(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 101370069 B
(45)授权公告日 2011.04.20

(21)申请号 200810001577.9
(22)申请日 2008.01.14
(30)优先权数据
11/755,278 2007.05.30 US
(73)专利权人 富士通株式会社
地址 日本神奈川县川崎市
(72)发明人 仓木健介 福井宏治 阿南泰三 中潟昌平
(74)专利代理机构 北京三友知识产权代理有限公司 11127
代理人 李辉
(51)Int.Cl.
H04N 1/32(2006.01)
H04L 29/06(2006.01)
H04L 9/32(2006.01)
G06F 21/00(2006.01)

(56)对比文件
WO 2006/028103 A1,2006.03.16,
US 2001/0004736 A1,2001.06.21,
US 6839844 B1,2005.01.04,
CN 1333973 A,2002.01.30,
CN 1717640 A,2006.01.04,
CN 1613255 A,2005.05.04,
WO 2006/028103 A1,2006.03.16,

审查员 王博

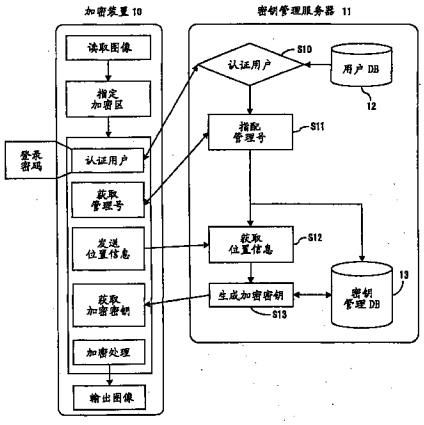
权利要求书 3 页 说明书 7 页 附图 17 页

(54)发明名称

图像加密/解密系统

(57)摘要

本发明涉及图像加密/解密系统。当对文件的被加密并由此模糊的一部分的图像进行解密时,用户使用解密装置(15)以电子图像来读取该文件,并且还通过访问密钥管理服务器(11)来接收用户认证。接着,用户从解密装置(15)向密钥管理服务器(11)发送从图像获取的管理号。密钥管理服务器(11)从密钥管理数据库(13)提取文件的被加密部分的位置信息和用于解密该部分的解密密钥,并将该解密密钥发送至解密装置(15)。解密装置(15)利用从密钥管理服务器(11)接收到的位置信息和解密密钥来处理所述电子图像,以解密被加密部分,使其容易辨认。



CN 101370069 B

1. 一种用于加密电子文件图像的图像加密和解密系统，该图像加密和解密系统包括：

用户认证单元，该用户认证单元用于对加密所述图像的用户进行认证；

加密区域获取单元，该加密区域获取单元用于获取由用户指定的要加密的图像的局部区域的位置信息；

管理号授予单元，该管理号授予单元用于授予标识所述图像的管理号；

加密密钥生成单元，该加密密钥生成单元用于生成对图像进行加密的加密密钥；

解密密钥生成单元，该解密密钥生成单元用于生成与所述加密密钥对应的解密密钥；

解密密钥存储单元，该解密密钥存储单元用于按将所述管理号、所述局部区域的所述位置信息、以及所述解密密钥相互关联的方式，来存储所述管理号、所述局部区域的所述位置信息、以及所述解密密钥；加密密钥发送单元，该加密密钥发送单元用于向用户发送所述加密密钥和所述管理号；以及

解密限制信息获取单元，该解密限制信息获取单元用于获取用于限制解密的解密限制信息；其中

所述解密密钥存储单元按将所述解密限制信息与所述管理号、所述位置信息以及所述解密密钥相互关联的方式，来存储所述解密限制信息；并且

在所述解密限制信息获取单元处获取的所述解密限制信息，是对仅准许具有执行解密的特定权限的用户和组执行解密的授权。

2. 根据权利要求 1 所述的图像加密和解密系统，其中，

在所述解密限制信息获取单元处获取的所述解密限制信息，是用于准许仅在特定时间段内进行解密的解密准许时段。

3. 根据权利要求 1 所述的图像加密和解密系统，其中，

在所述解密限制信息获取单元处获取的所述解密限制信息，包括准许解密的次数和执行解密的次数，所述次数用于限制可以执行解密的次数。

4. 根据权利要求 1 所述的图像加密和解密系统，其中，

所述解密密钥是加密密钥的副本。

5. 根据权利要求 1 所述的图像加密和解密系统，其中，

所述管理号被按诸如条形码、二维条形码、电子水印、隐写等的机器可读形式添加至图像。

6. 根据权利要求 1 所述的图像加密和解密系统，所述图像加密和解密系统还包括：

管理号获取单元，该管理号获取单元用于从一用户获取针对要解密图像的管理号，

位置信息获取单元，该位置信息获取单元用于利用所述管理号作为主键值来获取所述局部区域的所述位置信息，

解密密钥获取单元，该解密密钥获取单元用于利用所述管理号作为主键值来获取针对所述局部区域的解密密钥，以及

解密密钥发送单元，该解密密钥发送单元用于向所述用户发送所述解密密钥。

7. 根据权利要求 1 所述的图像加密和解密系统，所述图像加密和解密系统还包括：

管理号获取单元，该管理号获取单元用于从一用户获取要解密的图像的管理号，

位置信息获取单元，该位置信息获取单元用于利用所述管理号作为主键值来获取所述局部区域的所述位置信息，

解密限制信息获取单元，该解密限制信息获取单元用于利用所述管理号作为主键值来获取所述解密限制信息，

解密准许判断单元，该解密准许判断单元用于利用所述解密限制信息来判断针对用户的解密准许，以及

解密密钥获取和发送单元，该解密密钥获取和发送单元用于利用所述管理号作为主键值来获取针对所述局部区域的解密密钥，并且向被准许执行解密的所述用户发送所述解密密钥。

8. 根据权利要求 7 所述的图像加密和解密系统，其中，

在所述解密限制信息获取单元处获取的所述解密限制信息，是准许仅在特定时间段内进行解密的解密准许时段。

9. 根据权利要求 7 所述的图像加密和解密系统，其中，

在所述解密限制信息获取单元处获取的所述解密限制信息，包括准许解密的次数和执行解密的次数，所述次数用于限制可以执行解密的次数。

10. 根据权利要求 1 到 9 中任一项所述的图像加密和解密系统，其中，

所述加密区域获取单元根据所加密的图像文件的预设格式信息指定加密区域。

11. 一种在用于加密电子文件图像的图像加密和解密系统中使用的控制方法，所述控制方法包括以下步骤：

对加密所述图像的用户进行认证；

获取由用户指定的要加密的图像的局部区域的位置信息；

授予标识所述图像的管理号；

生成用于加密所述图像的加密密钥；

生成与所述加密密钥对应的解密密钥；

按将所述管理号、所述局部区域的所述位置信息、以及所述解密密钥相互关联的方式，来存储所述管理号、所述局部区域的所述位置信息、以及所述解密密钥；

向所述用户发送所述加密密钥和所述管理号；以及

获取用于限制解密的解密限制信息，并且

按将所述解密限制信息与所述管理号、所述位置信息以及所述解密密钥相互关联的方式，来存储所述解密限制信息；其中

获取的所述解密限制信息是对仅准许具有执行解密的特定权限的用户和组执行解密的授权。

12. 根据权利要求 11 所述的控制方法，

从一用户获取针对要解密的图像的管理号，

利用所述管理号作为主键值来获取所述局部区域的所述位置信息，

利用所述管理号作为主键值来获取所述局部区域的所述解密密钥，以及

向所述用户发送所述解密密钥。

13. 根据权利要求 11 所述的控制方法，

从一用户获取针对要解密的图像的管理号，

利用所述管理号作为主键值来获取所述局部区域的所述位置信息，

利用所述管理号作为主键值来获取所述解密限制信息，

利用所述解密限制信息来判断对所述用户进行解密的准许，以及

利用所述管理号来获取针对所述局部区域的解密密钥并且向被准许执行解密的用户发送所述解密密钥。

图像加密 / 解密系统

技术领域

[0001] 本发明涉及用于通过针对数字图像和印制在印刷品上的图像可视地加密诸如个人信息的重要信息的一部分来防止信息泄露给第三方的图像加密 / 解密系统。

背景技术

[0002] 在信息化时代的发展中，秘密信息泄露已经成为严重的问题，由此，需要开发防止信息泄露的技术。 对于数字数据来说，例如，已经开发出了用于加密数据以使如果第三方取得信息则内容不可见的技术；这些技术中的一些已经被用为用于防止信息泄露的有用手段。

