HDD控制器21(F603)。HDD控制器21从加密单元22接收与HDD 23有关的基本信息(包括存储容量、型号和使用时间),并且将与HDD 23有关的基本信息(包括存储容量、型号和使用时间)传输至HDD驱动程序(F603)。

[0087] 然后,HDD驱动程序获取与HDD 23有关的基本信息(包括存储容量、型号和使用时间)。然后,当启动MFP 1或连接了HDD 23时,CPU 13基于HDD驱动程序所获取到的与HDD 23有关的基本信息(包括存储容量、型号和使用时间),来判断连接至MFP 1的HDD 23是否可用。如果CPU 13判断为连接至MFP 1的HDD 23可用,则定义使得可以允许对HDD 23的数据访问的设置。因而,HDD驱动程序将内部状态识别为“HDD 23连接至MFP 1的状态”(F604)。因而,加密驱动程序可以获取加密单元信息(诸如包括针对加密单元22的自测结果的加密单元22的状态和与HDD 23的镜像有关的信息等)。

[0088] 加密驱动程序请求HDD驱动程序获取加密单元信息(F309)。然后,HDD驱动程序从加密驱动程序接收加密单元信息的获取请求,并且将加密单元信息的获取请求传输至HDD控制器21(F605)。然后,HDD控制器21从HDD驱动程序接收加密单元信息的获取请求,并且将加密单元信息的获取请求传输至加密单元22(F605)。

[0089] 然后,加密单元22从HDD控制器21接收加密单元信息的获取请求。之后,加密单元22参考NVRAM 104中所保持的自测结果,并且将加密单元信息发送至HDD控制器21(F606)。然后,HDD控制器21接收从加密单元22发送来的加密单元信息,并且将所接收到的加密单元信息传输至HDD驱动程序(F606)。

[0090] 然后,HDD驱动程序从HDD控制器21接收加密单元信息,并且将所接收到的加密单元信息传输至加密驱动程序(F311)。

[0091] CPU 101判断从HDD驱动程序接收到的加密单元信息是否包括用于描述针对加密单元22的自测结果表示加密单元22的加密处理中的错误的信息。然后,由于针对加密单元22的自测结果表示加密处理中的错误,因此CPU 101经由图4所示的错误画面400将消息401显示在操作单元24中的显示单元上(F312)。

[0092] 根据第三实施例,如上所述,进行图6的F601~F606中的处理,以使得可以在加密单元22和HDD控制器21之间无需专用信号线的情况下向加密驱动程序通知针对加密单元22的自测产生了表示加密处理失败的结果。因而,在针对加密装置的测试表示加密处理中的错误的情况下,用户可以识别出存储装置中所存储的数据无法被获取到的原因是由于加密装置没有恰当地运行。

[0093] 第四实施例

[0094] 在根据第四实施例的变形例中,在针对加密单元22的自测结果表示加密处理中的错误的情况下,响应于HDD信息获取请求,加密单元22不向HDD控制器21返回错误。加密单元22被配置为向HDD控制器21返回包含加密单元信息的HDD信息,而不是返回错误。

[0095] 由于第四实施例在部分处理方面与第一实施例不同,因此将参考图7来主要说明与第一实施例的处理不同的处理。

[0096] 由于图7所示的F301~F303、F309、F311和F312中的流程与图3所示的F301~F303、F309、F311和F312中的流程相同,因此将省略任何重复的详细说明。

[0097] 加密单元22从HDD控制器21接收与HDD 23有关的基本信息(包括存储容量、型号和使用时间)的获取请求(F303)。然后,加密单元22生成包含加密单元信息的HDD信息(以下称为疑似HDD信息),而不是与HDD 23有关的基本信息(包括存储容量、型号和使用时间)。加密单元信息例如可以包括加密单元22的状态(包括针对加密单元22的自测结果)和与HDD 23的镜像有关的信息。为了生成这种疑似HDD信息,加密单元22参考NVRAM 104中所保持的自测结果,并且获取加密单元信息(包括用于描述针对加密单元22的自测结果为错误的信息)。因而,疑似HDD信息包括针对加密单元22的自测结果为错误的信息。

