

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.

H04N 1/44 (2006.01)

G06F 21/00 (2006.01)



[12] 发明专利申请公布说明书

[21] 申请号 200910142574.1

[43] 公开日 2010 年 2 月 24 日

[11] 公开号 CN 101656818A

[22] 申请日 2009.7.1

[21] 申请号 200910142574.1

[30] 优先权

[32] 2008.8.18 [33] JP [31] 2008-210171

[71] 申请人 富士通株式会社

地址 日本神奈川县川崎市

[72] 发明人 增井诚生 石井英昭 阿南泰三

高桥润 仓木健介 中濑昌平

[74] 专利代理机构 北京三友知识产权代理有限公司

代理人 李 辉

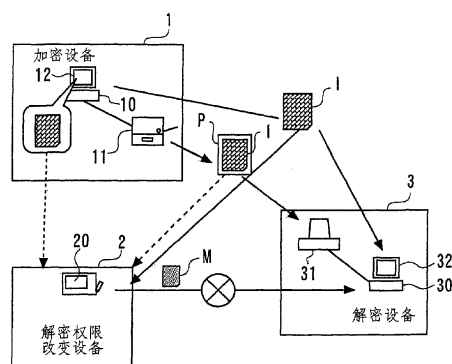
权利要求书 3 页 说明书 37 页 附图 30 页

[54] 发明名称

文档数据加密方法和文档数据加密系统

[57] 摘要

本发明提供文档数据加密方法和文档数据加密系统。加密设备通过使用收件人的密码来加密原始文档数据，从而产生加密文档数据。其操作权限由收件人拥有的解密权限改变设备产生通过用代理的密码加密收件人的密码而构成的权限改变信息 M，并且向解密设备通知该信息，该解密设备的操作权限由代理拥有。解密设备通过采用代理的密码来解密收件人的密码，并且通过使用经解密的收件人的密码来解密所述加密文档数据。



1、一种文档数据加密方法，其将要传递给收件人的文档数据以用所述收件人用的密钥进行解密的模式加密，并且通过使用所述密钥来解密所述文档数据，所述方法包括：

使得第一终端以用代理用的密钥进行解密的模式加密所述收件人用的密钥，并且将经加密的所述收件人用的密钥传输到所述代理，所述文档数据被转发给所述代理；以及

使得由所述代理操作的第二终端通过采用所述代理用的密钥来解密所述收件人用的密钥，并且通过使用经解密的所述收件人用的密钥来解密所述文档数据。

2、根据权利要求1所述的文档数据加密方法，其中，所述收件人用的密钥是加密和解密共享的共同密钥。

3、根据权利要求1所述的文档数据加密方法，其中，所述代理用的密钥是所述代理用的秘密密钥，并且用与该秘密密钥相关联的公共密钥来加密所述收件人用的密钥。

4、根据权利要求1所述的文档数据加密方法，其中，加密并由此传递所述文档数据的仅一部分。

5、根据权利要求4所述的文档数据加密方法，其中，以用所述收件人的互不相同的各个密钥解密的模式分别加密所述文档数据的多个区域。

6、根据权利要求4所述的文档数据加密方法，其中，分别通过使用所述代理的互不相同的各个密钥来加密用于对所述文档数据的所述多个区域进行加密的密码的密钥。

7、一种文档数据加密系统，其将要传递给收件人的文档数据以用该收件人用的密钥解密的模式加密，并且通过使用所述密钥来解密所述文档数据，所述系统包括：

加密设备，其以用所述收件人用的密钥解密的模式来加密所述文档数据；

解密权限改变设备，其以用代理用的密钥解密的模式来加密所述收件人用的密钥，并将经加密的所述收件人用的密钥或经加密的密码传输给所述代理，所述文档数据被转发给所述代理；以及

解密设备，其通过使用所述代理用的密钥来解密所述收件人用的密钥，并且通过使用经解密的所述收件人用的密钥来解密所转发的文档数据。

8、一种文档数据加密方法，其将要传递给收件人的文档数据以用该收件人用的密钥解密的模式进行加密，并且通过使用该密钥来解密所述文档数据，所述方法包括：

使得加密设备以用所述收件人用的密钥解密的模式对要传递给所述收件人的文档数据进行加密，并且输出经加密的文档数据，并且向服务器传输以将所述文档数据的标识信息与所述收件人用的密钥相关联的方式组成的解密权限信息；

使得所述服务器将接收的解密权限信息存储在存储设备中；

使得第一终端将权限改变信息传输到所述服务器，所述权限改变信息是以将所述文档数据的标识信息与代理的标识信息相关联的方式组成的，所述文档数据被转发给所述代理；

使得所述服务器将所述权限改变信息中包含的代理标识信息添加到所述存储设备中的解密权限信息，该解密权限信息包含与所接收的权限改变信息相同的文档数据的标识信息；

使得第二终端将包含所转发的文档数据的标识信息和所述代理的标识信息的解密请求传输到所述服务器；

只要在所述存储设备中的包含与解密请求中的相同文档数据的标识信息的所述解密权限信息中包含与所述解密请求中的标识信息相同的代理的标识信息，就使得所述服务器将在所述解密权限信息中包含的收件人的密钥传输到规定为解密请求的发送者的第二终端；以及

使得所述第二终端通过使用所接收的收件人的密钥来解密所述文档数据。

9、根据权利要求8的文档数据加密方法，其中，所述加密设备以用

所述收件人的互不相同的密钥解密的模式加密所述文档数据的多个区域，

所述第一终端产生针对每个区域的权限改变信息，并且将所述权限改变信息传输到所述服务器，并且

所述服务器将所述代理的标识信息添加到针对每个区域的解密权限信息。

10、一种文档数据加密系统，其用于以用收件人的密钥解密的模式加密要传递给所述收件人的文档数据，并且通过使用所述密钥来解密所述文档数据，该文档数据加密系统包括：

加密设备，其以用所述收件人的密钥解密的模式加密要传递给所述收件人的文档数据，然后输出该文档数据，并且将解密权限信息传输到服务器，所述解密权限信息是以将所述文档数据的标识信息与所述收件人的密钥相关联的方式组成的；

解密权限改变设备，其将权限改变信息传输到所述服务器，所述权限改变信息是以将所述文档数据的标识信息与所述文档数据被转发到的代理的标识信息相关联的方式组成的；

服务器，其将接收的解密权限信息存储在存储设备中，将所述权限改变信息中包含的所述代理的标识信息添加到所述存储设备中的包含与所接收的权限改变信息相同的文档数据的标识信息的解密权限信息，并且只要在所述存储设备中的包含与解密请求中的相同文档数据的标识信息的解密权限信息中包含与所述解密请求中的标识信息相同的代理的标识信息，就将在所述解密权限信息中包含的收件人的密钥传输到所述解密请求的发送者；以及

解密设备，其产生解密请求并将其传输到所述服务器，并且通过使用从所述服务器接收的所述收件人的密钥来解密所述文档数据。

文档数据加密方法和文档数据加密系统

技术领域

这里讨论的实施方式涉及文档数据加密方法和文档数据加密系统。

背景技术

随着近年来高度复杂的信息化，通过传输电子数据可以传播这样一类信息，该类信息传统上通过移动纸质介质来传递。因此，一方面，通过采用各种传播手段来传播各种类别的信息，另一方面，随着日本 2003 年个人信息保护法的建立，在社会上认识到了保护诸如个人信息和商业机密的信息的必要性。

在这点上，通常对于作为电子数据传播的信息所采用的技术是下述技术，该技术在将电子数据存储在电子邮件或分组中以进行数据传输之前，以仅使得收件人能够解密该电子数据的模式来加密该电子数据，使得即使第三方在传播中截获了该信息，信息的内容也不会泄露出去。

另一方面，在传统的信息传播模式中，将信息的内容打印在纸质介质上，并且通过物理移动手段传递，如通过邮件传送，在该传统的信息传播模式中，还没有利用诸如如上所述的加密以防止信息泄露的技术。因此，如果在纸质介质的移动中该纸质介质被第三方窃取，或者如果该纸质介质被错误地传送到第三方，则简单地通过查看打印面，信息的内容就容易地泄露给第三方。具有信息泄露风险的信息例如有用于购买商品的账单、信用卡等的明细单、医院的医疗卡、学校的报告卡、姓名列表等。

因此，本申请人提出了一种将要打印在纸质介质上的信息（文档数据）可视化为图像数据的方法，该方法之前在日本专利局提交，其日本专利公开号是 No. 2008-301044（以下将其简称为“在先申请”），该方法以仅利用仅由信息的收件人知道的密钥（密码）解密的模式，首先特别

对于要隐藏的区域执行加密（扰码）处理，并且以得到不可视觉识别的原始内容的方式打印该信息。根据该方法，信息的有效收件人通过用扫描仪将在纸质介质上打印的信息读取到计算机中，仅提取经历加密（扰码）处理的区域，然后通过采用密钥（密码）解密原始部分图像，将该部分图像插入到电子数据的原始剪切位置，然后实现整个原始图像（即，要恢复的可视化文档数据），来将数据电子化。

根据在先申请的所述方法，即使第三方看见在纸质介质上打印的包含加密区域的信息，该第三方也不能识别加密区域的含义的内容，从而可以防止信息泄露。

注意到，在在先申请中提出的仅对图像的一部分执行加密（扰码）处理的方法不仅可应用于打印在纸质介质上的图像，而且可应用于作为电子数据传播的可视化文档数据的加密。

另一方面，作为在不可可视化的情况下加密文档数据的一部分的方法，除了在先申请的方法外，还存在这样的方法，其将诸如 PDF（便携文档格式）的结构文档数据中的部分区域指定为遮盖区域，并且以将诸如黑色的色彩叠加在指定区域上的方式显示文档数据。该方法涉及使用删除遮盖区域的信息、并且将打黑点的图像插入到删除了信息的区域以便防止分发的文档中的遮盖区域被第三方读取的方案。该方案意图使得即使文档创建者他自己或她自己也不能从文档中的遮盖区域获取删除的内容。

考虑到上述情况，作为电子文档传播的现有文档数据被分类为由电子文档创建工具产生的电子文档数据和电子文档数据的可视化数据。此外，文档数据被定义为包括图像数据的高级概念。[文档数据]的内含除了包括通过电子数据传播的文档数据和图像数据之外，还包括在纸质介质上打印的文档数据和图像数据。

[专利文献 1]日本专利特开 No. 2007-194962

[专利文献 2]日本专利特开 No. 2000-69300

视觉加密文档数据的全部或一部分的方法包括对可视化文档数据的全部或一部分执行加密（扰码）处理的方法，或者对文档数据的部分区

域执行打黑点处理、然后同时从文档数据中删除用遮盖区域隐藏的区域、并且将加密数据存储诸如文档的头部区域的可视区域中的方法。

然而，即使使用任何方法，除非使用在加密的时间点采用的仅由收件人知道的密钥，否则不能对加密区域进行解密，使得在将信息传输到收件人之后，即使在需要将解密权限让与给收件人以外的人（以下将称为“代理”）的情况下，该代理也不能基于已经传输的文档数据自身来解密该文档数据。这将参照图 37 来讨论。注意，图 37 中例示的示例是通过采用对于加密和解密共同的密钥（共同密钥）来加密和解密文档数据的一部分的示例。

然而，在图 40 中描述的示例中，首先，初始“经理”是文档数据（a）的收件人，因此，文档数据用分配给“经理”并且仅由“经理”知道的密钥（密码）加密，然而，该密钥（密码）能由文档数据发送者（b）使用的加密设备使用。因此，“经理”可通过使用自己的密钥（密码）（c）解密文档数据。关于此点，假设由于不允许“经理”他自己或她自己执行解密的情况，“经理”请求“部门负责人”作为处理具有文档数据的打印文档或电子文档的代理。然而，在此情况下，“部门负责人”不拥有用于解密文档数据的密钥（密码），因此不能解密文档数据。注意到，“部门负责人”在附图中缩写为“负责人”。

在此情况下，在请求时，简单地，如果“经理”以口头方式或通过书写的便条让“部门负责人”知道自己的密钥（密码），则“部门负责人”可以解密文档数据。然而，考虑到引起安全性的许多问题，不推荐让别人知道自己的密钥。

在这样的情况下，考虑这样的方法，其在不让“部门负责人”知道用于加密文档数据的“经理”的密钥的情况下使得“部门负责人”能够解密文档数据，如图 41 所示，所述方法例如为这样的方法，该方法通过用仅分配给“部门负责人”并仅由“部门负责人”知道的密钥（密码）加密原始文档数据（然而，该密钥（密码）可由文档数据的发送者使用的加密设备使用），与用“经理”的密钥加密的文档数据分开地重新发布加密文档数据，传递该重新发布的加密文档数据，并使得“部门负责人”

能够用自己的密钥（密码）解密该加密文档数据。然而，该方法必须涉及再次执行加密相同区域的操作，而这是耗时的。此外，如果文档数据的发布者不是“经理”他自己或她自己，则请求“部门负责人”成为代理的“经理”必须请求文档数据的发布者重新发布加密文档数据，这又是耗时的。在此情况下，如果发布者处理操作有延迟，此时“经理”不能请求“部门负责人”处理打印文档或电子文档，因此发布者负担了对重新发布加密文档数据的请求进行快速响应的责任，然而，这种责任的出现成为系统操作方面的约束，这是不期望的。

此外，考虑在不让“部门负责人”知道用于加密文档数据的“经理”的密钥的情况下使得“部门负责人”能够解密文档数据的另一种方法，如图 42 所示，其中，在“经理”他自己或她自己已经用自己的密钥（密码）对加密文档数据进行了一次解密之后，用“部门负责人”的密钥或即使让“部门负责人”知道也不会造成麻烦的密钥来加密所述文档数据，然后输出重新加密的文档数据，将该重新加密的文档数据传递到“部门负责人”，并且使得“部门负责人”能够用自己的密钥（密码）解密该重新加密的文档数据。然而，该方法必须在已经对加密区域进行一次解密后重新加密数据，因此是耗时的。此外，当加密文档数据是打印材料时，需要用扫描仪将数据读入计算机，这又是耗时的，并且考虑到加密文档数据的质量下降也不是优选的。

发明内容

因此，实施方式的一个方面的目的是提供一种文档数据加密方法，该文档数据加密方法在使得加密文档数据的初始收件人以外的代理能对加密文档数据进行解密的情况下，可以消除向代理通知仅由收件人知道的密钥的必要性和重新加密文档数据的必要性。

根据实施方式的一方面，提供一种文档数据加密方法，其将要传递给收件人的文档数据以用所述收件人用的密钥进行解密的模式加密，并且通过使用所述密钥来解密所述文档数据，所述方法包括：使得第一终端以用代理用的密钥进行解密的模式加密所述收件人用的密钥，并且将

经加密的所述收件人用的密钥传输到所述代理，所述文档数据被转发给所述代理；以及使得由所述代理操作的第二终端通过采用所述代理用的密钥来解密所述收件人用的密钥，并且通过使用经解密的所述收件人用的密钥来解密所述文档数据。

实施方式的目的和优点将通过在权利要求中具体指出的要素和组合来实现和达到。

应当理解，前面的概括描述和后面的详细描述是示例性和说明性的，而非对所要求保护的实施方式的限制。

附图说明

图 1 是例示根据第一实施方式的文档数据加密系统的配置概要的框图。

图 2 是例示根据第一实施方式的加密设备的功能之间的关联的框图。

图 3 是例示根据第一实施方式的解密权限改变设备的功能之间的关联的框图。

图 4 是例示根据第一实施方式的解密设备的功能之间的关联的框图。

图 5 是例示在根据第一实施方式的加密设备中执行的处理的流程图。

图 6 是例示在根据第一实施方式的解密权限改变设备中执行的处理的流程图。

图 7 是例示在根据第一实施方式的解密设备中执行的处理的流程图。

图 8 是例示如何加密和解密文档数据的示例的图。

图 9 是例示经加密的文档数据的示例的图。

图 10 是例示根据第一实施方式的解密权限信息的表格。

图 11 是描绘用于输入文档 ID 的 GUI 画面的图。

图 12 是描绘用于输入区域 ID 的 GUI 画面的图。

图 13 是描绘用于输入密码的 GUI 画面的图。

图 14 是描绘用于输入译码者的名称 (ID) 的 GUI 画面的图。

图 15 是例示根据第一实施方式的权限改变信息的数据结构的表格。

图 16 是根据第一实施方式的文档数据加密系统的操作的说明图。

图 17 是例示第一实施方式的第一修改示例中的加密的图。

图 18 是例示在第一实施方式的第一修改示例中如何让与权限的图。

图 19 是例示第一实施方式的第一修改示例中的解密的图。

图 20 是例示加密文档数据的修改示例的图。

图 21 是例示在第一实施方式的第二修改示例中如何校正失真的图。

图 22 是例示在第一实施方式的第二修改示例中如何指定区域的图。

图 23 是例示在第一实施方式的第二修改示例中的权限改变信息的图。

图 24 是例示在第一实施方式的第三修改示例中如何指定区域的图。

图 25 是例示在第一实施方式的第三修改示例中如何输入密码的图。

图 26 是例示在第一实施方式的第三修改示例中如何输入译码者的名称 (ID) 的图。

图 27 是例示根据第二实施方式的文档数据加密系统的配置概要的框图。

图 28 是例示根据第二实施方式的加密设备的功能之间的关联的框图。

图 29 是例示根据第二实施方式的解密权限改变设备的功能之间的关联的框图。

图 30 是例示根据第二实施方式的解密权限管理设备的功能之间的关联的框图。

图 31 是例示根据第二实施方式的解密设备的功能之间的关联的框图。

图 32 是例示在根据第二实施方式的加密设备中执行的处理的流程图。

图 33 是例示在根据第二实施方式的解密权限改变设备中执行的处理的流程图。

图 34 是例示在根据第二实施方式的解密权限管理设备中执行的处理的流程图。

图 35 是例示在根据第二实施方式的解密设备中执行的处理的流程

图。

图 36 是例示根据第二实施方式的权限改变信息的表格。

图 37 是例示更新的解密权限信息的表格。

图 38 是根据第二实施方式的文档数据加密系统的操作的说明图。

图 39 是根据第二实施方式的文档数据加密系统的操作的说明图。

图 40 是在先文档数据加密方法的问题的说明图。

图 41 是在先文档数据加密方法的问题的说明图。

图 42 是在先文档数据加密方法的问题的说明图。

具体实施方式

以下将基于附图描述本发明的两个实施方式。每个实施方式的特征在于，用于对加密的文档数据进行加密的原始收件人的密钥（密码）用被定义为受让人的代理的密钥（密码）加密，经加密的密码作为权限改变信息被发送到代理的计算机（解密设备），所述解密设备以从外部不可识别的模式解密权限改变信息中的收件人的密钥（密码），并且通过如此解密的收件人的密钥（密码）来解密所述经加密的文档数据。注意，“收件人的密钥（密码）”可以是仅由收件人和发送者知道的共同密钥，还可以是与仅由收件人知道的秘密密钥对应的公共密钥。此外，对“密码”加括号意在表示使用通过对密码执行预定算术运算而产生的加密密钥的加密。然而，本发明的实质不在于采用什么加密方法，因此，在下面的讨论中，为了简化描述，将在通过使用收件人的密码进行加密（简称为“收件人的密码”）的假设下来进行描述。类似地，“代理的密钥（密码）”可以是仅由代理和收件人知道的共同密钥，还可以是与仅由代理知道的秘密密钥对应的公共密钥。此外，对“密码”加括号意在表示使用通过对密码执行预定算术运算而产生的加密密钥的加密。然而，本发明的实质不在于采用什么加密方法，因此，在下面的讨论中，为了简化描述，将在通过使用代理的密码进行加密（简称为“密码”）的假设下来进行描述。

第一实施方式

第一实施方式的特征在于，通过由加密文档数据的原始收件人拥有和操作的单个终端（权限改变设备）的功能产生权限改变信息。

<系统架构>

图 1 是示意性示出构成根据如所示的第一实施方式的文档数据加密系统的各个设备之间的关联的框图。具体地说，根据第一实施方式的文档数据加密系统由加密设备 1、权限改变设备 2 和解密设备 3 构成。然后，加密设备 1 可经由未例示的网络向权限改变设备 2 和解密设备 3 发送电子邮件，而权限改变设备 2 可经由未例示的通信网络或红外线通信向解密设备 3 发送数据。

[加密设备]

加密设备 1 是这样的计算机系统，其以与在先申请的描述中相同的方式，通过使用原始收件人的密码来加密传输目标文档数据的一部分或全部，在显示器 12 上显示加密后的传输目标文档数据（以下将称为[加密文档数据]），将附到电子邮件中的该加密文档数据传输到由邮件地址指定的目的地，根据传真协议将该加密文档数据传真到收件人的传真号码，以及通过打印机将该加密文档数据打印并输出为打印材料 P。加密设备 1 由具有通常配置的个人计算机（PC）10 和连接到 PC 10 的打印机 11 构造，所述计算机包括显示器 12、CPU（未例示）、键盘（未例示）、鼠标（未例示）、扫描仪（未例示）、盘设备（未例示）和通信接口、以及加密程序，所述加密程序使得 CPU 执行安装在盘设备中的、图 5 所示的处理流程的处理。

图 2 是例示当在上述加密设备 1 中执行上述加密程序时由 CPU 执行的功能的框图。具体地说，如图 2 所示，加密设备 1 的功能通过输入单元 13、加密单元 14 和输出单元 15 实现。

输入单元 13 获取经由未例示的盘设备、相机、扫描仪等输入的文档数据（原始文档数据），然后获取经由鼠标和键盘输入的用于指定加密区域的位置的信息，并且获取经由键盘输入的用于加密每个加密区域的密码。输入单元 13 向加密单元 14 通知由此获取的原始文档数据、加密区域的位置以及针对每个区域的密码，并且向输出单元 15 通知当操作者输

入加密区域的位置指定信息时应当参考的原始文档数据，从而在显示器 12 上显示原始文档数据。

加密单元 14 获取输入单元 13 所通知的原始文档数据，并且通过使用输入单元 13 所通知的密码，对原始文档数据中、由输入单元 13 所通知的位置指定的加密区域进行加密。例如，如图 8 (a) 所示，当假设在原始文档数据中指定三个加密区域 (ID1-ID3) 时，在第一加密区域 (ID1) 中指定密码 (加密密钥 1)，在第二加密区域 (ID2) 中指定密码 (加密密钥 2)，并且在第三加密区域 (ID3) 中指定密码 (加密密钥 3)，如图 8 (b) 所示，由此用各个密码 (加密密钥 1-3) 加密各个加密区域 (ID1-ID3)。注意，根据对原始文档数据的光栅扫描顺序唯一地确定各个加密区域 (ID1-ID3)。加密单元 14 向输出单元 15 通知各个加密区域被加密的文档数据 (加密文档数据 I)。