[0003] 同时，用于防止信息从印制在纸上的印刷品等泄露的技术尚未充分发展，也不存在商业化产品的示例。 所有信息泄露中的半数被认为涉及印刷品，因此，迫切需要开发已针对数字数据采取的用于防止信息泄露的技术。

[0004] 需要针对从印刷品泄露信息的防范措施的示例，包括在购买商品时发出的钞票、信用卡账户报表、医院的病历卡、学校报告单，以及姓名列表。 参考专利文献 1 中提出的图像加密技术使得能够通过对数字图像以及印制在纸上的图像（注意：因为可以将账户报表、医院病历卡等定义为一种可视图像，所以在本说明书中将它们总称为“图像”）进行加密来防止信息泄露。

[0005] 本发明基于在相关申请（即，2007 年 3 月 13 日提交的 PCT/JP2007/000215）中提出的技术。 首先，对专利文献 1 进行说明，以使容易理解。

[0006] 图 1 是描述图像加密技术的图。

[0007] 一种图像加密技术是例如基于密码向输入图像的指定区域（下文中，称为“加密区”）应用图像处理，以使原始内容不可识别（参照图 1）。 该图像加密技术使得可以对图像的一部分内的多个局部区域进行加密，并且还使得能够针对单个局部区域利用不同密钥进行加密。 利用这种特性，可以想到适用于针对每一个局部区域的权限管理。 作为示例，可能需要用于加密一图像内的三个局部区域（例如，在工商企业的内部使用文件中），其中可以想得到的利用加密的情况是，因为给项目领导者看的局部区域 1 包含重要信息，所以将密钥 A 用于该局部区域 1，将密钥 B 用于局部区域 2 并且仅供项目成员看，而将密钥 C 用于局部区域 3，该局部区域 3 仅供内部公司使用。 然而，对于解密该图像的人来说，不能找出利用哪个密钥来加密什么局部区域，而且让加密该图像的人向要解密该图像的人提供密钥，就安全性和 / 或便利性而言也是不切实际的。

发明内容

[0008] 本发明的目的是，提供一种使得可以在图像加密技术中安全且便利地为解密方提供与解密相关的信息的加密 / 解密系统。

[0009] 根据本发明的加密 / 解密系统，是用于加密电子文件图像的系统，其使得能够进行加密的特征在于包括：用于对加密所述图像的用户进行认证的用户认证单元；用于

获取由用户指定的要加密的图像的局部区域的位置信息的加密区域获取单元；用于授予标识所述图像的管理号的管理号授予单元；用于生成用于加密图像的加密密钥的加密密钥生成单元；用于生成与所述加密密钥对应的解密密钥的解密密钥生成单元；用于按将所述管理号、所述局部区域的所述位置信息、以及所述解密密钥相互关联的方式，来存储所述管理号、所述局部区域的所述位置信息、以及所述解密密钥的解密密钥存储单元；以及用于向用户发送所述加密密钥和所述管理号的加密密钥发送单元。

[0010] 该加密 / 解密系统的使得能够进行加密的特征在于，除了包括上述单元外，还包括：用于从一用户获取针对要解密的图像的管理号的管理号获取单元；用于利用所述管理号作为主键值来获取所述局部区域的所述位置信息的位置信息获取单元；用于利用所述管理号作为主键值来获取针对所述局部区域的解密密钥的解密密钥获取单元；以及用于向所述用户发送所述解密密钥的解密密钥发送单元。

附图说明

[0011] 图 1 是描述图像加密技术的图；

[0012] 图 2 是描述第一优选实施方式的图（部分 1）；

[0013] 图 3 是描述第一优选实施方式的图（部分 2）；

[0014] 图 4 是例示用户数据库的图；

[0015] 图 5 是例示供在第一实施方式中使用的密钥管理数据库的图；

[0016] 图 6 是描述根据本发明的第二优选实施方式的图；

[0017] 图 7 是描述根据本发明的第二优选实施方式的图；

[0018] 图 8 是例示供在第二实施方式中使用的密钥管理数据库的图（部分 1）；

[0019] 图 9 是例示供在第二实施方式中使用的密钥管理数据库的图（部分 2）；

[0020] 图 10 是例示供在第二实施方式中使用的用户组数据库的图；

[0021] 图 11 是例示供在第二实施方式中使用的另一密钥管理数据库的图；

[0022] 图 12 是利用文件格式数据库的图像加密系统的图；

[0023] 图 13 是例示供图 12 所示实施方式使用的文件格式数据库的表的图（部分 1）；

[0024] 图 14 是例示供图 12 所示实施方式使用的文件格式数据库的表的图（部分 2）；

[0025] 图 15 是例示利用文件格式数据库的另一图像加密系统的图；

[0026] 图 16 是例示供在图 15 所示实施方式中使用的另一密钥管理数据库的图；

[0027] 图 17 是例示利用文件格式数据库的又一图像加密系统的图；

[0028] 图 18 是例示供图 17 所示实施方式使用的另一密钥管理数据库的图；

[0029] 图 19 是例示用于限制可以执行解密的次数的解密系统的图；以及

[0030] 图 20 是例示供图 19 所示实施方式使用的密钥管理数据库的表的图。

具体实施方式

[0031] 本发明被设计为构建一种包括用于管理加密密钥的密钥管理服务器的系统，由此，使得即使利用不同加密密钥来加密多个局部区域，也能够安全地执行解密，而不丧失便利性。

[0032] 下面，对具体解决方案进行说明。

[0033] 根据本发明的系统包括用于加密图像的加密装置、用于对加密的图像进行解密的解密装置以及用于管理密钥的密钥管理服务器。 本说明书中提到的加密装置和解密装置可以通过在除了个人计算机 (PC) 以外的诸如复印机 (包括混合复印机)、传真机、打印机、扫描仪、置顶 (overhead) 读取器、便携式电话、个人数字助理 (PDA)、数字摄像机或电视的其它设备中合并本发明的功能来实现。 根据优选实施方式的系统被设置成，独立包括加密装置、解密装置以及服务器 ; 然而，包括类似功能的集成装置也是合适的。

[0034] [加密]

[0035] 接下来，对加密装置中的加密过程进行说明。 加密装置选择通过应用生成的数字数据或通过诸如数字摄像机或扫描仪的光学装置读取的图像中的希望被加密的区域。在选定区域之后，加密装置向密钥管理服务器发送用于用户认证的询问。 密钥管理服务器利用用户数据库等执行认证，并且如果用户是合法用户，则给出针对加密的准许。 接着，加密装置从密钥管理服务器获取用于标识加密图像的管理号，并且向密钥管理服务器发送选定局部区域的位置信息和解密所需信息 (即，通过利用扫描仪读取整个图像并且获取选定区域位于整个图像中的位点的位置信息)。 在此提到的解密所需信息是诸如用户被准许执行解密的权限信息的信息，和诸如用于仅准许在指定时段内执行解密的时段、日期等的时间信息。 密钥管理服务器生成并且向加密装置发送用于加密局部区域的加密密钥，并且把从加密装置接收到的信息、管理号以及加密密钥存储在密钥管理数据库中。 用于加密的加密密钥可以和在解密时从前述数据库中取出的解密密钥相同。 如果加密密钥和解密密钥不同，则生成解密密钥并且及时存储。 加密装置利用从密钥管理服务器接收到的加密密钥来加密选定的局部区域。 当加密多个局部区域时，重复上述发送位置信息与加密之间的处理。

[0036] [解密]

[0037] 接下来，对解密装置中的解密过程进行说明。 如果图像被存储为数字数据，则解密装置读取数字数据，或者如果图像是打印在纸上的硬拷贝等或在显示装置中显示的图像，则解密装置读取通过诸如数字摄像机或扫描仪的光学装置数字化的图像。 解密装置向密钥管理服务器发送询问，并且认证用户。 密钥管理服务器经由用户数据库等认证用户，并且如果该用户是合法用户，则向解密装置请求在加密时指配的管理号。 解密装置向密钥管理服务器发送管理号。 密钥管理服务器针对解密所需信息搜索被加密局部区域的位置信息，并且基于管理服务器从密钥管理数据库中搜索解密密钥。 还分析解密所需信息，并且如果试图解密它的用户的权限等不存在问题，则向解密装置发送解密密钥。 如果用户存在权限问题或用户存在其它这种问题，则密钥管理服务器不发送解密密钥。 在接收到解密密钥后，解密装置利用该解密密钥来解密数据。

