



(12)发明专利

(10)授权公告号 CN 104811580 B

(45)授权公告日 2018.06.22

(21)申请号 201510040821.2

(51)Int.Cl.

(22)申请日 2015.01.27

H04N 1/32(2006.01)

(65)同一申请的已公布的文献号

申请公布号 CN 104811580 A

(56)对比文件

US 2009/0049310 A1,2009.02.19,

CN 101465937 A,2009.06.24,

US 2010/0296651 A1,2010.11.25,

CN 103425937 A,2013.12.04,

(43)申请公布日 2015.07.29

(30)优先权数据

2014-014560 2014.01.29 JP

审查员 章婧

(73)专利权人 佳能株式会社

地址 日本东京都大田区下丸子3-30-2

(72)发明人 安川朱里

(74)专利代理机构 北京怡丰知识产权代理有限公司 11293

代理人 迟军

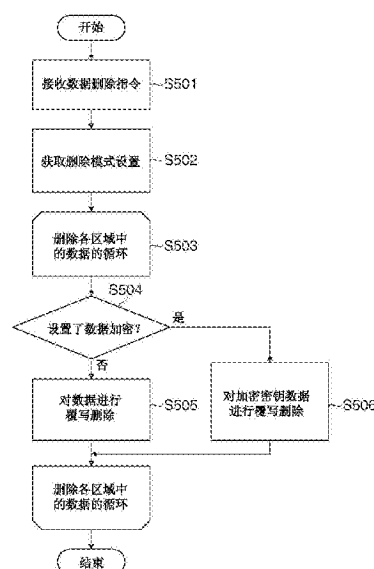
权利要求书2页 说明书9页 附图8页

(54)发明名称

能够有效地删除存储的数据的图像处理装置及其控制方法

(57)摘要

本发明提供能够有效地删除存储的数据的图像处理装置及其控制方法。图像处理装置甚至在加密数据和未加密数据混合的环境下,在维持针对数据泄露的安全性的同时,减少使数据无效所需的时间段。图像处理装置包括用于存储数据的HDD。确定是否对存储在HDD中的数据进行了加密,如果确定对数据进行了加密,则进行覆写删除,以使得无法读出在对数据进行加密时使用的加密密钥、或者创建加密密钥所需的信息,而如果确定未对数据进行加密,则进行覆写删除,以使得无法从HDD中读出数据。



1. 一种图像处理装置,其包括:

存储单元,被构造为存储数据;

确定单元,被构造为确定存储在所述存储单元中的数据是否由加密单元进行了加密;

第一删除单元,被构造为在所述确定单元确定对数据进行了加密的情况下,使得无法读出所述加密单元使用的加密密钥或者用于创建所述加密密钥的信息;以及

第二删除单元,被构造为在所述确定单元确定未对数据进行加密的情况下,使得无法读出存储在所述存储单元中的数据,

其中,在确定对数据进行了加密的情况下,所述第一删除单元使用预定数据,针对所述存储单元的、存储有所述加密密钥或者用于创建所述加密密钥的信息的存储区域,进行预定次数的覆写处理,

其中,在确定未对数据进行加密的情况下,所述第二删除单元使用与存储的数据不同的数据,针对所述存储单元的存储有数据的存储区域,进行预定次数的覆写处理,并且

其中,能够经由用户接口画面选择覆写处理的预定次数。

2. 根据权利要求1所述的图像处理装置,其中,根据用户的删除指令,所述确定单元进行确定,由此执行所述第一删除单元的处理和/或所述第二删除单元的处理。

3. 根据权利要求1所述的图像处理装置,所述图像处理装置还包括:

设置单元,用于进行使得无法读出存储在所述存储单元中的数据的设置,并且

其中,即使在所述确定单元确定对数据进行了加密的情况下,当所述设置单元进行了所述设置时,所述第一删除单元也使得无法读出存储在所述存储单元中的数据。

4. 根据权利要求1所述的图像处理装置,其中,所述加密单元对要存储在所述存储单元中形成的多个存储区域中的、预先设置的预定存储区域中的数据进行了加密。

5. 一种图像处理装置,其包括:

存储单元,被构造为包括用于存储加密单元进行了加密的数据的加密数据区域和用于存储所述加密单元未进行加密的数据的未加密数据区域;以及

删除单元,被构造为使得无法读出在所述加密单元对存储在所述加密数据区域中的数据进行加密时使用的加密密钥、或者用于创建所述加密密钥的信息,并且使得无法从所述存储单元中读出存储在所述未加密数据区域中的数据,

其中,使用预定数据将所述加密密钥或者用于创建所述加密密钥的信息覆写预定次数,

其中,使用与存储的数据不同的数据将存储在所述加密数据区域中的数据覆写预定次数,并且

其中,能够经由用户接口画面选择覆写的预定次数。

6. 一种图像处理装置的控制方法,所述图像处理装置包括存储数据的存储单元,所述控制方法包括:

确定是否对存储在所述存储单元中的数据进行了加密;

在所述确定步骤确定对数据进行了加密的情况下,使得无法读出用于加密的加密密钥或者用于创建所述加密密钥的信息;以及

在所述确定步骤确定未对数据进行加密的情况下,使得无法读出存储在所述存储单元中的数据,

其中,在确定对数据进行了加密的情况下,使用预定数据,针对所述存储单元的、存储有所述加密密钥或者用于创建所述加密密钥的信息的存储区域,进行预定次数的覆写处理,

其中,在确定未对数据进行加密的情况下,使用与存储的数据不同的数据,针对所述存储单元的存储有数据的存储区域,进行预定次数的覆写处理,并且

其中,能够经由用户接口画面选择覆写处理的预定次数。

7.一种图像处理装置的控制方法,所述图像处理装置包括存储数据的存储单元,所述控制方法包括:

在所述存储单元中配设用于存储加密数据的加密数据区域和用于存储未加密数据的未加密数据区域;以及

使得无法读出在对存储在所述加密数据区域中的数据进行加密时使用的加密密钥、或者用于创建所述加密密钥的信息,并且使得无法从所述存储单元中读出存储在所述未加密数据区域中的数据,

其中,使用预定数据将所述加密密钥或者用于创建所述加密密钥的信息覆写预定次数,

其中,使用与存储的数据不同的数据将存储在所述加密数据区域中的数据覆写预定次数,并且

其中,能够经由用户接口画面选择覆写的预定次数。

能够有效地删除存储的数据的图像处理装置及其控制方法

技术领域

[0001] 本发明涉及图像处理装置、其控制方法和存储介质,尤其涉及删除存储在图像处理装置中的加密数据和未加密数据的方法。

背景技术

[0002] 能够使用诸如硬盘驱动器(HDD)的存储设备累积信息的信息处理装置,包括被构造为将接收到的信息(下文中也称为“数据”)临时存储在HDD中,并且在使用该数据的处理完成之后从HDD中删除该数据的信息处理装置。在这种信息处理装置中,HDD存储数据和指示数据在HDD上的位置的位置信息(下文中称为“FAT(文件分配表)”)。当从HDD中删除数据时,从高速数据删除处理的观点来看,通常仅删除FAT。残留在HDD上的数据迟早会被其他数据覆写(overwrite)。

[0003] 然而,在当上述信息处理装置被丢弃时,数据残留在HDD上的情况下,担心通过将HDD从信息处理装置移除,并且将HDD连接到例如计算机(PC)以对数据进行分析而导致数据被窃取。

[0004] 近年来,随着信息安全意识的提高,不仅用于删除FAT、还用于删除残留在HDD上的数据的覆写删除功能变得广为人知。在具有这种覆写删除功能的信息处理装置中,通过一次或多次在不再需要的数据上写入0、随机数或者固定值来防止数据残留(例如参见日本特许第3715711号公报)。