输出单元 15 在显示器 12 上显示输入单元 13 通知的原始文档数据和加密单元 14 已经通知的加密文档数据，并且使得打印机 11 输出打印材料 P，或者通过电子邮件或通过传真信号将加密文档数据 I 传输到收件人的地址或由收件人指定的代理的地址，其中，在所述打印材料 P 中，根据输入到输入单元 13 的操作者的选择，在输出纸张上打印了该加密文档数据 I。注意，加密文档数据 I 的标识号 (文档 ID) 和每个加密区域的区域 ID 存储在通过电子邮件传输的加密文档数据 I 的文档数据的头部中。此外，加密文档数据的文档 ID 以明文打印在从打印机 11 输出的打印材料 P 上的头部位置处 (见图 9)。

[解密权限改变设备]

接下来，解密权限改变设备 2 是通过收件人保持其操作权限的通信终端，其产生权限改变信息 M，并且传输权限改变信息 M，所述权限改变信息 M 由诸如由收件人输入的加密文档数据 I 的 ID (文档 ID)、用于指定加密区域的区域 ID 或位置信息 (坐标) 和收件人的密码的信息项组成，在这些信息项中至少密码是用代理的密码加密的。虽然未例示，但是解密权限改变设备 2 由能够执行应用的 CPU、包括十个键的键盘、存储有应用的存储器、用于显示 GUI (图形用户界面) 画面的显示器 12、

相机和通信设备构成。具体地说，解密权限改变设备 2 例如为移动电话（如所谓的智能电话）、PDA（个人数字助理）和个人计算机。注意，在解密权限改变设备 2 中包括的通信设备可以是能连接到移动电话网络的通信模块，也可以是红外线通信模块，还可以是能连接到固定电话网络和 LAN（局域网）的通信模块。即，解密权限改变设备 2 所需要的通信功能可以是经由通信线路执行数据通信的功能，还可以是执行红外线通信的功能。在第一实施方式中，将图 6 中例示了其处理流程的解密权限改变程序作为应用安装到解密权限改变设备 2 的未例示的存储器中。

图 3 是例示在未例示的 CPU 执行上述解密权限改变设备 2 中的解密权限改变程序的情况下由 CPU 实现的各个功能的框图。具体地说，如图 3 所示，解密权限改变设备 2 的功能通过输入单元 21、控制单元 22、密码存储单元 23、输出单元 24 和通信单元 15 来实现。

输入单元 21 获取经由键盘输入的文档 ID、每个加密区域的区域 ID 或位置指定信息、以及代理关于每个加密区域的选择信息（权限转交目的地），然后获取用于对经由键盘输入的每个加密区域进行加密的收件人的密码和用于对收件人的密码进行加密的每个个人代理的密码，进一步获取经由捕获输入材料 P 的图像的相机或扫描仪输入的加密文档数据 I，或者从经由通信设备接收的寻址到收件人的电子邮件获取加密文档数据 I。注意，个人可以被指定为代理，并且包括该个人的指定组也可被指定为代理，在后一情况下，获取分配给该组的密码。该方案使得能够与每个加密区域的机密级别相对应地对于代理的访问权限给出差别。然后，输入单元 21 向控制单元 22 通知由此获取的文档 ID、每个区域 ID、与每个加密区域对应的收件人的密码和权限转交目的地。此外，输入单元 21 向输出单元 24 通知当操作者输入加密区域的位置指定信息时应当参考的加密文档数据 I，并且在显示器 20 上显示该加密文档数据 I。

密码存储单元 23 以对于每个对象（具有解密权限改变设备 2 的操作权限的收件人、作为个人的代理、代理组）将标识信息和密码彼此关联的方式，将这些信息项存储在存储器中。优选的是，由密码存储单元 23 处理的密码涉及使用每个代理的公共密钥。

控制单元 22 产生权限改变信息 M，所述权限改变信息 M 由以下信息项组成：输入单元 21 通知的收件人密码、对于输入单元 21 通知的文档 ID 的每个元组输入单元 21 通知的权限转交目的地、输入单元 21 通知的个体区域 ID 以及加密区域的位置指定信息，此外，控制单元 22 通过采用输入单元 21 所通知的代理密码、或密码存储单元 23 中以与输入单元 21 所通知的权限转交目的地相关联的形式存储的代理密码，至少加密权限改变信息 M 中的收件人密码。然后，控制单元 22 向输出单元 24 通知加密前权限改变信息 M，并且向通信单元 25 通知加密后权限改变信息 M。

输出单元 24 在显示器 20 上显示输入单元 21 所通知的加密文档数据 I 和控制单元 22 所通知的加密前权限改变信息 M，以用于确认。

通信单元 25 经由通信线路或通过红外线通信，将控制单元 22 所通知的加密后权限改变信息 M 传输到每个个人代理的解密设备 3（权限转交目的地）。

注意，如果加密文档数据 I 通过电子邮件传输到收件人，则在解密权限改变设备 2 已经接收到电子邮件后，收件人可以将电子邮件转发给代理，并且还可通过使用不同终端（其操作权限由收件人他自己或她自己保持的解密设备等）转发电子邮件。

[解密设备]

接下来，作为由代理操作的计算机系统的解密设备 3，由具有通常配置的个人计算机（PC）30 以及与 PC 30 连接的扫描仪 31 构成，所述个人计算机 30 包括：显示器 32、CPU（未例示）、盘设备（未例示）和通信接口、以及用于使得 CPU 执行在盘设备中安装的、在图 7 中例示的处理流程中的处理的解密程序。解密设备 3 基于该解密程序，从自加密设备 1 直接接收或由收件人转发的电子邮件或传真信号提取加密文档数据 I，或者一方面，通过扫描仪 31 读取由收件人移交的或从收件人发送的打印材料 P 上的加密文档数据 I，然后用代理的秘密密码解密从权限改变设备 2 接收的权限改变信息 M 中的密码，并且进一步通过采用解密的密码对加密文档数据 I 中的加密区域进行解密，从而恢复原始文档数据。

图 4 是例示当未例示的 CPU 执行上述解密设备 3 中的上述解密程序时由 CPU 实现的各个功能的框图。具体地说, 如图 4 所示, 解密设备 3 的功能通过输入单元 33、控制单元 34、解密单元 35、输出单元 36 和通信单元 37 来实现。

输入单元 33 获取经由扫描仪 31 输入的打印材料 P 上的加密文档数据 I, 然后获取经由鼠标和键盘输入的加密区域的区域 ID 或位置指定信息, 并且获取通过键盘输入的、具有解密设备 3 的操作权限的代理的密码(代理组的密码)。然后, 输入单元 33 向控制单元 34 通知由此获取的加密文档数据 I、与每个加密区域相关联的区域 ID 或位置指定信息以及密码。此外, 输入单元 33 向输出单元 36 通知当输入加密区域的位置指定信息时操作者应当参考的加密文档数据 I, 并且在显示器 32 上显示该加密文档数据 I。

通信单元 37 获取经由通信接口接收的电子邮件或传真信号中的加密文档数据 I, 并且获取通过通信接口接收的权限改变信息 M。然后, 通信单元 37 向控制单元 34 通知由此获取的加密文档数据 I、权限改变信息 M 和密码。此外, 通信单元 37 向输出单元 36 通知当操作者输入加密区域的位置指定信息时应当参考的加密文档数据 I, 并且在显示器 32 上显示该加密文档数据 I。

控制单元 34 在输入单元 33 所通知的各条权限改变信息 M 中, 通过使用与权限改变信息 M 中的权限转交目的地相对应的输入单元 33 所通知的密码, 解密与输入单元 33 所通知的加密区域的区域 ID 或位置指定信息相关联的权限改变信息 M。然后, 控制单元 34 从解密的权限改变信息 M 中提取收件人密码, 然后向解密单元 35 通知收件人密码、以及输入单元 33 所通知的加密区域的区域 ID 或位置指定信息以及加密文档数据 I, 并且请求解密单元 35 解密该加密区域。然后, 当从解密单元 35 接收到对所有允许解密的加密区域完成了解密的文档数据(已经解密的文档数据)时, 控制单元 34 向输出单元 36 通知该已经解密的文档数据。

解密单元 35 通过采用从控制单元 34 接收的密码, 解密从控制单元 34 接收的加密文档数据 I 中、由从控制单元 34 接收的区域 ID 或位置指

定信息标识的每个加密区域,由此将加密文档数据 I 解密到具有解密设备 3 的操作权限的代理可以进行解密的程度,并且通过对控制单元 34 的响应发送作为已经解密的文档数据的解密结果。例如,在图 8 中的上述示例中,用相关联的密码解密图 8 (b) 中例示的加密文档数据的各个加密区域 (ID1-ID3),从而获得如图 8 (c) 所示的已经解密的文档数据。

输出单元 36 在显示器 32 上显示输入单元 33 或通信单元 37 所通知的加密文档数据 I,以及控制单元 34 所通知的已经解密的文档数据。

<数据处理流程>

以下将参照图 5 到图 7 的流程图,描述构成根据第一实施方式的具有上述配置的文档数据加密系统的加密设备 1、权限改变设备 2 和解码设备 3 的数据处理流程。

[加密设备]

图 5 是示出由 CPU 根据安装到加密设备 1 的盘设备中的加密程序执行的加密处理的流程图。通过向键盘输入用于读取原始文档数据的预定命令来触发该流程图中的处理的开始。在开始加密处理后的第一步骤 S001 中,加密设备 1 (输入单元 13 和加密单元 14) 以上述方式获取加密目标输入文档数据 (原始文档数据)。

在下一步骤 S002,加密设备 1 (输出单元 15) 在显示器 12 上显示在 S001 获取的原始文档数据。

接下来,执行 S003 到 S008 的循环处理,以便执行关于文档数据的发送器要求其机密性的区域的加密处理。在进入该循环处理后的第一步骤 S003,加密设备 1 (加密单元 14) 获取通过操作键盘或鼠标而输入的、一条未处理的关于加密区域的位置指定信息。

在下一步骤 S004,加密设备 1 (加密单元 14) 在显示器 12 上显示用于接受输入文档数据的地址的密码的输入的 GUI 画面 (密码输入画面)。注意,用于各个加密区域的密码可以是共同的,然而,例如,在将相同加密文档数据分发到多个人的情况下,可通过使用对于每个加密区域各不相同的密码来加密数据,从而可以对具有用于解密各加密区域的权限的人的范围给出差别。例如,图 10 中的示例是,将包括“经理 A”的组

“公共”的密码应用于区域（ID1）和区域（ID2），因此，知道该密码的“经理 A”和其他组“公共”的成员可以解密这些区域（ID1，ID2）。将“经理 A”的密码应用于区域（ID3），因此“经理 A”可以解密该区域（ID3），然而，其他人不可以解密该区域（ID3）。此外，如果存在在发送者和收件人之间使用的多个密码，则在之前以将解密权限彼此相关联的方式对各个区域分开使用所述多个密码，这使得即使请求代理用作解密的代理时，也能对每个代理区分加密区域的可译码范围。

在下一步骤 S005，加密设备 1（加密单元 14）获取通过操作在 S004 所示的密码输入画面上的键盘而输入的密码。

在下一步骤 S006，加密设备 1（加密单元 14）通过使用在 S005 获取的密码，加密在 S001 获得的原始文档数据中的由在 S003 获取的指定信息指定的区域。

在下一步骤 S007，加密设备 1（加密单元 14）在 S002 所示的原始文档数据上覆写包含到该时间点完成了加密处理的每个加密区域的加密结果的文档数据，并且显示覆写的文档数据。

在随后的步骤 S008，加密设备 1（加密单元 14）检查是否存在未处理的加密区域的位置指定信息，或者发送者是否经由鼠标输入关于加密区域的处理终止的声明（事件）。然后，如果存在未处理的加密区域的位置指定信息，则加密设备 1（加密单元 14）将处理循环回到 S003，以便执行关于未处理的加密区域的加密处理。

而如果没有未处理的加密区域的位置指定信息，并且当发送者经由键盘输入关于所有加密区域的处理终止的声明时，加密设备 1（加密单元 14）假设完成了关于所有加密区域的加密处理，而将处理前进到 S009。

在 S009，根据发送者经由键盘输入的指令，加密设备 1（加密单元 14）从打印机将完成了关于所有加密区域的加密处理的加密文档数据 I 输出为打印材料 P，或者以附到电子邮件的方式或以在传真信号上携带的方式将该加密文档数据 I 传输到收件人的地址。图 9 示出由此输出的加密文档数据 I 和传真信号的示例，并且如上所述，在图 9 的示例中，明文的文档 ID 打印在其头部位置。

顺带提及，作为完成到目前为止的处理的结果，如图 10 所示，在加密设备 1 的存储器上，对于加密文档数据 I 和加密区域的每个元组，产生登记为一条记录的解密权限信息，该记录包括诸如文档 ID、区域 ID（在光栅扫描序列中附到在 S003 中指定其位置的加密区域的序列号）、包含区域位置信息（在 S003 中进行位置指定的加密区域的坐标范围）、密码和解密权限的解密权限信息的字段。当加密文档数据 I 作为打印材料 P 和传真信号被输出时，不将解密权限信息输出到外部，而当附到电子邮件并由此输出时，其存储在文档数据的头部（这包括由于附到电子邮件而将加密文档数据 I 暂时存储在文档数据文件中的情况）。

在完成 S009 之后，加密设备 1 完成其所有处理。

[解密权限改变设备]

图 6 是示出由 CPU 根据安装到解密权限改变设备 2 的存储器中的解密权限改变程序执行的加密处理的流程图。基于该流程图的处理的开始通过对键盘输入预定命令而触发。在开始该加密处理后的第一步骤 S101，解密权限改变设备 2（输出单元 24）显示用于接受文档 ID 的输入的 GUI 画面（见图 11）。收件人被要求在文本框中输入在打印材料 P 的头部字段中打印的文档 ID。

在下一步骤 S102，解密权限改变设备 2（输入单元 21，控制单元 22）获取通过针对在 S101 显示的 GUI 画面操作键盘而输入的文档 ID。

随后，执行 S103 到 S107 的循环处理，用于获取加密文档数据 I 的每个加密区域的密码。在进入该循环处理后的第一步骤 S103，解密权限改变设备 2（输出单元 24）在显示器 20 上显示用于接受区域 ID 的输入的 GUI 画面（见图 12）。收件人被要求从加密文档数据 I 内指定应当被设置为处理目标区域的加密区域，按照加密文档数据 I 中的加密区域的光栅扫描序列确定顺序，并且请求将该顺序作为区域 ID 的值输入到 GUI 画面上的文本框中。

在下一步骤 S104，解密权限改变设备 2（输入单元 21，控制单元 22）获取通过针对在 S103 显示的 GUI 画面操作键盘而输入的区域 ID。

在随后的步骤 S105，解密权限改变设备 2（输出单元 24）在显示器

20 上显示用于接受与在 S104 获取的区域 ID 相关联的收件人密码的输入、和代理的密码的输入的 GUI 画面（见图 13）。可以在该 GUI 画面上选择代理的密码的指定或公共密钥的指定。在输入代理的密码的情况下，代理的密码用于加密在以下将说明的权限改变信息加密步骤（S114）中的收件人（见图 16 和“添加的图”）的密码。注意，如果直接指定代理的密码，则需要向代理通知该密码。在指定关于代理的公共密钥的情况下，在该步骤中不需要输入代理的密码。

在下一步骤 S106，解密权限改变设备 2（输入单元 21，控制单元 22）获取通过针对在 S105 显示的 GUI 画面操作键盘而输入的所有密码。

在下一步骤 S107，解密权限改变设备 2 检查发送者是否经由键盘输入仍然存在未处理的加密区域的声明或用于加密区域的处理终止的声明。然后，在输入仍然存在未处理的加密区域的声明的情况下，解密权限改变设备 2 将处理循环回到 S103，以便执行对于未处理的加密区域的循环处理。相反，在输入用于加密区域的处理终止的声明的情况下，解密权限改变设备 2 将处理前进到 S108。

随后，执行 S108 到 S112 的循环处理，以便对于加密文档数据 I 的每个加密区域获取权限转交目的地。在进入该循环处理后的第一步骤 S108，解密权限改变设备 2（输入单元 21，控制单元 22）指定在 S104 获取的未处理的区域 ID 中的一个。

在下一步骤 S109，解密权限改变设备 2（输出单元 24）在显示器 20 上显示用于接受权限转交目的地的输入的 GUI 画面（见图 14），以便获取关于由在 S108 指定的区域 ID 标识的加密区域的权限转交目的地。在密码存储单元 23 中存储的个体对象的名称作为列表显示在该 GUI 画面上。注意，在图 14 中的项目类别“公共”是由在单元中的所有成员构成的组的名称。

在下一步骤 S110，解密权限改变设备 2（输入单元 21，控制单元 22）获取通过针对在 S109 显示的 GUI 画面操作键盘而选择的权限转交目的地（代理）。注意，如果不能针对由在 S108 指定的区域 ID 标识的加密区域获取在 S106 中的代理的密码，或者如果选择使用公共密钥，则解密权限

改变设备 2（控制单元 22）以与在该步骤中选择的权限转交目的地相关联的方式，获取在密码存储单元 23 中存储的密码（示例：公共密钥）。

在下一步骤 S111，解密权限改变设备 2（输出单元 24）在显示器 20 上显示权限改变内容，即，关于在 S108 指定的区域 ID 而在 S110 获得的权限转交目的地的名称。

在随后的步骤 S112，解密权限改变设备 2（输入单元 21，控制单元 22）在 S108 检查是否完成指定所有加密区域的区域 ID。然后，如果还没有完成指定所有加密区域的区域 ID，则解密权限改变设备 2 将处理循环回到 S108。而如果已经完成指定所有加密区域的区域 ID，则处理进行到 S113。

在 S113，解密权限改变设备 2（控制单元 22）对于每个区域 ID，以与区域 ID 相关联的方式组合在 S106 或 S110 获取的收件人密码、在 S110 获取的权限转交目的地、以及在 S102 获取的文档 ID，从而以图 15 所示的格式产生权限改变信息 M（明文）。

在下一步骤 S114，对于每个区域 ID，通过使用在 S106 获得的代理密码，至少加密以与权限改变信息 M 相关联的方式在 S113 产生的所述权限改变信息 M 中的收件人密码。

在随后的步骤 S115，解密权限改变设备 2（通信单元 25）将在 S114 中完成的所有各条权限改变信息 M（加密）经由通信接口传输到每个权限转交目的地。在完成 S115 后，解密权限改变设备 2 终止该权限改变处理。

[解密设备]

图 7 是示出由 CPU 根据安装到解密设备 3 的盘设备中的解密程序执行的解密处理的流程图。通过对键盘输入预定命令来触发基于该流程图的处理的开始。在开始该解密处理之后的第一步骤 S201，解密设备 3（输入单元 33 或通信单元 37）以上述方式获取解密目标加密文档数据 I。

在下一步骤 S202，解密设备 3（输出单元 36）在显示器 32 上显示在 S201 获取的加密文档数据 I。

在下一步骤 S203，解密设备 3（控制单元 34）获取在 S201 中获取的

加密文档数据 I 的文档 ID。具体地说, 在通过电子邮件获取加密文档数据 I 的情况下, 解密设备 3 (控制单元 34) 从在文档数据的头部中存储的解密权限信息中提取文档 ID。与此相对照, 当通过扫描仪 31 获取加密文档数据 I 时, 和当通过传真信号获取加密文档数据 I 时, 通过与图 6 的 S101 和 S102 相同的处理获得文档 ID。

在下一步骤 S204, 解密设备 3 (控制单元 34) 尝试经由通信线路或通过红外线通信, 从解密权限改变设备 2 获取在由通信单元 37 到目前接收的各条权限改变信息 M 中、包含在 S203 获取的文档 ID 的权限改变信息 M。

在接下来的 S205, 解密设备 3 (控制单元 34) 检查作为 S204 的结果是否可获取权限改变信息 M。然后, 如果不能获取权限改变信息 M, 则存在解密设备 3 的操作者是加密文档数据 I 的原始收件人的可能性, 因此解密设备 3 将处理前进到 S213。相反, 如果作为 S204 的结果可以获取权限改变信息 M, 则解密设备 3 (控制单元 34) 将处理前进到 S206。

在 S206, 解密设备 3 (控制单元 34) 获取解密设备 3 的个人操作者的密码和该操作者所属的组的密码。可以通过读取例如存储在 IC 卡中的密码来获取密码, 并且还可经由在显示器 32 上显示的 GUI 画面来获取密码。

在接下来的 S207, 解密设备 3 (控制单元 34) 尝试通过使用在 S206 获取的密码, 解密在 S204 获取的所有权限改变信息 M。

在接下来的 S208, 解密设备 3 (控制单元 34) 检查作为 S207 的结果是否存在可以解密的权限改变信息。然后, 没有解密的权限改变信息 M, 这显然证明操作者没有作为代理的权限, 然而, 操作者有是原始收件人的可能性, 因此, 处理进行到 S213。

与此相反, 作为 S207 的结果存在可以解密的一条或多条权限改变信息 M, 操作者被授权为代理, 因此处理前进到 S209。

在 S209, 解密设备 3 (控制单元 34) 检测来自在 S201 获取的加密文档数据 I 的所有加密区域, 并且计算每个检测的加密区域的位置 (坐标)。

在接下来的 S210, 解密设备 3 (控制单元 34) 分别从在 S207 解密的

所有条权限改变信息 M 获取区域 ID。

在接下来的 S211, 解密设备 3 (控制单元 34) 获取关于在 S210 获得的每个区域 ID 而在 S209 计算的对应位置 (坐标)。

在接下来的 S212, 解密设备 3 (控制单元 34) 从在 S207 解密的所有条权限改变信息 M 中分别获取收件人的密码。注意, 由此获取的收件人的密码不输出到外部, 因此不会被泄露。在完成 S212 后, 解密设备 3 (控制单元 34) 将处理前进到 S216。

另一方面, 在 S213, 解密设备 3 (控制单元 34) 获取在 S201 中获取的加密文档数据 I 中、操作者经由键盘或鼠标指定的区域的位置 (坐标)。

在接下来的 S214, 如果操作者是加密文档数据 I 的收件人, 则解密设备 3 (输出单元 36) 在显示器 32 上显示用于接受密码的输入的 GUI 画面 (密码输入画面)。

在接下来的 S215, 解密设备 3 (输入单元 33, 控制单元 34) 获取通过针对在 S214 显示的密码输入画面对键盘的操作而输入的每个密码。当完成 S215 时, 解密设备 3 (控制单元 34) 将处理前进到 S216。

在 S216, 解密设备 3 (解密单元 35) 提取在加密文档数据 I 中的、由在 S211 或 S213 获取的坐标指定的每个范围, 然后基于在 S212 或 S215 获得的密码执行解密, 并且将通过解密获得的部分图像附到加密文档数据 I, 从而获得已经解密的文档数据。