[0038] 图 2 和 3 是描述第一优选实施方式的图。

[0039] 根据第一实施方式的系统包括加密图像的加密装置、解密被加密图像的解密装置，以及管理密钥的密钥管理服务器。

[0040] 接下来，参照图 2，对加密装置 10 处的加密过程进行说明。 在加密装置 10 中，通过指针等来选择希望通过利用扫描仪等读取图像来加密的图像中的区域。 在预定格式等的文件图像的情况下，可以在加密装置 10 中预登记希望加密的区域的坐标等。

[0041] 在选定区域之后，加密装置 10 向密钥管理服务器 11 发送询问并且认证用户 (S10)。 密钥管理服务器 11 利用用户数据库 (DB)12 等来认证用户，并且如果该用户是合法用户，则给出针对加密的准许。 用户认证例如利用用户 ID、密码、IC 卡以及生物特征。 顺便提及，密钥管理服务器 11 与加密装置 10 之间的通信可以利用诸如安全套接层 (SSL) 的加密通信。

[0042] 密钥管理服务器 11 生成用于独特表示要加密图像的管理号 (S11)。 加密装置 10 从密钥管理服务器 11 获取用于标识被加密图像的管理号，并且向密钥管理服务器 11 发送选定局部区域的位置信息。 如果加密物是纸介质，则首先利用扫描仪等导入在该纸介质的整个幅面中位置信息作为一图像，接着获取选定局部区域的位置，作为整幅图像的坐标。 如果加密物是电子图像，则在字处理器软件等中显示图像，并且使用字处理器画面中的坐标信息。

[0043] 在从加密装置 10 接收到局部区域的位置信息 (S12) 后，密钥管理服务器 11 利用随机数生成用于加密该局部区域的加密密钥 (S13)，并且向加密装置 10 发送加密密钥。

[0044] 本发明的优选实施方式假定使用对称密钥加密，即，简单地说，使用相同的加密密钥和解密密钥；然而，本系统也可以通过组合公钥加密系统来对加密和解密使用不同密钥。 将从加密装置接收到的管理号和解密密钥（或在对称密钥加密的情况下加密密钥的副本）以及位置信息登记在密钥管理数据库 (DB)13 中。 当解密时从前述数据库中获取解密密钥。

[0045] 在从密钥管理服务器 11 接收到加密密钥后，加密装置 10 利用加密密钥来加密局部区域。 如果要加密多个局部区域，则要重复如上所述向密钥管理服务器 11 发送位置信息与利用加密密钥进行加密之间的处理达指定局部区域的数量次。 另选的是，可以把多个局部区域的位置信息汇成列表，并且将该列表发送至密钥管理服务器 11，以使一次接收多个加密密钥。

[0046] 在加密装置侧获取的管理号被已经加密它的用户记住，或者添加至完成加密之后的图像。 用于将管理号添加至图像的方法包括将管理号直接绘制在图像的一部分中，或者采用诸如条形码、二维条形码、电子水印的机器可读格式或通过隐写 (steganography) 将它添加至图像。 在完成加密之后可以擦除在加密装置 10 处接收到的加密密钥。

[0047] 接下来，参照图 3，对解密装置处的解密过程进行说明。 解密装置 15 读取被加密图像并且通过向密钥管理服务器 11 询问来认证用户 (S15)。 密钥管理服务器 11 利用用户数据库 (DB)12 来认证该用户，并且如果该用户是合法用户，则向解密装置 15 请求在加密时指配的管理号 (S16)。

[0048] 解密装置 15 向密钥管理服务器 11 发送管理号。 如果管理号被以条形码、电子水印或隐写添加至图像，则从图像读取它 (S17)。

[0049] 密钥管理服务器 11 基于该管理号从密钥管理数据库 (DB)13 获取被加密局部区域的位置信息和解密密钥，并将它们发送至解密装置 15(S18 和 S19)。

[0050] 解密装置 15 利用接收到的解密密钥和位置信息来解密被加密局部区域。 如果图像在加密之后被打印在纸上并且通过扫描仪读取该纸的图像，接着解密该图像，则在从密钥管理服务器 11 接收到的局部区域的位置信息与实际局部区域的位置信息之间很可能

存在位置和 / 或尺寸的偏移；因此，把要解密的局部区域的范围设置成稍大点。

[0051] 采用上述系统的加密和解密使得即使单个图像具有利用不同密钥加密的多个加密区域，也可以在使用户意识不到密钥差别的情况下执行解密。

[0052] 图 4 是例示用户数据库的图。 如图 4 所示，用户数据库按将用户 ID 和密码相互关联的方式来存储用户 ID 和密码，以验证用户。 当用户登录时，将用户 ID 和密码发送至密钥管理服务器 11，密钥管理服务器 11 接着通过确认发送的用户 ID 和密码是否为存储在用户数据库 12 中的用户 ID 和密码并且确认该用户 ID 和密码是否彼此正确对应，来认证该用户。

[0053] 图 5 是例示供在第一实施方式中使用的密钥管理数据库的图。

[0054] 在该密钥管理数据库中，管理号和位置信息是主键值；当解密装置按管理号发送询问时，参照它们以向解密装置发送与管理号对应的位置信息和解密密钥，如图 5 所示。 一个管理号表示一个文件，而与其对应的位置信息存储文件中包括的所有加密部分的位置信息。 而且，将用于解密这些位置中存在的被加密部分的解密密钥和管理号以及位置信息互相关联地存储在一起。

[0055] 图 6 和 7 是描述根据本发明的第二优选实施方式的图。

[0056] 根据第二实施方式的系统包括用于加密图像的加密装置 10a、用于解密被加密图像的解密装置 15，以及用于管理密钥的密钥管理服务器 11a。

[0057] 接下来，对加密装置 10a 处的加密过程进行说明。 在加密装置 10a 中，通过利用指针等来选择图像中希望加密的区域。 另选的是，在确定了文件图像的格式的情况下，在加密装置 10a 或密钥管理服务器 11a 中预登记希望加密的区域的坐标等，接着在加密该区域时获取它们，或者通过网络从外部存储装置等获取它们。

[0058] 在选定区域之后，加密装置 10a 通过向密钥管理服务器 11a 发送询问来认证用户 (S10)。 密钥管理服务器 11a 利用用户数据库 (DB) 12 等来认证用户，并且如果该用户是合法用户，则给出针对加密的准许。 用户认证利用利用诸如用户 ID、密码、IC 卡或生物特征的信息。 同时，密钥管理服务器 11a 与加密装置 10a 之间的通信可以利用诸如 SSL 的加密通信。

[0059] 加密装置 10a 从密钥管理服务器 11a 获取用于标识被加密图像的管理号 (S11)，并且向密钥管理服务器 11a 发送选定局部区域的位置信息和解密限制信息 (S12a)。 这里提到的解密限制信息是被准许进行解密的用户的权限信息、诸如用于准许仅在任意时段内进行解密的解密准许时段的时间信息等。

[0060] 用户的权限信息是指诸如 “仅特定用户被准许解密” 和 “仅属于特定组的用户被准许解密” 的信息；通过组数据库 (DB) 16 来管理用户所属的组的信息。 对于解密用户来说，例如当生成内部公司文件时，通过改变已被准许针对每一个局部区域进行解密的用户或组所执行的解密，使得仅属于组 A 的用户能够解密该文件的最重要部分，仅属于组 A 和组 B 的用户能够解密第二重要部分，而属于组 A、组 B 以及组 C 的用于能够解密第三重要部分。

[0061] 在从加密装置 10a 接收到局部区域的位置信息和解密限制信息之后，密钥管理服务器 11a 利用随机数等生成用于加密该局部区域的加密密钥 (S13)，并将该密钥发送至加密装置 10a，接着，在密钥管理数据库 (DB) 13 中登记管理号、解密密钥 (其在使用对称

密钥加密时是加密密钥的副本）以及从加密装置 10a 接收到的信息。 当解密时从该数据库中获取解密密钥。

[0062] 在从密钥管理服务器 11a 接收到加密密钥后，加密装置 10a 利用加密密钥来加密局部区域。 如果加密多个局部区域，则重复向密钥管理服务器 11a 发送位置信息与利用加密密钥来执行加密之间的处理达指定局部区域的数量次。 另选的是，可以将所述多个局部区域的多条位置信息汇集成列表来发送至密钥管理服务器 11a，以使一次接收多个加密密钥。