[0005] 然而,当丢弃信息处理装置时,需要在HDD上的所有存储区域中写入覆写数据,这产生了如下问题:进行覆写处理与HDD的容量成比例地花费很长的时间。此外,作为保护HDD上的数据的方法,广泛使用利用加密的数据保护。在日本特许第4606808号公报中,为了解决上述处理时间的问题,提出了如下方法:通过进行使得无法对加密数据进行解密而需要删除的最小数据量的覆写删除,作为删除加密数据的手段,来减少覆写处理时间。

[0006] 然而,在日本特许第4606808号公报所描述的技术中,在存储设备上混合了加密数据区域和未加密数据区域的环境下,或者在数据的加密取决于其设置的环境下,难以在短时间段内选择性地并且有效地删除存储设备上的数据。

发明内容

[0007] 本发明提供了如下技术:甚至在混合了加密数据和未加密数据的环境下,通过在维持针对数据泄露的安全性的同时,减少使数据无效所需的时间段,来提高图像处理装置的用户友好性。

[0008] 在本发明的第一方面,提供一种图像处理装置,其包括:存储单元,被构造为存储数据;确定单元,被构造为确定存储在所述存储单元中的数据是否由加密单元进行了加密;第一删除单元,被构造为在所述确定单元确定对数据进行了加密的情况下,使得无法读出所述加密单元使用的加密密钥或者创建所述加密密钥所需的信息;以及第二删除单元,被构造为在所述确定单元确定未对数据进行加密的情况下,使得无法读出存储在所述存储单

元中的数据。

[0009] 在本发明的第二方面,提供一种图像处理装置,其包括:存储单元,被构造为包括用于存储加密单元进行了加密的数据的加密数据区域和用于存储所述加密单元未进行加密的数据的未加密数据区域;以及删除单元,被构造为使得无法读出在所述加密单元对存储在所述加密数据区域中的数据进行加密时使用的加密密钥、或者创建所述加密密钥所需的信息,并且使得无法从所述存储单元中读出存储在所述未加密数据区域中的数据。

[0010] 在本发明的第三方面,提供一种图像处理装置的控制方法,所述图像处理装置包括存储数据的存储单元,所述控制方法包括:确定是否对存储在所述存储单元中的数据进行加密;在所述确定步骤确定对数据进行了加密的情况下,使得无法读出用于加密的加密密钥或者创建所述加密密钥所需的信息;以及在所述确定步骤确定未对数据进行加密的情况下,使得无法读出存储在所述存储单元中的数据。

[0011] 在本发明的第四方面,提供一种图像处理装置的控制方法,所述图像处理装置包括存储数据的存储单元,所述控制方法包括:在所述存储单元中配设用于存储加密数据的加密数据区域和用于存储未加密数据的未加密数据区域;以及使得无法读出在对存储在所述加密数据区域中的数据进行加密时使用的加密密钥、或者创建所述加密密钥所需的信息,并且使得无法从所述存储单元中读出存储在所述未加密数据区域中的数据。

[0012] 在本发明的第五方面,提供一种非易失性计算机可读存储介质,其存储用于执行图像处理装置的控制方法的计算机可执行程序,所述图像处理装置包括存储数据的存储单元,其中,所述控制方法包括:确定是否对存储在所述存储单元中的数据进行加密;在所述确定步骤确定对数据进行了加密的情况下,使得无法读出用于加密的加密密钥或者创建所述加密密钥所需的信息;以及在所述确定步骤确定未对数据进行加密的情况下,使得无法读出存储在所述存储单元中的数据。

[0013] 在本发明的第六方面,提供一种非易失性计算机可读存储介质,其存储用于执行图像处理装置的控制方法的计算机可执行程序,所述图像处理装置包括存储数据的存储单元,其中,所述控制方法包括:在所述存储单元中配设用于存储加密数据的加密数据区域和用于存储未加密数据的未加密数据区域;以及使得无法读出在对存储在所述加密数据区域中的数据进行加密时使用的加密密钥、或者创建所述加密密钥所需的信息,并且使得无法从所述存储单元中读出存储在所述未加密数据区域中的数据。

[0014] 根据本发明,能够通过维持针对数据泄露的安全性的同时,减少使数据无效所需的时间段,来提高图像处理装置的用户友好性。

[0015] 通过以下(参照附图)对示例性实施例的描述,本发明的其他特征将变得清楚。

附图说明

[0016] 图1是示出根据本发明的第一实施例的图像处理装置的硬件配置的框图。

[0017] 图2是示出图1所示的图像处理装置的软件配置的框图。

[0018] 图3是示出在HDD中形成的分区的图。

[0019] 图4A是在HDD中写入数据的处理的流程图。

[0020] 图4B是从HDD中读取数据的处理的流程图。

[0021] 图5是删除存储在图像处理装置中的所有数据的处理的流程图。

[0022] 图6A是示出在图5中的步骤中用户接口控制器在用户接口上显示的画面的示例的图。

[0023] 图6B是示出在图7中的步骤中用户接口控制器在用户接口上显示的画面的示例的图。

[0024] 图7是根据本发明的第二实施例的删除存储在图像处理装置中的所有数据的处理的流程图。

[0025] 图8是示出由数据加密部管理的加密设置管理信息的示例的图。

[0026] 图9是示出使用专用硬件进行加密的图像处理装置的硬件配置的框图。

具体实施方式

[0027] 现在,下面参照示出本发明的实施例的附图,详细描述本发明。

[0028] 图1是示出根据本发明的第一实施例的图像处理装置的硬件配置的框图。

[0029] 用附图标记10表示的图像处理装置由CPU 11、RAM 12、硬盘控制器(HDC)13、图像控制器14、控制台部(用户接口)15、硬盘驱动器(HDD)16、扫描器部17、打印机部18和非易失性存储器19构成。

[0030] CPU 11是用于控制图像处理装置10的总体操作的控制器,其通过读取存储在RAM 12中的程序和数据来进行控制处理。RAM 12是用于临时保持程序和图像数据的可读写易失性存储设备。HDD 16是用于将程序、图像数据、用户设置等作为文件保持的可读写非易失性存储设备。HDC 13是用于控制HDD 16的控制器,其对向HDD 16中的数据写入和从HDD 16中的数据读取进行控制。

[0031] 图像控制器14是用于控制扫描器部17和打印机部18的控制器。图像控制器14根据来自下文中描述的在图2中示出的数据输入和输出控制器23的指令,向RAM 12传输从扫描器17获得的要存储的图像数据,并且向打印机部18传输存储在RAM 12中的图像数据。由未示出的原稿照明灯、扫描镜、CCD传感器等构成的扫描器部17,使用CCD传感器读取经由扫描镜、透镜等从原稿反射的光,以创建图像数据,并且向RAM12传输所创建的图像数据。由未示出的激光器、多边扫描器、感光鼓等构成的打印机部18,将从RAM 12传输的图像数据转换为电信号,并且使用基于电信号的激光束照射感光鼓,由此在片材上形成图像。

[0032] 由未示出的液晶显示部、触摸面板、硬键等构成的控制台部15,接收来自用户的操作指令,并且显示图像处理装置10的状态等。

[0033] 非易失性存储器19是例如由闪存实现的、用于存储程序、下文中参照的加密密钥等的可读写非易失性存储设备。

[0034] 图像处理装置10不限于所示出的配置,其可以包括用于连接到LAN的网络连接部和用于发送/接收FAX(传真)的FAX输入/输出控制器。

[0035] 此外,虽然在本实施例中,HDD 16用作用于存储图像数据和用户设置信息的非易失性存储设备,但是非易失性存储器19或者未示出的诸如SSD(固态驱动器)的非易失性存储设备也可以用于该用途。此外,可以组合使用多个存储设备。

[0036] 图2是示出图1所示的图像处理装置10的软件配置的框图。

[0037] 图像处理装置控制程序20是存储在RAM 12中的由CPU 11执行的用于控制图像处理装置10的程序模块。图像处理装置控制程序20由下列各种程序构成:用户接口控制器21、

