(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 102073236 B
(45)授权公告日 2014.10.01

(21)申请号 201010557633.4

(22)申请日 2009.03.02

(30)优先权数据
10-2008-0019844 2008.03.03 KR
10-2008-0063068 2008.06.30 KR

(62)分案原申请数据
200910007789.2 2009.03.02

(73)专利权人 三星电子株式会社
地址 韩国京畿道水原市

(72)发明人 李在成 李允太 赵原逸

(74)专利代理机构 北京铭硕知识产权代理有限公司 11286
代理人 韩明星 李娜娜

(51)Int.Cl.
G03G 21/18(2006.01)
G06F 21/10(2013.01)
G06F 21/62(2013.01)
G06F 21/64(2013.01)
G06F 21/72(2013.01)
H04L 9/32(2006.01)

(56)对比文件
US 2005/0172118 A1,2005.08.04,说明书第5-8页,附图1.
CN 1377481 A,2002.10.30,说明书第7页第26-第8页第2行,第8页第24-27行.
JP 特开2005-202364 A,2005.07.28,全文.

审查员 丁沙

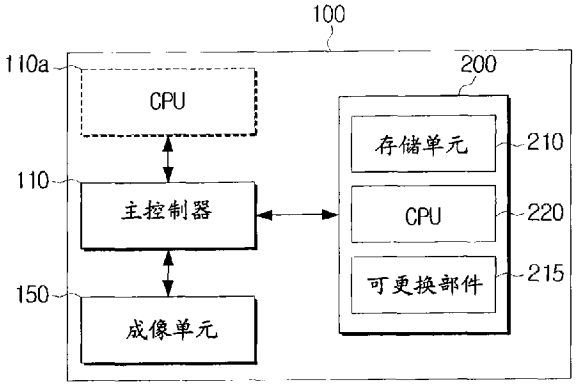
权利要求书4页 说明书15页 附图5页

(54)发明名称

使用操作系统的单元和使用该单元的成像设备

(57)摘要

本发明提供一种使用操作系统的单元和使用该单元的成像设备。一种可安装在用户可更换单元监控(CRUM)单元上的芯片,所述CRUM单元用于成像设备,所述芯片包括:中央处理单元(CPU),使用自己的操作系统(OS)执行与成像设备的主体的加密数据通信。由此,可增强安装有所述芯片的单元的安全性,并且可防止所述单元的数据的随意改变。



CN 102073236 B

1. 一种成像设备，包括：

成像设备的主体；

至少一个可更换单元，安装到成像设备的主体，用于执行成像操作，

其中，成像设备的主体包括用于控制成像设备的操作的主控制器，

其中，所述至少一个可更换单元包括：

存储单元，存储关于可更换单元的信息，并存储操作系统；

CPU，连接到存储单元，其中，当可更换单元安装到成像设备时，CPU 使用存储在可更换单元的存储单元中的操作系统执行初始化，CPU 被配置为访问存储在存储单元中的信息，并执行与成像设备的主控制器的加密数据通信，

其中，CPU 的操作系统与主控制器的另一操作系统独立地进行操作，

其中，CPU 执行所述加密数据通信，使得当包括数据和第一消息认证码信息的通信消息从成像设备的主体被发送时，所述 CPU 通过将密钥和加密算法应用于发送的通信消息的数据部分来产生第二消息认证码，并且当产生的第二消息认证码与发送的通信消息的第一消息认证码信息进行比较并与所述第一消息认证码信息一致时，产生的第二消息认证码被认为是有效的通信消息并被处理。

2. 根据权利要求 1 所述的成像设备，其中，可更换单元的存储单元存储将被 CPU 执行的操作系统，并且用于执行初始化的程序包括在操作系统中，CPU 的操作系统与主控制器的操作系统不同。

3. 根据权利要求 1 所述的成像设备，其中，所述至少一个可更换单元通过应用在多种加密算法中选择的加密算法来执行与主控制器的加密数据通信。

4. 根据权利要求 1 所述的成像设备，其中，主控制器通过使用为所述至少一个可更换单元中的每个设置的独有数字签名信息，来执行与所述至少一个可更换单元的加密数据通信。

5. 根据权利要求 1 所述的成像设备，其中，主控制器通过应用 ARIA、TDES、SEED 和 AES 对称密钥算法之一以及 RSA 非对称密钥算法来执行加密数据通信，并且所述至少一个可更换单元的 CPU 通过应用 ARIA、TDES、SEED 和 AES 对称密钥算法之一来执行加密数据通信。

6. 根据权利要求 1 所述的成像设备，其中，可更换单元还包括：

密码机单元，允许 CPU 执行与成像设备的主控制器的加密数据通信；

篡改检测器，对物理窃用尝试进行响应。

7. 根据权利要求 1 所述的成像设备，其中，存储单元具有包括存储器恢复区域的软件结构，并且当对于存储单元的数据写入操作被执行时，CPU 将先前记录的值备份在存储器恢复区域中并设置开始标志。

8. 根据权利要求 7 所述的成像设备，其中，当特定事件发生时，CPU 检查开始标志的改变的值，然后确定改变的值是否退回到先前记录的值。

9. 根据权利要求 1 所述的成像设备，其中，主控制器通过一个串行 I/O 通道连接到所述至少一个可更换单元，并且使用分配给每个可更换单元各自的地址来访问所述至少一个可更换单元。

10. 根据权利要求 1 所述的成像设备，其中，当执行成像作业时，主控制器测量用于所述成像作业的耗材使用的程度的值，将测量的值发送到所述至少一个可更换单元的每个

CPU，所述 CPU 将所述值与预先存储在每个存储单元中的关于耗材使用的信息相加，然后更新关于耗材使用的信息。

11. 根据权利要求 10 所述的成像设备，其中，成像设备的主体还包括用于存储关于耗材使用的信息的存储单元，

其中，主控制器将测量的耗材使用的程度的值与预先存储在存储单元中的关于耗材使用的信息相加，并且与所述至少一个可更换单元分离地管理关于耗材使用的信息。

12. 根据权利要求 11 所述的成像设备，其中，主控制器将存储在存储单元中的关于耗材使用的信息与存储在可更换单元中的关于耗材使用的信息进行比较，来确定存储的关于耗材使用的信息的准确性。

13. 根据权利要求 1 所述的成像设备，其中，可更换单元的存储单元存储用于执行与主控制器的加密数据通信的程序，所述用于执行加密数据通信的程序在 CPU 的初始化之后被执行。

14. 根据权利要求 1 所述的成像设备，其中，可更换单元是内置在用户可更换单元监控单元中的芯片。

15. 一种用于可更换单元的用户可更换单元监控单元，所述可更换单元可移除地安装在成像设备中，所述成像设备具有主控制器，所述用户可更换单元监控单元包括 ：

存储单元，存储关于可更换单元的信息，并存储操作系统 ；

CPU，连接到存储单元，其中，当可更换单元安装到成像设备时，CPU 使用存储在可更换单元的存储单元中的操作系统执行初始化，CPU 被配置为访问存储在存储单元中的信息，并执行与成像设备的主控制器的加密数据通信，

其中，CPU 的操作系统与主控制器的另一操作系统独立地进行操作，

其中，CPU 执行所述加密数据通信，使得当包括数据和第一消息认证码信息的通信消息从成像设备的主控制器被发送时，所述 CPU 通过将密钥和加密算法应用于发送的通信消息的数据部分来产生第二消息认证码，并且当产生的第二消息认证码与发送的通信消息的第一消息认证码信息进行比较并与所述第一消息认证码信息一致时，产生的第二消息认证码被认为是有效的通信消息并被处理。

16. 根据权利要求 15 所述的用户可更换单元监控单元，其中，存储单元存储将被 CPU 执行的操作系统，并且用于执行初始化的程序包括在操作系统中，CPU 的操作系统与由主控制器执行的操作系统不同。

17. 根据权利要求 15 所述的用户可更换单元监控单元，其中，在与成像设备的主控制器的认证完成之后，CPU 执行所述加密数据通信。

18. 根据权利要求 15 所述的用户可更换单元监控单元，其中，当成像设备开启时，并且当具有所述用户可更换单元监控单元的可更换单元被安装在成像设备上时，CPU 执行初始化，并且在初始化被完成之前对来自主控制器的命令不进行响应。

19. 根据权利要求 15 所述的用户可更换单元监控单元，其中，存储单元包括下列中的至少一个 ：操作系统存储器 ；非易失性存储器，以非易失性的形式存储数据 ；易失性存储器，用作操作所需的临时存储空间。

20. 根据权利要求 15 所述的用户可更换单元监控单元，还包括 ：

接口单元，将主控制器连接到 CPU ；

篡改检测器，对物理窃用尝试进行响应；以及

密码机单元，允许 CPU 执行与主控制器的加密数据通信。

21. 根据权利要求 15 所述的用户可更换单元监控单元，其中，所述用户可更换单元监控单元通过应用在多种加密算法中选择的加密算法来执行与主控制器的加密数据通信。

22. 根据权利要求 15 所述的用户可更换单元监控单元，其中，存储单元具有包括存储器恢复区域的软件结构，并且当对于存储单元的数据写入操作被执行时，CPU 将先前记录的值备份在存储器恢复区域中并设置开始标志。

23. 根据权利要求 22 所述的用户可更换单元监控单元，其中，当特定事件发生时，CPU 检查开始标志的改变的值，然后确定改变的值是否退回到先前记录的值。

24. 根据权利要求 15 所述的用户可更换单元监控单元，其中，CPU 从主控制器接收当执行成像作业时用于成像作业的耗材使用的程度的值，并且 CPU 将所述值与存储在存储单元中的关于耗材使用的信息相加，然后刷新关于耗材使用的信息。