[0098] 加密单元22将疑似HDD信息返回至HDD控制器21(F701)。HDD控制器21从加密单元22接收疑似HDD信息,并且将该疑似HDD信息传输至HDD驱动程序(F701)。

[0099] HDD驱动程序判断针对加密单元22的自测结果是否为错误。HDD驱动程序从疑似HDD信息中所包括的加密单元信息中提取针对加密单元22的自测结果,并且判断针对加密单元22的自测结果是否为错误。基于针对加密单元22的自测结果为错误的判断,HDD驱动程

序将内部状态识别为“HDD 23连接至MFP 1的状态”(F702)。在这种情况下,HDD驱动程序识别为“HDD 23连接至MFP 1的状态”,加密驱动程序可以获取加密单元信息。

[0100] 加密驱动程序请求HDD驱动程序获取加密单元信息(F309)。然后,HDD驱动程序从加密驱动程序接收加密单元信息的获取请求,并且将加密单元信息的获取请求传输至HDD控制器21(F703)。然后,HDD控制器21从HDD驱动程序接收加密单元信息的获取请求,并且将加密单元信息的获取请求传输至加密单元22(F703)。

[0101] 然后,加密单元22从HDD控制器21接收加密单元信息的获取请求。之后,加密单元22参考NVRAM 104中所保持的自测结果,并且将加密单元信息(包括用于描述针对加密单元22的自测结果表示加密处理中的错误的信息)发送至HDD控制器21(F704)。然后,HDD控制器21接收从加密单元22发送来的加密单元信息,并且将所接收到的加密单元信息传输至HDD驱动程序(F705)。

[0102] 然后,HDD驱动程序从HDD控制器21接收加密单元信息(包括用于描述针对加密单元22的自测结果表示加密处理中的错误的信息),并且将所接收到的加密单元信息传输至加密驱动程序(F311)。

[0103] 然后,CPU 101判断从HDD驱动程序接收到的与加密单元有关的信息是否包括用于描述针对加密单元22的自测结果表示加密处理中的错误的信息。由于针对加密单元22的自测结果表示加密处理中的错误,因此CPU 101经由图4所示的错误画面400将消息401显示在操作单元24中的显示单元上(F312)。

[0104] 根据第四实施例,如上所述,进行图7的F701~F705中的处理,以使得可以在加密单元22和HDD控制器21之间无需专用信号线的情况下向加密驱动程序通知针对加密单元22的自测产生了表示加密处理失败的结果。因而,在针对加密装置的测试表示加密处理中的错误的情况下,用户可以识别出存储装置中所存储的数据无法被获取到的原因是由于加密装置具有错误。

[0105] 应当理解,上述实施例并不限制权利要求书。反而,在不偏离本发明的精神的情况下,可以进行各种改变(包括实施例的有机组合),并且并不从本发明的范围内排除这各种改变。

[0106] 例如,根据实施例,已经将包括扫描器装置2和打印机装置4的MFP 1描述为数据处理装置。本发明的实施例不限于此。为了例示,如上所述的控制还可以适用于例如作为数据处理装置的包括扫描器装置2而不包括打印机装置4的图像输入装置。这些控制还可以适用于作为数据处理装置的包括打印机装置4而不包括扫描器装置2的图像输出装置。

[0107] 例如,根据各种实施例,MFP 1的控制器单元3中的CPU 13是本发明中所说明的控制的主体。然而,本发明的实施例不限于此。可以配置其它实施例,以使得这些控制的一部分或全部可以由诸如与MFP 1分离的壳体中的外部控制器等的打印控制装置执行。

[0108] 其它实施例

[0109] 本发明的实施例还可以通过如下的方法来实现,即,通过网络或者各种存储介质将执行上述实施例的功能的软件(程序)提供给系统或装置,该系统或装置的计算机或是中央处理单元(CPU)、微处理单元(MPU)读出并执行程序的方法。

[0110] 尽管已经参考典型实施例说明了本发明,但是应该理解,本发明不局限于所公开的典型实施例。所附权利要求书的范围符合最宽的解释,以包含所有这类修改、等同结构和