[0063] 在加密装置侧获取的管理号被加密用户记住，或者添加至完成加密之后的图像。 用于将管理号添加至图像的方法包括将管理号直接在图像的一部分中绘制该号，和采用诸如条形码、二维条形码、电子水印或隐写的机器可读格式将该号添加至图像。 在完成加密之后可以擦除在加密装置 10 处接收到的加密密钥。

[0064] 接下来，参照图 7，对解密装置中的解密过程进行说明。 解密装置 15 读取被加密图像并且通过向密钥管理服务器 11a 发送询问来认证用户 (S15)。 密钥管理服务器 11a 利用用户数据库 (DB)12 等来认证该用户，并且如果该用户是合法用户，则向解密装置 15 请求在加密时指配的管理号 (S16)。

[0065] 解密装置 15 向密钥管理服务器 11a 发送管理号 (S17)。 如果管理号已经被以条形码或电子水印添加至图像，则从图像读取该管理号。

[0066] 密钥管理服务器 11a 基于该管理号从密钥管理数据库 (DB)13 中获取被加密局部区域的位置信息、解密限制信息以及解密密钥 (S18a)。 它在组信息数据库 (DB)16 内查找解密限制信息和试图解密被加密数据的用户的信息，并且如果该用户具有执行解密的权限并且如果解密的日期和时间是准许解密的日期和时间，则将解密密钥和该局部区域的位置信息发送至解密装置 15(S20 和 S19)。

[0067] 解密装置 15 利用接收到的解密密钥和位置信息来解密被加密局部区域。 然而，对于解密在加密之后被打印在纸上接着使用扫描仪读取该纸的情况或类似情况来说，因为从密钥管理服务器 11a 接收到的局部区域与实际局部区域之间很可能出现位置和尺寸上的偏移，所以把要解密的局部区域的范围设置成稍大点。

[0068] 采用上述系统执行的加密和解密，使得即使单个图像具有利用不同密钥加密的多个加密区域，也可以在不使用户意识到密钥差别的情况下执行解密，并且应用这个特征还使得用户能够基于权限和 / 或时间来限制解密的执行。

[0069] 图 8 和 9 是例示供在第二实施方式中使用的密钥管理数据库的图。

[0070] 在图 8 所示的数据库中，管理号和位置信息是用于获取解密密钥的主键值。 通过限制解密权限和解密时段来控制发送解密密钥。 至于时段，可以设想指定任意日期和时间。 作为示例，可以在 4 月 1 日在密钥管理服务器中登记，并且设置解密结束日期为 5 月 31 日。 在这种情况下，使得能够在从 4 月 1 日在密钥管理服务器中进行登记与结束日期 5 月 31 日之间的时段内进行解密，而从 6 月 1 日起之后禁止解密。 还可以设置解密开始日期。 作为示例，如果在 4 月 1 日设置密钥管理服务器中的登记，并且如果将解密开始日期和结束日期分别设置为 5 月 1 日和 5 月 31 日，则在 4 月 1 日与 4 月 31 日之间不准许解密，在 5 月 1 日与 5 月 31 日之间准许解密，而在 6 月 1 日起以后不准许解密。 图 9 例示了利用解密开始日期和时间以及解密结束日期和时间的数据库。

[0071] 在图 8 的示例中，按将管理号与相关位置信息、解密权限、解密时段以及加密密钥相互关联的方式来存储管理号。 解密权限表示一组用户被分级，并且指定哪一级被准许解密。 解密时段表示从发出由所述管理号表示的文件起的日期数。 用“∞”表示列出的文件中被准许无限期地解密的文件。

[0072] 图 10 是例示供在第二实施方式中使用的用户组数据库的图。

[0073] 用户组数据库由两个表组成，表 1 登记由用户 ID 标识的用户属于哪一个用户组，而表 2 登记用户组被授予哪一级解密权限。 图 9 所示示例示出了属于组 A 的用户（即，AB1234 和 CD5678）被准许仅解密 1 级的加密区域，属于组 B 的用户（即，EF9977）被准许解密 1 级到 3 级的加密区域，而属于组 C 的用户（即， GH9021）被准许解密 1 级到 8 级的加密区域。

[0074] 图 11 是例示供在第二实施方式中使用的另一密钥管理数据库的图。

[0075] 图 11 所示的表存储有被准许解密的用户 ID，代替了图 8 所示的表中的“解密权限”。 这种构造使得仅参照密钥管理数据库而不需专门设置用户组数据库，就可以获知询问所关注的用户是否具有解密由特定管理号所标识的文件的权限。

[0076] 图 12 例示了当加密和解密固定格式的文件图像时利用（图 13 所示的）文件格式数据库的情况。 当在加密装置中指定用于加密的区域时，假定对于每次加密或解密诸如固定格式文件的文件，用指针等来指定同一坐标。 为了节省这种工作，在文件格式数据库 (DB) 中预先管理要加密区域的针对每一种格式的位置信息，并且在加密时通过用户指定格式来向密钥管理服务器发送询问，以使密钥管理服务器从文件格式数据库获取要加密区域的坐标，并将该坐标发送至加密装置。 在图 12 所示的示例中，密钥管理服务器参照文件格式数据库；然而，该数据库另选地也可以设置在加密装置、解密装置中或连接至网络的除了密钥管理服务器以外的其它装置的存储区中。 文件格式数据库在图 13 所示的表中登记加密区的数量和针对每种文件格式的相关位置信息。 而且，除了设置如图 14 所示的文件格式和加密区域的位置信息外，还设置其它解密限制信息，消除了每次执行加密时输入限制信息的必要性，如同图 15 中的情况一样，由此，使得能够在加密 / 解密大量信息时进行批处理。

[0077] 当利用文件格式数据库时，密钥管理数据库 (DB) 可以使用图 17 所示的表。 当用户解密一图像时，服务器可以从文件格式数据库获取位置信息和解密限制信息，并将它们发送至解密装置，如图 17 所示。

[0078] 图 18 是当利用解密次数作为解密限制信息时的密钥管理数据库。 加密系统将准许解密的次数设置为解密限制信息。 如图 19 所示，按下面的方式来进行控制，即，解密系统在密钥管理服务器处管理解密次数，并且在解密被指配了管理号的特定加密图像的情况下，如果迄今为止已对图像执行解密的次数不大于密钥管理数据库中的针对准许解密的次数设置的次数，则准许发送加密密钥，而如果迄今为止已执行解密的次数大于设置次数，则不准许发送解密密钥。 服务器在发送解密密钥之后，将已执行解密的次数添加至密钥管理数据库，作为已执行解密的次数。 另选的是，如图 20 所示，可以通过用户来限制并管理已执行解密的次数。