25. 一种可移除地安装在成像设备中的可更换单元，所述成像设备具有主控制器，所述可更换单元包括：

存储单元，存储关于可更换单元的信息，并存储操作系统；

CPU，连接到存储单元，其中，当可更换单元安装到成像设备时，CPU 使用存储在可更换单元的存储单元中的操作系统执行初始化，CPU 被配置为访问存储在存储单元中的信息，并执行与成像设备的主控制器的加密数据通信，

其中，CPU 的操作系统与主控制器的另一操作系统独立地进行操作，

其中，CPU 执行所述加密数据通信，使得当包括数据和第一消息认证码信息的通信消息从成像设备的主控制器被发送时，所述 CPU 通过将密钥和加密算法应用于发送的通信消息的数据部分来产生第二消息认证码，并且当产生的第二消息认证码与发送的通信消息的第一消息认证码信息进行比较并与所述第一消息认证码信息一致时，产生的第二消息认证码被认为是有效的通信消息并被处理。

26. 根据权利要求 25 所述的可更换单元，其中，存储单元存储将被 CPU 执行的操作系统，并且用于执行初始化的程序包括在操作系统中，CPU 的操作系统与由主控制器执行的操作系统不同。

27. 根据权利要求 25 所述的可更换单元，其中，在与成像设备的主控制器的认证完成之后，CPU 执行所述加密数据通信。

28. 根据权利要求 25 所述的可更换单元，其中，当成像设备开启时，并且当所述可更换单元被安装在成像设备上时，CPU 执行初始化，并且在初始化被完成之前对来自成像设备的主控制器的命令不进行响应。

29. 根据权利要求 25 所述的可更换单元，其中，存储单元包括下列中的至少一个：操作系统存储器；非易失性存储器，以非易失性的形式存储数据；易失性存储器，用作操作所需的临时存储空间。

30. 根据权利要求 25 所述的可更换单元，还包括：

接口单元，将所述主控制器连接到 CPU；

篡改检测器，对物理窃用尝试进行响应；以及

密码机单元，允许 CPU 执行与所述主控制器的加密数据通信。

31. 根据权利要求 25 所述的可更换单元，其中，所述可更换单元通过应用在多种加密算法中选择的加密算法来执行与主控制器的加密数据通信。

32. 根据权利要求 25 所述的可更换单元，其中，存储单元具有包括存储器恢复区域的软件结构，并且当对于存储单元的数据写入操作被执行时，CPU 将先前记录的值备份在存储器恢复区域中并设置开始标志，并且当特定事件发生时，CPU 还检查开始标志的改变的值，然后确定改变的值是否退回到先前记录的值。

33. 根据权利要求 25 所述的可更换单元，其中，CPU 从成像设备的主控制器接收当使用所述可更换单元执行成像作业时使用的耗材的使用程度的值，并且 CPU 将所述值与存储在存储单元中的关于耗材使用的信息相加，然后刷新关于耗材使用的信息。

使用操作系统的单元和使用该单元的成像设备

[0001] 本申请是申请日为 2009 年 3 月 2 日、申请号为 200910007789.2、发明名称为“使用操作系统的单元和使用该单元的成像设备”的发明专利申请的分案申请。

技术领域

[0002] 本发明总体构思涉及一种包括内置的中央处理单元 (CPU) 的单元和使用该单元的成像设备。更具体地讲，本发明总体构思涉及一种通过包含具有操作系统 (OS) 的 CPU 而变得更安全的单元以及使用该单元的成像设备。

背景技术

[0003] 随着计算机被广泛地使用，外围设备也变得普遍。外围设备的示例是成像设备，例如，打印机、扫描仪、复印机和多功能装置。

[0004] 成像设备使用墨或调色剂将图像打印到纸上。每当执行成像操作时就使用墨和调色剂，直到墨或调色剂最终耗尽。如果缺少墨或调色剂，则用户必须更换用于存储墨或调色剂的单元。这些在使用成像设备时可更换的组件被称为耗材或可更换单元。

[0005] 在可更换单元中，除了墨或调色剂耗尽时不得不更换的单元之外的一些单元在使用预定的时间段之后必须被更换。由于在预定的时间段之后这些单元的性质改变并且打印质量因此下降，所以即使墨或调色剂没有耗尽，也必须更换这些单元。

[0006] 例如，激光成像设备包括充电单元、转印单元、定影单元等，在每个单元中使用的不同类型的辊和带由于使用超过限定的寿命而可能用坏或损坏。结果，打印质量会显著地下降。因此，用户不得不在合适的时间更换这样的可更换单元。

[0007] 可利用使用状态指标 (use state index) 来确定更换可更换单元的时间。使用状态指标表示用于指示成像设备的使用程度的指标，例如，成像设备打印的纸的页数以及形成图像的点的数量。成像设备可通过测量成像设备打印的纸的页数或点的数量来确定更换可更换单元的时间。

[0008] 近来，为了使用户精确地确定更换每个可更换单元的时间，每个可更换单元包括内置的用户可更换单元监控存储器 (CRUM 存储器)。每个可更换单元的使用状态指标被存储在 CRUM 存储器中。因此，即使每个可更换单元被分离并使用在不同的成像设备中，每个可更换单元的使用状态也可被精确地确定。

[0009] 然而，具有 CRUM 存储器的传统可更换单元具有用户能够容易地访问 CRUM 存储器的问题。存储在 CRUM 存储器中的信息从关于制造商的基本信息到关于最近使用状态的信息有很大的不同。如果修改该信息，则难以享受售后服务和计算更换可更换单元的合适时间。具体地说，如果关于制造商的信息被修改，则不能确定关于制造商的信息是否可信，因此，难以管理可更换单元。

发明内容

[0010] 本发明总体构思提供一种通过具有内置的 CPU 而变得更加安全的单元，所述 CPU

具有自己的操作系统 (OS)，还提供一种具有该单元的成像设备。

[0011] 将在接下来的描述中部分阐述本发明总体构思的另外的特点和效用，还有一部分通过描述将是清楚的，或者可以经过本发明总体构思的实施而得知。

[0012] 可通过提供一种可安装在用于成像设备的可更换单元上的芯片来实现本发明总体构思的实施例，所述芯片包括：中央处理单元 (CPU)，具有自己的操作系统 (OS)，所述 OS 与成像设备的 OS 分开，从而所述 CPU 使用自己的 OS 来执行与成像设备的主体的加密数据通信。

[0013] 所述 CPU 可独立于成像设备的主体使用自己的 OS 执行初始化。

[0014] 所述 CPU 可执行所述加密数据通信，使得当包括数据和第一消息认证码 (MAC) 信息的通信消息从成像设备的主体被发送时，所述 CPU 通过将密钥和加密算法应用于发送的通信消息的数据部分来产生第二 MAC 信息，并且当产生的第二 MAC 与发送的通信消息的第一 MAC 信息进行比较并与所述第一 MAC 信息一致时，产生的第二 MAC 被认为是有效的通信消息并被处理。

[0015] 当成像设备开启时，或者当具有所述芯片的可更换单元被安装在成像设备上时，所述 CPU 可根据自己的 OS 执行初始化，所述 CPU 可在初始化被完成之前对来自成像设备的主体的命令不进行响应，并且当初始化被完成时，所述 CPU 可执行加密数据通信。

[0016] 所述芯片还可包括：存储单元，存储关于所述芯片、用户可更换单元监控 (CRUM) 单元、具有所述 CRUM 单元的可更换单元以及所述 CPU 的 OS 中的至少一个的信息。

[0017] 所述 CPU 的 OS 可驱动所述芯片、CRUM 单元以及可更换单元中的至少一个，所述 CPU 的 OS 可以是一种软件，所述软件执行下列中的至少一个：独立地对所述芯片、CRUM 单元以及可更换单元的一个状态进行初始化的初始化操作；执行公共加密算法的处理操作；以及与成像设备的主体的相互认证操作。

[0018] 所述芯片还可包括：篡改检测器，对物理窃用尝试进行响应；以及密码机单元，通过应用多种加密算法中的预设加密算法，允许所述 CPU 执行与成像设备的主体的加密数据通信。

[0019] 应用于加密数据通信的加密算法是可改变的。

[0020] 所述 CPU 可从成像设备的主体接收当执行成像作业时用于成像作业的耗材的程度的值，并且所述 CPU 将所述值与存储在存储单元中的关于耗材使用的信息相加，然后刷新存储在存储单元中的关于耗材使用的信息。

[0021] 可通过提供一种能够用于成像作业的 CRUM 单元来实现本发明总体构思的实施例，所述 CRUM 单元包括：存储单元，存储关于安装有 CRUM 单元的单元的信息；以及 CPU，使用自己的操作系统 (OS) 管理存储单元，并且执行与成像设备的主体的加密数据通信，所述 CPU 的 OS 与成像设备的 OS 分开。

[0022] 所述 CPU 可独立于成像设备的主体使用自己的 OS 执行初始化。

[0023] 所述 CPU 的 OS 可驱动 CRUM 单元或安装有所述 CRUM 单元的可更换单元，所述 CPU 的 OS 可以是一种软件，所述软件执行下列中的至少一个：独立地对所述 CRUM 单元或所述可更换单元的状态进行初始化的初始化操作；执行公共加密算法的处理操作；以及与成像设备的主体的相互认证操作。