作业控制器22、数据输入和输出控制器23、文件管理部24、设置管理部25、日志管理部26、数据删除部27、数据加密部28以及HDD控制器29。

[0038] 控制台部控制器21是用于控制控制台部15的程序,其经由触摸面板接收来自用户的指令,并且在液晶面板上显示图像处理装置10的状态。

[0039] 作业控制器22是用于控制由图像处理装置10进行的诸如复印的处理(作业)的程序,其与控制台部控制器21、数据输入和输出控制器23、文件管理部24等协作执行作业。

[0040] 数据输入和输出控制器23是用于控制图像控制器14的程序,其与RAM 12交换数据,由此将图像数据保持在RAM 12中,并且向打印机部18发送存储在RAM 12中的图像数据。

[0041] 文件管理部24是用于从HDD 16中读取数据并且向HDD 16中写入数据的程序,其对在HDD 16上创建的文件系统进行管理,由此作为文件向HDD 16中存储各个数据项并且从HDD 16中读取各个数据项。

[0042] 设置管理部25是用于对图像处理装置10的各种操作的设置以及用户信息和地址簿的设置进行管理的程序,其与文件管理部24协作,将由控制台部控制器21指定的设置作为文件存储在HDD 16中。

[0043] 日志管理部26是用于作为日志记录由作业控制器22和设置管理部25进行的处理的结果的程序,其与文件管理部24协作,将记录的日志数据作为文件存储在HDD 16中。

[0044] 数据删除部27是用于删除存储在图像处理装置10中的诸如图像数据和日志数据的所有数据的程序,其基于来自控制台部控制器21的指令,进行覆写删除。通过删除由文件管理部24管理的文件信息,然后将覆写数据写入下文中描述的各个分区的全部中,来进行覆写删除。覆写删除的方法不限于此。数据删除部27对未删除数据信息30和删除完成信息31进行管理,并且在删除操作时根据需要更新这些信息项。

[0045] 数据加密部28对从文件管理部24向HDD控制器29传送的数据进行加密处理。数据加密部28保持加密设置管理信息32,并且基于加密设置管理信息32对HDD 16中的用于加密的存储区域和加密密钥的信息(例如创建加密密钥所需的信息(种子(seed)值))进行管理。下文中将描述对数据进行加密的处理。

[0046] HDD控制器29根据来自文件管理部24、数据删除部27和数据加密部28的各个请求,从HDD 16中读取数据并且向HDD 16中写入数据。

[0047] 图3是示出在HDD中形成的分区的图。

[0048] 如图3所示,通过将HDD 16划分为多个分区,来对HDD 16进行管理。附图标记301和302表示两个图像文件区域(第一和第二图像文件区域),其主要用于存储与作业控制器22使用的图像相关联的数据。附图标记303表示设置文件区域,其用于存储由设置管理部25管理的各种设置的数据。附图标记304表示日志区域,其用于存储由日志管理部26记录的、由作业控制器22和设置管理部25进行的处理的结果的数据。附图标记305表示系统数据区域,其用于存储图像处理装置控制程序20的操作所需的各种数据。附图标记306表示临时区域,其用于存储图像处理装置控制程序20临时使用的数据。

[0049] 虽然在本实施例中,描述了在HDD 16中形成图3所示的分区的状况,但是可以以分布方式将分区设置为多个非易失性存储设备。此外,在HDD 16中形成的分区可以不是物理构成的分区,而是由文件管理部24管理的逻辑构成的分区。

[0050] 接下来,参照图4A和图4B,对图像处理装置10进行的向HDD 16输入数据/从HDD 16

输出数据的处理给出描述。

[0051] 图4A是向HDD 16中写入数据的处理的流程图。本处理由CPU 11进行。

[0052] 首先,在步骤S401中,作业控制器22、设置管理部25等请求文件管理部24向HDD 16中写入数据。

[0053] 为了在HDD 16的预定区域中写入数据,文件管理部24请求数据加密部28执行数据的写入(步骤S402)。

[0054] 在接收到来自文件管理部24的执行数据写入的请求时,数据加密部28确定是否需要将要写入HDD 16的数据进行加密(步骤S403)。具体来说,数据加密部28基于加密设置管理信息32,确定文件管理部24指定的HDD 16的数据写入区域,是否是要对数据进行加密的区域(下文中称为“加密区域”)。图8示出了由数据加密部28管理的加密设置管理信息32的示例。

[0055] 参照图8,在加密设置管理信息32中,针对在HDD 16中设置的多个存储区域中的各个,对各个区域的起始地址、加密设置和加密密钥的信息进行管理。在所示出的加密设置管理信息32中,设置为对系统数据区域和临时区域之外的区域进行加密。例如,如果来自文件管理部24的数据写入请求是将数据写入第一和第二图像文件区域中的任意一个的请求,则数据加密部28基于所示出的加密设置管理信息32,确定数据写入请求所指定的区域是加密区域。

[0056] 虽然用户可以直接针对图像处理装置10设置由加密设置管理信息32管理的加密区域,但是例如也可以在制造图像处理装置10的阶段预先设置加密区域。例如,在进行了对要存储在HDD 16中的所有数据进行加密的设置的情况下,如果该设置有效,则将该设置登记在加密设置管理信息32中,使得所有存储区域是加密区域。此外,加密设置管理信息32可以被构造为可以根据是否存在用户的许可,或者是否使用可选硬件来改变设置。此外,虽然所示出的加密设置管理信息32被构造为针对各个区域管理的表,但是加密设置管理信息32可以被构造为针对整个非易失性存储设备仅进行一个设置。

[0057] 在对数据进行加密时使用的各个加密密钥存储在非易失性存储器19中,在进行加密之前,从非易失性存储器19中读取各个加密密钥,以对数据进行加密。基于加密设置管理信息32,对要使用哪个密钥进行控制。此外,不一定需要每次对数据进行加密时,都读出加密密钥,而可以在读出一个加密密钥之后,在RAM 12中对加密密钥进行管理。为了安全地管理各个加密密钥,可以使用进一步对要存储在非易失性存储器19中的加密密钥进行加密的方法、使用安全芯片对加密密钥进行管理的方法、以及通过将存储在非易失性存储器19中的信息与其他信息组合来重建加密密钥的方法。此外,例如可以在启动装置时、在使用HDD时或者在类似的其他定时自动创建加密密钥。虽然在加密设置管理信息32中,可以针对各个区域设置加密密钥和加密算法,但是这里省略其详细描述。

[0058] 返回参照图4A,如果在步骤S403中确定需要对数据进行加密,则数据加密部28对数据进行加密,并且向HDD控制器29传送加密的数据(步骤S404)。

[0059] HDD控制器29将接收到的数据写入HDD 16中的预定区域(步骤S405),之后终止本处理。

[0060] 另一方面,如果在步骤S403中确定不需要对数据进行加密,则数据加密部28在不对数据进行加密的情况下,直接向HDD控制器29传送数据。HDD控制器29将接收到的数据写

入HDD 16中的预定区域(步骤S405),之后终止本处理。

[0061] 接下来,描述从HDD 16中读取数据的处理。

[0062] 图4B是从HDD 16中读取数据的处理的流程图。本处理由CPU 11进行。

[0063] 首先,在步骤S406中,作业控制器22、设置管理部25等请求文件管理部24从HDD 16中读取数据。

[0064] 为了从HDD 16中的预定区域中读取数据,文件管理部24请求数据加密部28执行数据的读取(步骤S407)。

[0065] 数据加密部28请求HDD控制器29读取数据。其结果是,HDD控制器29从HDD 16中读取数据(步骤S408)。

[0066] 接下来,在步骤S409中,数据加密部28确定在步骤S408中读取的数据是否是加密的数据。在步骤S409中,与步骤S403类似,数据加密部28基于加密设置管理信息32,确定读取数据的区域是否是对数据进行加密的加密区域。如果确定该区域是对数据进行加密的加密区域,则数据加密部28对在步骤S408中读取的数据进行解密,并且向文件管理部24传送解密的数据(步骤S410),之后终止本处理。