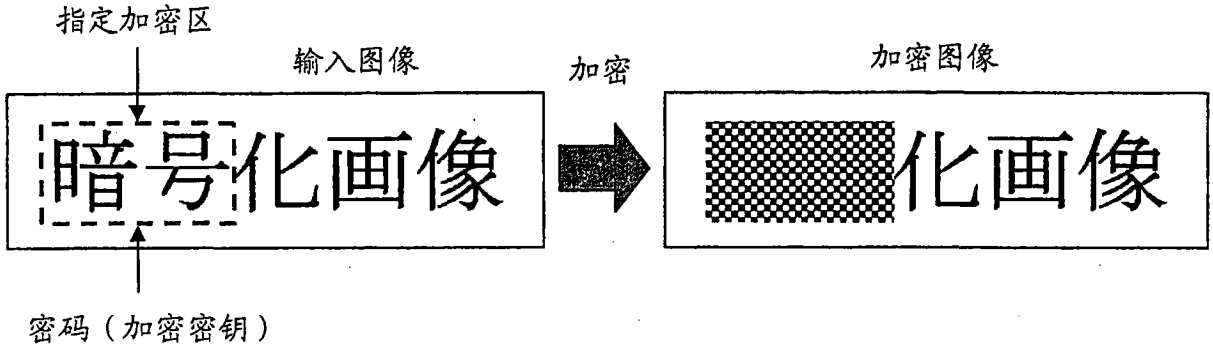


图 1

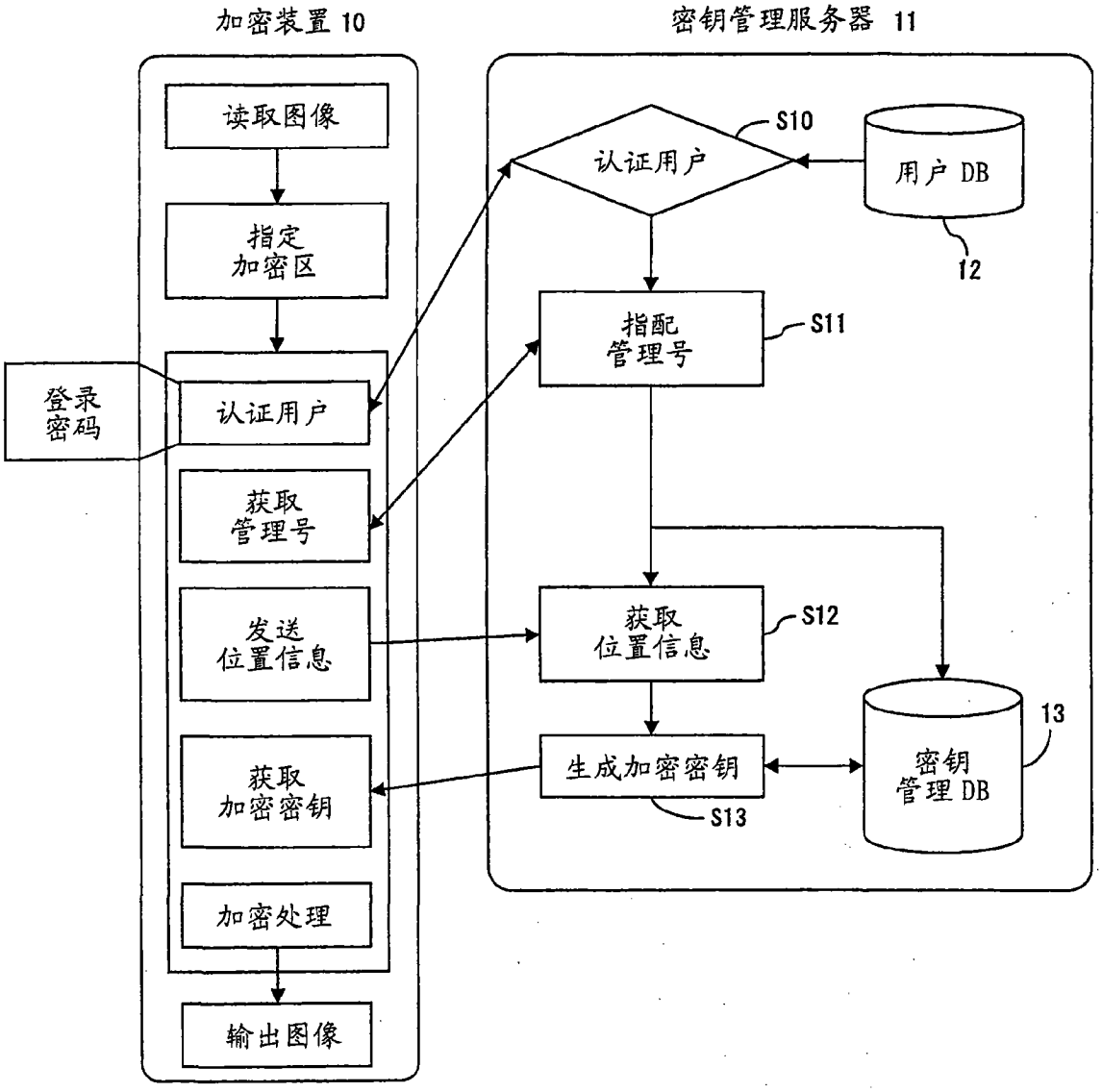

加密装置 10
密钥管理服务器 11
读取图像
指定
加密区
登录
密码
认证用户
获取
管理号
发送
位置信息
获取
加密密钥
加密处理
输出图像
认证用户
S10
用户 DB
12
指配
管理号
S11
获取
位置信息
S12
生成加密密钥
S13
密钥
管理 DB
13

图 2

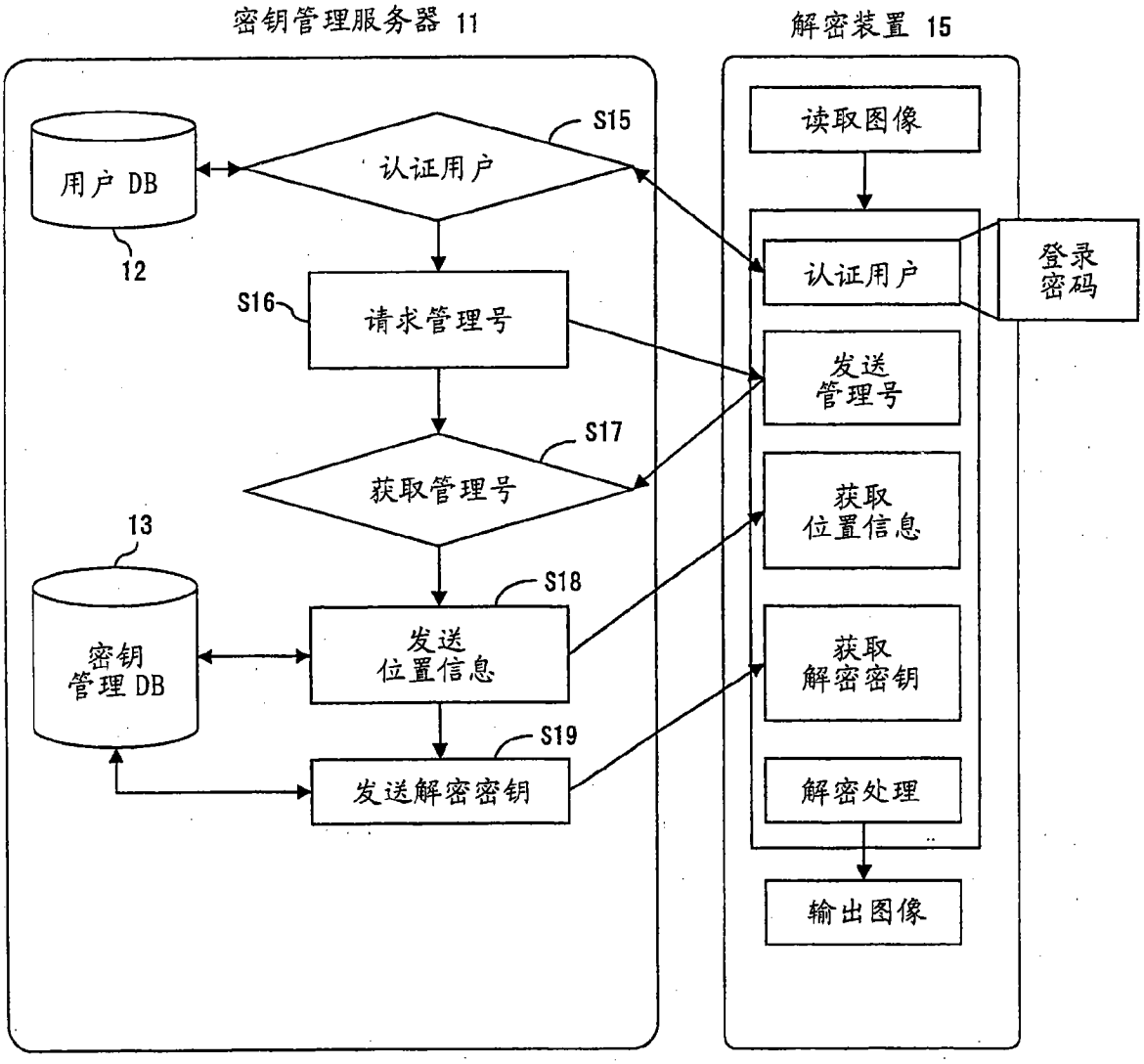

密钥管理服务器 11
解密装置 15
用户 DB
12
S15
认证用户
S16
请求管理号
S17
获取管理号
13
密钥
管理 DB
S18
发送
位置信息
S19
发送解密密钥
读取图像
认证用户
登录
密码
发送
管理号
获取
位置信息
获取
解密密钥
解密处理
输出图像

图 3

用户 ID	密码
AB1234	49g6x0z987
CD5678	38fg76dv76
EF9977	1098fg7674
GH9021	7fds09gf79

图 4

管理号	位置信息	解密密钥
1996040103	(20, 1502)-(40, 1720)	AD8CX65Y
2001100102	(356, 2498)-(396, 2742)	2BV5ZMUE
2003032101	(648, 232)-(900, 900)	P90EAQ1H
2003032101	(1988, 128)-(2512, 2498)	CXZ0W3FE