[0024] 所述 CPU 可执行所述加密数据通信，使得当包括数据和第一消息认证码 (MAC) 信

息的通信消息从成像设备的主体被发送时，所述 CPU 通过将密钥和加密算法应用于发送的通信消息的数据部分来产生第二 MAC，并且当产生的第二 MAC 与发送的通信消息的第一 MAC 信息进行比较并与所述第一 MAC 信息一致时，产生的第二 MAC 被认为是有效的通信消息并被处理。

[0025] 当成像设备开启时，或者当具有所述 CRUM 单元的可更换单元被安装在成像设备上时，所述 CPU 可根据自己的 OS 执行初始化，并且在初始化被完成之前对来自成像设备的主体的命令不进行响应。

[0026] CRUM 单元还可包括：接口单元，将成像设备连接到所述 CPU；篡改检测器，对物理窃用尝试进行响应；以及密码机单元，通过应用多种加密算法中的预设加密算法，允许所述 CPU 执行与成像设备的主体的加密数据通信。

[0027] 应用于加密数据通信的加密算法是可改变的。

[0028] 所述 CPU 可从成像设备的主体接收当执行成像作业时用于成像作业的耗材的程度的值，并且所述 CPU 将所述值与存储在存储单元中的关于耗材使用的信息相加，然后刷新存储在存储单元中的关于耗材使用的信息。

[0029] 可通过提供一种可安装在成像设备中以用于成像作业的可更换单元来实现本发明总体构思的实施例，所述可更换单元包括：存储单元，存储关于可更换单元的信息；以及 CPU，使用自己的操作系统 (OS) 管理存储单元，并且执行与成像设备的主体的加密数据通信，所述 CPU 的 OS 与成像设备的 OS 分开。

[0030] 所述 CPU 可独立于成像设备的主体使用自己的 OS 执行初始化。

[0031] 所述 CPU 的 OS 可驱动可更换单元，所述 CPU 的 OS 可以是一种软件，所述软件执行下列中的至少一个：独立地对可更换单元的状态进行初始化的初始化操作；执行公共加密算法的处理操作；以及成像设备的主体和可更换单元之间的相互认证操作。

[0032] 所述 CPU 可执行所述加密数据通信，使得当包括数据和第一消息认证码 (MAC) 信息的通信消息从成像设备的主体被发送时，所述 CPU 通过将密钥和加密算法应用于发送的通信消息的数据部分来产生第二 MAC，并且当产生的第二 MAC 与发送的通信消息的第一 MAC 信息进行比较并与所述第一 MAC 信息一致时，产生的第二 MAC 被认为是有效的通信消息并被处理。

[0033] 当成像设备开启时，或者当可更换单元被安装在成像设备上时，所述 CPU 可执行初始化，并且在初始化被完成之前可对来自成像设备的主体的命令不进行响应。

[0034] 所述可更换单元还可包括：接口单元，将成像设备连接到所述 CPU；篡改检测器，对物理窃用尝试进行响应；以及密码机单元，通过应用多种加密算法中的设置的加密算法，允许所述 CPU 执行与成像设备的主体的加密数据通信。

[0035] 应用于加密数据通信的加密算法是可改变的。

[0036] 所述 CPU 可从成像设备的主体接收当执行成像作业时用于成像作业的耗材的程度的值，并且所述 CPU 将所述值与存储在存储单元中的关于耗材使用的信息相加，然后刷新存储在存储单元中的关于耗材使用的信息。

[0037] 可通过提供一种成像设备来实现本发明总体构思的实施例，所述成像设备包括：主控制器；以及至少一个单元，包括存储单元和 CPU，所述存储单元存储信息，所述 CPU 使用自己的操作系统 (OS) 管理存储单元并执行与主控制器的加密数据通信，所述 CPU 的 OS 与

主控制器的 OS 分开。

[0038] 所述 CPU 可独立于主控制器使用自己的操作系统执行初始化。

[0039] 所述 CPU 可执行所述加密数据通信，使得当包括数据和第一消息认证码 (MAC) 信息的通信消息从成像设备的主体被发送时，所述 CPU 通过将密钥和加密算法应用于发送的通信消息的数据部分来产生第二 MAC，并且当产生的第二 MAC 与发送的通信消息的第一 MAC 信息进行比较并与所述第一 MAC 信息一致时，产生的第二 MAC 被认为是有效的通信消息并被处理。

[0040] 在所述加密数据通信之前，主控制器可通过接收为所述至少一个单元中的每个单元设置的独有数字签名信息来尝试执行认证。

[0041] 主控制器可通过应用 RSA 非对称密钥算法以及 ARIA、三重数据加密标准 (TDES)、SEED 和高级加密标准 (AES) 对称密钥算法之一来执行加密数据通信，并且所述单元的 CPU 通过应用 ARIA、TDES、SEED 和 AES 对称密钥算法之一来执行加密数据通信。

[0042] 所述单元还可包括：密码机单元，通过应用多种加密算法中的设置的加密算法，允许所述 CPU 执行与主控制器的认证或加密数据通信；以及篡改检测器，对物理窃用尝试进行响应。

[0043] 主控制器可通过一个串行 I/O 通道连接到所述至少一个单元，并且使用分配给每个单元各自的地址来访问所述至少一个单元。

[0044] 当执行作业时，主控制器可测量用于所述作业的耗材的程度的值，将测量的值发送到所述至少一个单元的每个 CPU，将所述值与预先存储在存储单元中的关于耗材使用的信息相加，然后刷新存储在存储单元中的关于耗材使用的信息。

[0045] 所述 CPU 的 OS 可驱动所述单元，并且所述 CPU 的 OS 可以是一种软件，所述软件执行下列中的至少一个：初始化操作；执行公共加密算法的处理操作；以及主控制器和所述单元之间的相互认证操作。

[0046] 所述单元可以是下列中的一个：与成像设备的成像作业直接相关的可更换单元；可安装在可更换单元上的 CRUM 单元；以及可安装在 CRUM 单元上的芯片。

[0047] 可通过提供一种计算机可读介质来实现本发明总体构思的实施例，所述计算机可读介质包含计算机可读代码作为执行一种方法的程序，所述方法包括：使用中央处理单元 (CPU) 的操作系统 (OS) 来执行与成像设备的主体的加密数据通信，所述 CPU 的 OS 与成像设备的 OS 分开。

[0048] 可通过提供一种可安装在用于成像设备的可更换单元上的芯片来实现本发明总体构思的实施例，所述芯片包括：中央处理单元 (CPU)，具有自己的操作系统 (OS)，所述 OS 与成像设备的 OS 分开，从而所述 CPU 使用自己的 OS 来执行与成像设备的主体的加密数据通信；以及存储单元，存储关于所述芯片、用户可更换单元监控 (CRUM) 单元、具有所述 CRUM 单元的可更换单元以及所述 CPU 的操作系统中的至少一个的信息，其中，所述 CPU 的 OS 设置在位于所述芯片内的存储单元中，或者设置在位于所述芯片外部的存储器中。

[0049] 根据本发明总体构思的示例性实施例，具有自己的操作系统 (OS) 的 CPU 被安装在所述单元上，从而所述单元可独立地管理存储单元。所述单元可以是芯片、CRUM 单元或可更换单元。所述 OS 被驱动，从而可执行初始化、加密算法驱动以及与成像设备的主体的认证。

[0050] 即使当主密钥没有被存储在具有所述单元的成像设备中，所述成像设备也可执行与所述单元的认证或加密数据通信。因此，可防止主密钥被泄露。可使用基于随机值和电子签名信息产生的MAC来执行认证或加密数据通信。通过应用对称密钥算法和非对称密钥算法来执行认证，从而该加密提供高等级的数据安全性。

[0051] 多种加密算法可被选择性地应用于认证和加密数据通信。即使当前使用的加密算法受到物理窃用而被攻击，也可通过应用其它加密算法的密钥来替换当前使用的密钥（而不需要用新的单元来更换所述单元）来防止攻击。

[0052] 如果使用多个单元，则对每个单元设置电子签名信息。为每个单元分配各自的地址，因此所述单元可通过串行接口被连接到成像设备。可有效地实现多个单元之间的认证和加密数据通信。

[0053] 如果完成了成像作业，则成像设备测量用于成像作业的耗材的程度，并且将测量的值发送到多个单元中的每个。因此，可防止由于错误而记录关于使用的耗材的程度的不正确信息。

[0054] 其结果是，防止了存储在内置于成像设备中的存储单元中的数据被拷贝或复制，并且增强了数据的安全性。也可防止用户使用未经认证的单元。

附图说明

[0055] 通过下面结合附图对实施例进行描述，本发明总体构思的上述和/或其它方面和特点将会变得清楚，并更易于理解，其中：

[0056] 图1是示出根据本发明总体构思的示例性实施例的包括可更换单元的成像设备的构造的示意性框图；

[0057] 图2是示出根据本发明总体构思的示例性实施例的可更换单元的详细框图；

[0058] 图3是示出根据本发明总体构思的示例性实施例的成像设备的示意性框图；

[0059] 图4是示出根据本发明总体构思的示例性实施例的内置到成像设备和可更换单元的软件的配置的示意性框图；

[0060] 图5是示出根据本发明总体构思的示例性实施例的操作可更换单元和成像设备的方法的流程图；

[0061] 图6是示出根据本发明总体构思的示例性实施例的由可更换单元改变加密算法的过程的流程图；以及

[0062] 图7是示出根据本发明总体构思的示例性实施例的执行成像设备和可更换单元之间的认证和加密数据通信的方法的流程图。

具体实施方式

[0063] 现在，将详细参照本发明总体构思的实施例，其示例在附图中被示出，其中，相同的标号始终表示相同的元件。以下，通过参照附图描述实施例，以解释本发明总体构思。