在接下来的 S217, 解密设备 3 (输出单元 36) 在显示器 32 上显示在 S216 中获得的已经解密的文档数据。在完成 S217 后, 完成了基于解密程序的处理。

<实施方式中的操作>

以下将参照图 16 描述根据实施方式如上所述配置的文档数据加密系统的操作。这里的假设是, 当具有加密设备 1 的操作权限的文档数据的发送者传递 (或传输加密文档数据 I, 或发布打印材料 P) 加密文档数据 I 给收件人 “经理” 时, 收件人 “经理” 他自己或她自己既不执行解密, 也不执行随后的用于文档数据的处理, 而是请求代理 “部门负责人” 充当 “经理”。然后, 还假设发送者知道 “经理” 的在发送者和 “经理” 之

间使用的一条或多条密码，而“经理”知道“部门负责人”的在“经理”和部门负责人之间使用的一条或多条密码，然而，部门负责人不知道“经理”的任何密码。

然后，传递的目标文档数据是由扫描仪等读入到加密设备 1 或由加密设备 1 中的应用程序产生的文档数据，在此通过如“IMAGE ENCRYPTION”、“ENCRYPTED IMAGE”、“IMAGE DECRYPTION”的字符串识别。然后，需要对第三方隐藏这些字符串中包括“encryption”和“decryption”的字符串。

因此，在由发送者操作的加密设备 1 中，将显示要隐藏的字符串的三个区域指定为加密区域(S003)，并且分别用“经理”的密码加密(S006)，所述“经理”的密码作为加密密码与其相关联地输入(S005)。作为其结果获得的加密文档数据 I 被传递给“经理”。

然而，在上述情况下，会将包含加密文档数据 I 的打印材料 P 或电子邮件从“经理”转发给部门负责人，或者在从“经理”接收到请求的发送者他自己或她自己已经将目的地改变到部门负责人之后，最终部门负责人接收打印材料 P 或电子邮件。

另一方面，“经理”必须通过使用其操作权限由“经理”他自己或她自己拥有的解密权限改变设备 2 来产生权限改变信息 M，为实现该目的，“经理”必须知道加密设备 1 内产生的解密信息中的文档 ID 和区域 ID。此时，如果打印材料 P 或传真信号经由“经理”的现有(on-hand)路线发送，则“经理”可以识别在打印材料 P 上的头部位置处打印的文档 ID，并且可以基于每个加密区域的位置确定每个区域 ID。此外，如果“经理”暂时接收包含加密文档数据 I 的电子邮件，则解密权限改变设备 2 可从文档数据的头部提取解密权限信息。

即使在除此以外的其它情况下，如果“经理”可以看到在显示器 12 上显示的加密文档数据 I（例如，在发送者与“经理”相同的情况下（尽管很少）），“经理”可以从显示的内容知道文档 ID 和每个区域 ID。

“经理”将由此获知的文档 ID 和区域 ID 输入给解密权限改变设备 2，并且对每个区域 ID 输入自己的密码、“部门负责人”的密码和“部门负

责人”的名称（S102、S104、S106）。然后，解密权限改变设备 2 产生权限改变信息 M，所述权限改变信息 M 包括文档 ID、区域 ID、“经理”的密码和被定义为权限受让人的“部门负责人”的名称，其中，对于每个加密区域，将至少“经理”的密码用“部门负责人”的密码加密（S113，S114），并且将权限改变信息 M 传输到“部门负责人”的解密设备 3（S115）。操作解密设备 3 的部门负责人对于每条接收的权限改变信息 M，将自己的密码（或部门负责人他自己或她自己所属的组的密码）输入到解密设备 3（S206），从而尝试解密“经理”的每个密码（S207）。此时，如果用于对“经理”的密码进行加密的密码与部门负责人的密码（部门负责人所属的组的密码）一致，则解密了“经理”的密码。针对具有由此解密的“经理”的密码的权限改变信息 M，可以解密与文档 ID 和区域 ID 的元组相关联的加密文档数据 I 中的加密区域（S216）。因此，当针对所有条权限改变信息 M 解密了“经理”的密码时，并且当用“经理”的密钥解密了对应的加密区域时，已经解密的文档数据变为与原始文档数据一致。

<第一修改示例>

实施方式中的加密设备 1 不必限于通过成像处理对成像的文档数据的各个区域的全部或一部分进行加密的设备，而可以是这样的设备，所述设备被配置为，使得在如 PDF（便携文档格式）的情况下的构造文档数据中，由用鼠标和键盘指定的坐标所限定的区域被存储为文档数据中的加密区域。以下第一修改示例将讨论使用支持构造文档的加密设备 1 和解密设备 3 的情况。

由第一修改示例中的加密设备 1 产生的加密文档数据在于，从文档数据中删除在加密区域中包含的文档构造元素（字符、图形等），用打黑点的图像代替所指定的加密区域，并且将作为用收件人的密钥（密码）加密的加密区域内的文档构造元素的对象存储在文档数据的头部区域内。

注意，构造文档数据的头部区域可包含用多个密钥加密的文档构造元素。因此，以与基于成像处理的加密相同的方式，可以用对于每个区

域不同的收件人的密钥进行加密。

在第一修改示例中通过加密设备 1 产生的加密文档数据在显示器上显示为指定区域被打黑点的文档图像。

因此，在权限改变者视觉识别在显示器上显示的加密文档数据之后，解密权限改变设备 2 通过权限改变者的操作，获取文档 ID、区域 ID 和委托密码设置，并且输出具有这些信息项的数据作为权限改变信息。即，第一修改示例中的解密权限改变设备 2 可以具有与第一示例中完全相同的配置。因此，省略对该权限改变设备的配置和操作的描述。

如图 18 所示，第一修改示例中的解密设备 3 用由译码者输入的代理的密钥（密码），来解密收件人的密钥（密码），该收件人的密钥（密码）包含在从解密权限改变设备 2 获取的权限改变信息中，并且如图 19 所示，所述解密设备 3 通过使用收件人的解密密钥，来解密在加密文档数据的头部区域中存储的用收件人的密钥（密码）加密的加密区域中的信息。此外，通过删除加密文档数据中的（附有黑点图像的）区域，并且将用收件人的密钥解密的加密区域的信息叠加在该区域上，来再现原始文档数据。

<第二修改示例>

关于在打印材料 P 上打印文档 ID，如图 20 所示，可将通过对文档 ID 编码而产生的条形码打印在打印材料 P 的头部位置。在此情况下，收件人难以简单地通过观看条形码而识别文档 ID，因此期望解密权限改变设备 2 具有作为条形码读取器的功能。因此，在支持如此的条形码的解密权限改变设备 2 的第二修改示例中，通过经由相机或扫描仪捕获包含条形码的加密文档数据 I 的图像来代替图 6 中的 S101 和 S102 的处理、然后从图像捕获的文档数据提取条形码并解密该条形码，来获取文档 ID。

因此，在用相机对加密文档数据 I 进行成像的情况下，可以以使得收件人通过进行逻辑思考而不麻烦地鉴别每个加密区域的区域 ID 的方式，获取每个加密区域的位置（坐标）。具体地说，在第二修改示例中，如图 21 所示，在已经通过分别用触摸笔指定（触摸）在触摸屏显示器 20 上显示的加密文档数据 I 的四个角而校正失真（这是通过坐标转换处理将应当

为矩形的文档图像改变（校正）为矩形的处理）之后，如图 22 所示，通过指定（触摸）每个加密区域的四个角来指定处理目标加密区域的位置（坐标），以代替图 6 中的 S103 和 S104 的处理。

在此情况下，不指定区域 ID，而是替代地指定每个加密区域的位置（坐标），因此如图 23 所示，与图 15 中的信息 M 相比，在图 6 中的 S113 产生的权限改变信息 M 是将位置信息（坐标）存储为加密区域的区域 ID 的替代的信息。

<第三修改示例>

第三修改示例是，在解密权限改变设备 2 中，在通过电子邮件获取加密文档数据 I 的情况下，便于针对每个加密区域输入区域 ID 和收件人的密码以及代理的密码。

具体地说，对于每个加密区域，通过电子邮件获取的加密文档数据 I 的头部与解密权限信息一起存储，如图 10 所示，所述解密权限信息通过将区域 ID、位置信息、收件人的密码以及文档 ID 彼此关联而构成。因此，第三修改示例中的解密权限改变设备 2 直接从该解密权限信息读取文档 ID，来代替执行图 6 中的 S101 和 S102 的处理。

此外，代替执行图 6 中的 S103 和 S104 的处理，如图 24 所示，当通过鼠标点击任何一个加密区域的内部位置时，第三修改示例中的解密权限改变设备 2 获取与由位置信息指定的范围中包括点击位置的加密区域相关联的区域 ID。

此外，如图 6 中的 S105 的处理，当由鼠标点击时，第三修改示例中的解密权限改变设备 2 将如图 25 所示的气球状对话框（即，用于输入收件人的密码和代理的密码的对话框）附到加密区域，因此显示该对话框。类似地，通过图 6 中的 S109 的处理，将图 26 中例示的下拉菜单（即，用于选择代理的菜单）附到加密区域，并由此进行显示。

顺带提及，这样，当通过电子邮件传输加密文档数据 I 时，解密权限改变设备 2 将权限改变信息 M 存储在电子邮件中，并且将权限改变信息 M 与加密文档数据 I 一起传输给代理的解密设备可能就足够了。在此情况下，删除电子邮件中包含的文档数据的头部内存储的解密权限信息，

并且替代地可以在其中存储权限改变信息 M。

第二实施方式

第二实施方式的特征在于，与上述第一实施方式相比，将由解密权限改变设备产生的权限改变信息 M 传输给解密权限管理设备，并且解密权限设备基于权限改变信息 M 更新解密权限信息，并响应于从由常规代理操作的解密设备给出的请求，发送收件人的密码作为响应。

<系统架构>

图 27 是示意性例示构成上述第二实施方式的文档数据加密系统的各设备之间的关联的框图。具体地说，根据第二实施方式的文档数据加密系统通过加密设备 4、解密权限改变设备 5、解密权限管理设备 6 和解密设备 7 构成。然后，加密设备 4 可以经由未例示的网络向解密权限改变设备 5 和解密设备 7 传输电子邮件，而加密设备 4 和解密权限改变设备 5 可以经由未例示的通信网络或红外线通信，向解密权限管理设备 6 传输数据。

[加密设备]

加密设备 4 具有与第一实施方式中的加密设备基本相同的配置和功能，但是不同点仅在于，无论通过电子邮件或传真信号传输加密文档数据 I 还是将加密文档数据 I 作为打印材料输出，图 28 例示的输出单元 45 都经由通信接口，将在加密单元 44 中产生的解密权限信息（图 10）R 传输到解密权限管理设备 6。因此，以下省略其描述。

[解密权限改变设备]

接下来，解密权限改变设备 5 是其操作权限由收件人拥有的通信终端，并且是产生由诸如收件人输入的加密文档数据 I 的 ID（文档 ID）、用于指定加密区域的区域 ID 或位置信息（坐标）、收件人的名称（ID）和代理的名称（ID）的信息项构成的权限改变信息 M，然后传输该权限改变信息 M 的设备。虽然省略了例示，但是解密权限改变设备 5 由能够执行应用的 CPU、包括十个键的键盘、存储有应用的存储器、用于显示 GUI 画面的显示器 50、相机和通信设备构成。具体地说，解密权限改变设备 5 例如为移动电话（如智能电话）、PDA（个人数字助理）和个人计

算机。注意，解密权限改变设备 5 中包括的通信设备是能连接到诸如移动电话网的网络的通信模块。在第二实施方式中，如此的解密权限改变设备 5 的未例示的存储器安装有解密权限改变程序作为应用，该解密权限改变程序的处理流程在图 33 中示出。

图 29 是例示当解密权限改变设备 5 中的未例示的 CPU 执行上述解密权限改变程序时由 CPU 实现的各个功能的框图。具体地说，如图 29 所示，解密权限改变设备 5 的功能包括输入单元 51、控制单元 52、受让人列表 53、输出单元 54 和通信单元 55。

输入单元 51 获取经由键盘输入的文档 ID、每个加密区域的区域 ID、以及收件人（权限让与人）的名称和关于每个加密区域的代理（权限受让人）的选择性信息。注意，可以指定个人为代理，并且可以指定包括个人的组为代理。在后一情况下，获取分配给该组的密码。该方案使得能够与每个加密区域的机密性的级别对应地对代理的访问权限给出差别。然后，输入单元 51 向控制单元 52 通知由此获取的文档 ID、以及每个加密区域对应的区域 ID 和权限受让人。此外，输入单元 51 向输出单元 54 通知加密文档数据 I，用于将数据 I 作为用于操作者输入用于指定加密区域的位置的信息的参考而显示在显示器 50 上。

受让人列表 53 是列出拥有解密权限改变设备 5 的操作权限的收件人（权限改变者）的名称（ID）、和预先登记的个人代理（受让人）的名称（ID）的列表，并且存储在存储器中。

控制单元 52 针对输入通知的文档 ID 和加密区域的区域 ID 或位置指定信息的每个组合，产生权限改变信息 M（图 36），所述权限改变信息 M 由输入单元 51 通知的收件人（让与人）的名称（ID）以及输入单元 51 通知的以与权限受让人相关联的方式存储在受让人列表 53 中的代理（受让人）的名称（ID）组成。然后，控制单元 52 向输出单元 54 和通信单元 55 通知该权限改变信息 M。

输出单元 54 在显示器 50 上显示输入单元 51 所通知的加密文档数据 I 的内容、和控制单元 52 所通知的未加密的权限改变信息 M 的内容，以用于检查。

通信单元 55 将控制单元 52 所通知的权限改变信息 M 经由通信线路或红外线通信, 传输到解密权限管理设备 6。

注意, 当收件人接收到通过电子邮件传输的加密文档数据 I 时, 在解密权限改变设备 5 暂时接收到电子邮件后, 在另一情况下收件人可以将该电子邮件转发给代理, 并且还可以通过使用另一终端 (如解密设备 7) 转发电子邮件, 所述另一终端的操作权限由收件人他自己或她自己拥有。

[解密权限管理设备]

接下来, 解密权限管理设备 6 是这样的服务器设备, 其对于文档 ID 和区域 ID 的每个组合, 对经由网络分别从加密设备 4 和解密权限改变设备 5 接收的解密权限信息 R 和权限改变信息 M 进行比对, 将在解密权限信息 R 中的“解密权限”字段中给出的描述改变为在权限改变信息 M 中包含的收件人 (让与人) 的名称 (ID) 和代理 (受让人) 的名称, 此后, 当从解密设备 7 接收到解密请求消息时, 只要解密设备 7 的操作者是由此改变的解密权限信息 R 中的“解密权限”字段中描述的操作者, 所述服务器设备就发送解密权限信息中包括的密码作为响应 (图 37)。该解密权限管理设备 6 由包括 CPU (未例示) 的服务器主体 60、安装有解密权限管理程序的盘设备 (未例示)、以及通信接口和存储有数据的存储设备 61 构成, CPU 通过该解密权限管理程序执行图 34 中例示的处理流程的处理。

图 30 是例示当未例示的 CPU 执行在解密权限管理设备 6 中的解密权限管理程序时、由该 CPU 实现的功能的框图。具体地说, 如图 30 所示, 解密权限管理设备 6 的功能包括接收单元 62、控制单元 63、解密权限信息存储单元 64 和发送单元 65。

接收单元 62 获取经由通信接口从加密设备 4 接收的解密权限信息 R、从解密权限改变设备 5 接收的权限改变信息 M、以及从解密设备 7 接收的解密请求、代理 ID、文档 ID 和区域 ID。然后, 接收单元 62 向控制单元 63 通知由此获取的解密权限信息 R、权限改变信息 M、解密请求、代理 ID、文档 ID 和区域 ID。

解密权限信息存储单元 64 是响应于从控制单元 63 给出的指令在存

储部 61 中存储解密权限信息 R 并且改变和读取解密权限信息 R 的功能。

控制单元 63 向解密权限信息存储单元 64 通知接收单元 62 所通知的解密权限信息 R，将该解密权限信息 R 存储在存储部 61 中，并且指示发送单元 65 给出关于是否成功存储解密权限信息 R 的响应。此外，控制单元 63 根据接收单元 62 所通知的权限改变信息 M，改变在解密权限信息 R 中的“解密权限”字段中的描述，并且指示发送单元 65 发送关于是否成功改变描述的响应。例如，当被通知关于具有图 10 所例示的内容的解密权限信息 R 的、具有图 36 所例示的内容的权限改变信息 M 时，将权限改变信息 M 中包含的“受让人”部门负责人 B 添加到下述解密权限信息 R 中的下述条目（记录）中的“解密权限”字段“经理 A”的描述中，所述条目（记录）包含与权限改变信息 M 中的区域 ID 相同的区域 ID：03，所述解密权限信息 R 包含与权限改变信息 M 中的文档 ID 相同的文档 ID：2008-0107-1400。结果，如图 37 所示更新解密权限信息 R。

此外，当控制单元 63 从接收单元 62 接收到解密请求的通知时，所述控制单元 63 认证接收单元 62 随后所通知的代理（译码者）的名称（ID），并且指令发送单元 65 发送关于是否成功认证的响应。此外，在成功认证的情况下，如果在与接收单元 62 随后所通知的文档 ID 和区域 ID 的元组相关联的权限改变信息 M 的“解密权限”字段中包含与接收单元 62 所通知的代理（译码者）的名称（ID）相关联的代理（受让人）的名称（ID），则向发送单元 65 通知从解密权限信息 R 内读取的密码，而在其他情况下，向发送单元 65 通知权限错误消息。

发送单元 65 经由通信接口，对加密设备 4、解密权限改变设备 5 或解密设备 7 给出关于是否成功的响应，并且将控制单元 63 所通知的密码或权限错误消息传输到作为解密请求发送者的解密设备 7。

[解密设备]

接下来，解密设备 7 是由代理操作的计算机系统，并且由具有通常配置的个人计算机（PC）70 以及与 PC 70 连接的扫描仪 71 构成，所述 PC 70 包括显示器 72、CPU（未例示）、盘设备（未例示）和通信接口，并且安装有用于使得 CPU 执行盘设备中的处理流程的如图 35 所示的处

理的解密程序。解密设备 7 基于该解密程序，从加密设备 41 直接接收加密文档数据 I，或者从收件人转发的电子邮件或传真信号中提取加密文档数据 I，或者用扫描仪 71 读取收件人转交或发送的打印材料 P 上的加密文档数据 I。此外，解密设备 7 根据从操作者（代理，译码者）给出的、经由键盘输入的命令，将上述解密请求传输到解密权限管理设备 6，并且响应于该解密请求，通过使用从解密权限管理设备 6 发送的密码，对加密文档数据 I 中的加密区域进行解密，从而恢复原始文档数据。

图 31 是例示当未例示的 CPU 执行解密设备 7 中的解码程序时、由 CPU 实现的功能的框图。即，如图 31 所示，解密设备 7 的功能包括输入单元 73、控制单元 74、解密单元 75、输出单元 76 和通信单元 77。

输入单元 73 获取经由扫描仪 71 输入的打印材料 P 上的加密文档数据 I，并且获取经由鼠标和键盘输入的文档 ID、加密区域的区域 ID 以及拥有解密设备 3 的操作权限的代理（译码者）的名称（ID）。然后，输入单元 73 向控制单元 74 通知由此获取的加密文档数据 I 和与每个加密区域相关联的区域 ID 或位置指定信息、以及代理（译码者）的名称（ID）。此外，输入单元 73 向输出单元 76 通知加密文档数据 I，用于将数据 I 显示在显示器 72 上，作为操作者输入用于指定加密区域的位置的位置指定信息时的参考。

通信单元 77 获取经由通信接口接收的电子邮件或传真信号中的加密文档数据 I，并且作为响应，将加密文档数据 I 发送到控制单元 74 和输出单元 76。此外，通信单元 77 响应于从控制单元 74 给出的指令，经由通信接口将解密请求等传输到解密权限管理设备 6，然后，接收从解密权限管理设备 6 响应于该请求而作为响应发送的密码，并且向控制单元 74 通知该密码。

控制单元 74 指示通信单元 77 传输解密请求和输入单元 73 所通知的代理（译码者）的名称（ID）、文档 ID 和区域 ID。此外，控制单元 74 向解密单元 75 通知从通信单元 77 接收的密码以及输入单元 33 所通知的区域 ID 和加密文档数据 I，并且请求解密单元 75 解密与区域 ID 相关联的加密区域。然后，在接收到关于能够从解密单元 75 解密的所有加密区

域的解密文档数据（已经解密的文档数据）时，控制单元 74 向输出单元 76 通知该已经解密的文档数据。

只要拥有解密设备 7 的操作权限的代理可以解密，解密单元 75 就通过采用从控制单元 74 接收的密码，针对由从控制单元 74 接收的区域 ID 指定的每个加密区域，解密从控制单元 74 接收的加密文档数据 I，并且将作为解密结果的已经解密的文档数据通过响应发送到控制单元 74。

输出单元 76 在显示器 72 上显示输入单元 73 或通信单元 77 所通知的加密文档数据 I、以及控制单元 74 所通知的已经解密的文档数据。

<数据处理流程>

以下将参照图 32 到图 35，描述构成第二实施方式中的如此配置的文档数据加密系统的加密设备 4、解密权限改变设备 5、解密权限管理设备 6 和解密设备 7 的操作权限的数据处理流程。

[加密设备]

图 32 是例示 CPU 根据安装到加密设备 4 的盘设备中的加密程序执行的加密处理的流程图。通过向键盘输入用于读取原始文档数据的预定命令而触发基于该流程图的处理的开始。加密处理中的 S301 到 S308 的处理与图 5 中的 S001 到 S008 的处理完全相同，因此省略其说明。

在当对要求加密的所有区域完成 S303 到 S307 的处理时执行的 S309 中，如图 10 所示，加密设备 4（文档数据加密单元 44）产生表格格式的解密权限信息 R，其中每一个记录包括文档 ID、区域 ID（光栅扫描序列中分配给在 S303 指定其位置的加密区域的序列号）、区域位置信息（其位置在 S303 指定的加密区域的坐标范围）、密码和解密权限。

在下一步骤 S310，加密设备 4（输出单元 45）将在 S309 产生的解密权限信息 R 经由通信接口传输到解密权限管理设备 6，并且请求解密权限管理设备 6 登记该信息。

在下一步骤 S311，加密设备 4 检查作为 S311 的请求的结果，是否存在声明在解密权限管理设备 6 的存储部 6 中登记了解密权限信息 R 的响应。然后，如果存在声明登记了解密权限信息 R 的响应，则加密设备 4（输出单元 45）根据经由键盘输入的发送者的指定，将对所有加密区域