[0067] 另一方面,如果在步骤S409中确定该区域不是对数据进行加密的加密区域,则数据加密部28直接向文件管理部24传送所读取的数据,之后终止本处理。

[0068] 在本实施例中,如此进行在HDD 16中输入数据/从HDD 16中输出数据的处理。

[0069] 注意,在上面描述的处理中,描述了如下配置:在文件管理部24进行的处理和HDD控制器29进行的处理之间,执行数据加密部28进行的处理。然而,数据加密部28进行的处理可以在文件管理部24进行的处理之前,或者在HDD控制器29进行的处理之后执行。此外,可以在文件管理部24进行的处理之前执行数据加密部28进行的处理的一部分,而在HDD控制器29进行的处理之后执行另一部分的方式,以分布的方式执行数据加密部28进行的处理。然而,假设分布式处理各自由加密设置管理信息32进行管理。

[0070] 虽然在上面对本实施例的描述中,使用软件来实现数据加密,但是可以使用如图9所示的专用硬件来实现数据加密。

[0071] 图9是示出使用专用硬件进行加密的图像处理装置10a的硬件配置的框图。

[0072] 参照图9,作为图1所示的根据本实施例的图像处理装置10的变型例的图像处理装置10a与图像处理装置10的不同之处在于,增加了加密芯片101。省略对加密芯片101之外的构成元件的描述。

[0073] 加密芯片101布置在HDC 13和HDD 16之间,并对由HDC 13写入HDD 16的所有数据进行加密。另一方面,当HDC 13从HDD 16中读出数据时,加密芯片101对数据进行解密,并且向HDC 13传送解密的数据。

[0074] 加密芯片101被构造为从图像处理装置10a可移除,并且例如被配设为图像处理装置10的可选项。当将加密芯片101安装在图像处理装置10上,以形成图像处理装置10a时,图像处理装置10a在加密设置管理信息32中将加密芯片101的所有区域设置为加密区域。因此,在图4A和4B中的步骤S403和S409中进行的确定中,依据是否安装了加密芯片101来确定区域是否是加密区域。

[0075] 接下来,参照图5,对删除存储在图像处理装置10中的所有数据的处理给出描述。

[0076] 例如,当使用图像处理装置10的用户丢弃图像处理装置10时,进行图像处理装置

10的数据删除处理。

[0077] 图5是删除存储在图像处理装置10中的所有数据的处理的流程图。本处理由CPU 11进行。

[0078] 首先,在步骤S501中,图像处理装置10接收来自用户的数据删除指令。例如,控制台部控制器21在控制台部15上显示图6A所示的画面600,以提示用户选择删除模式。当用户在画面600上选择了多个删除模式(601至605)中的一个,并且按下画面600上的OK按钮607时,控制台部控制器21接收来自用户的指令。

[0079] 在画面600上,可以选择“写入一次0数据”601、“写入一次随机数据”602、“写入三次随机数据”603、“写入九次随机数据”604和“DoD标准”605五个模式中的任意一个,作为删除模式。删除模式不限于这些,而可以使用户选择使用预定数据执行预定次数的覆写处理。

[0080] 在步骤S501中接收到来自用户的数据删除指令后,数据删除部27获取用户选择的删除模式的设置信息(步骤S502),并且开始删除数据(步骤S503)。数据删除部27以如下方式对图3所示的除了系统数据区域305之外的所有区域进行覆写删除。

[0081] 在步骤S504中,数据删除部27询问数据加密部28删除目标区域是否是加密区域。数据加密部28与图4A中的步骤S403类似地确定删除目标区域是否是加密区域。如果基于该确定的结果确定删除目标区域不是加密区域,则数据删除部27按照在步骤S502中获取的删除模式,针对删除目标区域进行数据的覆写处理(步骤S505)。在该覆写处理中,数据删除部27向HDD控制器29传送覆写模式数据,并且HDD控制器29按照覆写模式覆写所有删除目标区域上的数据。如果在步骤S502中获取的删除模式指定多次数据写入,则数据删除部27将覆写处理重复指定的次数。

[0082] 另一方面,如果在步骤S504中确定删除目标区域是加密区域,则数据删除部27参照由数据加密部28管理的加密设置管理信息32,并且获取存储加密密钥的区域在非易失性存储器19上的位置信息。然后,数据删除部27基于所获取的位置信息,针对非易失性存储器19中的存储加密密钥的区域,按照覆写模式,进行数据的覆写处理(步骤S506)。注意,不仅可以对存储加密密钥的区域,而且可以对存储创建加密密钥所需的信息的存储区域,进行按照覆写模式的数据的写入。

[0083] 如上所述,数据删除部27对图3所示的系统数据区域305之外的所有区域,重复上面描述的步骤S504和步骤S505或S506。这时,数据删除部27参照未删除数据信息30,对未删除的数据(或者数据区域)进行覆写,在删除完成信息31中登记该区域,并且确定是否对删除目标区域中的所有数据进行了覆写删除。

[0084] 如上所述,在本实施例中,在加密数据和未加密数据之间区分存储在存储设备中的数据,并且对加密数据进行覆写删除,使得不再能够读出在加密时使用的加密密钥。另一方面,对未加密数据进行覆写删除,使得不再能够从存储设备中读出该数据。因此,在确定是对数据、还是对加密密钥进行覆写删除之后,进行覆写删除,因此能够减少删除数据所需的时间。其结果是,能够在维持针对数据泄露的安全性的同时,尽可能将使数据无效所需的时间减少到最少。

[0085] 接下来,作为本发明的第二实施例,对使得即使在对数据区域中的数据进行了加密的情况下,也能够选择是否删除数据的方法给出描述。第二实施例具有与参照图1至3所描述的第一实施例的配置相同的配置。因此,用相同的附图标记表示与第一实施例相同的

部件,并且省略其描述。下面仅对与第一实施例的不同点给出描述。

[0086] 图7是根据本发明的第二实施例的删除存储在图像处理装置中的所有数据的处理的流程图。本处理由CPU 11进行。

[0087] 首先,在步骤S701中,图像处理装置10接收来自用户的数据删除指令。例如,控制台部控制器21在控制台部15上显示图6B所示的画面800,以提示用户选择删除模式和实际数据删除设置。当用户在画面800上选择了多个删除模式(801至805)中的一个、以及实际数据删除的“ON(开)”806或“OFF(关)”807,并且按下OK按钮809时,控制台部控制器21接收用户的指令。

[0088] 在画面800上,可以选择“写入一次0数据”801、“写入一次随机数据”802、“写入三次随机数据”803、“写入九次随机数据”804和“DoD标准”805五个模式中的任意一个,作为删除模式。删除模式不限于这些,而可以提示用户指定希望的删除执行次数。

[0089] 此外,画面800上的实际数据删除设置是用于甚至在对删除目标区域的数据区域中的数据进行了加密时,选择是否删除该数据的设置。当选择“ON”806时,针对数据区域进行覆写删除,而当选择“OFF”807时,仅针对存储加密密钥的区域进行覆写删除。也就是说,不进行在第一实施例中描述的对数据区域中的数据的覆写删除。虽然在本实施例中,针对所有区域设置了“ON”806或者“OFF”807,但是可以构造为按照区域或者按照数据类型,选择实际数据设置。

[0090] 在步骤S701中接收到来自用户的数据删除指令后,数据删除部27获取用户选择的删除模式的设置信息(步骤S702),进一步获取实际数据删除设置的值(步骤S703),然后开始删除数据(步骤S704)。数据删除部27以如下方式对图3所示的除了系统数据区域305之外的所有区域进行覆写删除。

[0091] 在步骤S705中,数据删除部27询问数据加密部28删除目标区域是否是加密区域。数据加密部28与图4A中的步骤S403类似地确定删除目标区域是否是加密区域。如果基于该确定的结果确定删除目标区域不是加密区域,则数据删除部27按照在步骤S702中获取的删除模式,针对删除目标区域进行数据的覆写处理(步骤S707)。该覆写处理与在图5中的步骤S505中进行的覆写处理相同。