[0064] 图1是示出根据本发明总体构思的示例性实施例的包括可更换单元的成像设备的构造的示意性框图。如图1所示，成像设备100包括主控制器110，单元200可内置在成像设备100中。成像设备100可以是复印机、打印机、多功能外设、传真机或扫描仪。

[0065] 成像设备100可包括CPU(OS)110a以控制成像设备100的操作。单元200是指被

设计为单独地安装和使用的组件。更具体地讲，单元 200 可以是包括可更换部件 215 的可更换单元，可更换部件 215 形成在成像设备中并直接介入成像操作。例如，可更换单元 200 的可更换部件 215 可以是调色剂盒或墨盒、充电单元、转印单元、定影单元、有机感光导体 (OPC)、输送单元或输送辊等。

[0066] 此外，单元 200 可以是成像设备 100 所需的任何其他组件，并且在使用期间可被更换。即，单元 200 可以是通过包含在可更换单元中能够监控并管理组件的状态的用户可更换单元监控 (CRUM) 单元，或者可以是内置在 CRUM 单元中的芯片。单元 200 可以以不同的形式被实现，但是为了便于说明，下面描述被实现为可更换单元的单元 200。

[0067] 主控制器 110 可具有与外部装置（未示出）通信以接收数据的接口，并且可使用接收的数据执行成像操作。主控制器 110 还可连接到例如传真单元或扫描单元，以接收或发送与成像设备相应的数据。

[0068] 成像设备 100 可包括成像单元 150，成像单元 150 使用单元 200 来执行成像操作。当单元 200 被安装到成像设备 100 的主体中时，单元 200 可以是成像单元 150 的一部分。主控制器 110 可控制存储单元 210 和成像单元 150，以输送介质从而在介质上形成图像，并且排放该介质。

[0069] 如图 1 所示，单元 200 包括存储单元 210 和中央处理单元 (CPU)220。

[0070] 存储单元 210 存储关于单元 200 的各种类型的信息，更具体地说，存储独有信息（例如，关于单元 200 的制造商的信息、关于制造时间的信息、序列号或型号）、各种程序、关于电子签名的信息、关于使用状态的状态信息（例如，到目前为止已经打印了多少张纸、剩余的可打印能力或者还剩下多少调色剂）。

[0071] 例如，存储单元 210 可存储如下面的表 1 中的信息。

[0072]

总体信息

[0073]

OS 版本 SPL-C 版本 引擎版本 USB 序列号 设置型号 服务起始日期	CLP300_V1.30.12.35 02-22-2007 5.24 06-28-2006 6.01.00(55) BH45BAIP914466B. DOM 2007-09-29
选项	
RAM 大小 EEPROM 大小 USB 连接(高)	32 兆字节 4096 字节
耗材寿命	
总页数计数 定影器寿命 转印辊寿命 托盘 1 辊寿命 总图像计数 成像单元/显影辊寿命 转印带寿命 调色剂图像计数	774/93 页(彩色/单色) 1636 页 864 页 867 页 3251 页 61 图像/19 页 3251 图像 14/9/14/19 图像(C/M/Y/K)
调色剂信息	
调色剂剩余百分比 调色剂平均覆盖	99%/91%/92%/100% (C/M/Y/K) 5%/53%/31%/3% (C/M/Y/K)
耗材信息	

[0074]

青色调色剂	SAMSUNG(DOM)
品红色调色剂	SAMSUNG(DOM)
黄色调色剂	SAMSUNG(DOM)
黑色调色剂	SAMSUNG(DOM)
成像单元	SAMSUNG(DOM)
颜色菜单	
自定义颜色	手动调整(CMYK : 0,0,0,0)
设置菜单	
节能	20 分钟
自动连续	开
海拔调节	平原

[0075] 如上面的表 1 所示，存储单元 210 可存储关于耗材的寿命的信息和设置菜单以及关于单元 200 的概略信息。存储单元 210 还可存储用于处理存储在存储单元 210 中的数据的操作系统 (OS) 的信息，从而主控制器 110 可控制成像单元 150 和单元 200 执行成像操作。

[0076] CPU 220 使用该 CPU 220 的操作系统 (OS) 管理存储单元 210。用于对单元 200 进行操作的 OS 是指操作通用应用程序的软件。因此，CPU 220 可通过使用 OS 来执行初始化。

[0077] 更具体地说，CPU 220 在特定事件的时间执行初始化，例如，当包括单元 200 的成像设备 100 开启时，或者当单元 200 或包括单元 200 的组件（例如，可更换单元）结合到成像设备 100 或者与成像设备 100 分离时。初始化包括在单元 200 中使用的各种应用程序的初始驱动、在初始化之后与成像设备进行数据通信所需的秘密计算信息、通信通道的设置、存储器值的初始化、更换时间的确认、单元 200 中的寄存器值的设置以及内部和外部时钟信号的设置。

[0078] 寄存器值的设置是指为了使单元 200 在与用户先前设置的状态相同的状态下操作而设置单元 200 中的功能寄存器值。此外，内部和外部时钟信号的设置是指将从成像设备 100 的主控制器 110 提供的外部时钟信号的频率调整为在单元 200 的 CPU 220 中使用的内部时钟的频率。

[0079] 更换时间的确认是指检查使用中的调色剂或墨的剩余量，预测调色剂或墨将会耗尽的时间，并将该时间通知主控制器 110。如果在初始化期间确定调色剂已经耗尽，则在完成初始化之后，单元 200 可被实现为自动通知主控制器 110 操作不能执行。在其它情况下，由于单元 200 包括 CPU 的 OS，因此可根据单元 200 的类型或特性执行各种形式的初始化。

[0080] 由单元 200 自己执行该初始化，从而该初始化独立于由成像设备 100 的主控制器 110 执行的初始化而被执行。

[0081] 如上所述，CPU 220 内置于单元 200 中，单元 200 具有自己的 OS，因此如果成像设备 100 开启，则主控制器 110 可在请求与单元 200 通信之前检查存储在存储单元 210 中的耗材的剩余量和再补充的量。因此，通知主控制器耗材需要更换要花费较短的时间。例如，如果调色剂不足，则用户可开启成像设备 100，并将成像设备 100 直接转换到调色剂节省模式。即使当仅一种特定的调色剂不足时，用户也可执行同样的操作。

[0082] 在初始化完成之前，CPU 220 不响应主控制器 110 的命令。主控制器 110 周期性地将命令发送到 CPU 220，直到主控制器 110 从 CPU 220 接收到响应。

[0083] 如果主控制器 110 接收到响应，即，应答，则在主控制器 110 和 CPU 220 之间开始认证。

[0084] 在此情况下，单元 200 中的 OS 通过单元 200 和成像设备 100 之间的交互作用进行认证。然而，为了使传统的成像设备执行认证，成像设备的主控制器单向访问所述单元，识别用于认证的独有信息，并将独有信息与存储的信息进行比较。

[0085] 然而，当前成像设备 100 中的主控制器 110 独立于单元 200 的初始化执行自己的初始化。由于系统大小的不同，单元 200 的初始化首先完成。如果单元 200 的初始化完成，则单元 200 可使用 OS 来驱动加密算法。更具体地说，单元 200 可响应于主控制器 110 的命令来驱动加密算法，从而可执行主控制器 110 和单元 200 之间的交互认证而非主控制器 110 的单向认证。因此，认证的安全性增加。

[0086] 这样的认证不限于上述示例，可以以不同的方式执行该认证。例如，主控制器 110 可从 CPU 220 接收响应，并将命令发送到请求认证的 CPU 220。在此情况下，随机值 R1 可与命令一起被发送到 CPU 220。CPU 220 接收对认证的请求和随机值 R1，使用随机值 R1 产生会话密钥，使用产生的会话密钥产生第一消息认证码 (MAC)，并将产生的第一 MAC、预先存储的电子签名信息以及随机值 R2 发送到主控制器 110。

[0087] 如果主控制器 110 通过验证第一 MAC、接收的电子签名信息识别认证，则主控制器 110 使用接收的随机值 R2 和预先产生的随机值 R1 产生会话密钥，并使用该会话密钥产生第二 MAC。最后，主控制器 110 通过识别产生的第二 MAC 与接收的第一 MAC 是否相同来验证第二 MAC。结果，主控制器 110 可确定是否成功地执行了认证。如上所述，由于在发送用于认证的信息或命令时使用了随机值，因此可防止第三方的恶意窃用 (hacking)。

[0088] 如果成功地执行了认证，则在主控制器 110 和单元 200 的 CPU 之间执行加密数据通信。如上所述，由于单元 200 具有自己的 OS，因此可以执行加密算法。因此，可通过将加密算法应用到从成像设备 100 接收的数据来确定数据有效性。作为确定的结果，如果数据有效，则单元 200 接收数据并执行用于处理数据的操作。如果数据无效，则单元 200 一接收到数据就丢弃该数据。在此情况下，单元 200 可通知主控制器 110 在数据通信中存在问题。

[0089] 加密算法可使用公共标准加密算法。当加密密钥被公开或者当需要增强安全性时，可以修改该加密算法。

[0090] 在上面的本发明总体构思的示例性实施例中，由于单元 200 具有自己的 OS、自己的初始化，因此可有效地执行单元 200 和成像设备 100 之间的认证和加密数据通信。

[0091] 图 2 是示出图 1 示出的成像设备 100 的可更换单元 200 的详细框图。图 2 的可更换单元 200 除了先前讨论的存储单元 210 和 CPU 220 之外还包括：密码机单元 230、篡改 (tamper) 检测器 240 以及接口单元 250。此外，可更换单元 200 还可包括输出时钟信号的