完成了加密处理的加密文档数据 I 作为打印材料 P 从打印机输出，并且以附到电子邮件或在传真信号上携带的方式将加密文档数据 I 传输到收件人。

而如果不存在声明登记了解密权限信息 R 的响应，或者如果存在声明登记失败的响应，则加密设备 4（输出单元 45）在显示器 42 上显示声明在解密权限信息 R 的登记中出现错误的消息。

在完成 S312 或 S313 后，加密设备 4 完成基于该加密处理程序的所有处理。

[解密权限改变设备]

图 33 是例示由 CPU 根据安装到解密权限改变设备 5 的存储器中的权限改变程序执行的加密处理的流程图。通过向键盘输入预定命令来触发基于该流程图的处理的开始。在开始该加密处理后的第一步骤 S401，解密权限改变设备 5（输出单元 54）在显示器 50 上显示用于接受文档 ID 的输入的 GUI 画面（见图 11）。请求收件人将在打印材料 P 的头部区域中打印的文档 ID 输入到 GUI 画面上的文本框。

在下一步骤 S402，解密权限改变设备 5（输入单元 51，控制单元 52）获取通过针对在 S401 显示的 GUI 画面对键盘的操作而输入的文档 ID。

随后，执行 S403 到 S407 的循环处理，用于获取加密文档数据 I 的每个加密区域的密码。在进入该循环处理之后的第一步骤 S403，解密权限改变设备 5（输出单元 54）在显示器 20 上显示用于接受区域 ID 的输入的 GUI 画面（见图 24）。

在下一步骤 S404，解密权限改变设备 5（输入单元 51，控制单元 52）获取通过针对在 S403 显示的 GUI 画面对键盘的操作而输入的区域 ID。

在随后的步骤 S405，解密权限改变设备 5（输出单元 54）在显示器 50 上显示用于接受与在 S404 获取的区域 ID 相关联的收件人（权限让与人）的名称（ID）的输入的 GUI 画面（未例示）。

在下一步骤 S406，解密权限改变设备 5（输入单元 51，控制单元 52）获取通过针对在 S405 显示的 GUI 画面对键盘的操作而输入的收件人（权限让与人）的名称（ID）。

在随后的步骤 S407，解密权限改变设备 5 检查发送者是否经由键盘输入仍有未处理的加密区域的声明或对于所有加密区域的处理终止的声明。然后，如果发送者输入仍有未处理的加密区域的声明，则解密权限改变设备 5 将操作循环回到 S403，以便执行对于未处理的加密区域的循环处理。而如果输入加密区域的处理终止的声明，则处理进行到 S408。

随后，执行 S408 到 S412 的循环处理，用于针对加密文档数据 I 的每个加密区域获取权限受让人。在进入该循环处理后的第一步骤 S408，解密权限改变设备 5（输入单元 51，控制单元 52）指定在 S404 获取的未处理的区域 ID 中的一个。

在下一步骤 S409，解密权限改变设备 5（输出单元 54）为获取关于由在 S408 指定的区域 ID 标识的加密区域的权限受让人，在显示器 50 上显示用于接受权限受让人的输入的 GUI 画面（见图 26）。

在随后的步骤 S410，解密权限改变设备 5（输入单元 51，控制单元 52）获取通过针对在 S408 显示的 GUI 画面对键盘的操作而选择的权限受让人。

在下一步骤 S411，解密权限改变设备 5（输出单元 54）在显示器 50 上显示关于在 S408 指定的区域 ID 的权限改变内容，即，在 S410 获取的权限受让人的名称。

在下一步骤 S412，解密权限改变设备 5（输入单元 51，控制单元 52）检查是否在 S408 完全指定了所有加密区域的区域 ID。然后，如果还没有完全指定所有加密区域的区域 ID，则处理循环回到 S408。而如果完全指定了所有加密区域的区域 ID，则处理进行到 S413。

在 S413，解密权限改变设备 5（控制单元 52）针对每个区域 ID 将根据区域 ID 而在 S406 获取的收件人的名称（ID）、在 S410 获取的权限受让人的名称（ID）以及在 S402 获取的文档 ID 组合起来，从而产生以图 36 所示的格式的权限改变信息 M。

在下一步骤 S414，解密权限改变设备 5（控制单元 52，通信单元 55）将在 S413 产生的权限改变信息 M 传输到解密权限管理设备 6，并且请求解密权限管理设备 6 更新具有相同文档 ID 的解密权限信息 R。

在随后的步骤 S415, 解密权限改变设备 5 (控制单元 52, 通信单元 55) 检查是否存在声明作为 S414 的请求的结果而完全改变了解密权限信息 R 的响应。然后, 在接收到声明完全改变了解密权限信息 R 的响应的情况下, 解密权限改变设备 5 (输出单元 54) 在显示器 50 上显示声明完全改变了解密权限信息 R 的消息。

相反, 在没有接收到声明完全改变了解密权限信息 R 的响应或者接收到解密权限信息 R 的改变失败的声明的情况下, 解密权限改变设备 5 (输出单元 54) 在显示器 50 上显示声明在改变解密权限信息 R 中出现错误的消息。

在完成 S416 或 S417 后, 解密权限改变设备 5 完成基于该权限改变处理程序的所有处理。

[解密权限管理设备]

图 34 是例示在由 CPU 根据安装到解密权限管理设备 6 的盘设备中的解密程序执行的处理中、当从解密设备 7 接收到解密请求时执行的处理的流程图。在开始该流程图中的处理后的第一步骤 S501 中, 解密权限管理设备 6 (控制单元 63) 等待从解密设备 7 传输的代理 (译码者) 的名称 (ID), 从而获取所述名称 (ID)。

在下一步骤 S502, 解密权限管理设备 6 (控制单元 63) 根据已知方法, 执行关于在 S501 获取的代理 (译码者) 的名称 (ID) 的认证处理。例如, 解密权限管理设备 6 (控制单元 63) 预先在存储部 61 中登记每个个人译码者的名称 (ID) 和密码的元组, 并且如果在存储部 61 中登记有代理 (译码者) 的名称 (ID) 和附于该名称而传输的密码的元组, 则证明认证成功。然后, 如果在 S502 中认证不成功, 则解密权限管理设备 6 (控制单元 63) 在 S510, 经由发送单元 65, 向作为解密请求者的解码设备 7 通知译码者的认证的错误, 并且终止该处理。

而如果在 S502 中认证成功, 则解密权限管理设备 6 向解密设备 7 通知已经在 S503 中登记了译码者的声明。在完成 S503 后, 解密权限管理设备 6 将处理前进到 S504。

在 S504, 解密权限管理设备 6 等待由解密设备 7 传输的文档 ID, 由

此获取文档 ID。

随后，解密权限管理设备 6 执行在 S505 到 S509 的循环处理，以便传输关于由在 S504 获取的文档 ID 指定的加密文档数据的每个加密区域的密码。在进入该循环处理之后的第一步骤 S505，解密权限管理设备 6 等待由解密设备 7 传输的区域 ID，由此获取所述区域 ID。

在下一步骤 S506，解密权限管理设备 6 基于知道在包含在 S504 获得的文档 ID 的解密权限信息 R 中、在 S503 获取的区域 ID 的条目中的“解密权限”字段中是否包含在 S501 获取的译码者的名称（ID），确定由区域 ID 指定的解密权限。然后，如果因为在“解密权限”字段中包含译码者的名称（ID）而允许解密权限，则解密权限管理设备 6（控制单元）将针对加密区域的密码传输到解密设备 7，并将处理前进到 S509。

而如果因为在“解密权限”字段中不包含译码者的名称（ID）而不允许解密权限，则解密权限管理设备 6（控制单元）将解密权限错误消息传输到解密设备 7，并将处理前进到 S509。

在 S509，解密权限管理设备 6 检查是否完成从解密设备 7 通知区域 ID。然后，如果解密设备通知下一区域 ID，则解密权限管理设备 6 将处理循环回到 S504。相反，如果解密设备 7 不传输下一区域 ID（如果预定超时时间段经过，或者如果解密设备 7 通知结束消息），则解密权限管理设备 6 终止该处理。

[解密设备]

图 35 是例示由 CPU 根据安装到解密设备 7 中的解密程序执行的解密处理的流程图。通过向键盘输入预定命令来触发基于该流程图的处理的开始。在开始该解密处理之后的第一步骤 S601，解密设备 7（输入单元 33 或通信单元 37）以上述方式获取解密目标加密文档数据 I。

在下一步骤 S602，解密设备 7（输出单元 36）在显示器 32 上显示在 S601 获取的加密文档数据 I。

在随后的步骤 S603，解密设备 7（控制单元 34）获取在 S601 获得的加密文档数据 I 的文档 ID。具体地说，在通过电子邮件获得加密文档数据 I 的情况下，解密设备 7（控制单元 34）从在文档数据的头部中存储的

解密权限信息 R 提取文档 ID。相反,在用扫描仪 31 或通过传真信号获取加密文档数据 I 的情况下,通过与图 6 中的 S401 和 S402 中相同的处理获得文档 ID。

在下一步骤 S604,解密设备 7(控制单元 74)获取解密设备 7 的个人操作者(译码者)的名称(ID)和密码、以及操作者(译码者)所属的组的名称(ID)和密码。可通过读取例如 IC 卡中存储的所述信息项来获取名称(ID),并且还可经由在显示器 72 上显示的 GUI 画面来获取名称(ID)。

在下一步骤 S605,解密设备 7(控制单元 74)将解密请求和在 S604 获取的译码者的名称(ID)和密码传输到解密权限管理设备 6。

在随后的步骤 S606,解密设备 7(控制单元 74)基于在 S502 由解密权限管理设备 6 进行认证的结果,确定认证是否成功。然后,如果认证失败(在 S503 接收到错误消息的情况下),则在 S607,解密设备 7 在显示器 72 上显示还没有请求解密的错误,并终止该解密处理。

相反,如果认证成功,则在 S608,解密设备 7 从在 S601 获取的加密文档数据 I 检测加密区域,并且计算各个位置(头部坐标)。

在下一步骤 S609,解密设备 7 根据在 S608 计算的各个加密区域的头部坐标,基于符合光栅扫描顺序的序列确定各个区域 ID。

随后,解密设备 7 执行 S610 到 S617 的循环处理,以用于对每个加密区域执行解密。在进入该循环处理之后的第一步骤 S610,解密设备 7 选择任一加密区域。

在下一步骤 S611,解密设备 7 将在 S603 获取的文档 ID 传输到解密权限管理设备 6。

在随后的步骤 S612,解密设备 7 将在 S610 选择的加密区域的、在 S609 确定的区域 ID 传输到解密权限管理设备 6。

在下一步骤 S613,解密设备 7 等待由解密权限管理设备 6 在 S507 传输的密码、或在 S508 传输的解密权限错误(消息),并且当接收到密码和错误消息中的任何一个时,在下一步骤 S614 检查是否成功获取密码。然后,如果未能获取密码,即,在接收到解密权限错误的情况下,解密

设备 7 将处理直接前进到 S617。

而如果成功获取密码,则在 S615,解密设备 7 通过使用在 S613 获得的密码,解密在 S610 选择的加密区域。

在下一步骤 S616,解密设备 7 在显示器 72 上显示作为到该时间点执行的 S615 的结果而获得的已经解密的文档数据。当完成 S616 时,解密设备 7 将处理前进到 S617。

在 S617,解密设备 7 检查是否仍有未处理的区域。然后,如果仍有未处理的区域,则解密设备 7 将处理循环回到 S610。而如果没有未处理的区域,则解密设备 7 终止该解密处理。

<实施方式的操作>

以下将参照图 38 和 39,描述由此配置的根据第二实施方式的文档数据加密系统的操作。以与图 16 的情况相同的方式,这里假设当具有加密设备 4 的操作权限的文档数据发送者向收件人“经理”传递加密文档数据 I (或传输加密文档数据 I,或发布打印材料 P) 时,收件人“经理”他自己或她自己既不执行解密,也不执行随后用于由文档数据指定的文档的处理,而是请求代理“部门负责人”担任“经理”。然后,还假设发送者知道要在发送者和“经理”之间使用的“经理”的一条或多条密码,然而,部门负责人不知道“经理”的任何密码。

然后,传递目标文档数据是由扫描仪等读入加密设备 4 或由加密设备 4 中的应用程序产生的文档的图像,在此通过诸如“IMAGE ENCRYPTION”、“ENCRYPTED IMAGE”、“IMAGE DECRYPTION”的字符串识别。然后,需要从第三方对这些字符串中包括“ENCRYPTION”和“DECRYPTION”的字符串进行加密。

因此,在发送者操作的加密设备 4 中,将显示要隐藏的字符串的三个区域指定为加密区域(S303),并且分别用“经理”的密码进行加密(S306),所述“经理”的密码作为与其关联的加密密码输入(S305)。作为其结果而获得的加密文档数据 I 被传递到“经理”。

然而,在上述情况下,将包含加密文档数据 I 的打印材料 P 或电子邮件从“经理”转发到部门负责人,或者在从“经理”接收到请求的发

送者他自己或她自己已经将目的地改变为部门负责人后，最终由部门负责人接收打印材料 P 或电子邮件。

与此同时，加密设备 4 产生解密权限信息 R，所述解密权限信息 R 关于加密文档数据 I 的每个区域，列出区域 ID、位置信息（坐标）、用于加密和解密权限的“经理”的密码（S309），并且将该解密权限信息 R 传输到解密权限管理设备 6（S310）。

另一方面，“经理”将文档 ID 和每个区域 ID 输入到解密权限改变设备 5，并且针对每个区域 ID 输入自己的名称（ID）和部门负责人的名称（ID）（S402，S404，S406，S408）。然后，解密权限改变设备 5 针对每个加密区域产生由文档 ID、区域 ID、作为权限让与人的“经理”的名称（ID）、和作为权限受让人的部门负责人的名称（ID）组成的权限改变信息 M（S413），并且将该信息 M 传输到解密权限管理设备 6（S414）。

解密权限管理设备 6 将从加密设备 4 接收的解密权限信息 R 存储在存储部 61 中，此后，当从解密权限改变设备 5 接收到权限改变信息 M 时，另外在与权限改变信息 M 中的文档 ID 和区域 ID 相关联的解密权限信息 R 的解密权限字段中的前一信息中输入部门负责人的名称（ID）。

此后，操作解密设备 7 的部门负责人读取接收的加密文档数据 I 的文档 ID（S603），将自己的名称（ID）输入到解密设备 7（S604），并且将该信息传输到解密权限管理设备 6（S605，S501）。当解密权限管理设备 6 认证了接收到的部门负责人的名称（ID）时（S502），所述解密权限管理设备 6 向解密设备 7 通知该解密设备 7 已经被登记的声明（S503）。此后，解密设备 7 将文档 ID 和区域 ID 传输到解密权限管理设备 6（S611，S612，S504，S505），然后解密权限管理设备 6 基于解密权限信息 R 确定解密权限（S506），并且如果部门负责人的名称（ID）与这两个 ID 相关联地登记，则作为响应，将与其关联登记的密码发送到解密设备 7（S507）。解密设备 7 通过使用接收的密码，解密由文档 ID 指定的加密文档数据 I 中的由区域 ID 指定的加密区域（S613，S614）（S615），并且显示经解密的加密区域（S616）。因此，当解密了所有加密区域时，解密的文档数据与原始文档数据一致。

<第二实施方式的修改示例>

以与第一实施方式的修改示例相同的方式，不使用在先申请的成像处理（采用扰码的加密处理）的加密设备用诸如 PDF 的构造文档数据中的加黑点的图像替代指定为加密区域的区域，删除区域内的文档成分（字符，图形），针对各个区域用密钥（密码）加密所删除的文档成分，并且将加密的区域存储在文档数据的头部区域中。此外，本修改示例中的解密设备针对从解密权限管理设备接收的各个加密区域，通过使用解密密钥（密码），来解密文档数据的头部区域中包含的每个区域的文档成分，替代加密文档数据上的带黑点图像的文档成分，从而恢复文档数据。加密设备的加密单元和解密设备的解密单元具有与第一实施方式的修改示例中相同的配置和相同的操作，因此省略其说明。

这里陈述的所有示例和条件式语言意在教导目的，以帮助读者理解由发明人为推进本领域所贡献的发明和概念，并且应被解释为不限于这样具体陈述的示例和条件，说明书中的这些示例的组织也不涉及示出本发明的优劣。尽管已经详细描述了本发明的实施方式，但是应当理解，在不偏离本发明的精神和范围的情况下，可以对其进行各种变化、替代和更改。