功能。

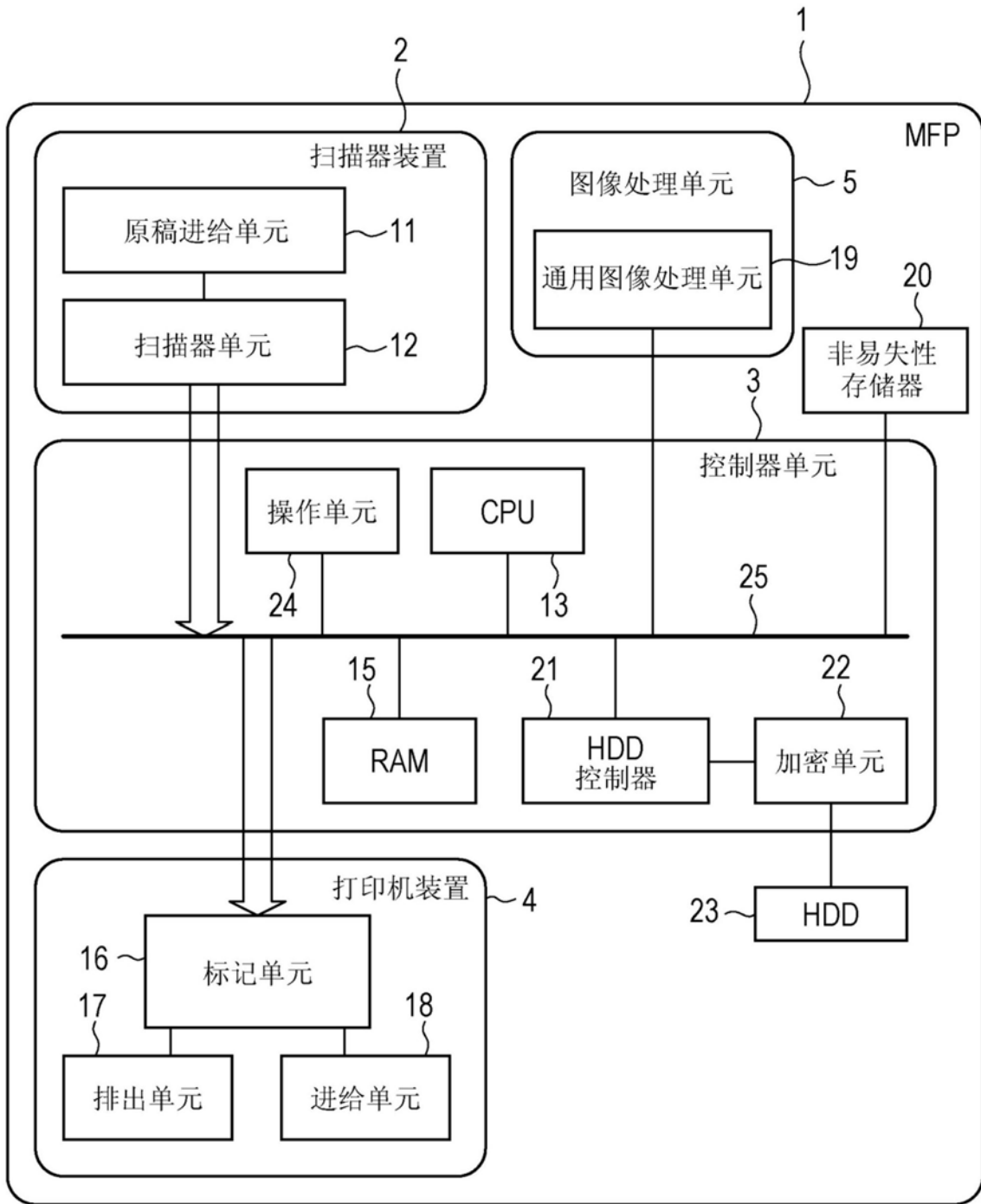


图1