时钟单元（未示出）或者产生用于认证的随机值的随机值产生器（未示出）。这里讨论的可更换单元 200 取决于应用可包括更少的组件或更多的组件。如果可更换单元 200 被实现为半导体芯片或芯片封装，则芯片或芯片封装自己可包括 CPU 220，或者可包括存储单元 210 和 CPU 220。如果芯片仅包括 CPU 220，则由 CPU 220 运行的 OS 可由外部存储器提供。

[0092] 密码机单元 230 支持加密算法，并使 CPU 220 执行与主控制器 110 的认证或加密数据通信。具体地讲，密码机单元 230 可支持四种加密算法（即，ARIA、三重数据加密标准 (TDES)、SEED 和高级加密标准 (AES) 对称密钥算法）中的一种。

[0093] 为了执行认证或加密数据通信，主控制器 110 也支持所述四种加密算法。因此，主控制器 110 可确定可更换单元 200 应用了哪种加密算法，可使用确定的加密算法执行认证，并且随后可执行与 CPU 220 的加密数据通信。结果，可更换单元 200 可容易地安装在成像设备 100 中，从而即使应用了特定加密算法的密钥被产生时也可执行加密数据通信。

[0094] 篡改检测器 240 防止各种物理的窃用攻击，即，篡改。更具体地说，如果通过监测操作条件（例如，电压、温度、压力、光或频率）来检测攻击，则篡改检测器 240 可删除与攻击有关的数据，或者可物理地防止攻击。在此情况下，篡改检测器 240 可包括额外的电源来供电以维持其操作。攻击可以是开盖 (decap) 攻击，所述开盖攻击例如可以是对 CRUM 单元 200 的潜在损害攻击。

[0095] 如上所述，可更换单元 200 包括密码机单元 230 和篡改检测器 240，可使用硬件和软件之一或者两者来系统地保护数据。

[0096] 参照图 2，存储单元 210 可包括 OS 存储器 211、非易失性存储器 212 和易失性存储器 213 中的至少一个。

[0097] OS 存储器 211 存储用于操作可更换单元 200 的 OS。非易失性存储器 212 以非易失性的形式存储数据，易失性存储器 213 用作操作所需的临时存储空间。当存储单元 210 包括如图 2 所示的 OS 存储器 211、非易失性存储器 212 和易失性存储器 213 时，这些存储器中的一些可内置于 CPU220 中作为内部存储器。与一般的存储器不同，可根据用于安全的设计（例如，地址 / 数据线置乱或比特加密）来实现 OS 存储器 211、非易失性存储器 212 和易失性存储器 213。

[0098] 非易失性存储器 212 可存储各种信息，例如，数字签名信息、关于各种加密算法的信息、关于可更换单元 200 的使用的状态的信息（例如，关于剩余的调色剂水平的信息、需要更换调色剂的时间、或者剩余的待打印的纸的数量）、独有信息（例如，关于可更换单元 200 的制造商的信息、关于制造的日期和时间的信息、序列号或型号）或者维修服务信息。

[0099] 接口单元 250 连接 CPU 220 和主控制器 110。接口单元 250 可被实现为串行接口或无线接口。例如，由于串行接口比并行接口使用更少的信号，因此串行接口具有降低成本的优点，并且串行接口适于产生大量噪声的操作条件（例如，打印机）。

[0100] 图 2 示出的组件经总线彼此连接，但这仅是示例性的。因此，应该理解，根据本发明总体构思的多个方面的组件可以在没有总线的情况下直接连接。

[0101] 图 3 是示出根据本发明总体构思的示例性实施例的成像设备 100 的框图。图 3 的成像设备 100 包括主控制器 110、存储单元 120、成像单元 150 和多个单元 200-1、200-2、...、200-n，主控制器 110 包括具有 OS 的 CPU 110a。图 3 的多个单元 200-1、200-2、...、200-n 可以是 CRUM 单元、半导体芯片、半导体芯片封装或可更换单元。仅为了

举例的目的，下面将多个单元 200-1、200-2、...、200-n 描述为可更换单元。

[0102] 如果单个系统需要各种耗材，则也需要多个单元。例如，如果成像设备 100 是彩色打印机，则为了表现期望的颜色在彩色打印机中安装四个色盒，即，青色 (C) 盒、品红色 (M) 盒、黄色 (Y) 盒和黑色 (K) 盒。此外，彩色打印机可包括其他耗材。因此，如果需要大量的单元，则每个单元需要其各自的输入 / 输出 (I/O) 通道，这种布置是低效率的。因此，如图 3 所示，单个串行 I/O 通道可用于将多个单元 200-1、200-2、...、200-n 中的每个连接到主控制器 110。主控制器 110 可使用分配给到多个单元 200-1、200-2、...、200-n 中的每个的不同地址来访问多个单元 200-1、200-2、...、200-n 中的每个。

[0103] 当主控制器 110 开启时，或者当多个单元 200-1、200-2、...、200-n 安装在成像设备 100 中时，如果多个单元 200-1、200-2、...、200-n 中的每个被完全初始化，则使用多个单元 200-1、200-2、...、200-n 中的每个的独有数字签名信息来执行认证。

[0104] 如果认证成功，则主控制器 110 与多个单元 200-1、200-2、...、200-n 中的多个 CPU（未示出）执行加密数据通信，并且将关于使用历史的信息存储在多个单元 200-1、200-2、...、200-n 中的多个存储单元（未示出）中。主控制器 110 和多个 CPU 可用作主装置和从装置。

[0105] 这里，通过将用户期望传输的数据与 MAC 一起传输来执行加密数据通信，所述 MAC 通过使用预设的加密算法和密钥对数据加密被产生。由于数据在每次被传输时发生变化，所以 MAC 也会改变。因此，即使当第三方介入数据通信操作并寻找 MAC 时，第三方使用 MAC 不能窃用随后的数据通信操作。

[0106] 如果完成了加密数据通信，则切断主控制器 110 和 CPU 之间连接的通道。

[0107] 存储单元 120 存储各种信息，所述信息包括对多个单元 200-1、200-2、...、200-n 中的每个进行认证所需的多个加密算法和密钥值。

[0108] 主控制器 110 使用存储在存储单元 120 中的信息来执行认证和加密数据通信。具体地讲，主控制器 110 通过应用例如 RSA 非对称密钥算法以及 ARIA、TDES、SEED、AES 对称密钥算法之一，来执行认证和加密数据通信。因此，非对称认证处理和对称认证处理都被执行，从而相对于传统技术，可提高加密级别。

[0109] 尽管图 3 显示了存储单元 120 作为单个单元，但是存储单元 120 可包括存储各种加密算法数据的存储单元、主控制器 110 的其它操作所需的存储单元、存储关于多个单元 200-1、200-2、...、200-n 的信息的存储单元、或存储关于多个单元 200-1、200-2、...、200-n 的使用的信息（例如，将被打印的页数或剩余调色剂水平）的存储单元。

[0110] 安装在图 3 的成像设备 100 中的多个单元 200-1、200-2、...、200-n 可具有图 1 或图 2 所示的结构。因此，在将访问命令发送到多个单元 200-1、200-2、...、200-n 的多个 CPU 并且接收到应答信号后，主控制器 110 可访问多个单元 200-1、200-2、...、200-n。因此，根据本发明总体构思的多个单元与能够访问 CRUM 数据的传统方案不同，所述传统方案使用简单的数据写入和读取操作。

[0111] 如果成像设备 100 开始成像作业，则主控制器 110 可测量用于该作业的耗材的程度，并且可将测量的所使用的耗材的程度发送到多个单元 200-1、200-2、...、200-n 中的每个。更具体地讲，成像设备 100 可将测量的所使用的耗材的程度与先前存储的关于耗材使用的信息相加，并且可刷新关于耗材使用的信息。当在现有技术中进行发送结果值的操作

时，如果由于错误而发送不正确的数据，则关于使用的耗材的程度的不正确的信息可被记录在多个单元 200-1、200-2、...、200-n 中的每个上。例如，如果在使用当前安装的显影剂盒打印 1000 页之后完成了新的 10 页的打印作业，则总值是 1010 页。但是，如果发生一些错误并且如果发送 0 页的值，则 0 页的打印作业可被记录在多个单元 200-1、200-2、...、200-n。其结果是，用户可能不能准确地知道需要更换耗材的时间。

[0112] 为了解决该问题，在本发明总体构思的实施例中，主控制器 110 可测量用于作业的耗材的程度，并且可仅将测量的所使用的耗材的程度发送到多个单元 200-1、200-2、...、200-n 中的每个。在这种情况下，主控制器 110 可发送 10 页的值，从而多个单元 200-1、200-2、...、200-n 可通过使用它们自己的 CPU 将新接收的值“10”与值“1000”（即，先前存储的值）相加。因此，存储在存储器中的关于耗材使用的信息可被准确更新为“1010”。

[0113] 另外，主控制器 110 可通过将测量的量与存储在存储单元 120 中的关于耗材使用的信息相加，与多个单元 200-1、200-2、...、200-n 分开而自己管理关于所使用的耗材的程度的信息。

[0114] 然而，在本发明总体构思的实施例中，在每次执行作业时，主控制器 110 可在将关于所使用的耗材的程度的信息发送到多个单元 200-1、200-2、...、200-n 的同时，自动更新存储在存储单元 120 中的关于耗材使用的信息。