本申请基于并要求 2008 年 8 月 18 日提交的在先日本专利申请 No. 2008-210171 的优先权，该申请的全部内容通过引用合并于此。

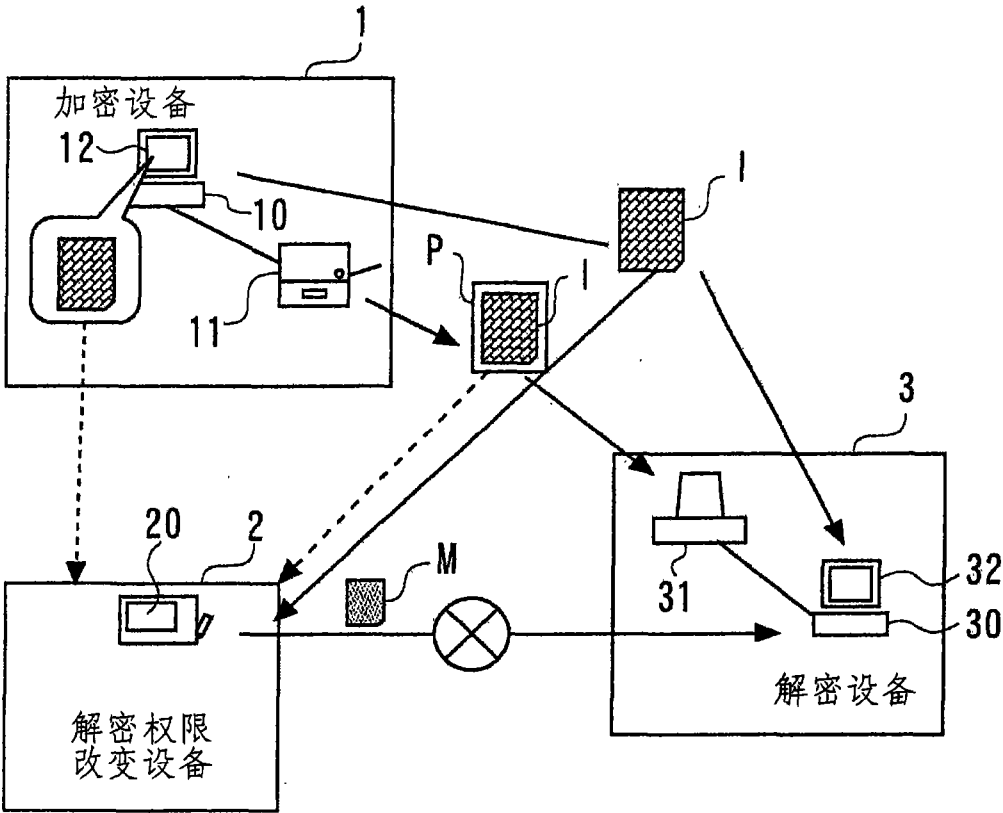


图 1

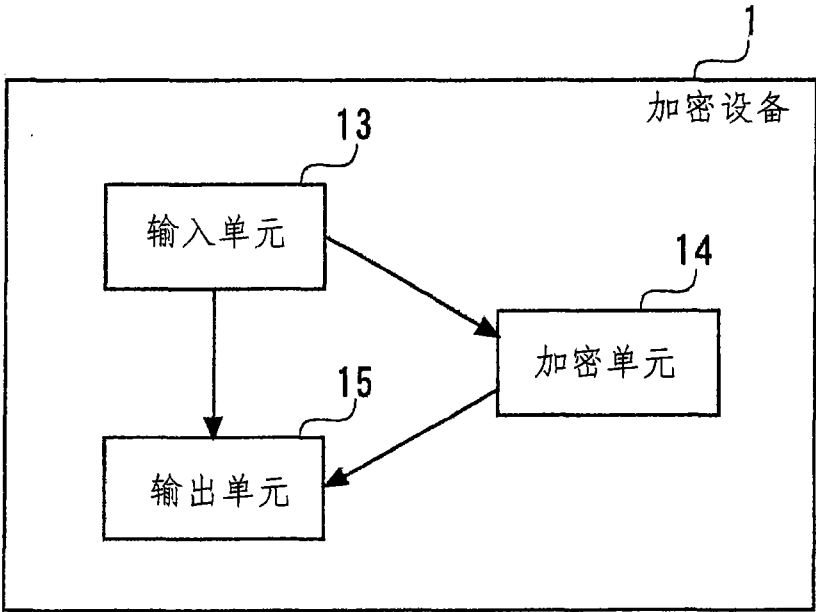


图 2

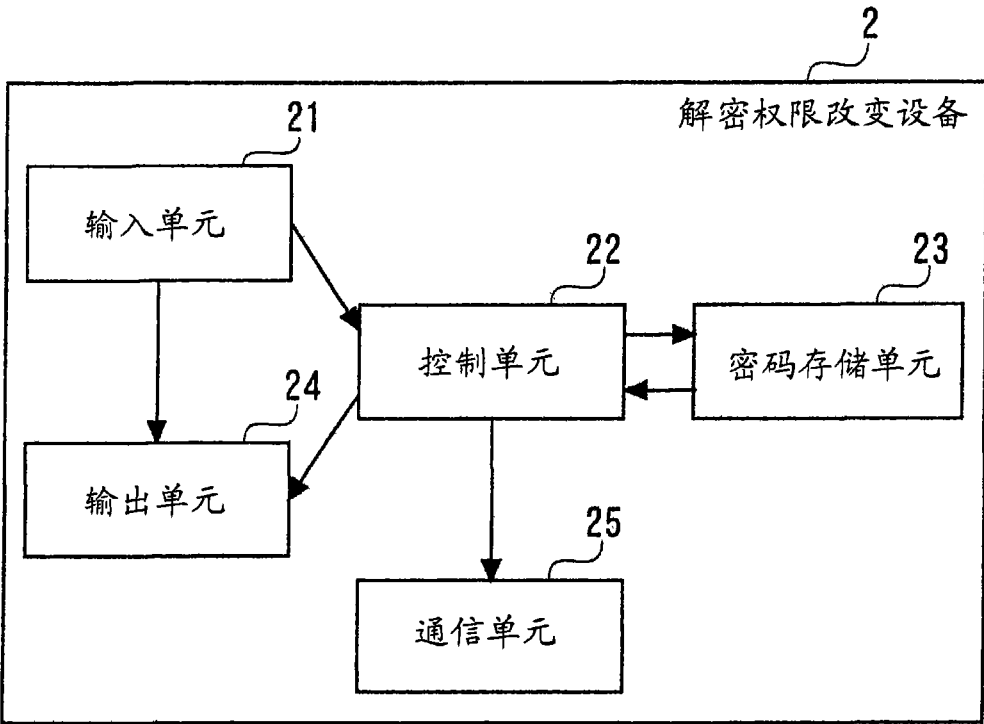


图 3

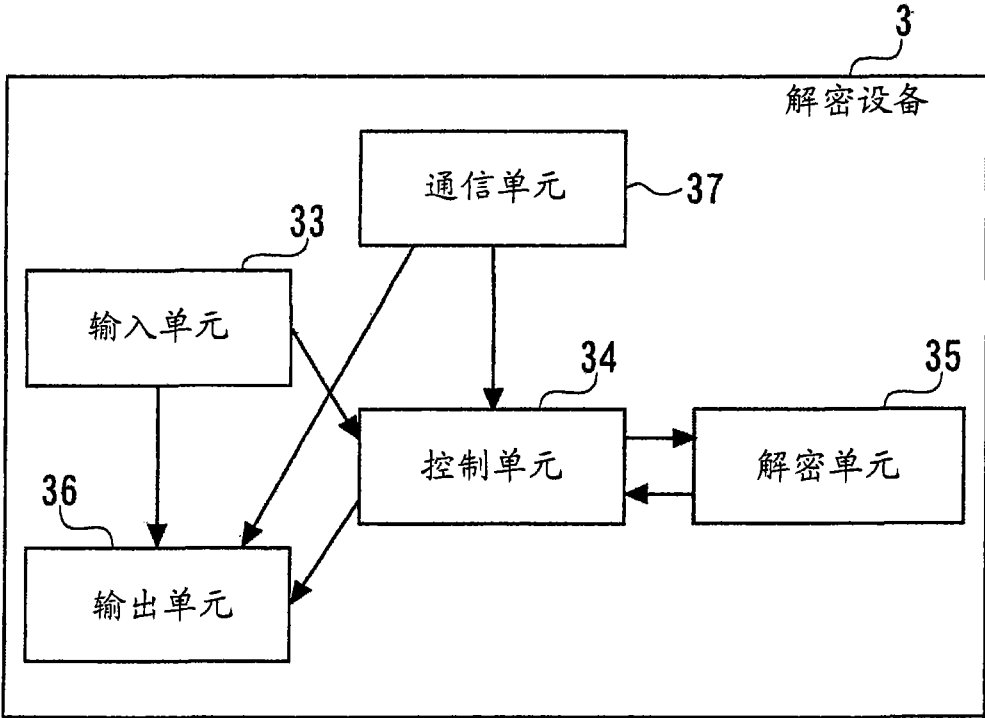


图 4

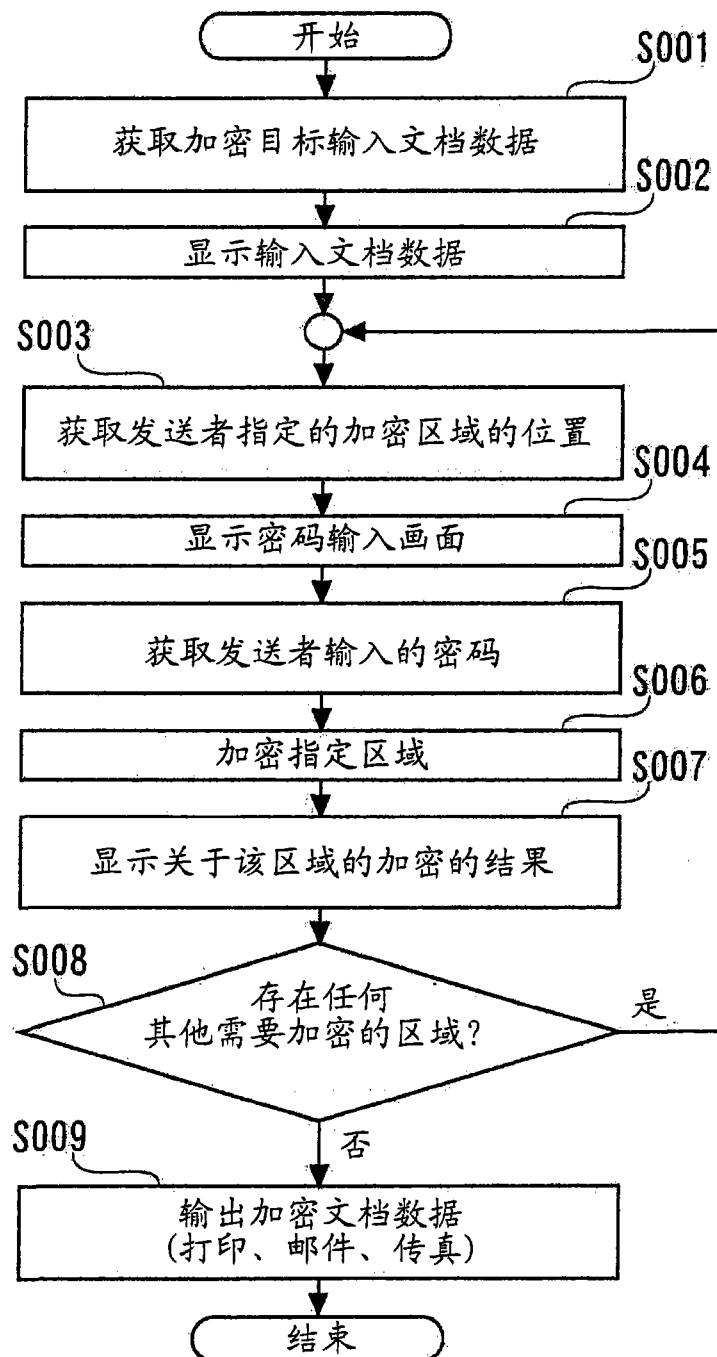


图5

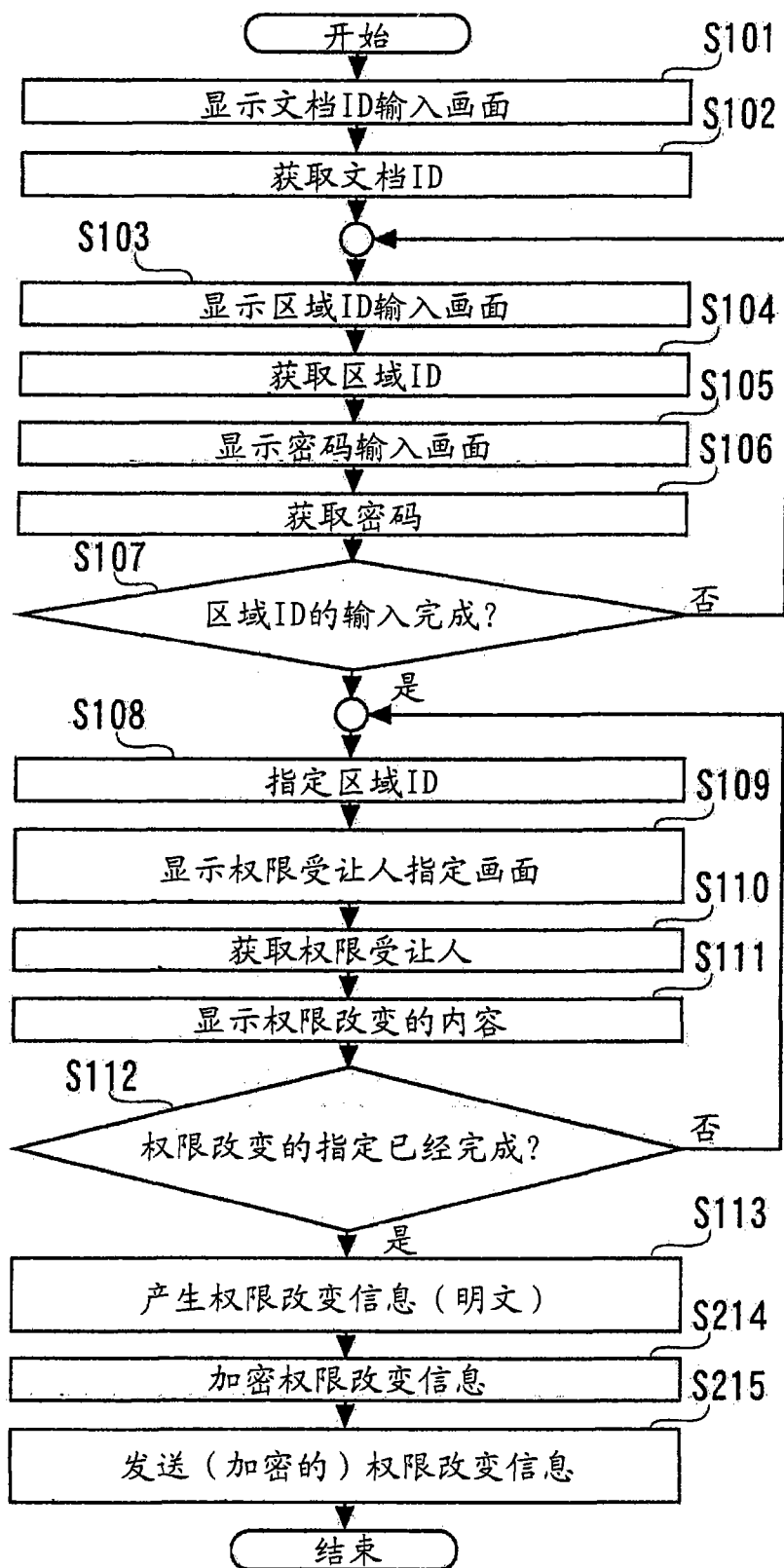


图6

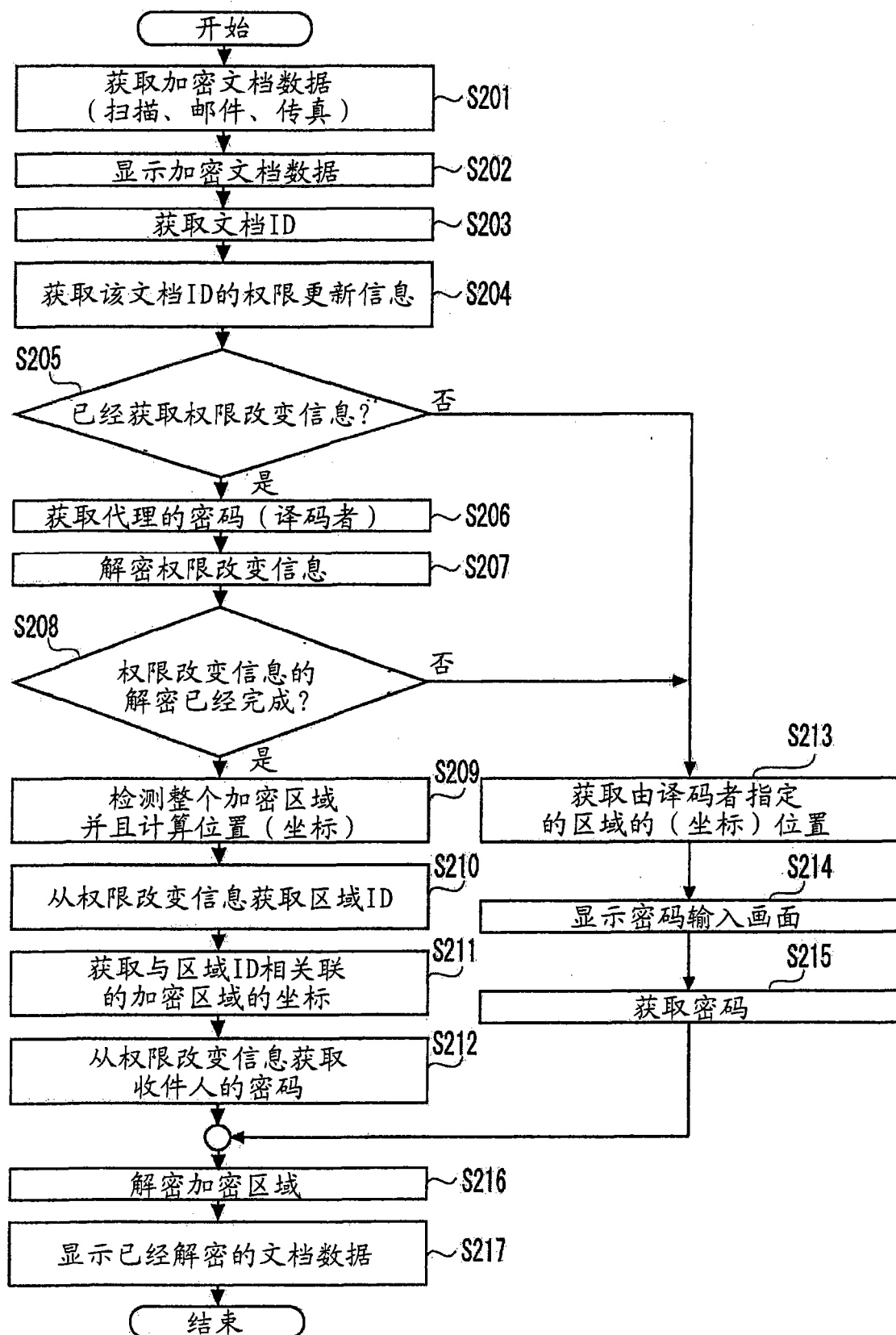


图7

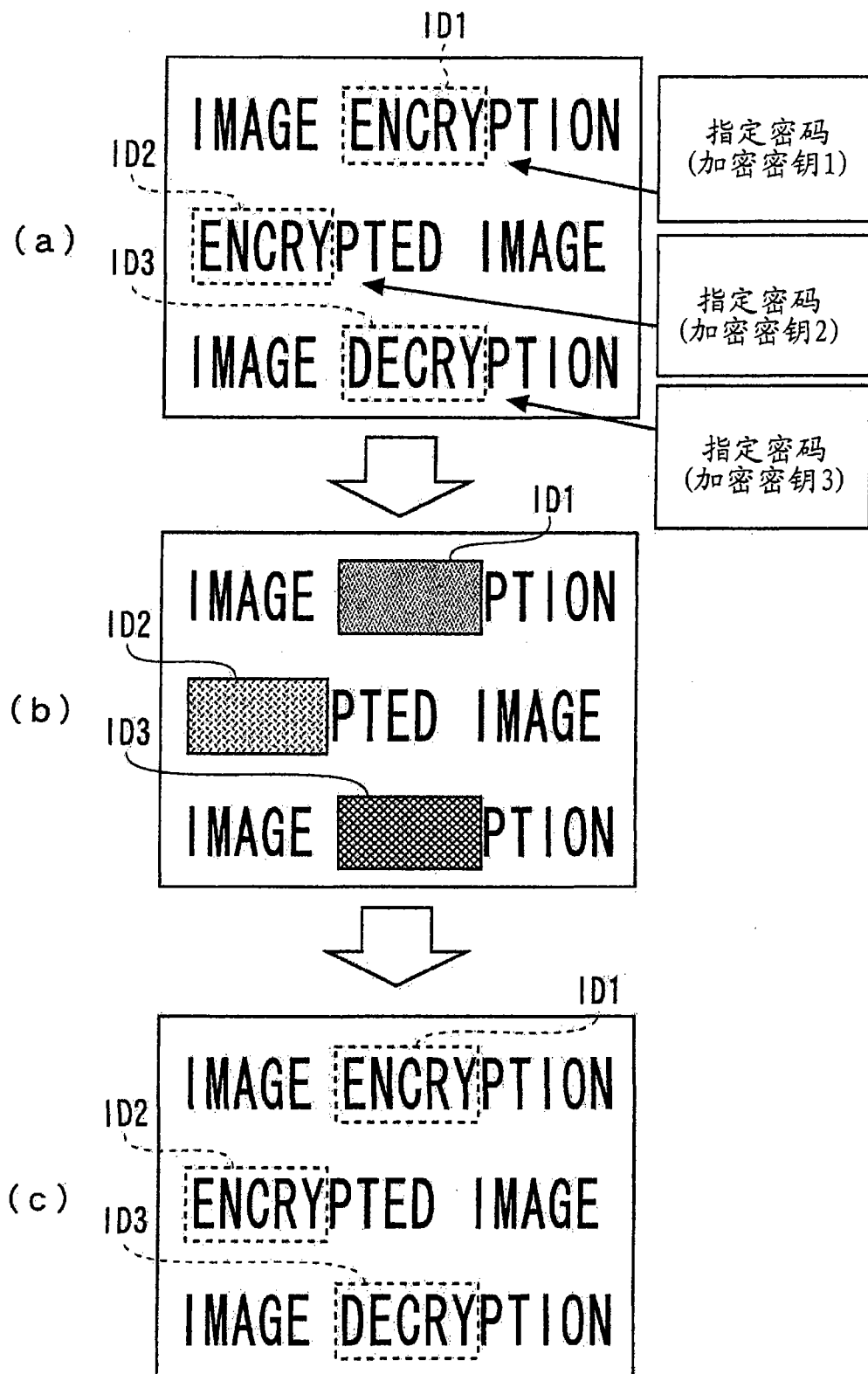


图8

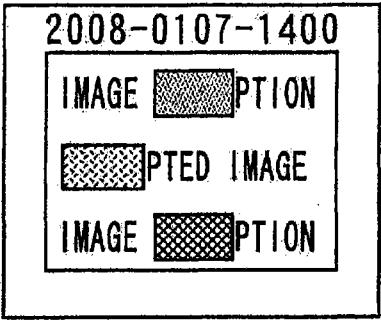


图9

解密权限信息

文档ID	区域ID	位置信息	密码	解密权限
2008-0107-1400	01	(290, 40) - (490, 140)	AD8CX65Y	公共C
2008-0107-1400	02	(75, 205) - (275, 305)	AD8CX65Y	公共C
2008-0107-1400	03	(295, 360) - (495, 460)	P90EAQ1H	经理A