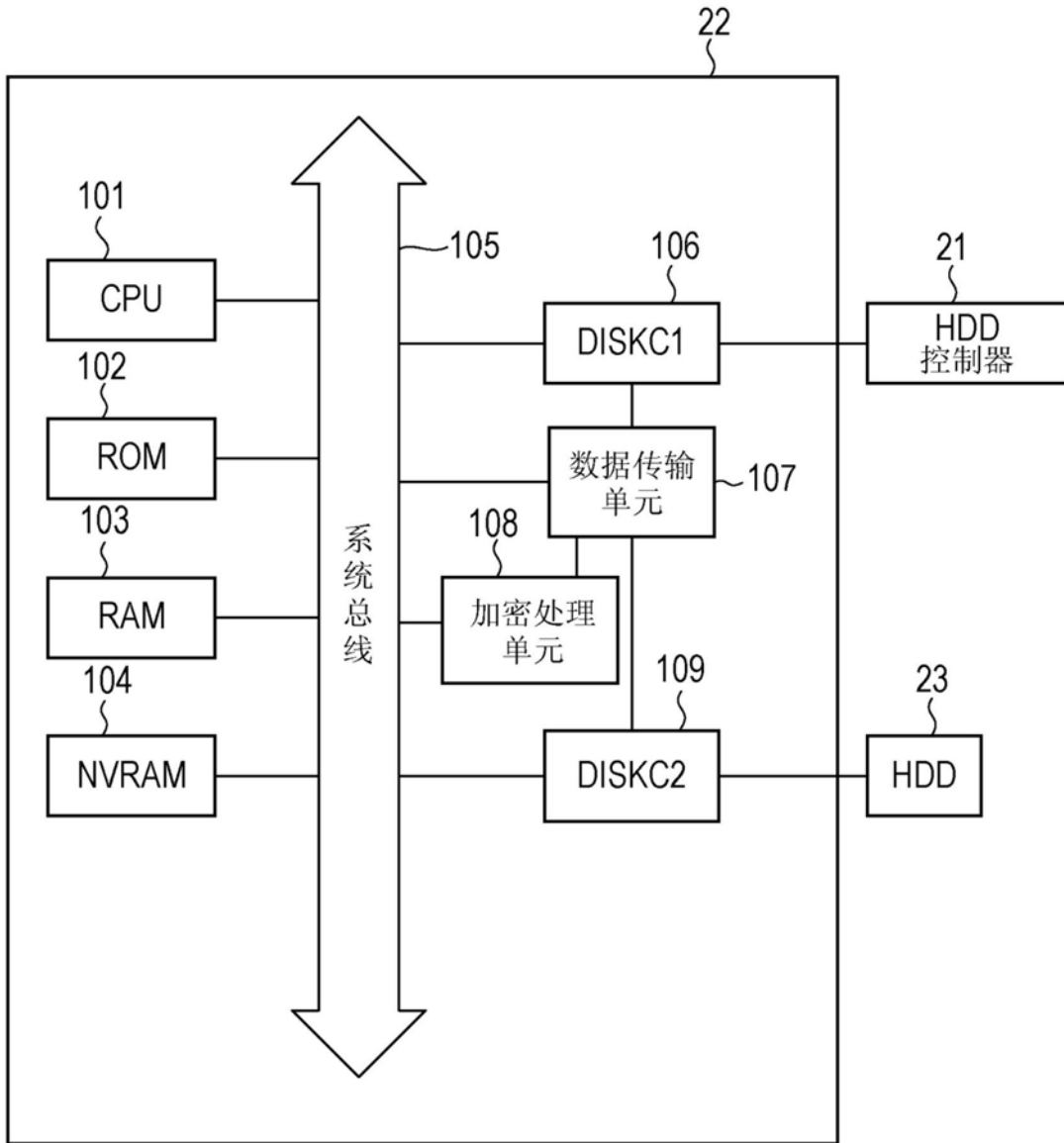


图2