[0092] 另一方面,如果在步骤S705中确定删除目标区域是加密区域,则数据删除部27参照在步骤S703中获取的实际数据删除设置,并且确定实际数据删除的设置是“ON”还是“OFF”(步骤S706)。如果确定设置为“ON”,则处理进行到步骤S707,其中,数据删除部27进行上面描述的数据的覆写处理。

[0093] 另一方面,如果在步骤S706中确定设置为“OFF”,则数据删除部27参照由数据加密部28管理的加密设置管理信息32,并且获取存储加密密钥的区域在非易失性存储器19中的位置信息。然后,数据删除部27基于所获取的位置信息,针对非易失性存储器19中的存储加密密钥的区域,按照覆写模式,进行数据的覆写处理(步骤S708)。

[0094] 如上所述,数据删除部27对图3所示的系统数据区域305之外的所有区域,重复上面描述的步骤S705、S706和S707或S708。这时,数据删除部27参照未删除数据信息30,对未删除的数据(或者数据区域)进行覆写,在删除完成信息31中登记该区域,并且确定是否对删除目标区域中的所有数据进行了覆写删除。

[0095] 如上所述,在本实施例中,即使在对数据进行了加密时,也使得用户能够选择是否

删除实际数据,由此能够减少使数据无效所需的时间,并且还减小了用户关于安全性的担忧。

[0096] 在第一和第二实施例中,基于在图5中的步骤S502中和图7中的步骤S702中获取的删除模式进行数据的覆写。然而,在存储数据或加密密钥的非易失性存储设备是例如闪存的情况下,如果覆写模式是“写入一次0数据”,则这足以删除数据。因此,设置删除模式的方式不限于在实施例中描述的那些方式,而根据非易失性存储设备的特性,删除模式可以是固定的,或者可以针对各个对象区域选择性地设置。

[0097] 其他实施例

[0098] 本发明的实施例还能够由系统或装置的计算机以及系统或装置的计算机执行的方法来实现,所述计算机读出并执行记录在存储介质(其还可以被更完整地称为‘非易失性计算机可读存储介质’)上的计算机可执行指令(例如一个或更多个程序),以执行上述实施例中的一个或更多个的功能,和/或所述计算机包括一个或更多个电路(例如专用集成电路(ASIC)),用于执行上述实施例中的一个或更多个的功能,所述方法例如从存储介质中读出并执行计算机可执行指令,以执行上述实施例中的一个或更多个的功能,和/或控制一个或更多个电路,执行上述实施例中的一个或更多个的功能。所述计算机可以包括一个或更多个处理器(例如中央处理单元(CPU)、微处理单元(MPU)),并且可以包括单独的计算机或单独的处理器网络,以读出并执行计算机可执行指令。例如可以从网络或存储介质向计算机提供计算机可执行指令。存储介质例如可以包括硬盘、随机存取存储器(RAM)、只读存储器(ROM)、分布式计算系统的存储设备、光盘(例如紧凑盘(CD)、数字通用盘(DVD)或蓝光盘(BD)TM)、闪存设备、存储卡等中的一个或更多个。

[0099] 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。

[0100] 虽然参照示例性实施例对本发明进行了说明,但是应当理解,本发明不限于所公开的示例性实施例。所附权利要求的范围符合最宽的解释,以使其涵盖所有这种变型、等同结构及功能。