[0115] 例如，当使用安装在成像设备 100 中的多个单元 200-1、200-2、...、200-n 打印 100 页时，如果在执行单个作业的同时还打印 10 页，则主控制器 110 可将值“10”发送到多个单元 200-1、200-2、...、200-n，并且可将值“10”与先前存储在存储单元 120 中的值“100”相加，从而存储指示打印了“110”页的历史信息。因此，如果发送特定事件（例如，如果成像设备 100 被重置，或者调色剂或墨被完全耗尽），或者预设的时间段到来，则主控制器 110 和多个单元 200-1、200-2、...、200-n 可通过使用它们各自的 CPU 来比较它们各自的历史信息，从而可检查数据是否被正常记录在多个单元 200-1、200-2、...、200-n 中的每个中。

[0116] 换句话说，可通过将存储在存储单元 120 中的关于耗材使用的信息与存储在多个单元 200-1、200-2、...、200-n 中的关于耗材使用的信息进行比较，来确定存储的关于耗材使用的信息的准确性或不准确性。更详细地讲，如果发生事件或预设的时间段到来，则主控制器 110 可将用于请求关于耗材使用的信息的命令发送到多个单元 200-1、200-2、...、200-n。响应于该请求命令，多个单元 200-1、200-2、...、200-n 的 CPU 可将存储在其中的关于耗材使用的信息发送到主控制器 110。

[0117] 如果存储在存储单元 120 中的关于耗材使用的信息与存储在多个单元 200-1、200-2、...、200-n 中的关于耗材使用的信息不同，则主控制器 110 可输出错误信息，或者可协调被确定为正确的信息并可更新关于耗材使用的信息。

[0118] 此外，如果存储在存储单元 120 中的关于耗材使用的信息与存储在多个单元 200-1、200-2、...、200-n 之一中的关于耗材使用的信息不同，则因为在数据被发送到存储单元 120 时可能出现错误，所以主控制器 110 可发送用于改变存储在存储单元 120 中的关于耗材使用的信息的命令。

[0119] 成像设备 100 可包括成像单元 150，成像单元 150 用于使用单元 200-1、200-2、...、200-n 来执行成像操作。当单元 200-1、200-2、...、200-n 被安装在成像设备 100 的主体中时，单元 200-1、200-2、...、200-n 可以是成像单元 150 的一部分。主控制器

110 可控制存储单元 120 和 210 以及成像单元 150，以输送介质从而在介质上形成图像，并排放该介质。

[0120] 图 4 是示出根据本发明总体构思的示例性实施例的单元 200 和使用该单元 200 的主机（即，成像设备的软件的配置）的分层图。

[0121] 参照图 1 和图 4，成像设备 100 的软件 (a) 除了包括通用应用程序、用于管理每个单元的数据的应用、执行自身管理的装置驱动程序以及执行命令的程序之外，还可包括执行与单元 200 的认证和加密的安全性机制区域以及执行软件加密的软件加密操作区域。

[0122] 单元 200 的软件 (b) 可包括：半导体 IC 芯片区域，具有保护数据的各种块；App 区域，与主机软件进行接口连接；以及 OS 区域，操作上述区域。

[0123] 图 4 的装置软件区域包括 OS 的基本部件，诸如保护数据所需的操作块和文件管理。简要地，所述块包括为安全性系统而控制硬件的程序、使用硬件控制程序的应用程序以及用于防止利用其它程序进行篡改的程序。由于用于实现 CRUM 的功能的应用程序被安装在如上面所解释的程序上，所以不能通过通信通道来检查存储在数据上的信息。可按照其它结构来实现所述程序以包括所述块。然而，为了有效地保护数据，需要细心地对程序进行编程，从而保护 OS。

[0124] 图 4 的软件结构中的 OS 区域包括存储器恢复区域 410。设置存储器恢复区域 410，以保证是否根据更新单元 200 的条件信息的处理成功完成了更新。

[0125] 再次参照图 1 和图 2，当数据被写入到存储单元 210 时，单元 200 的 CPU220 将先前记录的值备份在存储器恢复区域 410 中，并设置开始标志。

[0126] 例如，当使用单元 200 的成像作业被完成时，主控制器 110 访问单元 200 的 CPU 220，以重新记录条件信息（诸如当执行打印作业时消耗的页数或供应物的量）。如果电源被切断，或者在完成记录之前由于外部噪声导致打印作业被异常终止，则传统的 CRUM 不能确定新的条件信息是否被正常记录。如果这样的异常条件被重复，则难以信任该信息，并且即使使用 CRUM 也难以管理所述单元。

[0127] 为了防止该问题，根据本发明总体构思的示例性实施例的 OS 在该 OS 中设置存储器恢复区域 410。在这种情况下，CPU 在记录数据之前将先前记录的数据备份在存储器恢复区域 410 中，并且将开始标志设置为 0。如果处理数据写入操作，则开始标志根据该数据写入操作被不断更新。

[0128] 在这种情况下，如果数据写入操作被异常终止，则 CPU 在电源被接通之后或在系统稳定之后检查开始标志。CPU 由此根据开始标志值的变化条件确定数据是否被正常写入。如果开始标志值与初始设置值之间的差不显著，则 CPU 确定数据写入失败，并且将数据退回到先前记录的值。另一方面，如果开始标志值与最终值近似一致，则 CPU 确定当前记录的数据是正确的。因此，即使当电源被断开，或者当系统异常操作，写入到单元 200 中的数据也是可以被信任的。

[0129] 图 5 是示出根据本发明总体构思的示例性实施例的操作可更换单元和成像设备的方法的流程图。参照图 1 和图 5，在操作 S510，单元 200 的 CPU 确定是否发生了特定事件。特定事件可包括：成像设备 100 被开启的情况；或者单元 200 或包括该单元 200 的组件被安装在成像设备 100 中的情况。

[0130] 如果确定发生了特定事件，则在操作 S520，单元 200 执行自身的初始化。所述初始

化包括：计算在初始化之后与成像设备的数据通信所需的秘密信息、通信通道的设置、存储器值的初始化、检查调色剂或墨的剩余量、更换时间的确认或各种其它处理。

[0131] 在操作 S530，成像设备 100 的主控制器 110 发送用于尝试在主控制器 110 和 CPU 220 之间进行认证的命令。如果在操作 S540 主控制器 110 没有从 CPU220 接收到响应，则主控制器 110 重复发送该命令，直到接收到响应。

[0132] 当接收到响应时，在操作 S550，如上面所解释的，主控制器 110 对与 CPU 220 之间的通信进行认证。

[0133] 如果在操作 S560 成功执行了认证，则在操作 S570，使用加密算法来执行与主控制器 110 的加密数据通信。

[0134] 图 6 是被提供以解释根据本发明总体构思的示例性实施例的由单元 200 改变加密算法的过程的示意图。参照图 6，单元 200 可支持例如 ARIA、三重数据加密标准 (TDES)、SEED 和高级加密标准 (AES) 对称密钥算法。可在密钥管理系统 (KMS)600 中的密钥写入系统产生了密钥产生数据时确定使用何种算法。

[0135] 如果执行了加密算法的破解 (cracking)，则可通过从应用了上述四种加密算法的 KMS 获取新的密钥 (而不是制造新的单元 200)，来改变加密算法。

[0136] 如上所述，成像设备 100 除了支持 RSA 非对称密钥算法之外，还可支持 ARIA、TDES、SEED 和 AES 对称密钥算法。因此，即使应用于单元 200 的加密算法被改变，成像设备 100 也进行响应而改变加密算法，并且执行认证和加密数据通信。

[0137] 因此，相比于需要更换芯片的传统技术，可通过改变密钥值来方便地改变加密算法。

[0138] 图 7 是被提供以解释根据本发明总体构思的示例性实施例的执行认证和加密数据通信的方法的流程图。参照图 1 和图 7，在操作 S710，成像设备 100 将用于请求认证的命令与随机值 R1 一起发送。

[0139] 如果接收到用于认证的请求，则在操作 S715，单元 200 使用接收的随机值 R1 和单元 200 产生的随机值 R2 来产生会话密钥，并且在操作 S720，单元 200 使用产生的会话密钥来产生消息认证码 (MAC)。

[0140] 单元 200 产生的第一 MAC 是预先存储的电子签名信息，并且在操作 S725，第一 MAC 和随机值 R2 被一起发送到成像设备 100。

[0141] 在操作 S730，成像设备 100 通过将接收的电子签名信息与预先存储的电子签名信息进行比较，来验证接收的由单元 200 产生的第一 MAC 的电子签名。为了验证接收的电子签名，如果多个单元被安装在成像设备 100 中，则成像设备 100 可存储每个单元的电子签名信息。

[0142] 如果接收的电子签名被验证，则在操作 S735，成像设备 100 可将预先产生的随机值 R1 与接收的随机值 R2 进行组合来产生会话密钥，并且在操作 S740，成像设备 100 使用产生的会话密钥产生第二 MAC。

[0143] 然后在操作 S745，成像设备 100 将产生的成像设备 100 的第二 MAC 与可更换单元 200 的接收的第一 MAC 进行比较，以确定这两个独立的 MAC 是否一致。根据接收的可更换单元 200 的第一 MAC 的验证来完成认证。如果成功执行了认证，则可执行加密数据通信。

[0144] 为了执行加密数据通信，假设成像设备 100 使用与单元 200 的密钥和加密算法相

同的密钥和加密算法。密钥可以是如上所述的会话密钥。

[0145] 如果接收的可更换单元 200 的第一 MAC 被完全验证，则在操作 S750，成像设备 100 在产生通信消息时通过将密钥和加密算法应用于数据来产生第三 MAC。