图10

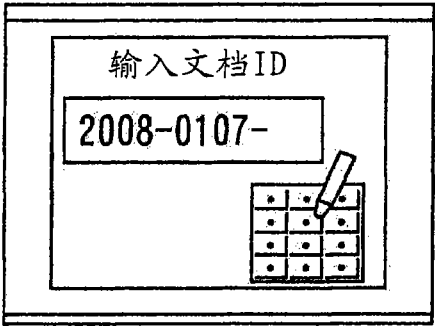


图 11

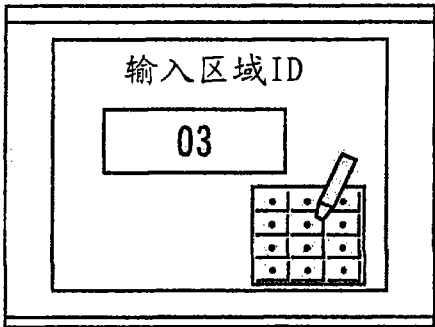


图 12

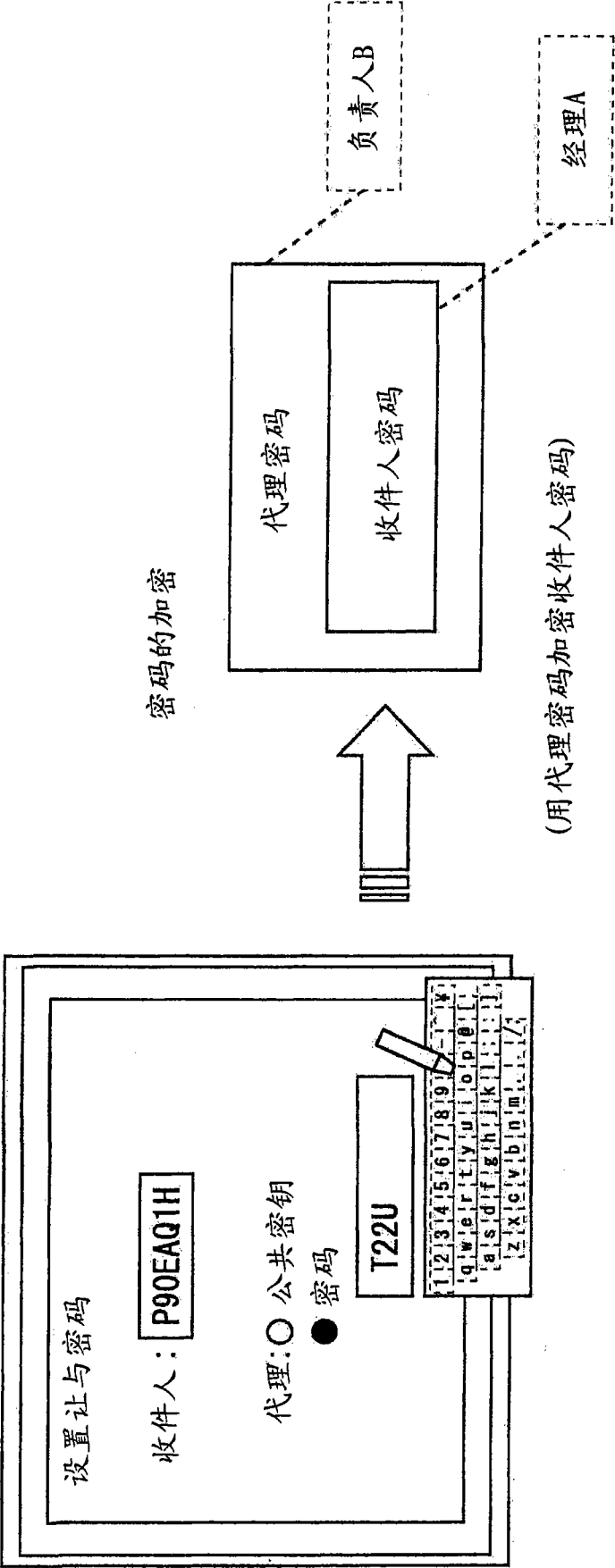


图13

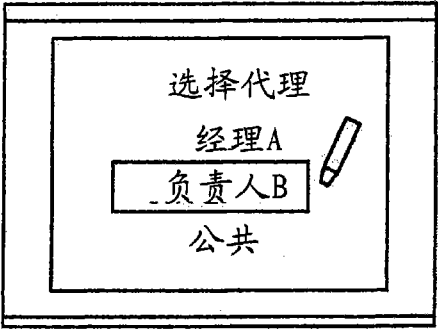


图 14

权限改变信息

文档ID	区域ID	密码	解密权限
2008-0107-1400	03	P90EAQ1H	负责人B

图 15

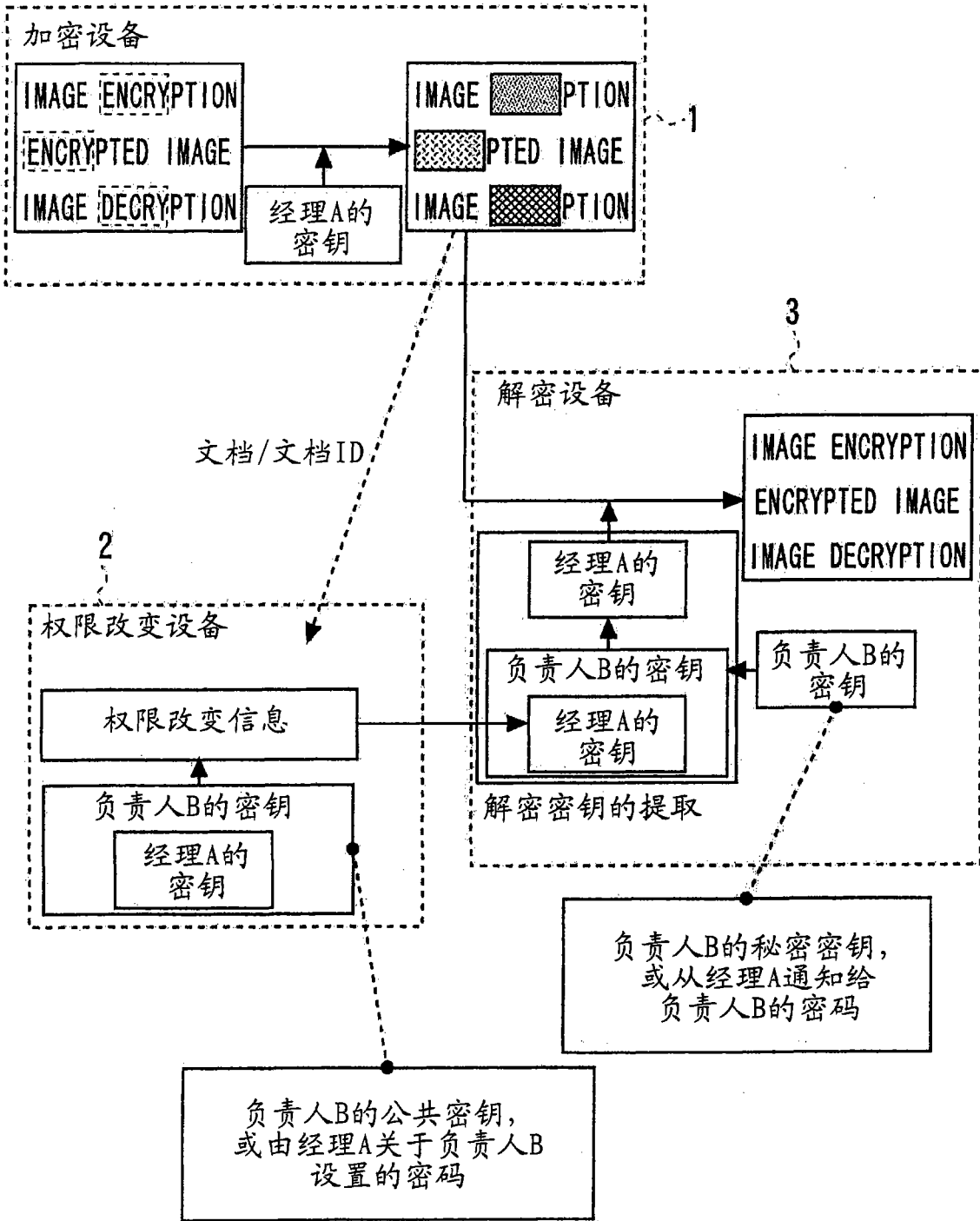


图16

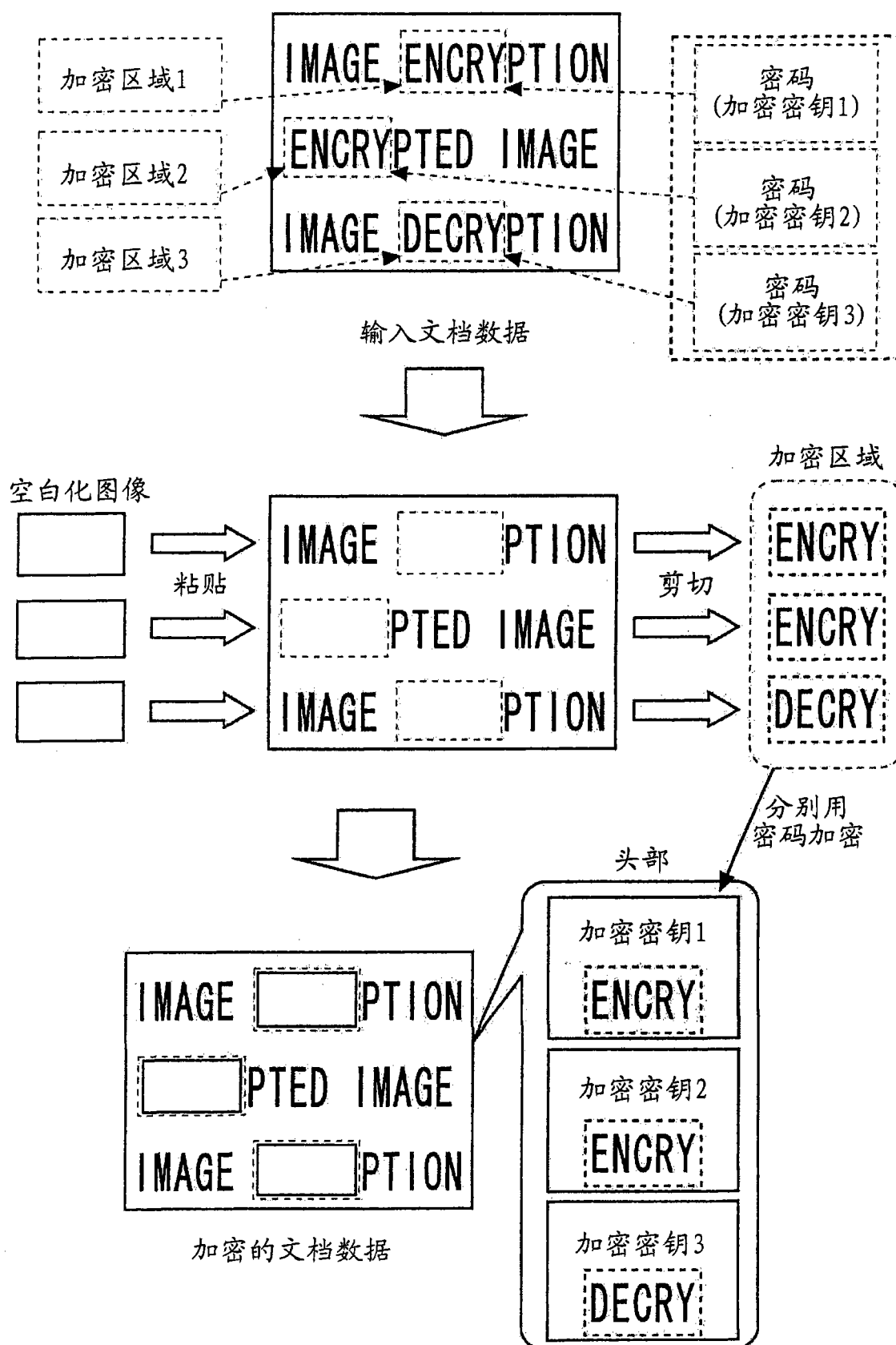


图 17

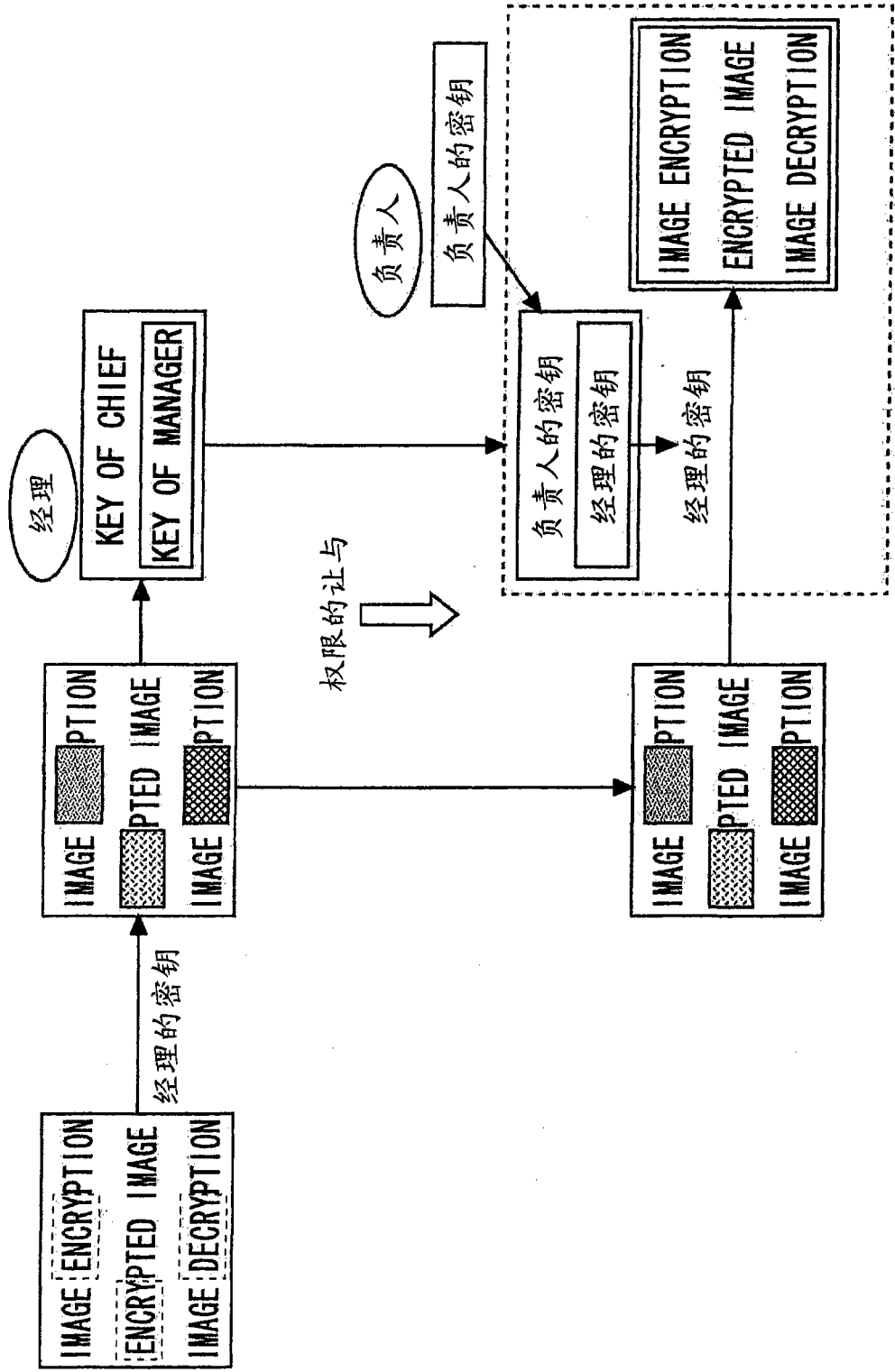


图18

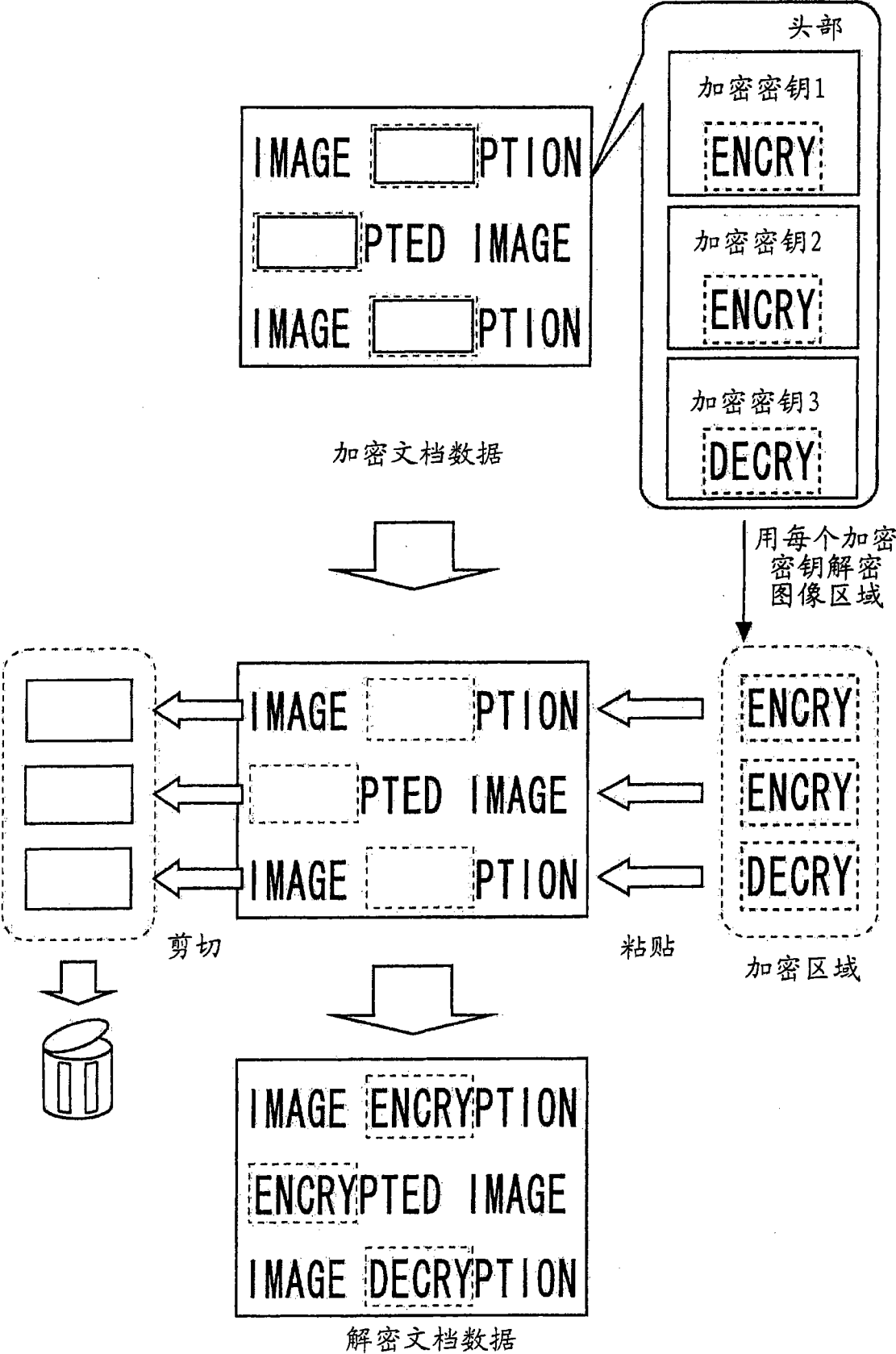


图19

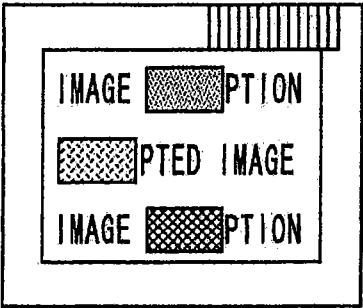


图 20

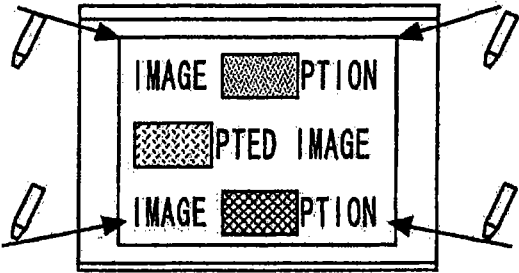


图 21

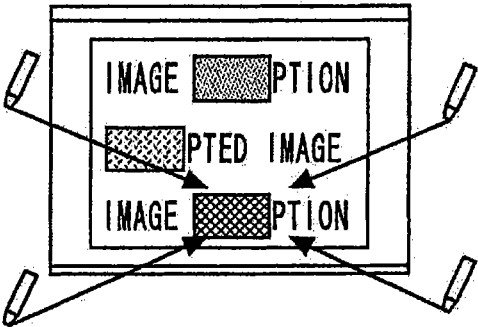