[0101] 本申请要求2014年1月29日提交的日本专利申请第2014-014560号的优先权,其全部内容通过引用,包含于此。

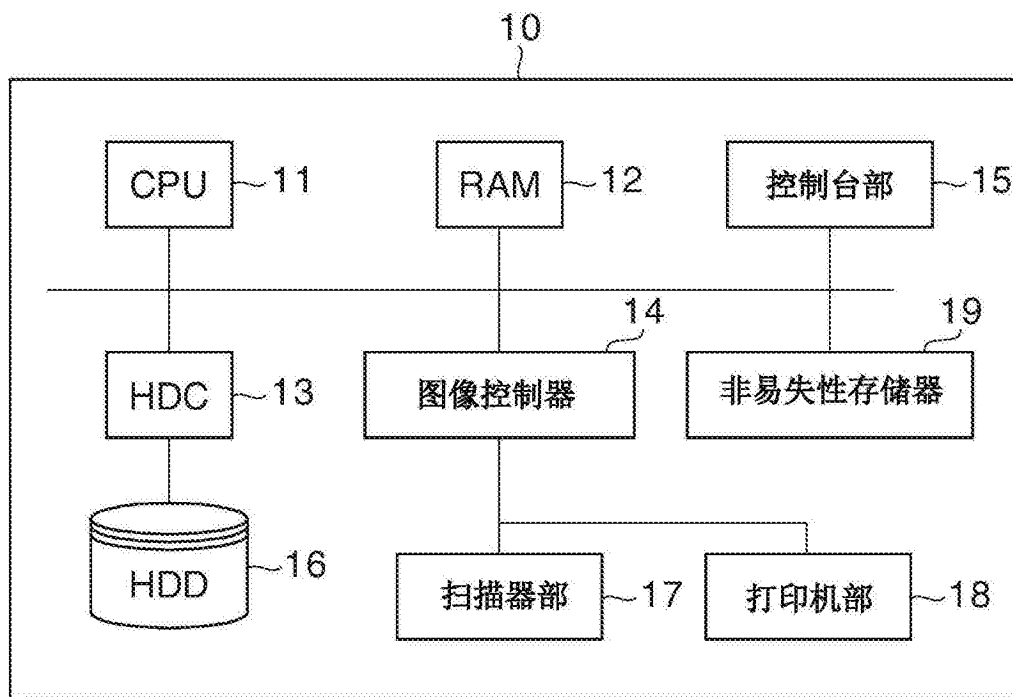


图1

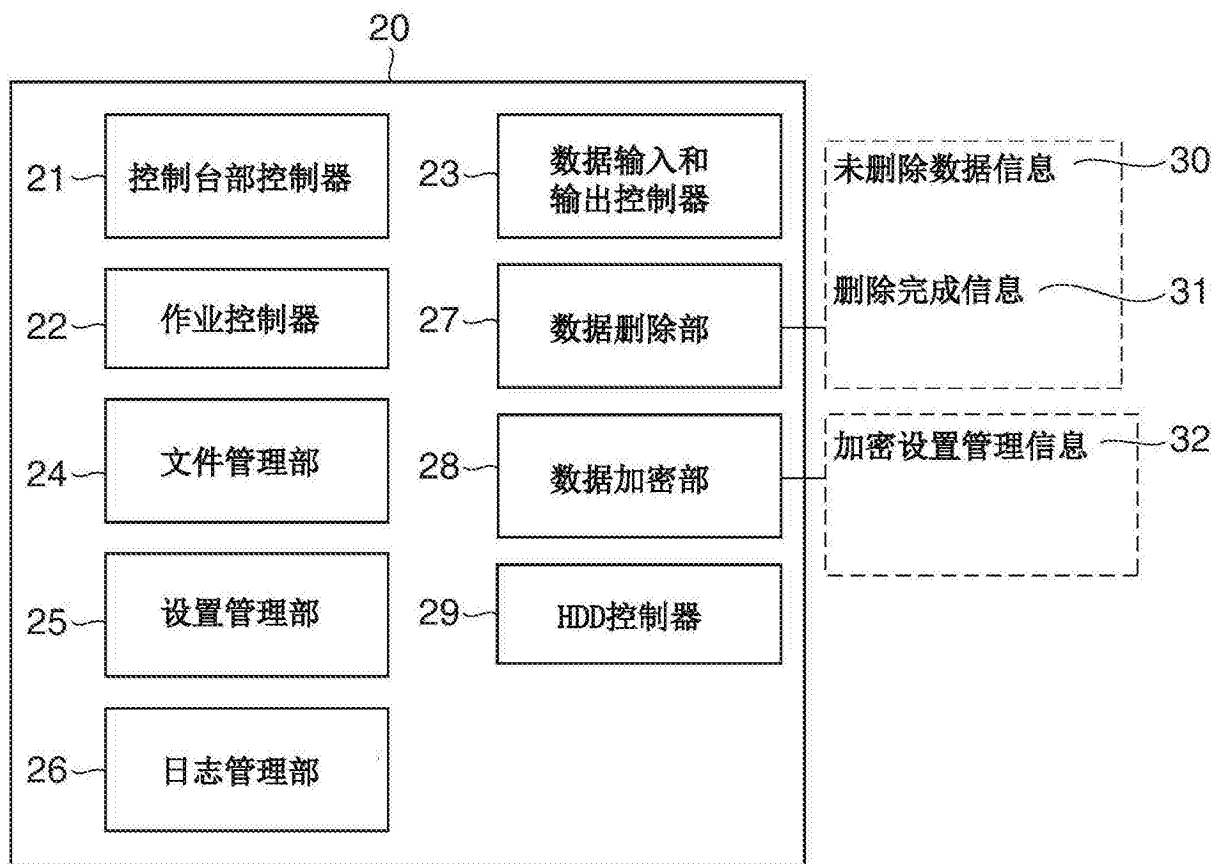


图2

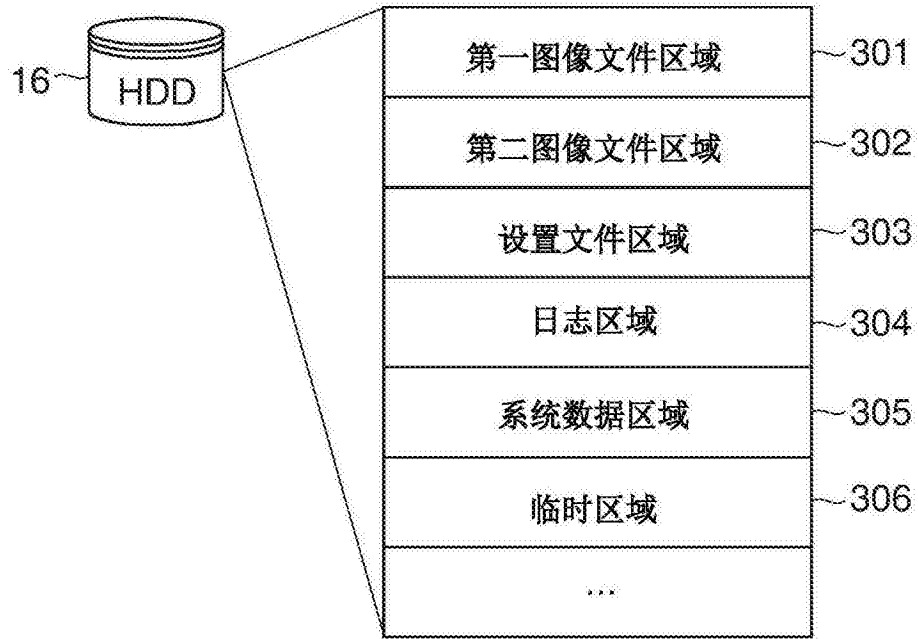


图3