[0146] 在操作 S755，成像设备 100 将包括第三 MAC 的通信消息发送到单元 200。

[0147] 在操作 S760，单元 200 从接收的通信消息提取数据部分，并且通过将上述密钥和加密算法应用于所述数据来产生第四 MAC。

[0148] 在操作 S765，单元 200 从接收的通信消息提取第三 MAC 部分，并且通过将提取的第三 MAC 与单元 200 计算的第四 MAC 进行比较来执行认证。

[0149] 如果提取的第三 MAC 与单元 200 计算的第四 MAC 一致，则在操作 S770，通信消息被认为是有效的通信消息，并因此执行与所述消息相应的操作。另一方面，如果第三 MAC 和第四 MAC 彼此不一致，则通信消息被认为是无效的通信消息，并且被丢弃。

[0150] 执行认证和加密数据通信的方法也可应用于参照附图所解释的示例性实施例。单元 200 可按照不同的形式（诸如半导体芯片或芯片封装、普通单元或可更换单元）被实现。

[0151] 本发明总体构思也可被实施为计算机可读介质上的计算机可读代码。计算机可读介质可包括计算机可读记录介质和计算机可读传输介质。计算机可读记录介质是可存储数据作为程序而其后可被计算机系统读取的任何数据存储装置。计算机可读记录介质的示例包括只读存储器 (ROM)、随机存取存储器 (RAM)、CD-ROM、磁带、软盘、光学数据存储装置。计算机可读记录介质也可以被分布在网络连接的计算机系统上，从而计算机可读代码以分布式方式被存储和执行。计算机可读传输介质可传输载波或信号（例如，通过互联网的有线或无线数据传输）。另外，本发明总体构思所属领域的程序设计员可容易地解释实现本发明总体构思的功能程序、代码和代码段。

[0152] 尽管已经显示和描述了本发明总体构思的一些实施例，但是本领域技术人员应该理解，在不脱离权利要求及其等同物限定其范围的本发明总体构思的原理和精神的情况下，可以对这些实施例进行改变。

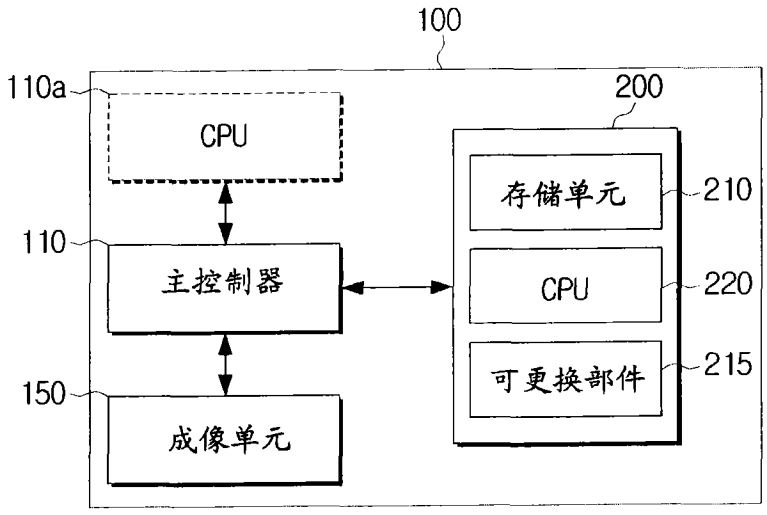

100
110a
CPU
200
存储单元
210
110
主控制器
CPU
220
可更换部件
215
150
成像单元

图 1

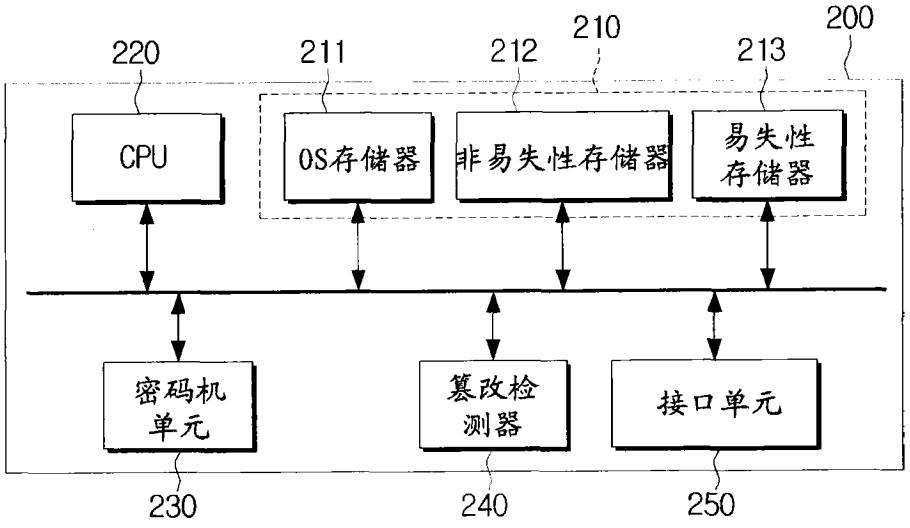

220
211
212
210
213
200
CPU
OS存储器
非易失性存储器
易失性
存储器
密码机
单元
篡改检
测器
接口单元
230
240
250

图 2

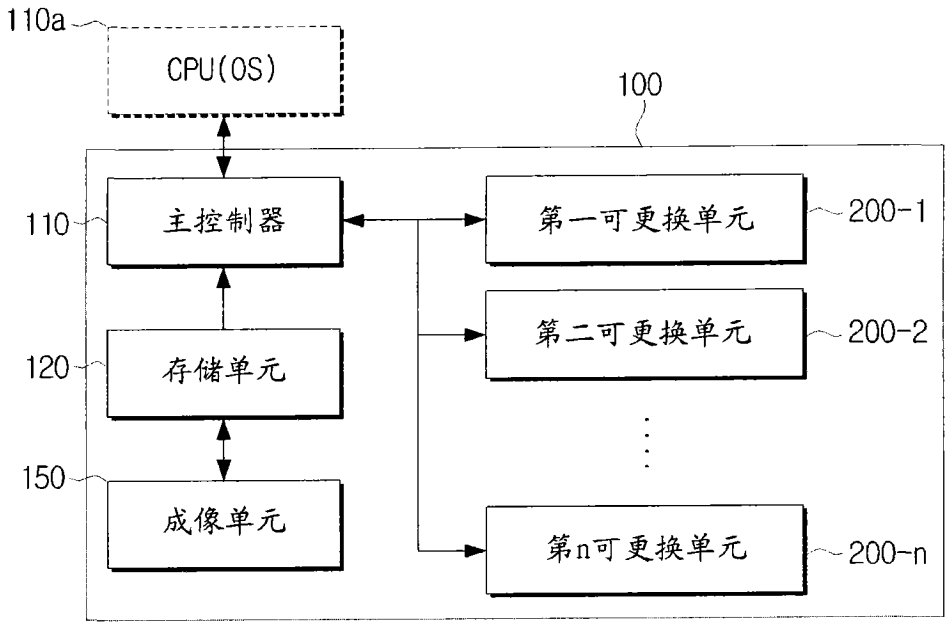

110a
CPU(OS)
100
110
主控制器
第一可更换单元
200-1
第二可更换单元
200-2
120
存储单元
150
成像单元
第n可更换单元
200-n