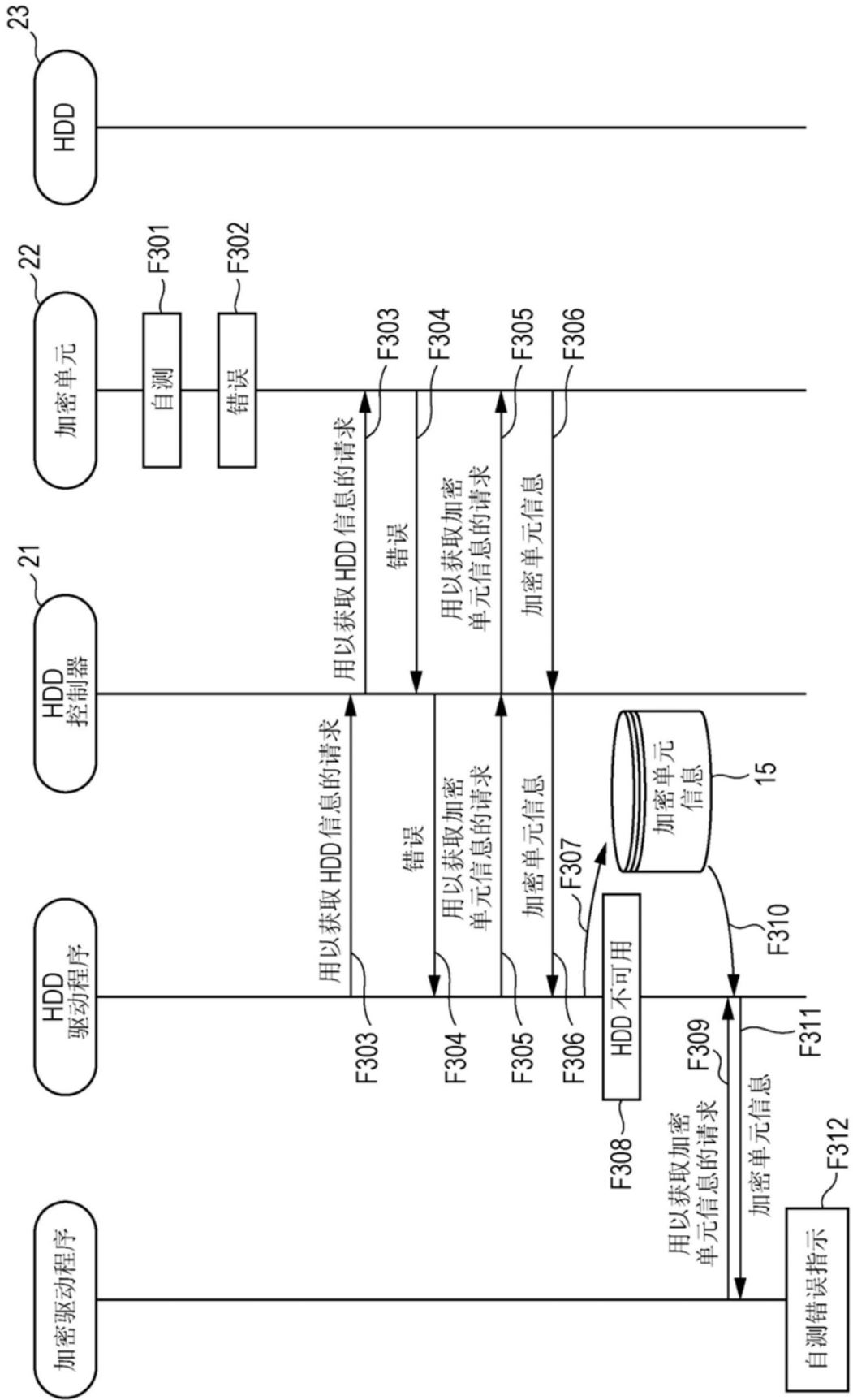


图3