图 5

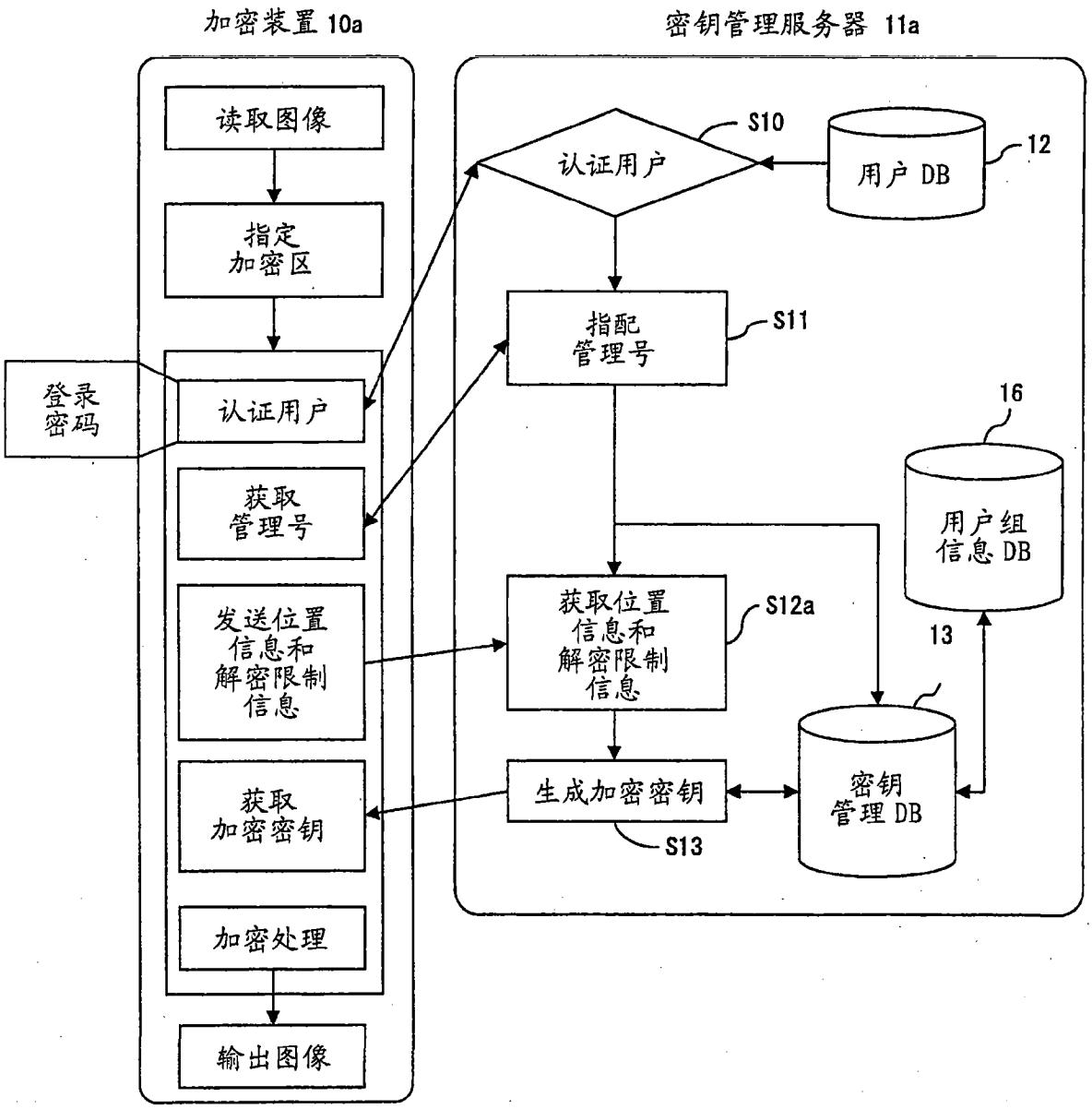

加密装置 10a
密钥管理服务器 11a
读取图像
指定
加密区
登录
密码
认证用户
获取
管理号
发送位置
信息和
解密限制
信息
获取
加密密钥
加密处理
输出图像
认证用户
S10
用户 DB
12
指配
管理号
S11
16
用户组
信息 DB
获取位置
信息和
解密限制
信息
S12a
13
生成加密密钥
密钥
管理 DB
S13

图 6

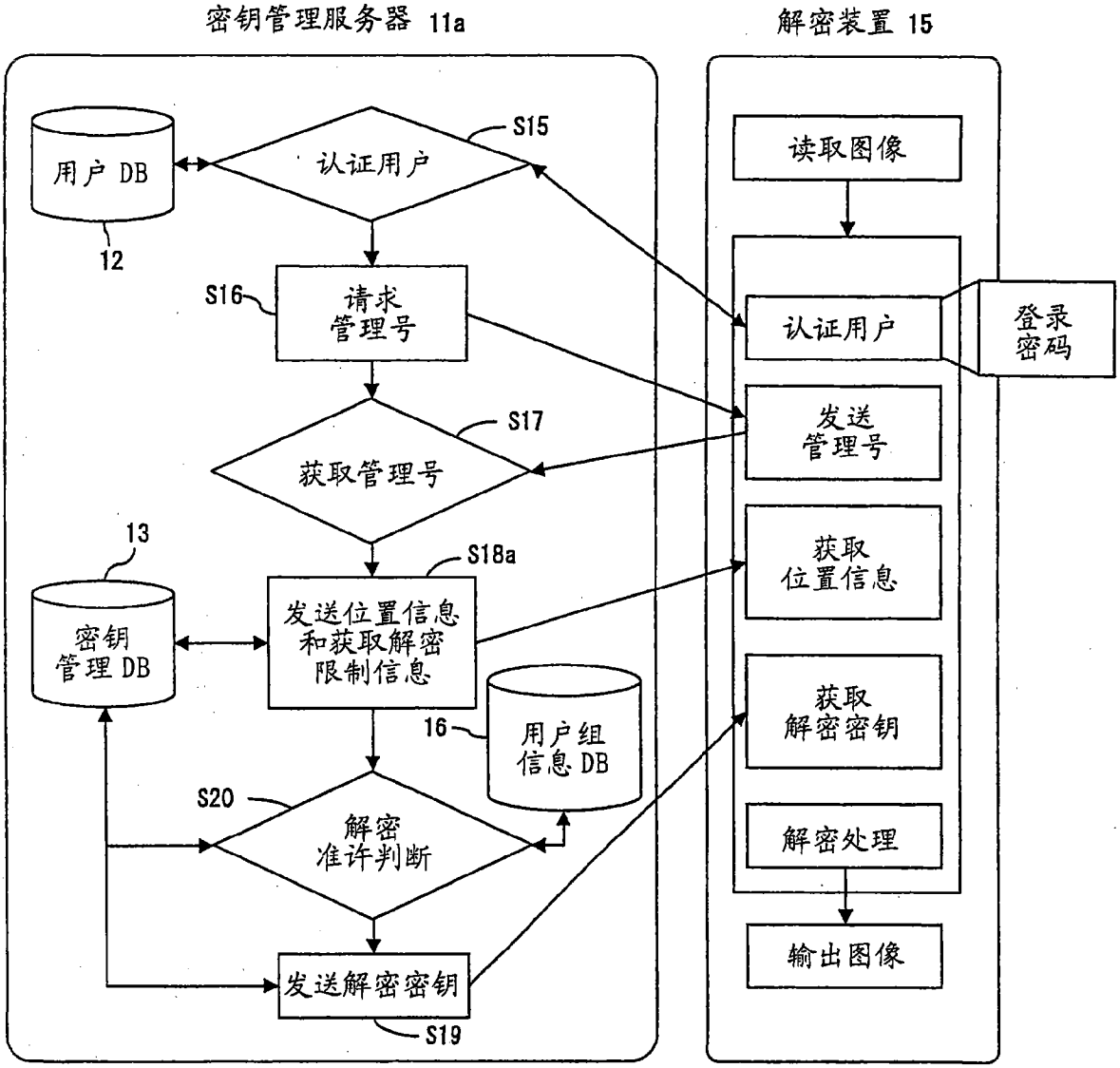

密钥管理服务器 11a
解密装置 15
用户 DB
12
认证用户
S15
请求
管理号
S16
获取管理号
S17
13
密钥
管理 DB
S18a
发送位置信息
和获取解密
限制信息
16
用户组
信息 DB
S20
解密
准许判断
发送解密密钥
S19
读取图像
认证用户
登录
密码
发送
管理号
获取
位置信息
获取
解密密钥
解密处理
输出图像