图 3

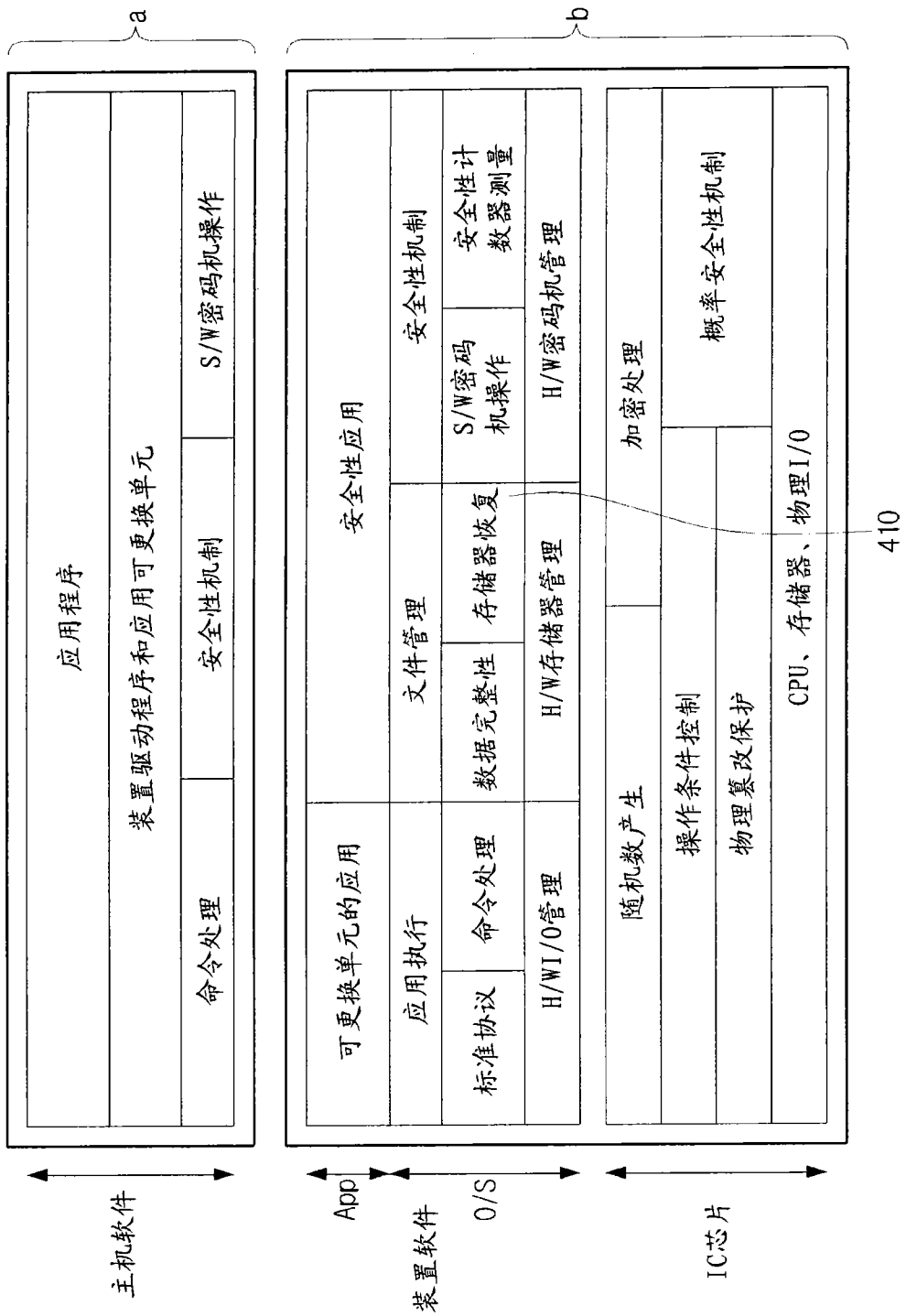

a
b
应用程序
装置驱动程序和应用可更换单元
命令处理
安全性机制
S/W密码机操作
可更换单元的应用
安全性应用
应用执行
文件管理
安全性机制
标准协议
命令处理
数据完整性
存储器恢复
S/W密码机操作
安全性计数器测量
H/WI/O管理
H/W存储器管理
H/W密码机管理
随机数产生
加密处理
操作条件控制
概率安全性机制
物理篡改保护
CPU、存储器、物理I/O
410
主机软件
App
装置软件
O/S
IC芯片

图 4

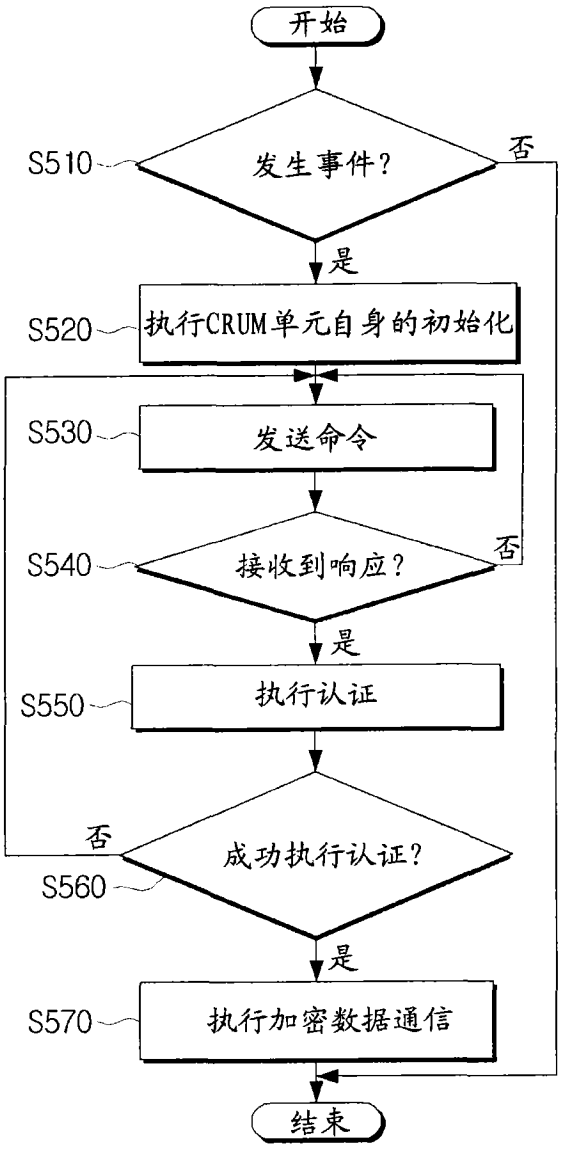

开始
S510
发生事件?
否
是
S520
执行CRUM单元自身的初始化
S530
发送命令
S540
接收到响应?
否
是
S550
执行认证
否
成功执行认证?
S560
是
S570
执行加密数据通信
结束

图 5

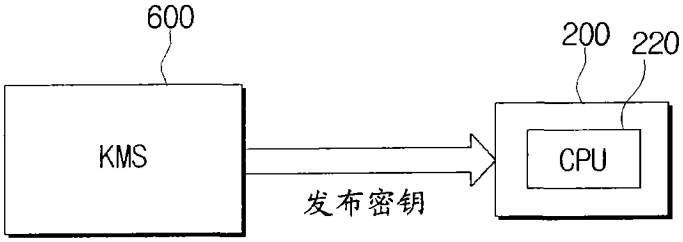

600
200
220
KMS
CPU
发布密钥

图 6

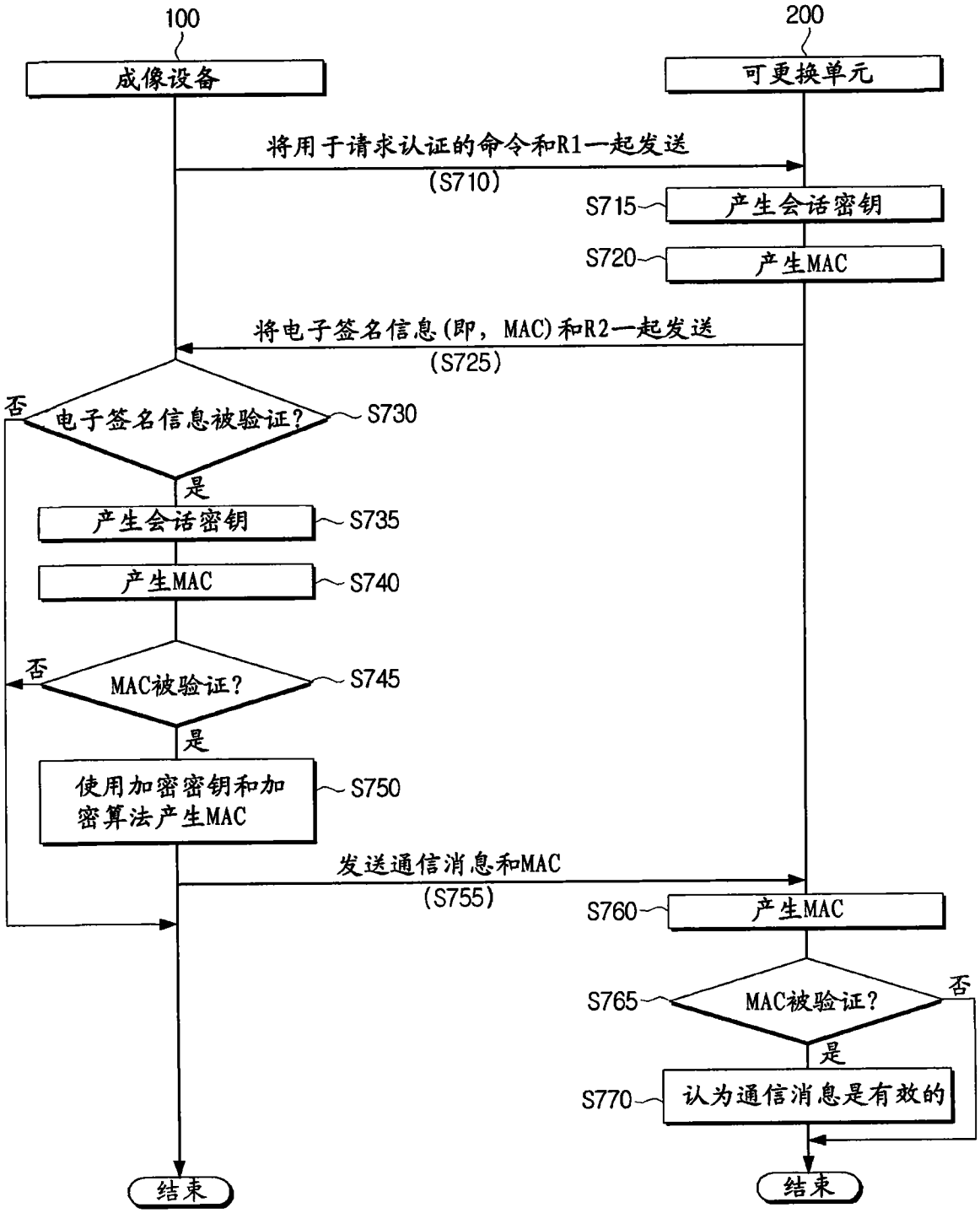

100
成像设备
200
可更换单元
将用于请求认证的命令和R1一起发送
(S710)
S715
产生会话密钥
S720
产生MAC
将电子签名信息(即，MAC)和R2一起发送
(S725)
否
电子签名信息被验证?
S730
是
产生会话密钥
S735
产生MAC
S740
否
MAC被验证?
S745
是
使用加密密钥和加密算法产生MAC
S750
发送通信消息和MAC
(S755)
S760
产生MAC
S765
MAC被验证?
否
是
S770
认为通信消息是有效的
结束
结束

图 7