图 22

权限改变信息

文档ID	位置信息	密码(默认)	解密权限
2008-0107-1400	(295, 360) - (495, 460)	P90EAQ1H	负责人B

图 23

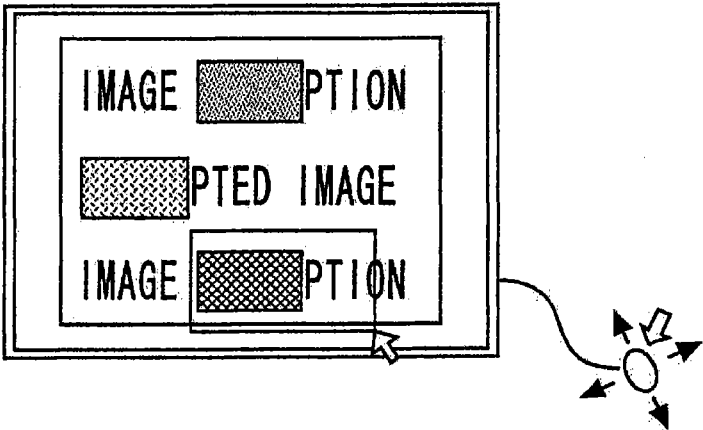


图 24

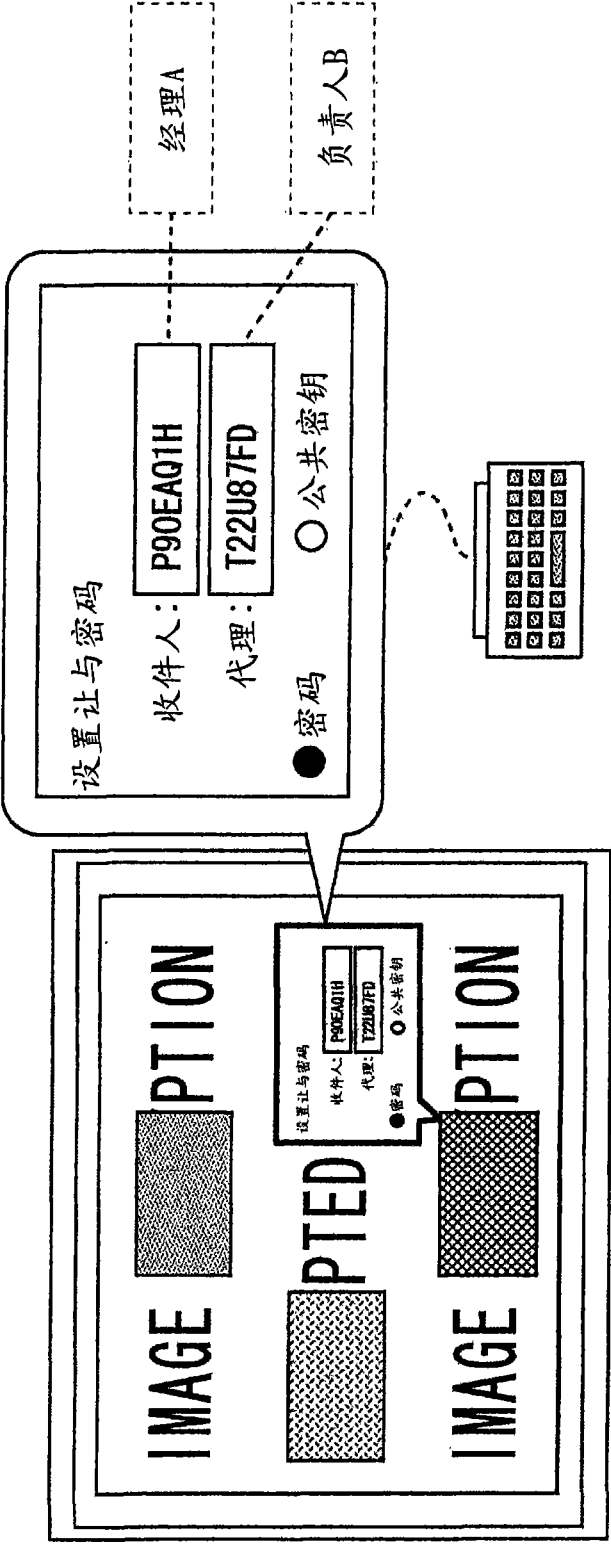


图25

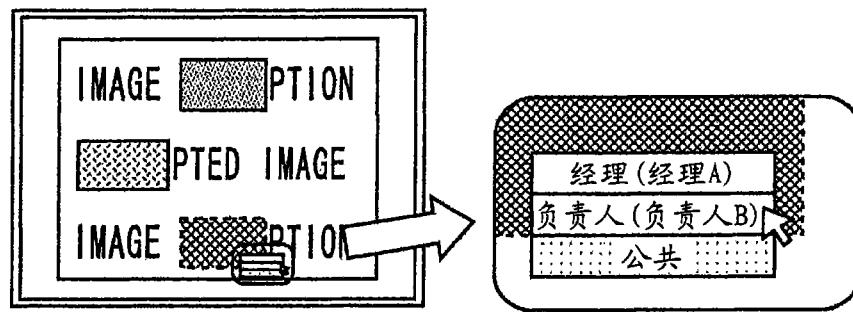


图 26

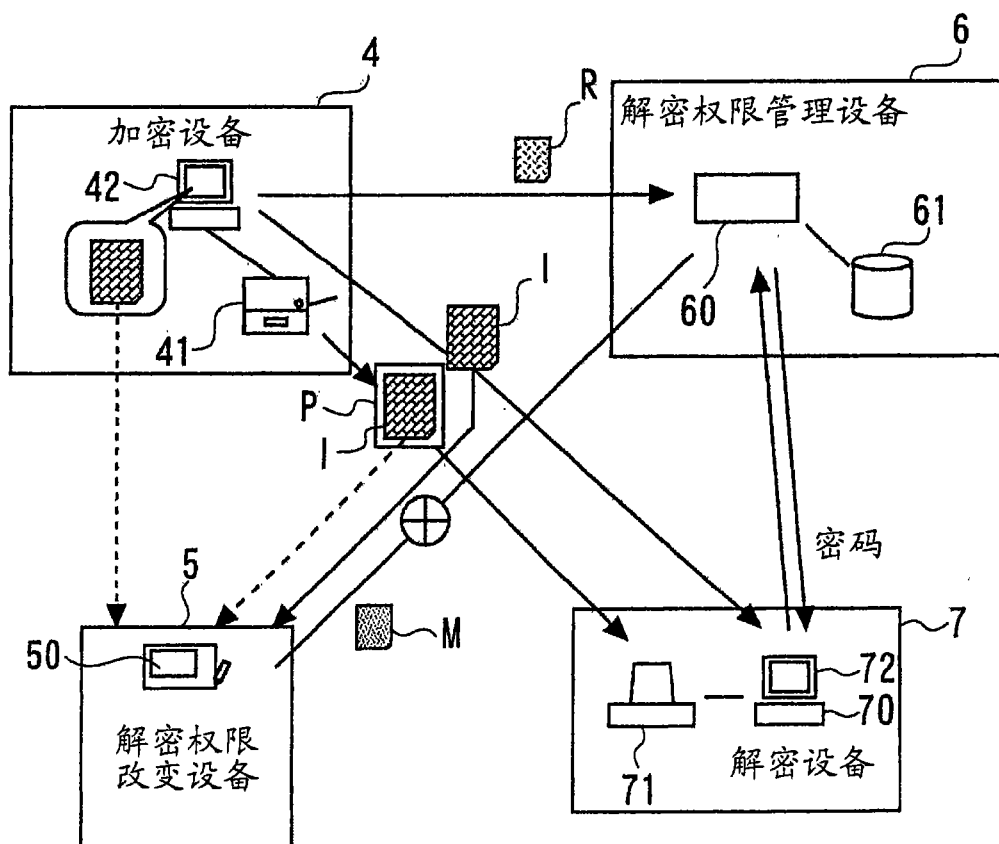


图 27

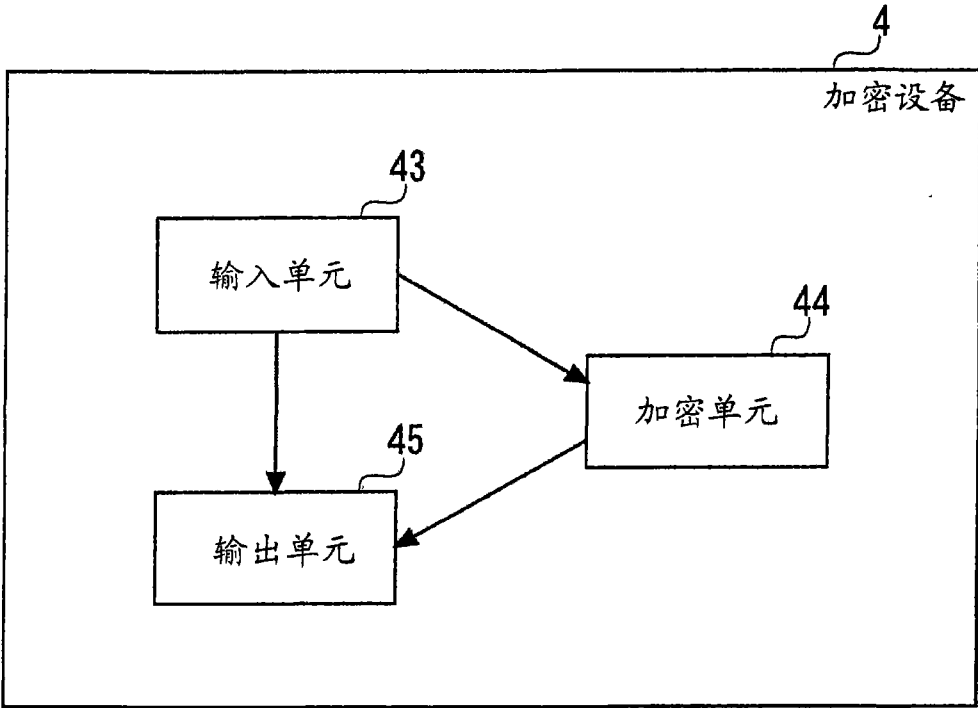


图 28

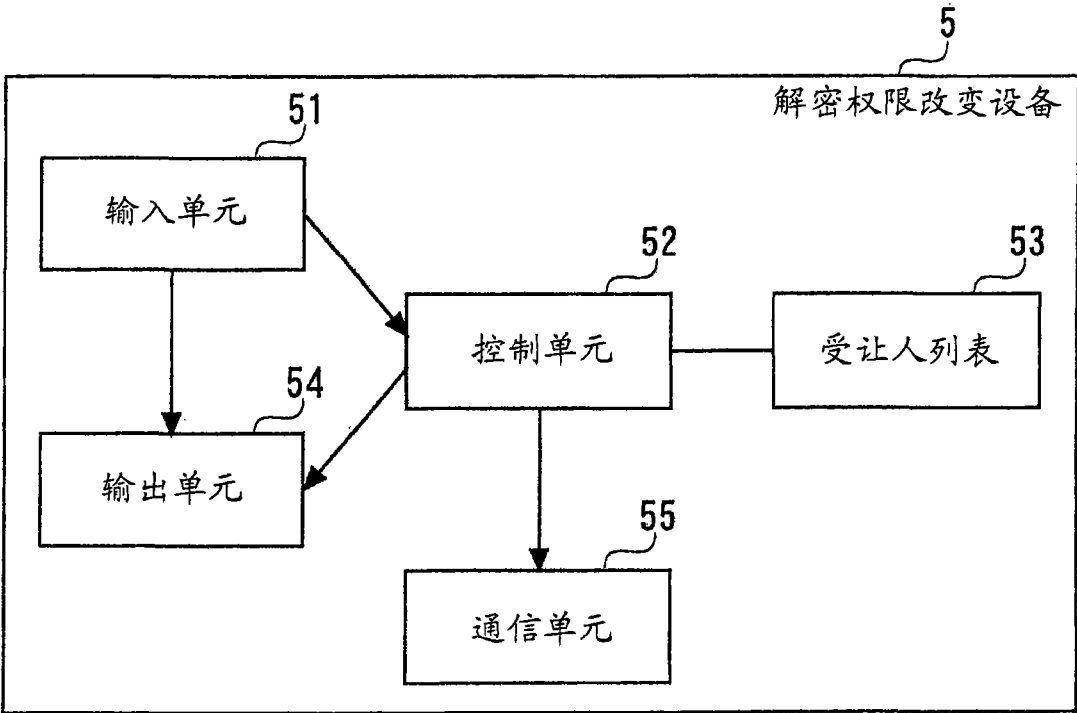


图 29

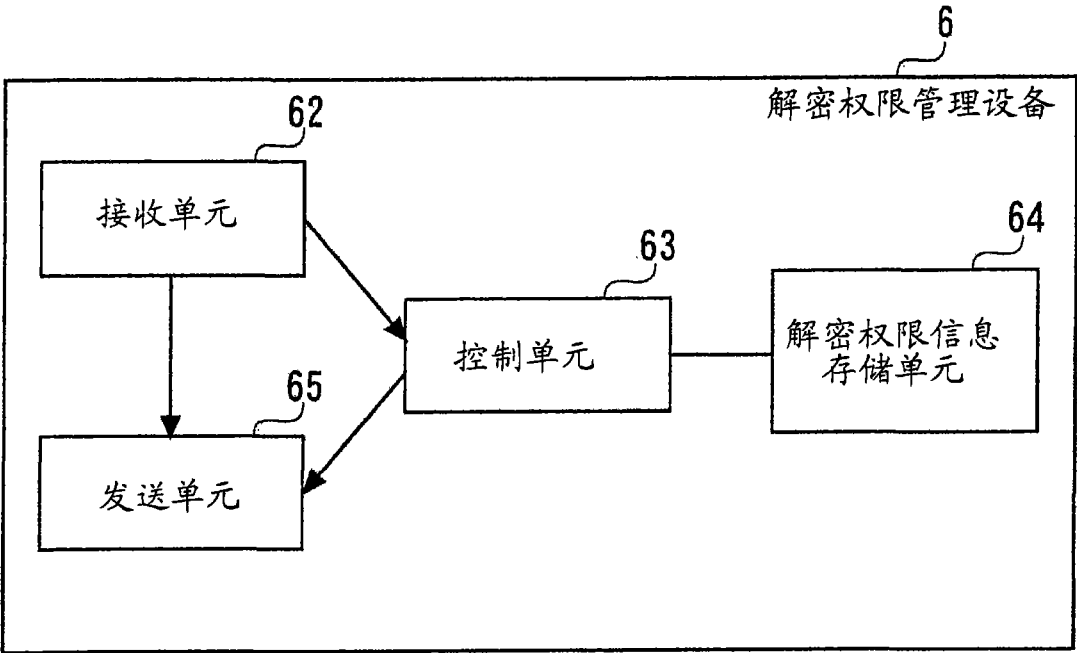


图 30

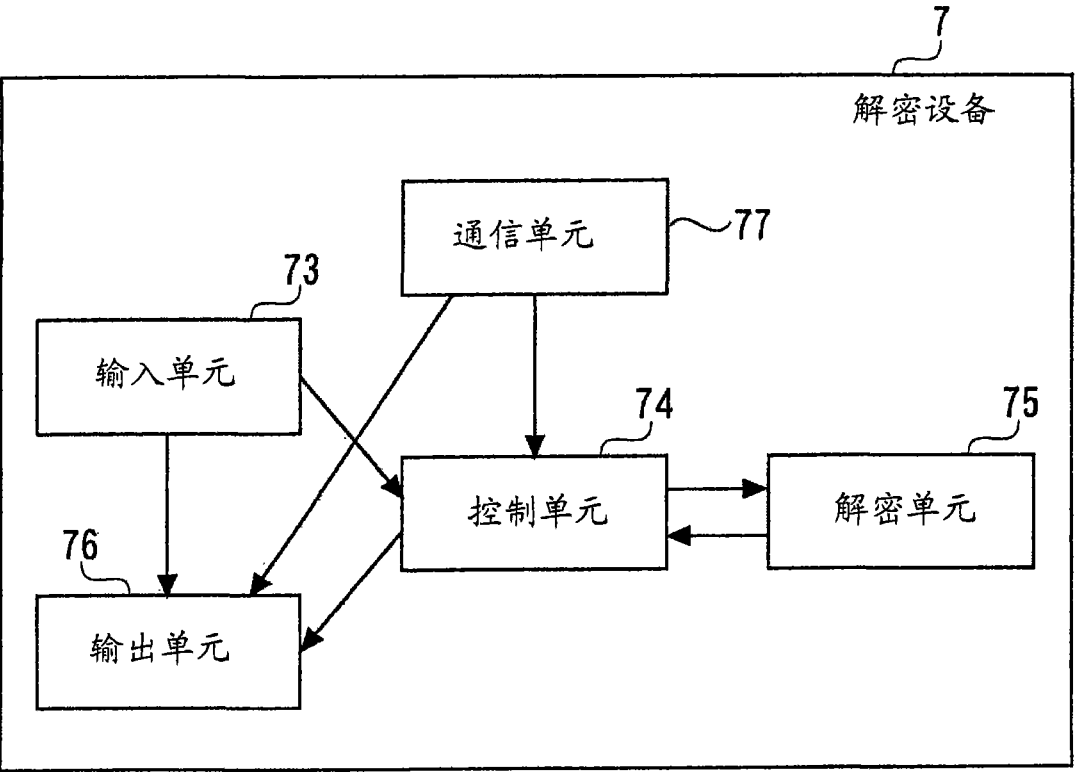


图 31

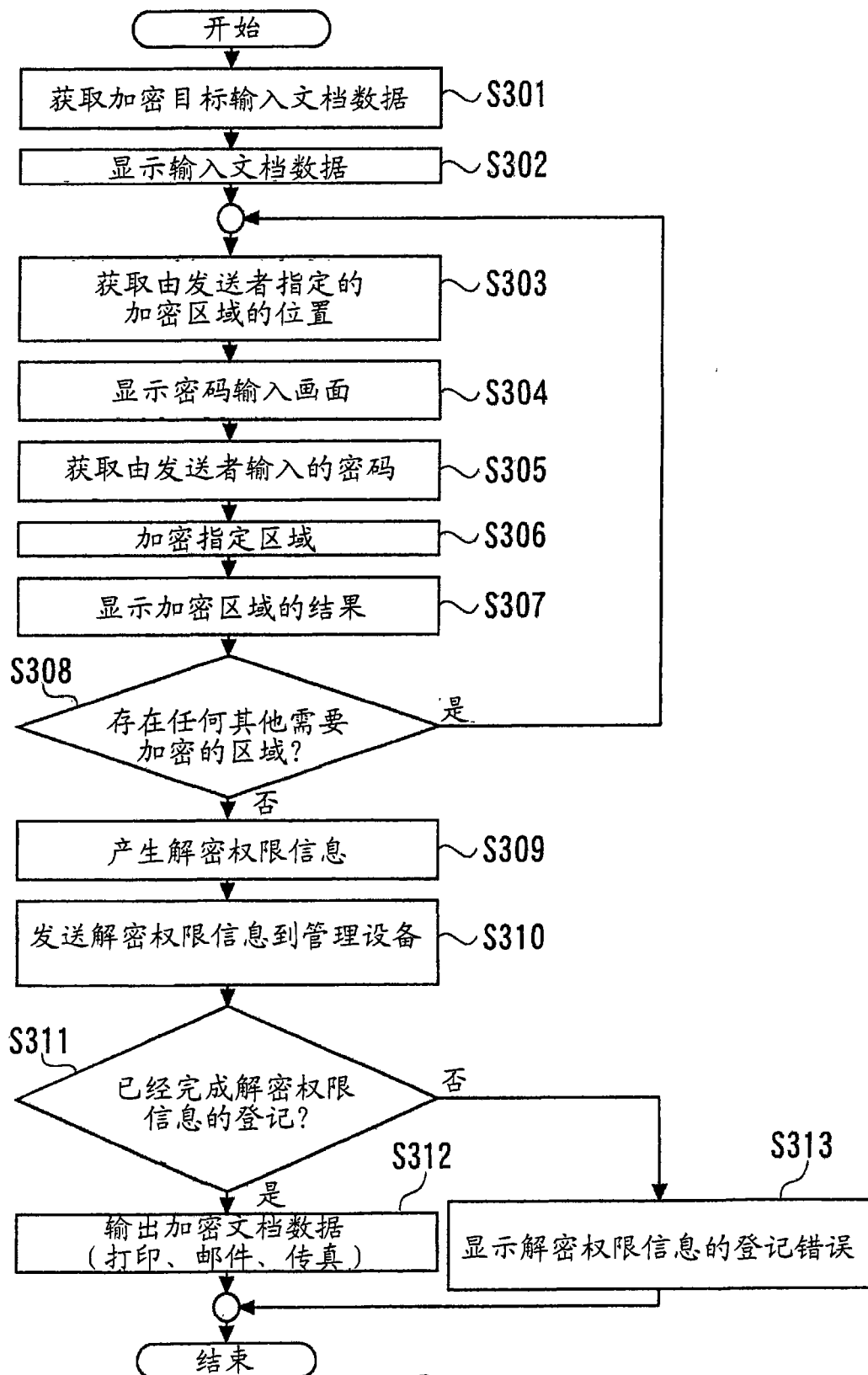


图 32

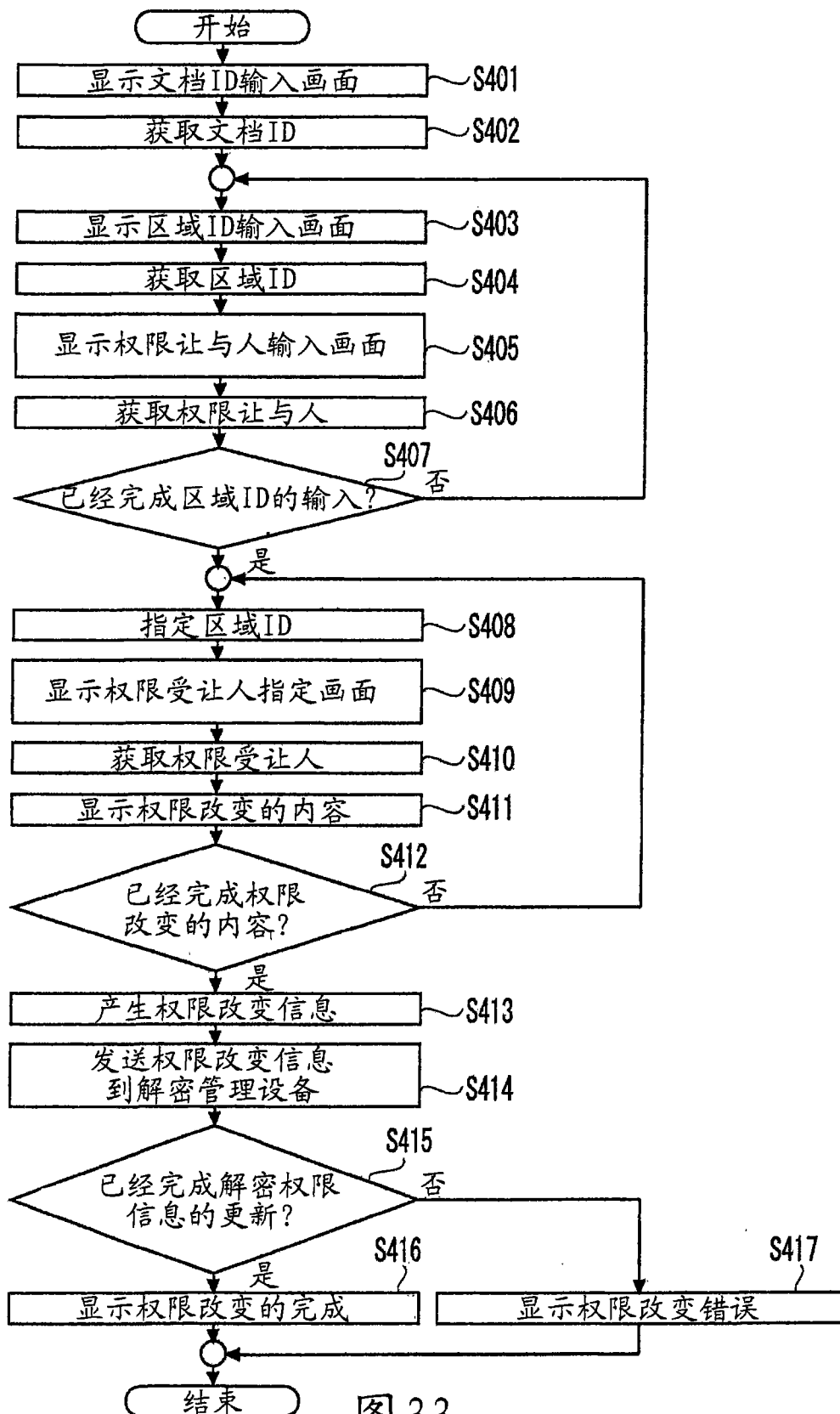


图 33