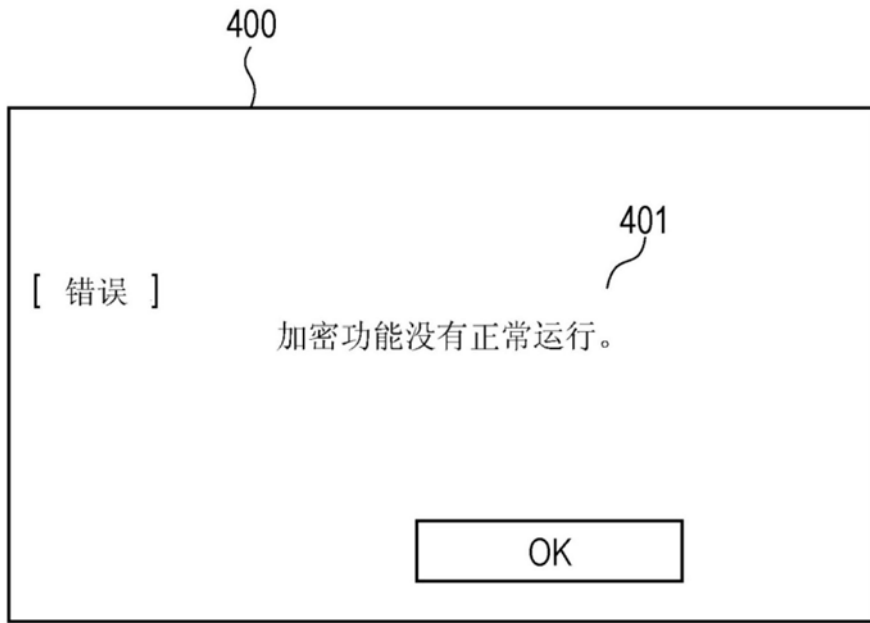


图4

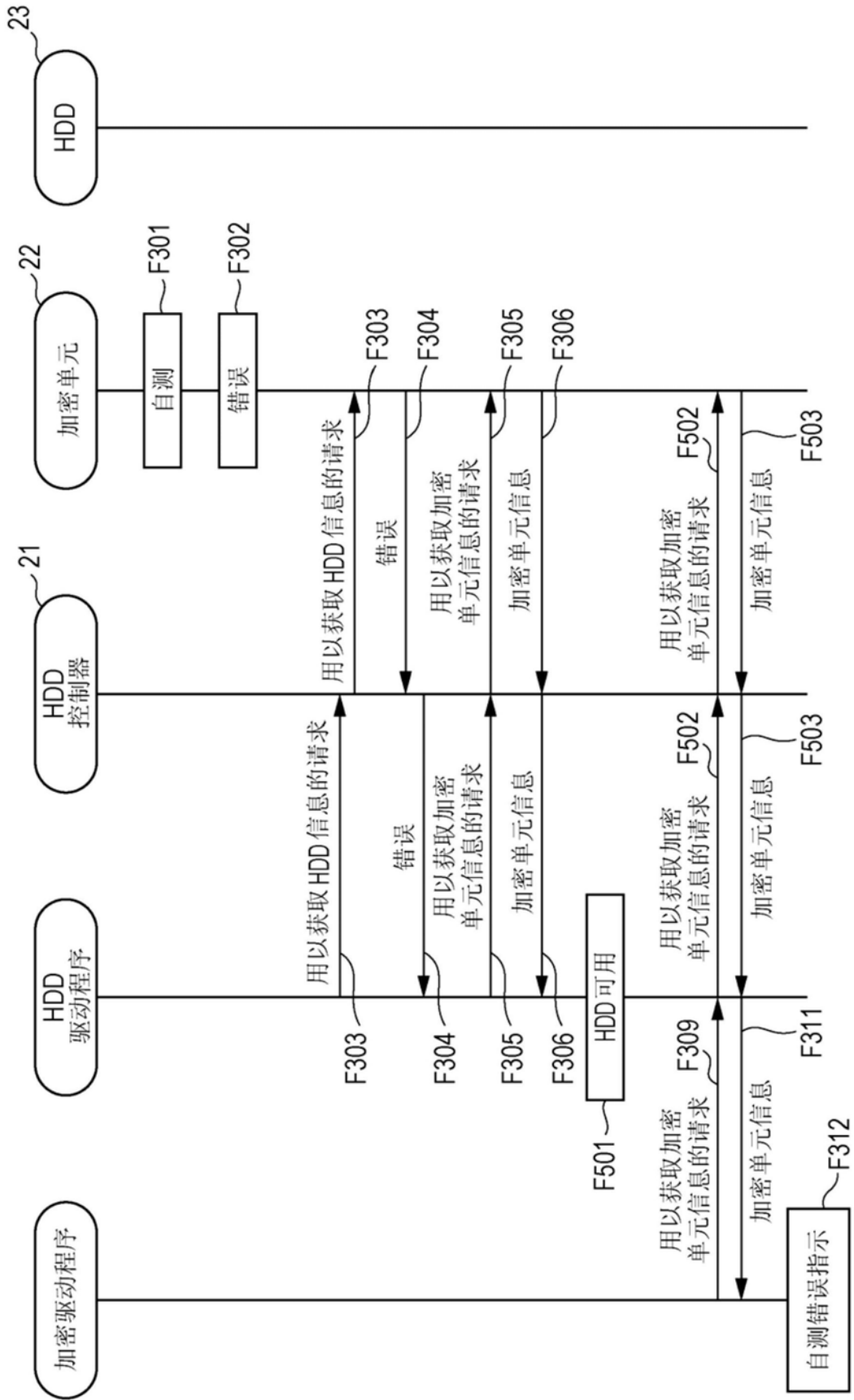