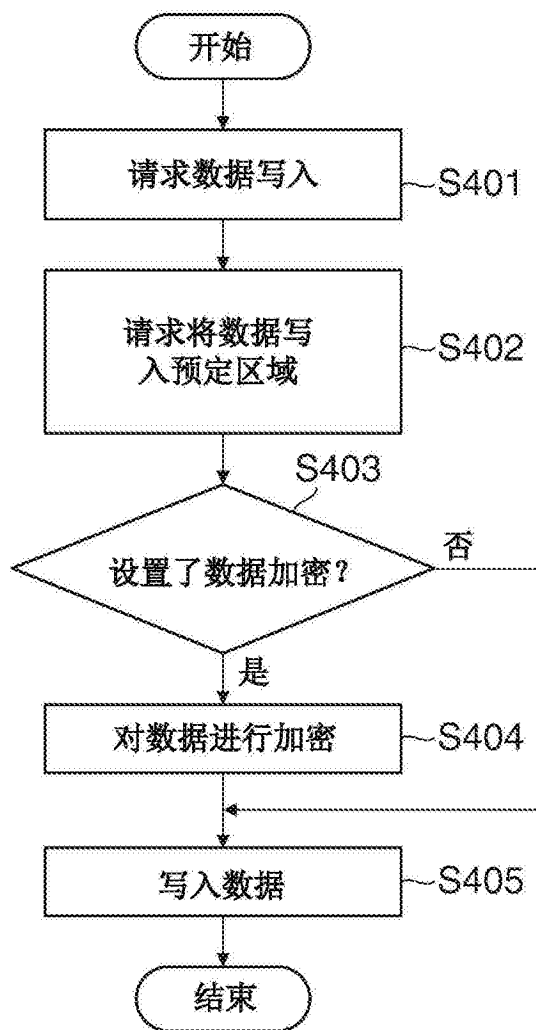


图4A

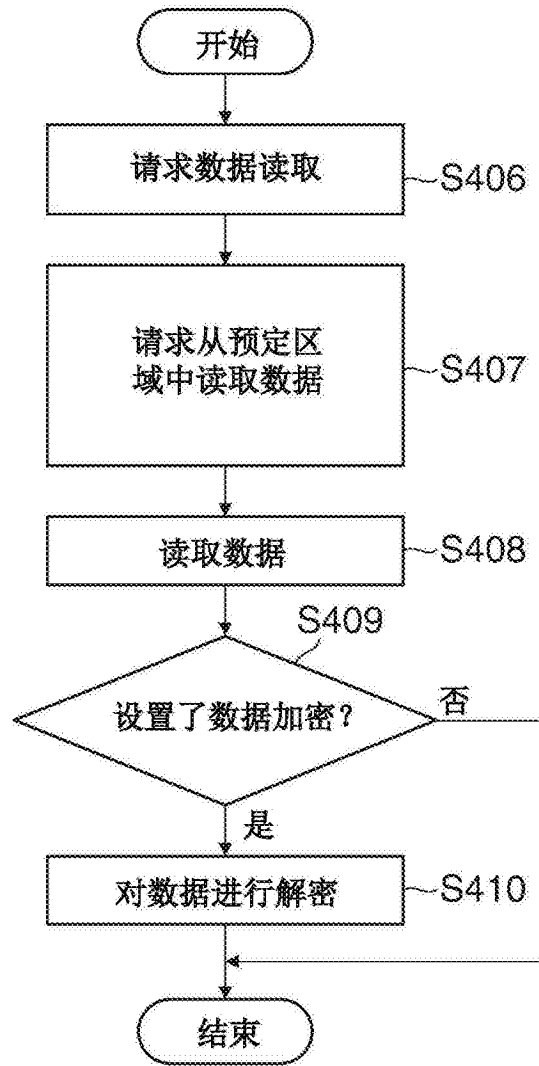


图4B

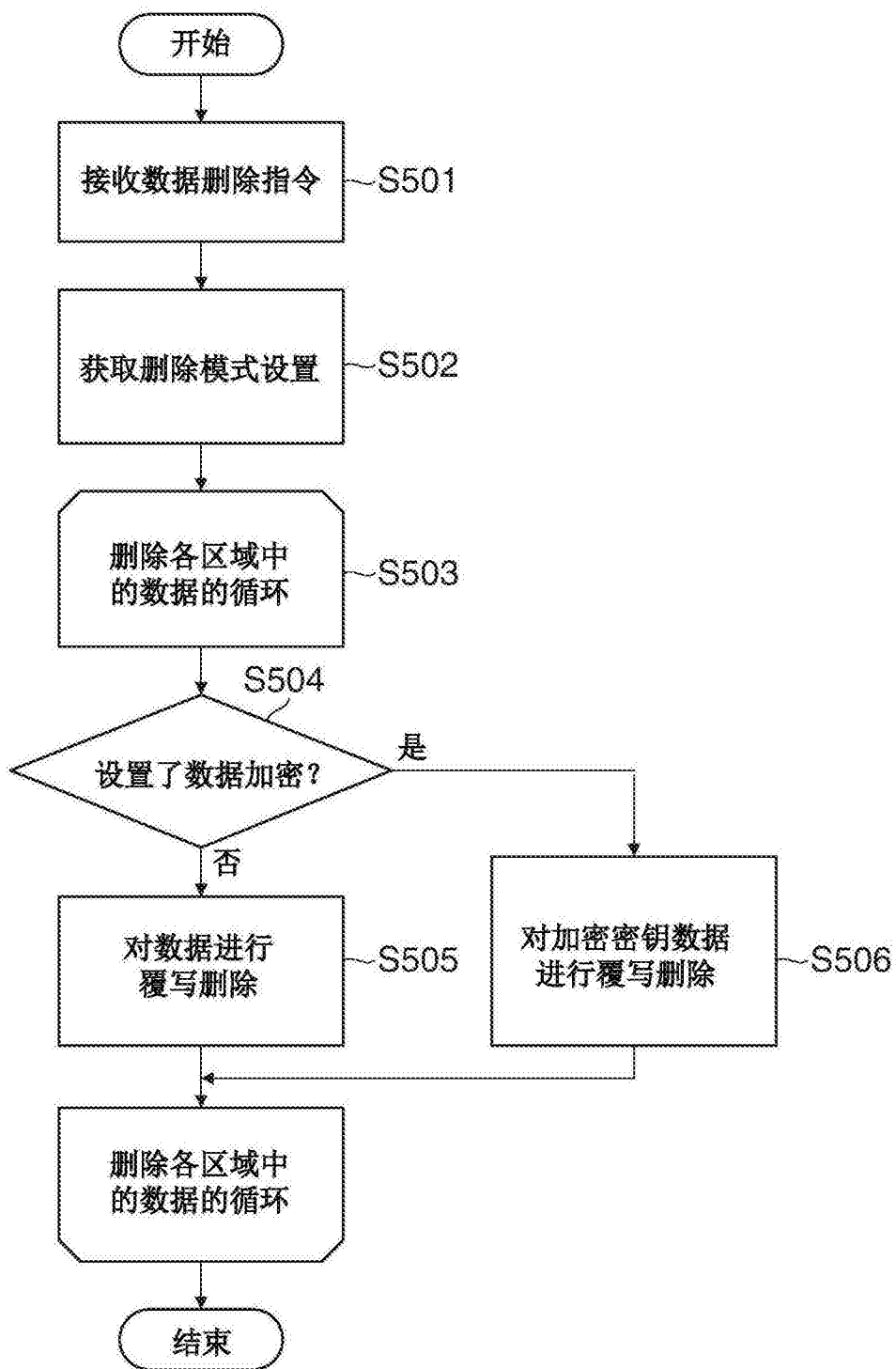


图5

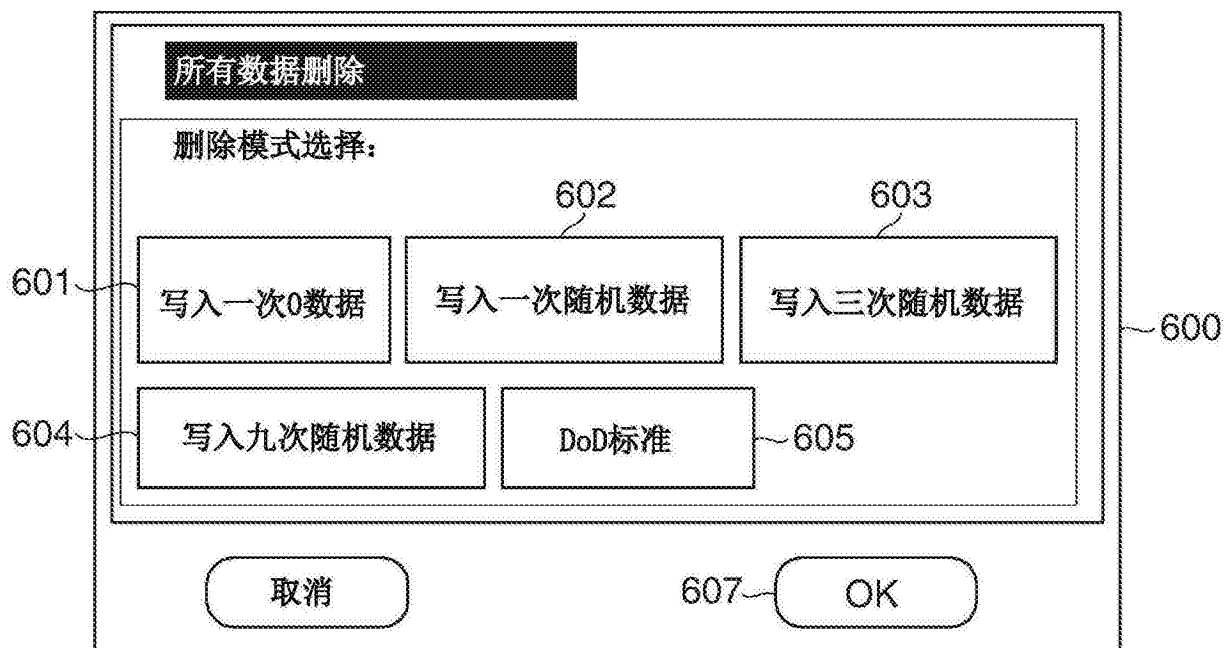


图6A

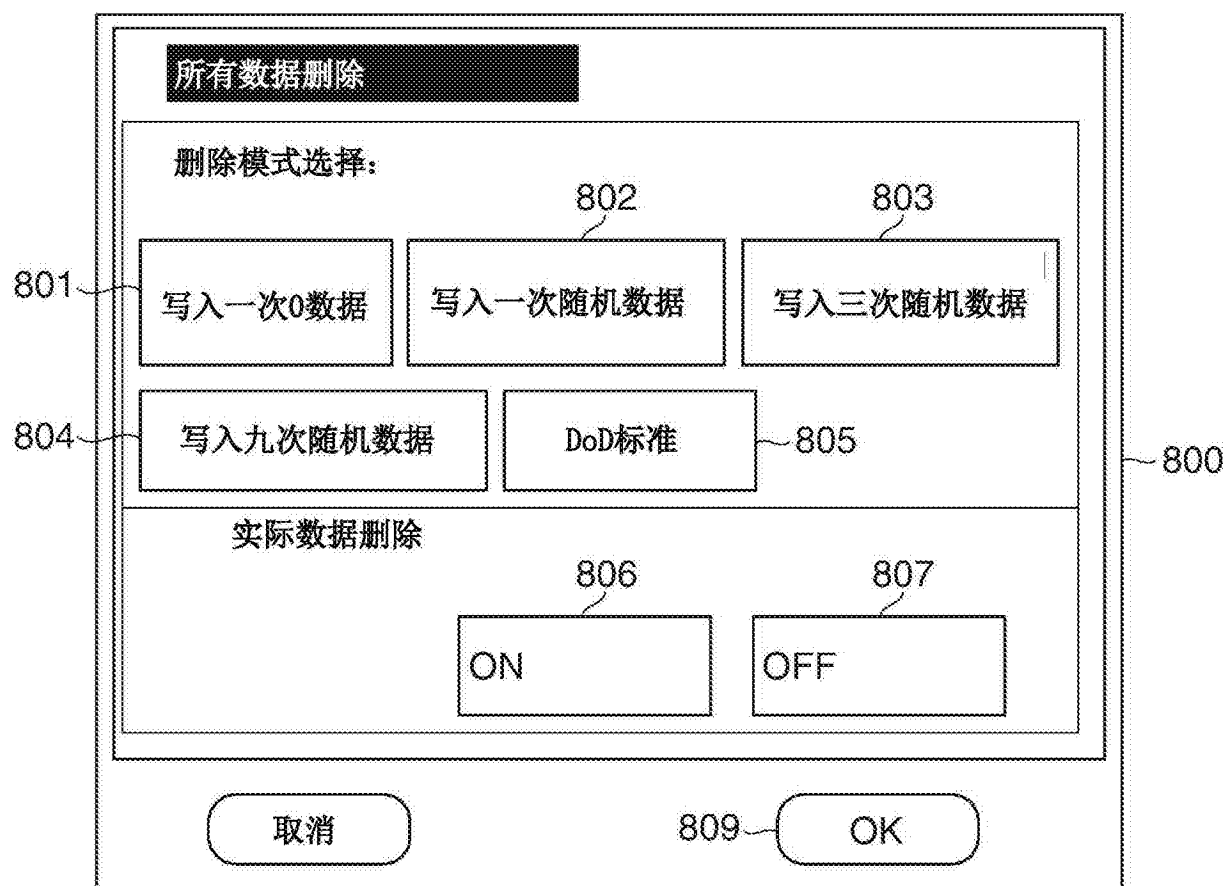


图6B