图 7

管理号	位置信息	解密权限	解密时段	解密密钥
1996040103	(20, 1502)-(40, 1720)	5 级	30 天	AD8CX65Y
2001100102	(356, 2498)-(396, 2742)	3 级	60 天	2BV5ZMUE
2003032101	(648, 232)-(900, 900)	8 级	7 天	P90EAQ1H
2003032101	(1988, 128)-(2512, 2498)	1 级	∞	CXZ0W3FE

图 8

管理号	位置信息	解密权限	解密开始日期和时间	解密结束日期和时间	解密密钥
1996040103	(20, 1502)-(40, 1720)	5 级	APL.1.1996 8:00	APL.30.1996 24:00	AD8CX65Y
2001100102	(356, 2498)-(396, 2742)	3 级	OCT.1.2001 10:00	DEC.30.2001 8:00	2BV5ZMUE
2003032101	(648, 232)-(900, 900)	8 级	MAR.21.2003 13:20	MAR.28.2003 12:20	P90EAQ1H
2003032101	(1988, 128)-(2512, 2498)	1 级	MAY.21.2003 13:00	∞	CXZ0W3FE

图 9

用户 ID	组
AB1234	组 A
CD5678	组 A
EF9977	组 B
GH9021	组 C

表 1

组	解密权限
组 A	1 级
组 B	3 级
组 C	3 级

表 2

图 10

管理号	位置信息	被准许解密的用户 ID	解密时段	解密密钥
1996040103	(20, 1502)-(40, 1720)	AB1234	30 天	AD8CX65Y
2001100102	(356, 2498)-(396, 2742)	AB1234	60 天	2BV5ZMUE
2003032101	(648, 232)-(900, 900)	EF9977	7 天	P90EAQ1H
2003032101	(1988, 128)-(2512, 2496)	CD5678, GH9021	∞	CXZ0W3FE

图 11

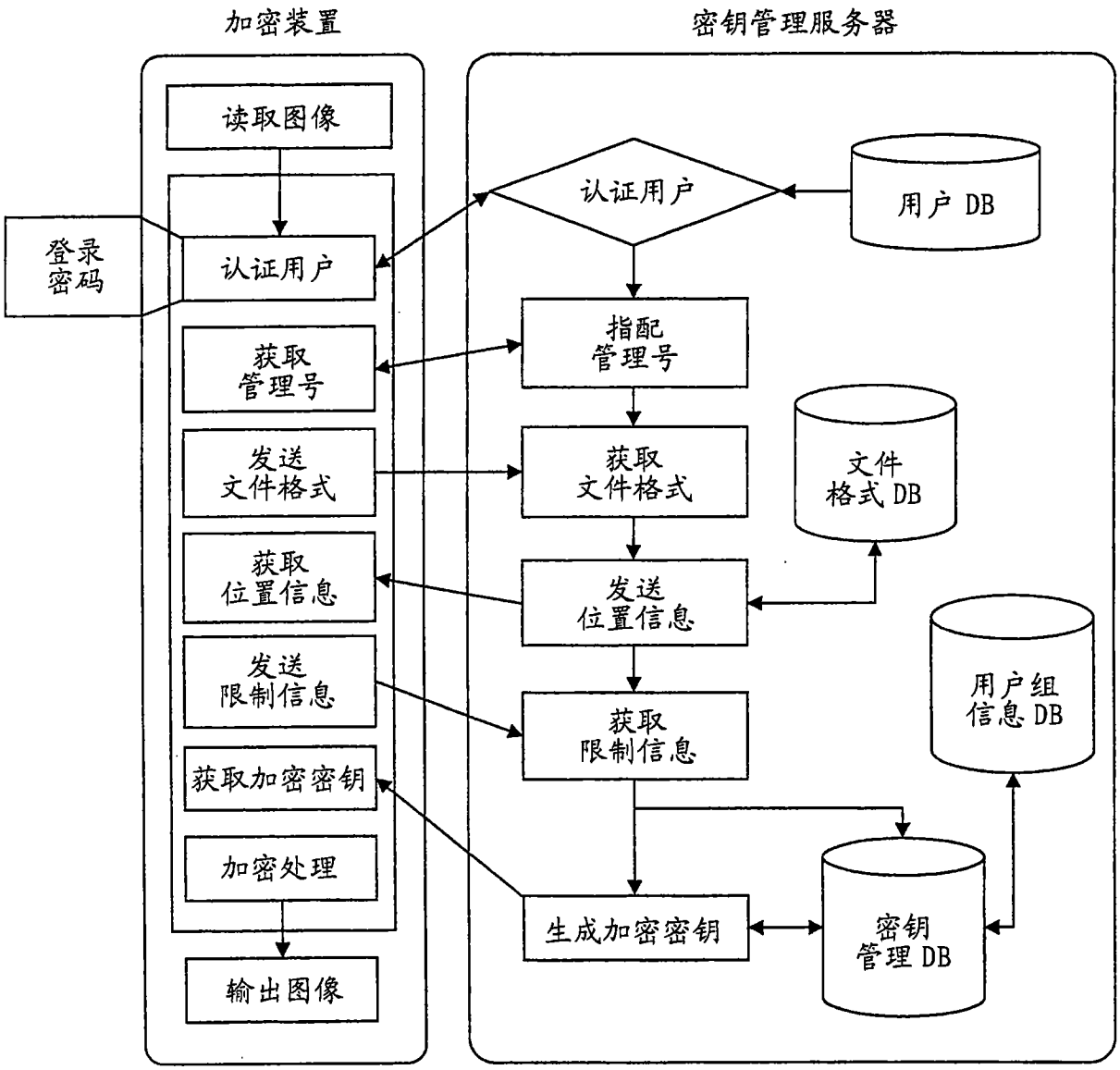

加密装置
密钥管理服务器
读取图像
登录密码
认证用户
获取管理号
发送文件格式
获取位置信息
发送限制信息
获取加密密钥
加密处理
输出图像
认证用户
用户 DB
指配管理号
获取文件格式
文件格式 DB
发送位置信息
用户组信息 DB
获取限制信息
生成加密密钥
密钥管理 DB

图 12

文件格式	区号	位置信息
类型 1	1	(20, 1502)·(40, 1720)
类型 1	2	(356, 2498)·(396, 2742)
类型 2	1	(102, 438)·(246, 238)
类型 2	2	(648, 232)·(900, 900)
类型 2	3	(1988, 128)·(2512, 2498)

图 13

文件格式	区号	位置信息	解密权限	解密开始日期和时间	解密结束日期和时间
类型 1	1	(20, 1502) - (40, 1720)	5 级	APL.1.1996 8:00	APL.30.1996 24:00
类型 1	2	(356, 2498) - (396, 2742)	3 级	OCT.1.2001 10:00	DEC.30.2001 8:00
类型 2	1	(102, 438) - (246, 238)	8 级	MAR.21.2003 13:20	MAR.28.2003 12:20
类型 2	2	(648, 232) - (900, 900)	1 级	MAY.21.2003 13:00	∞
类型 2	3	(1988, 128) - (2512, 2498)	2 级	JUN.1.2003 13:00	JUN.30.2003 13:00