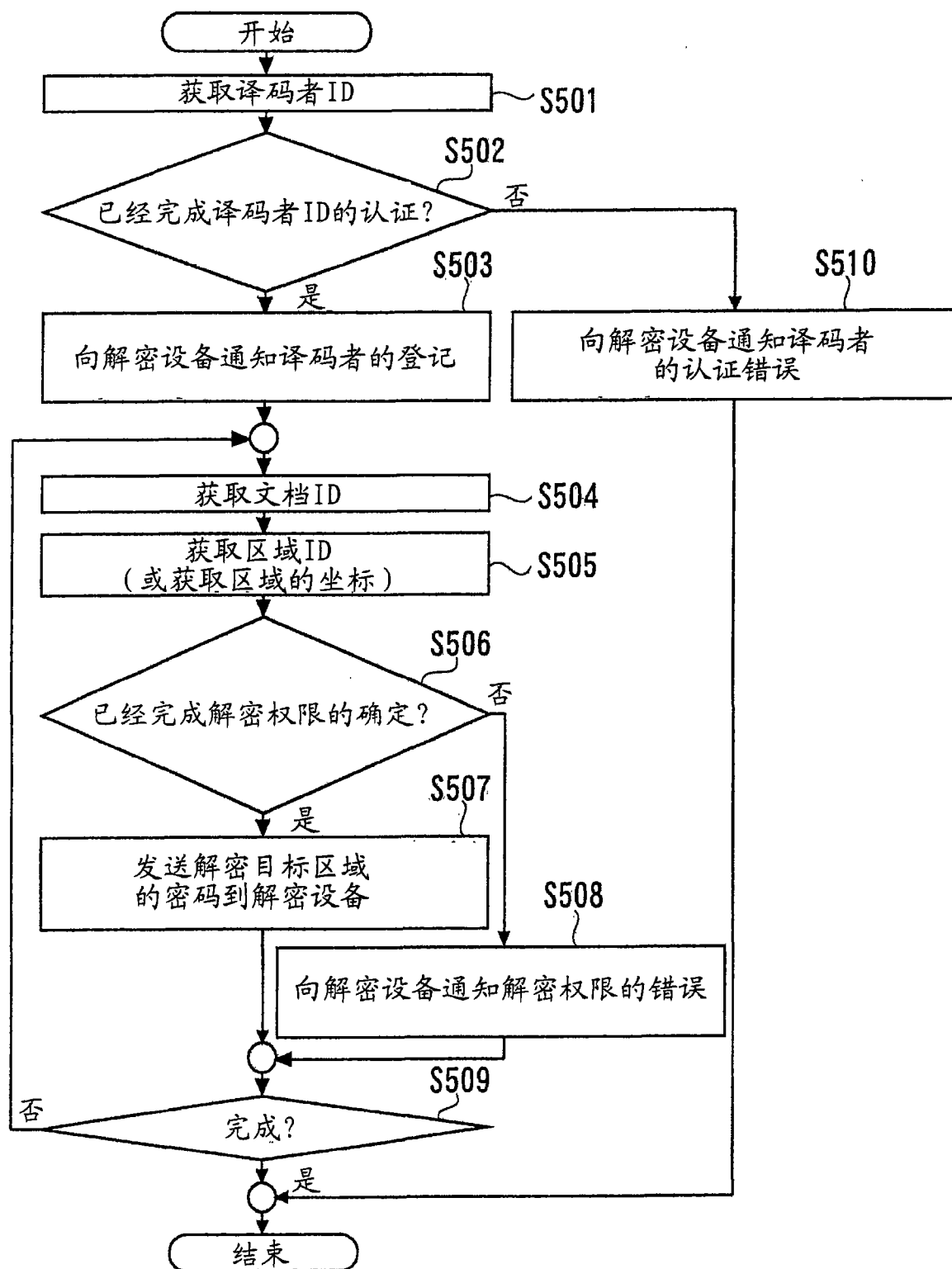


图 34

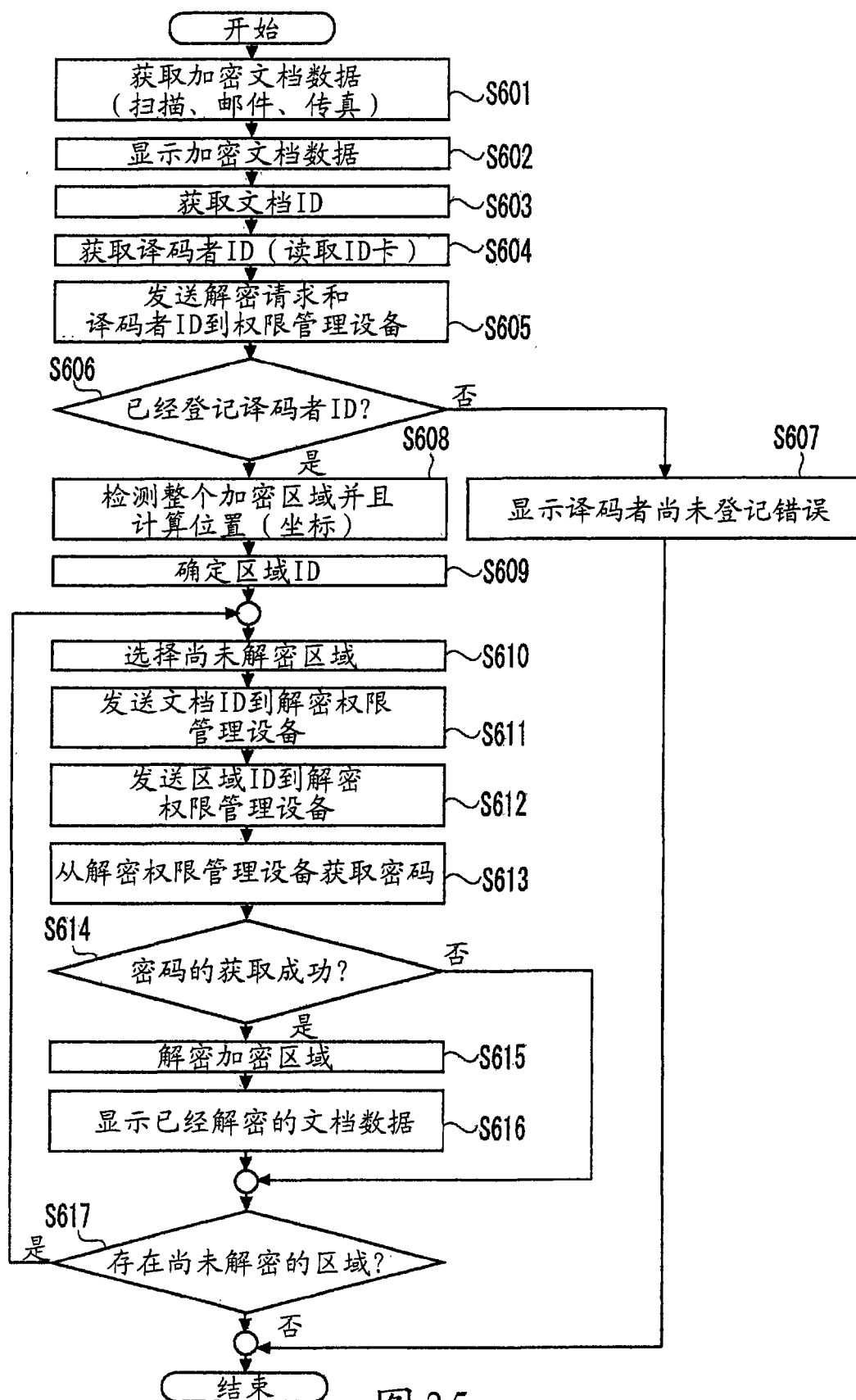


图 35

权限改变信息

文档ID	区域ID	解密权限 (让与人)	解密权限 (受让人)
2008-0107-1400	03	经理A	负责人B

图 36

更新的解密权限信息

文档ID	区域ID	位置信息	密码	解密权限
2008-0107-1400	01	(290, 40) – (490, 140)	AD8CX65Y	公共
2008-0107-1400	02	(75, 205) – (275, 305)	AD8CX65Y	公共
2008-0107-1400	03	(295, 360) – (495, 460)	P90EAQ1H	经理A+ 负责人B

图 37

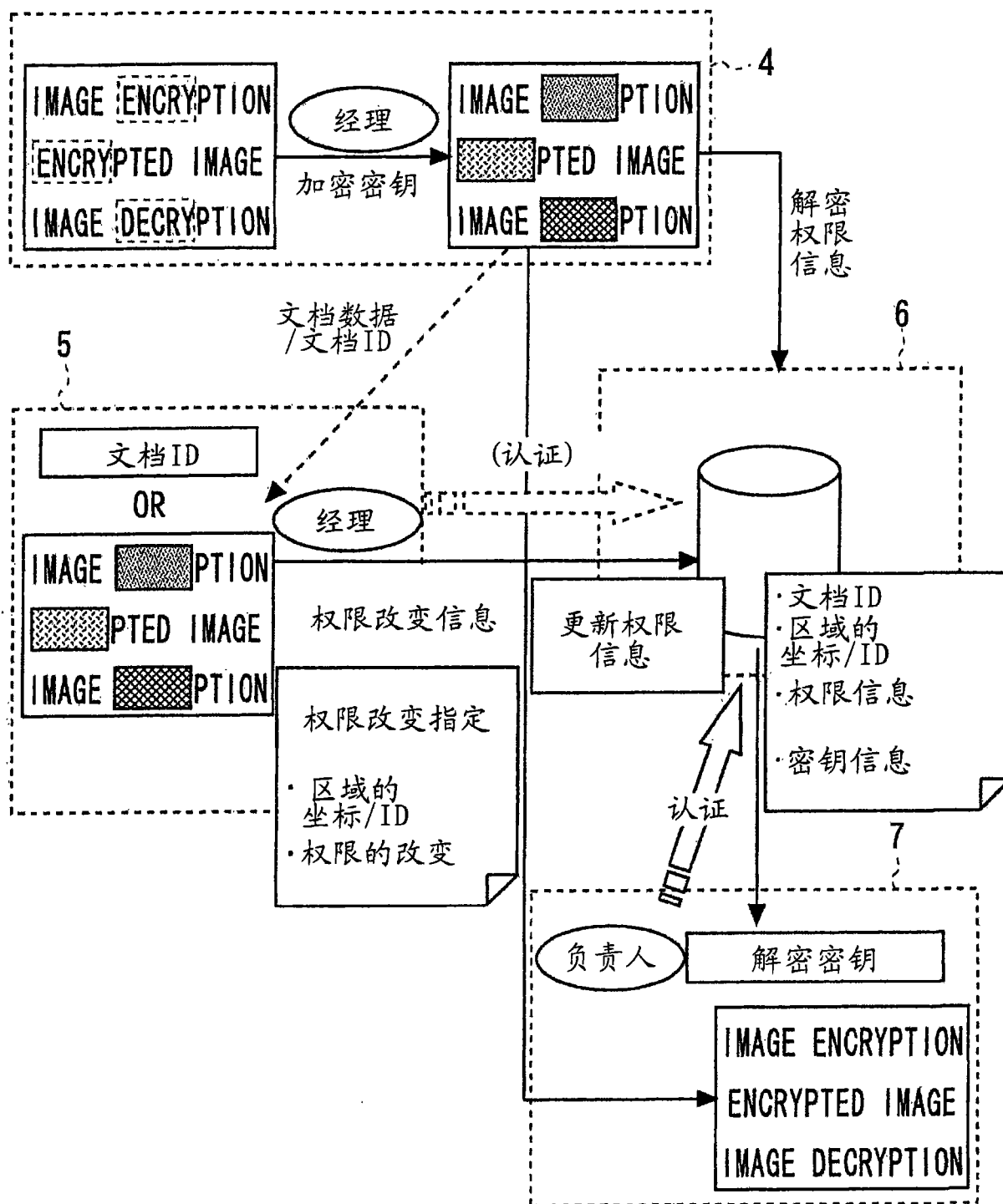


图 38

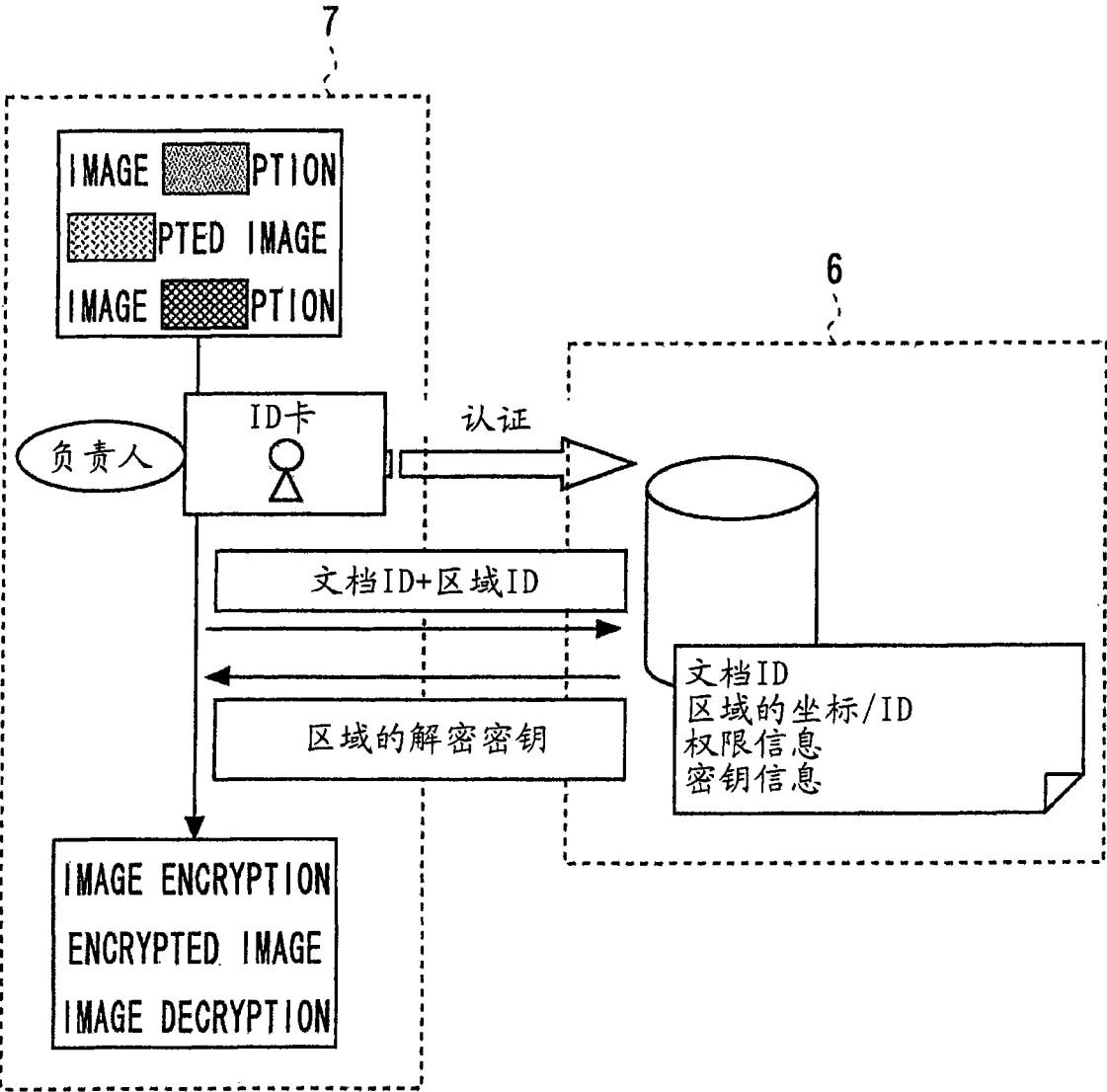


图 39

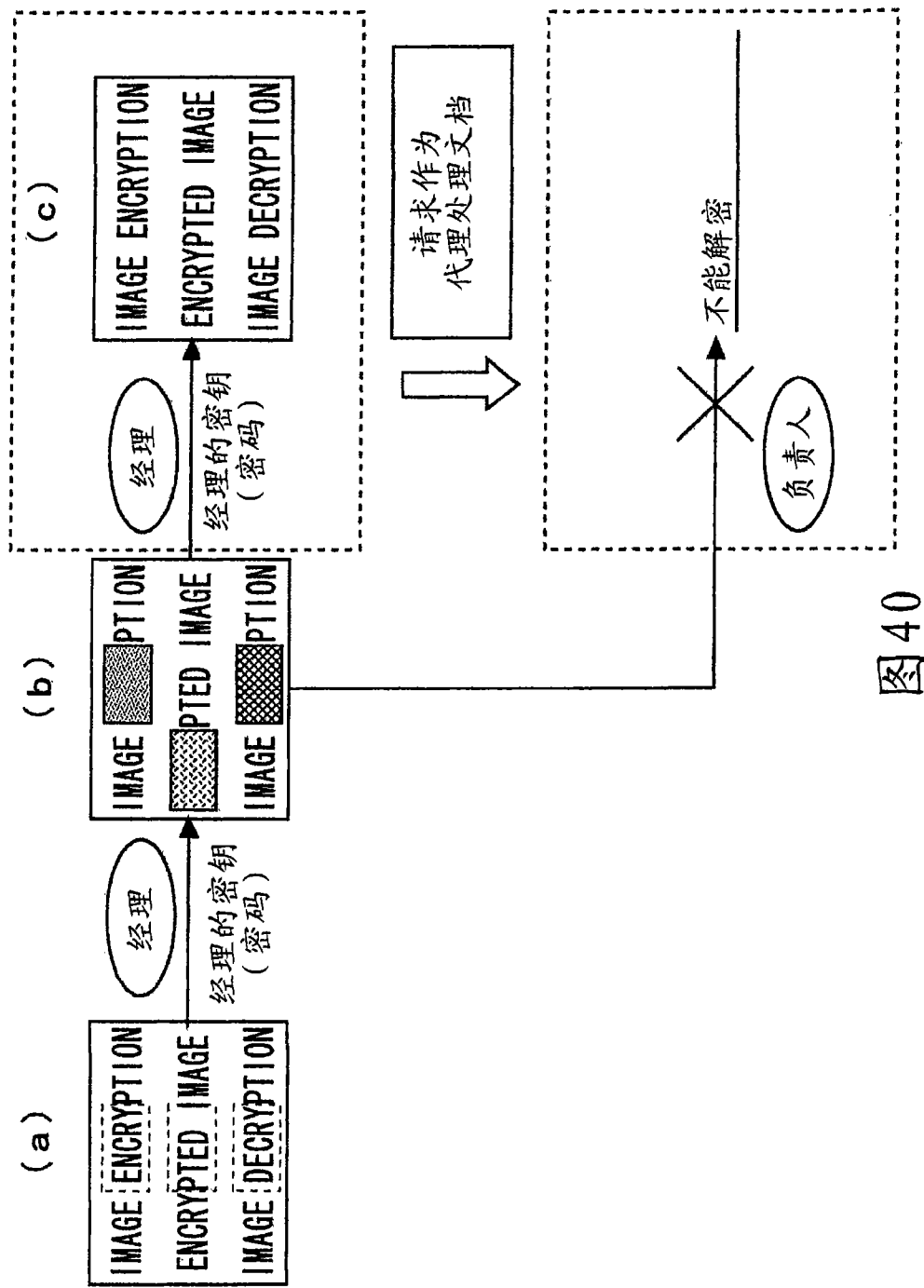


图40

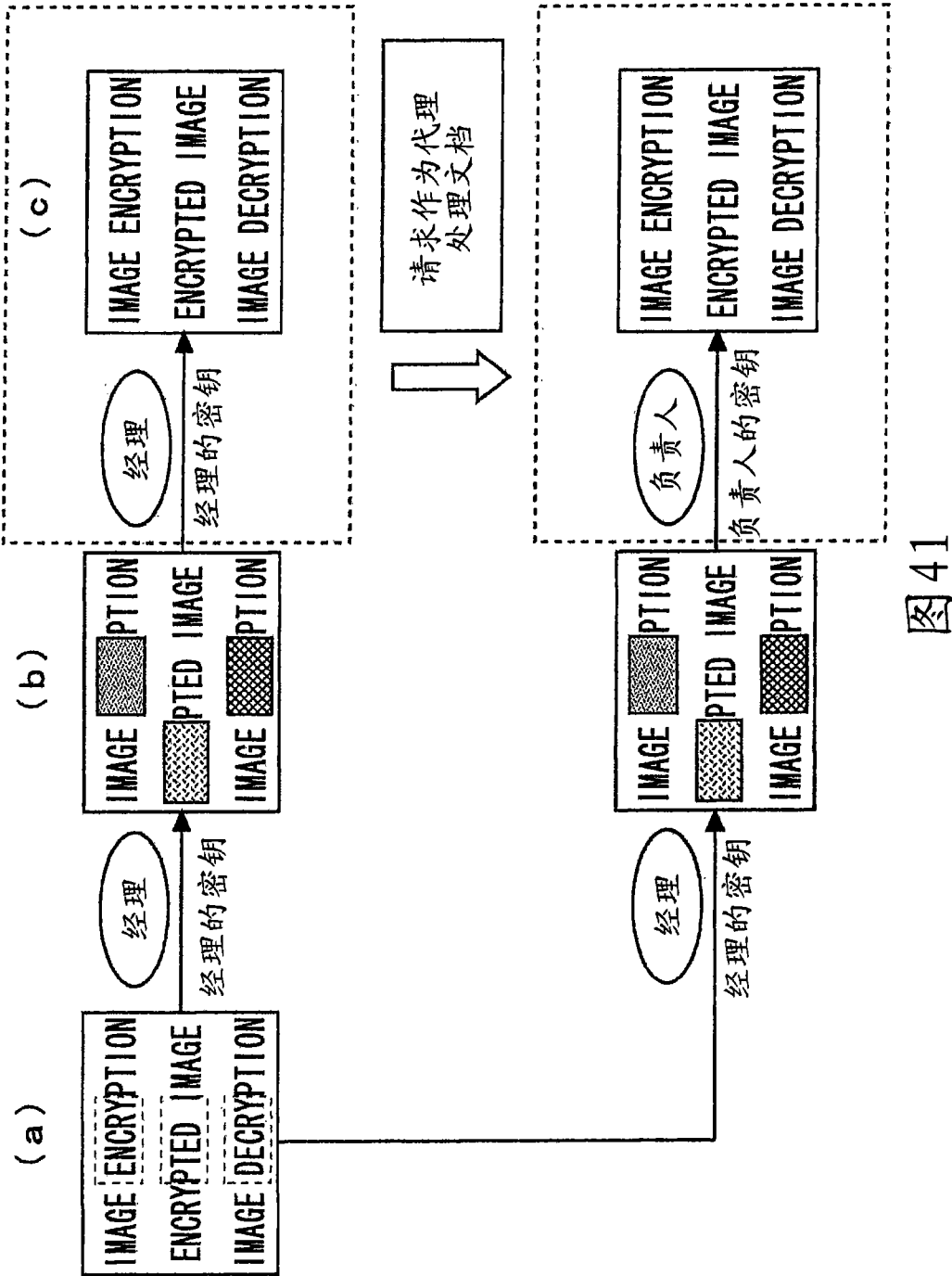


图41

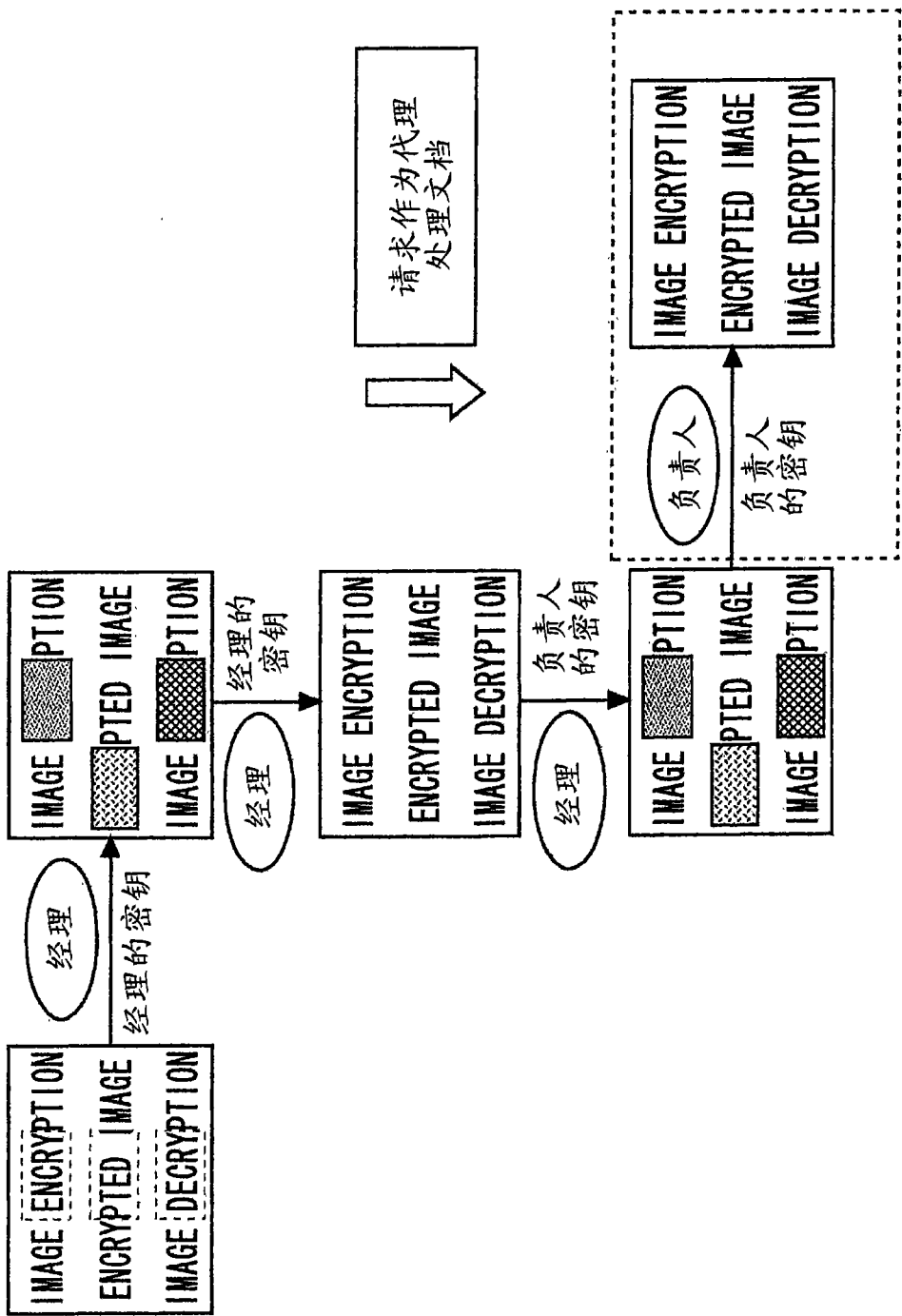


图42