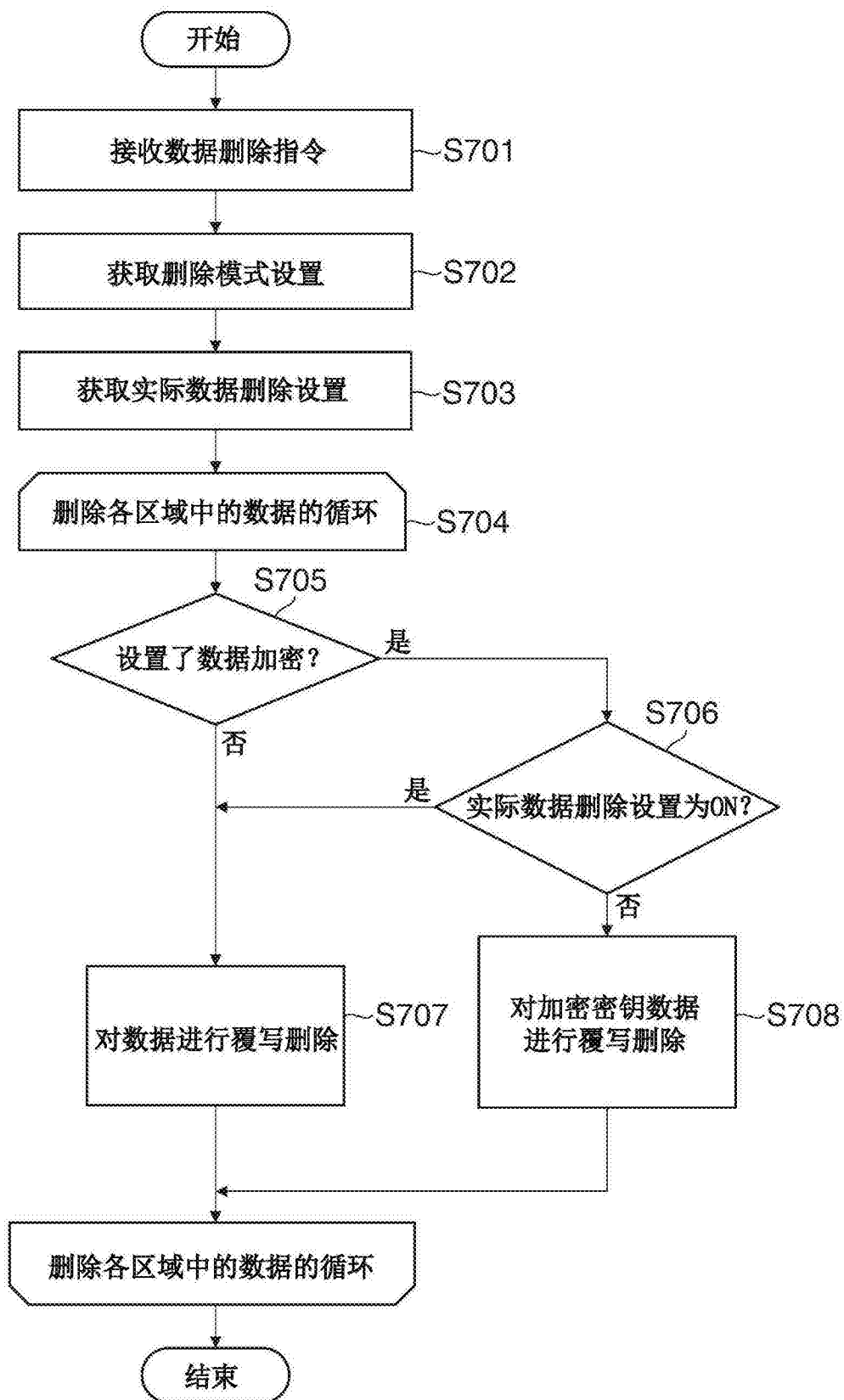


图7

32

区域名称	区域的起始地址	加密设置	加密密钥信息
第一图像文件区域	100	ON	key
第二图像文件区域	200	ON	key
设置文件区域	300	ON	key
日志区域	400	ON	key
系统数据区域	500	OFF	-
临时区域	600	OFF	-

图8

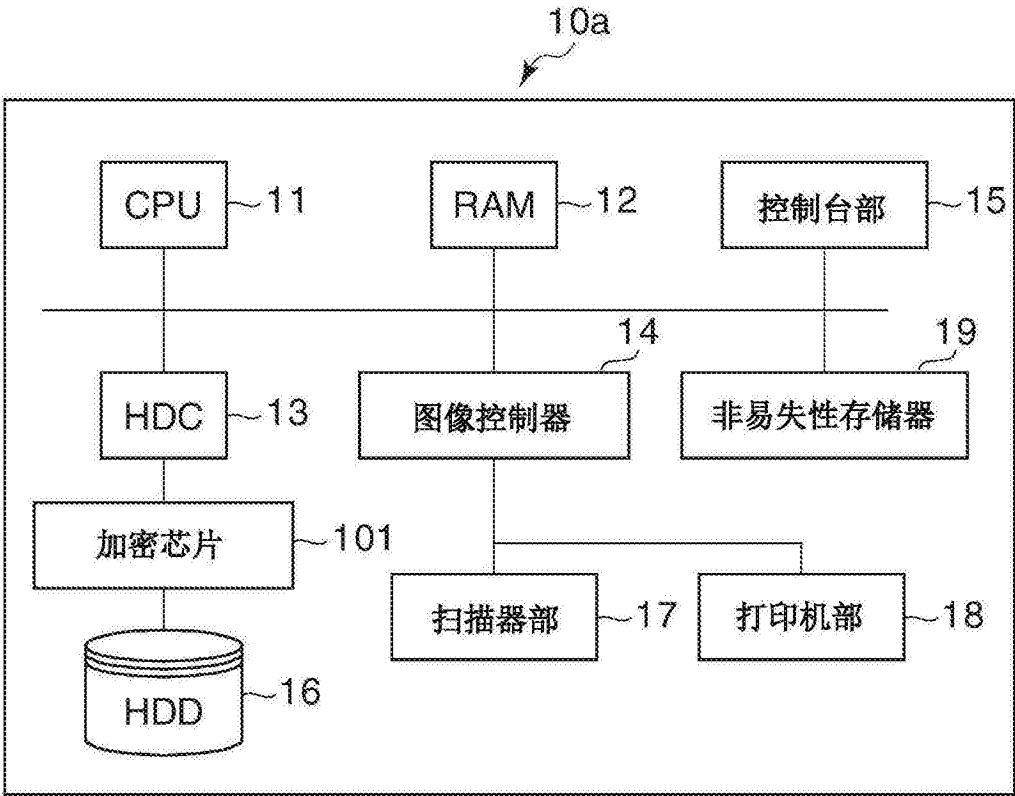


图9