图5

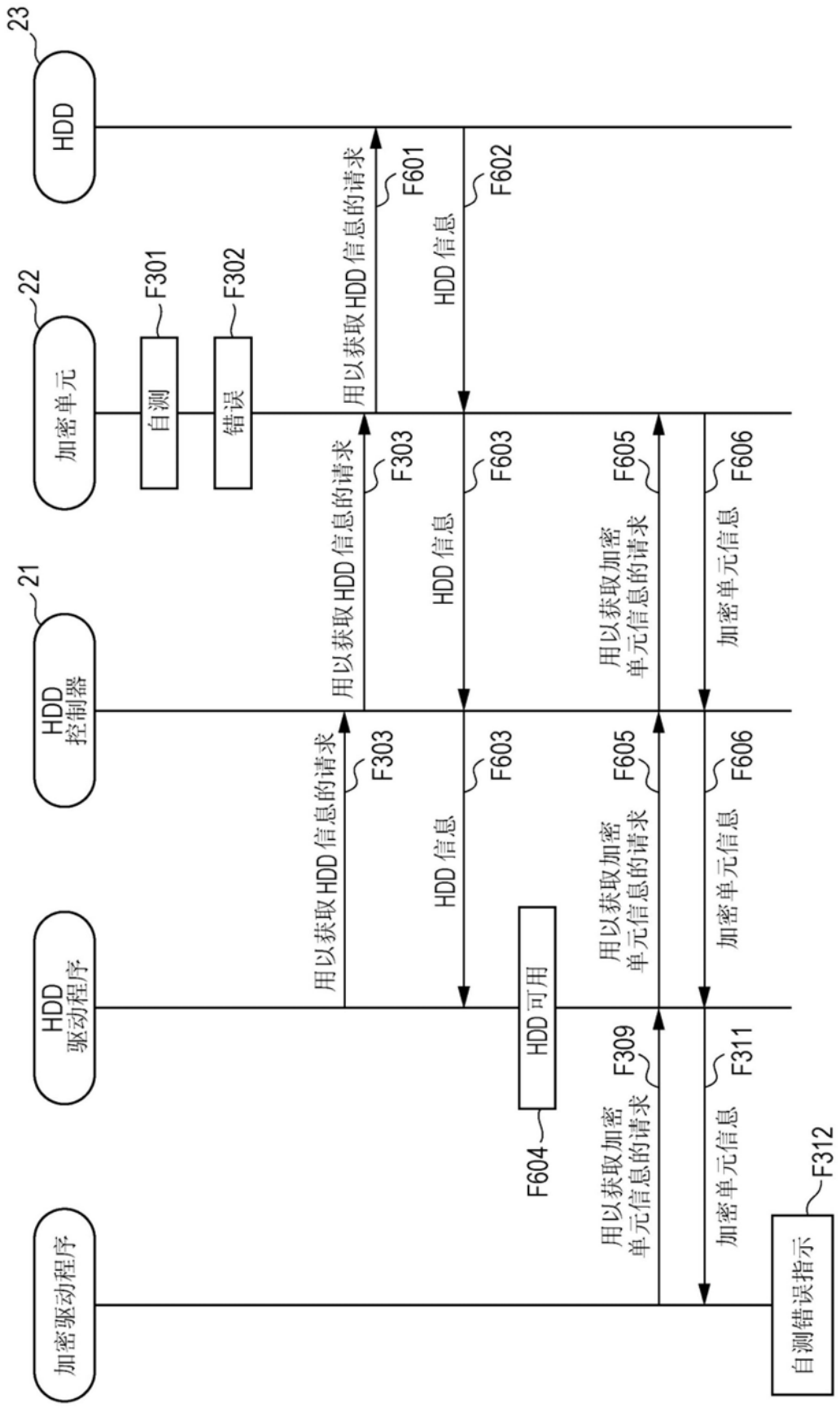


图6

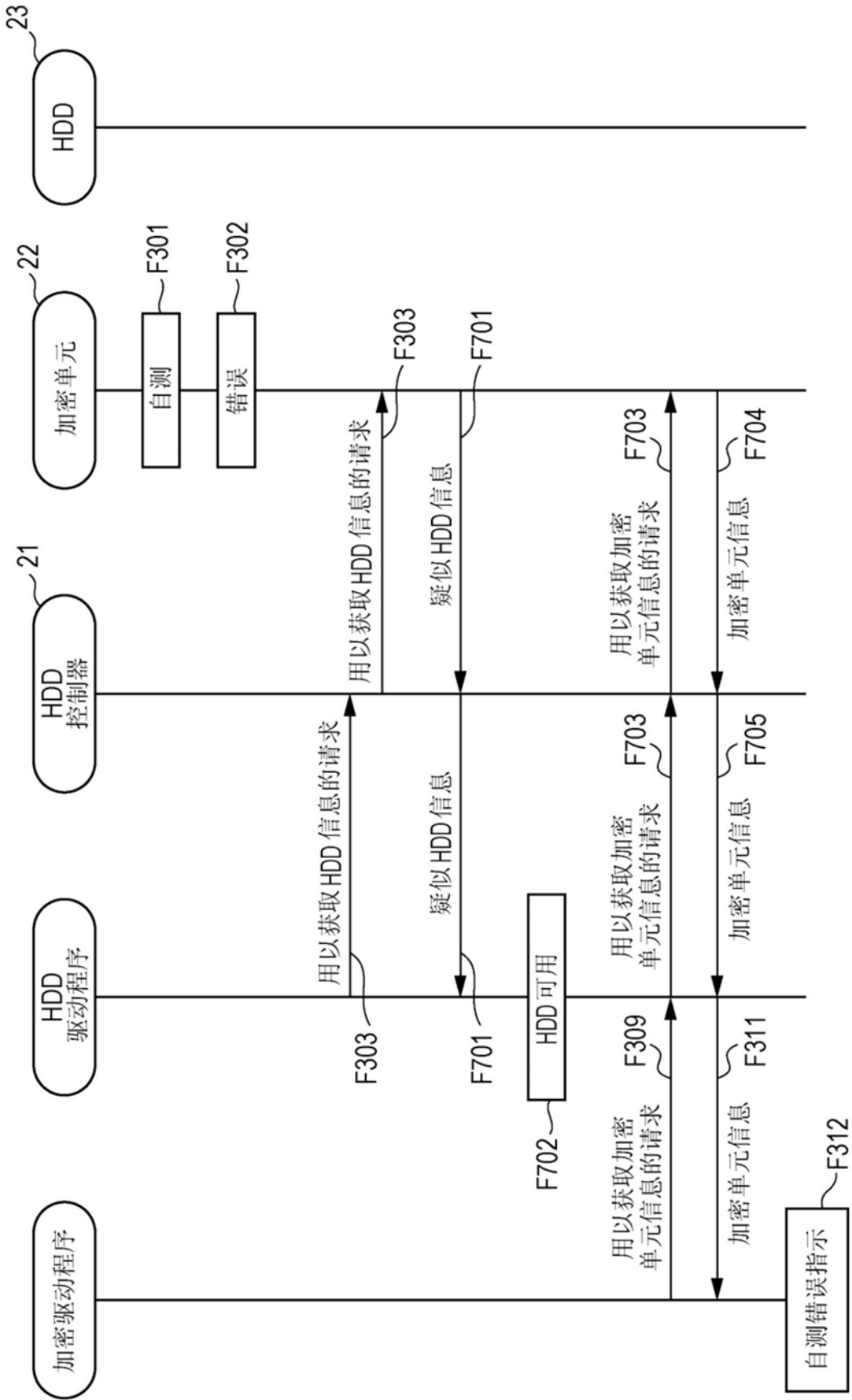


图7