图 14

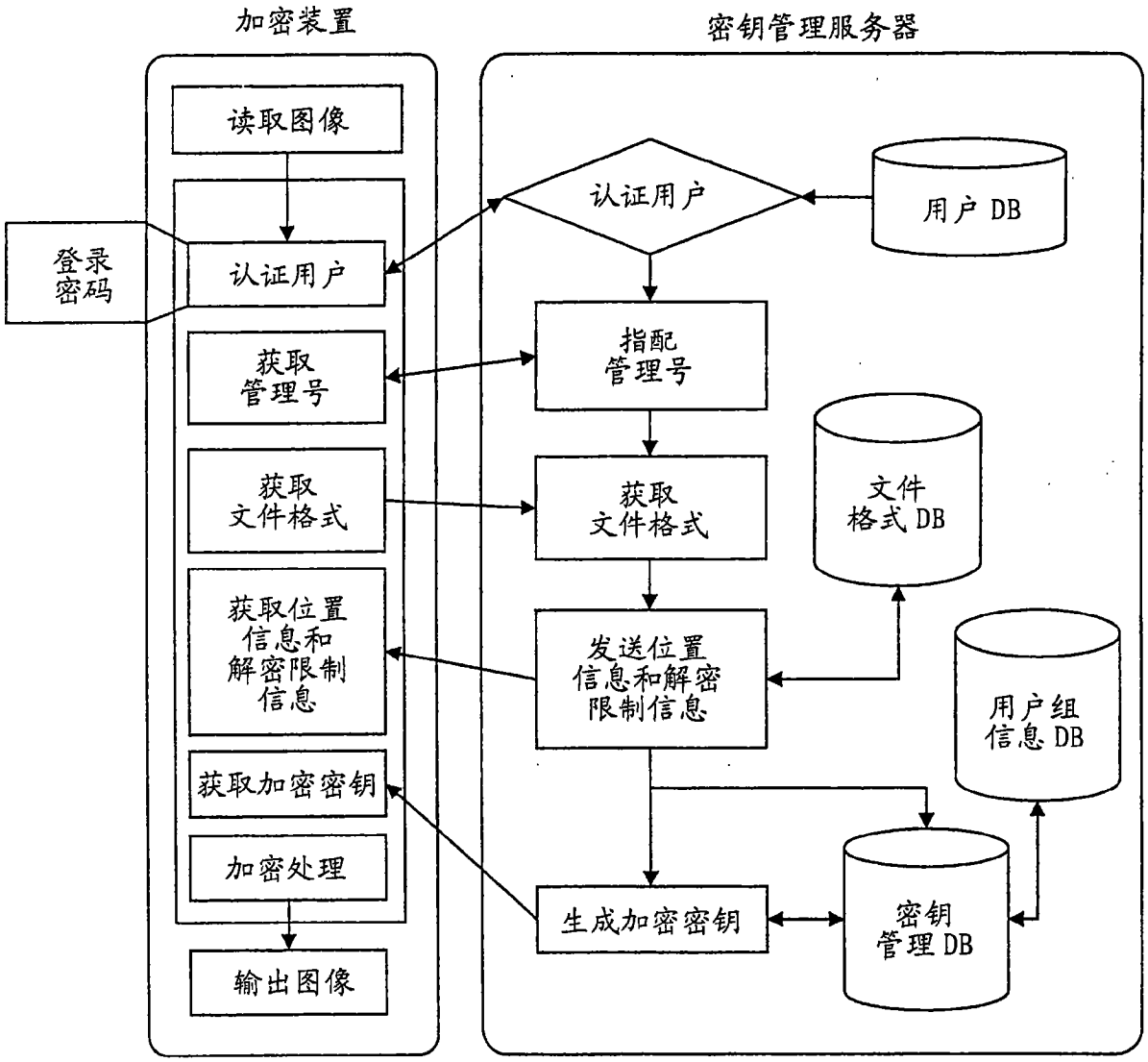

加密装置
密钥管理服务器
读取图像
登录密码
认证用户
获取管理号
获取文件格式
获取位置信息和解密限制信息
获取加密密钥
加密处理
输出图像
认证用户
用户 DB
指配管理号
获取文件格式
文件格式 DB
发送位置信息和解密限制信息
用户组信息 DB
生成加密密钥
密钥管理 DB

图 15

管理号	文件格式	区号	解密权限	解密开始日期和时间	解密结束日期和时间	解密密钥
1996040103	类型 1	1	5 级	APL.1.1996 8:00	APL.30.1996 24:00	AD8CX65Y
1996040103	类型 1	2	3 级	OCT.1.2001 10:00	DEC.30.2001 8:00	2BV5ZMUE
2003032101	类型 2	1	8 级	MAR.21.2003 13:20	MAR.28.2003 12:20	P90EAQ1H
2003032101	类型 2	2	1 级	MAY.21.2003 13:00	∞	CXZ0W3FE
2003032101	类型 2	2	2 级	JUN.1.2003 13:00	JUN.30.2003 13:00	SI78JH67

图 16

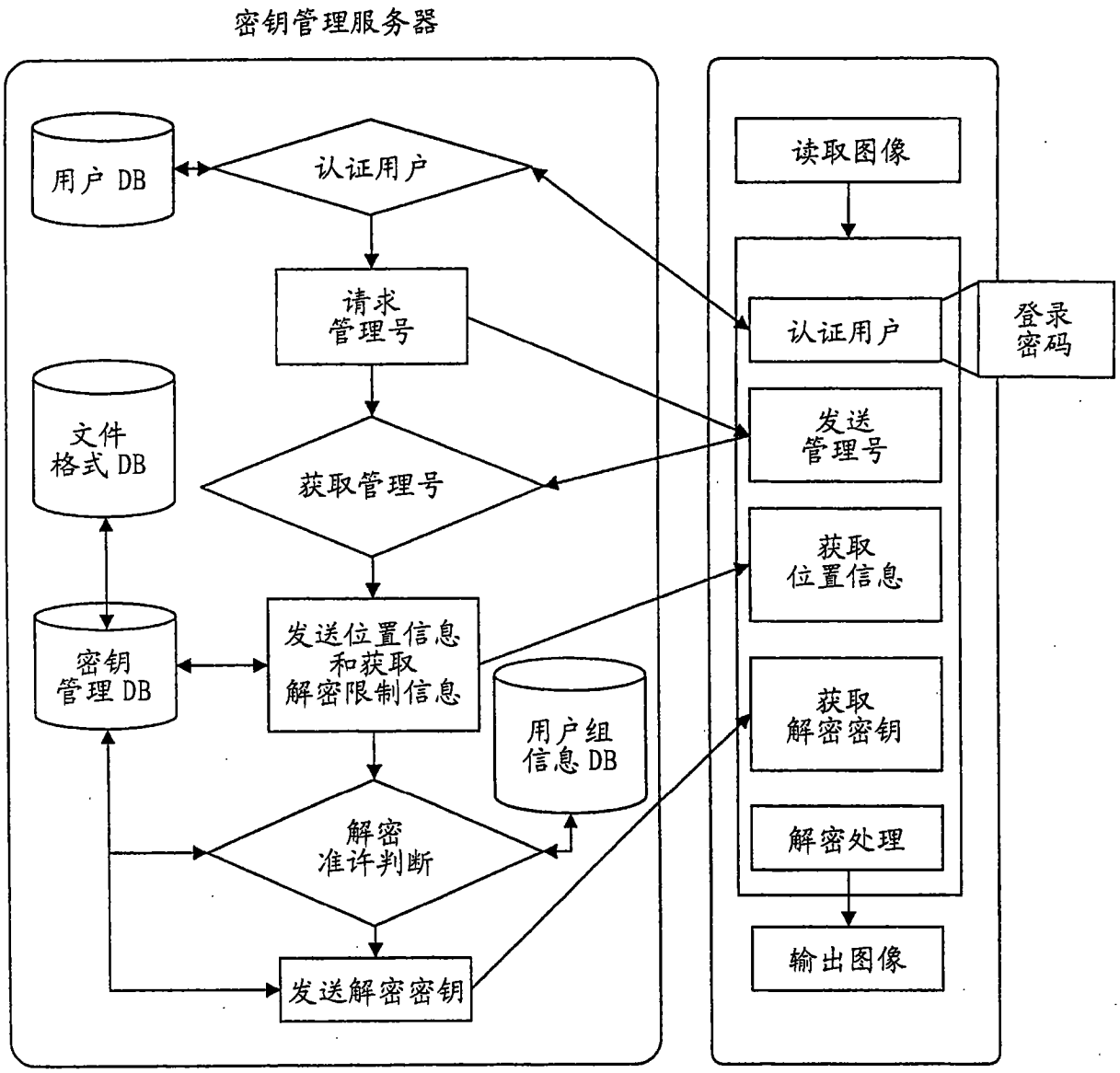

密钥管理服务器
用户 DB
认证用户
请求
管理号
文件
格式 DB
获取管理号
密钥
管理 DB
发送位置信息
和获取
解密限制信息
用户组
信息 DB
解密
准许判断
发送解密密钥
读取图像
认证用户
登录
密码
发送
管理号
获取
位置信息
获取
解密密钥
解密处理
输出图像

图 17

管理号	位置信息	准许解密的次数	执行解密的次数	解密密钥
1996040103	(20, 1502)・(40, 1720)	5	3	AD8CX65Y
2001100102	(356, 2498)・(396, 2742)	100	52	2BV5ZMUE
2003032101	(648, 232)・(900, 900)	1	0	P90EAQ1H
2003032101	(1988, 128)・(2512, 2498)	∞	19865	CXZ0W3FE

图 18

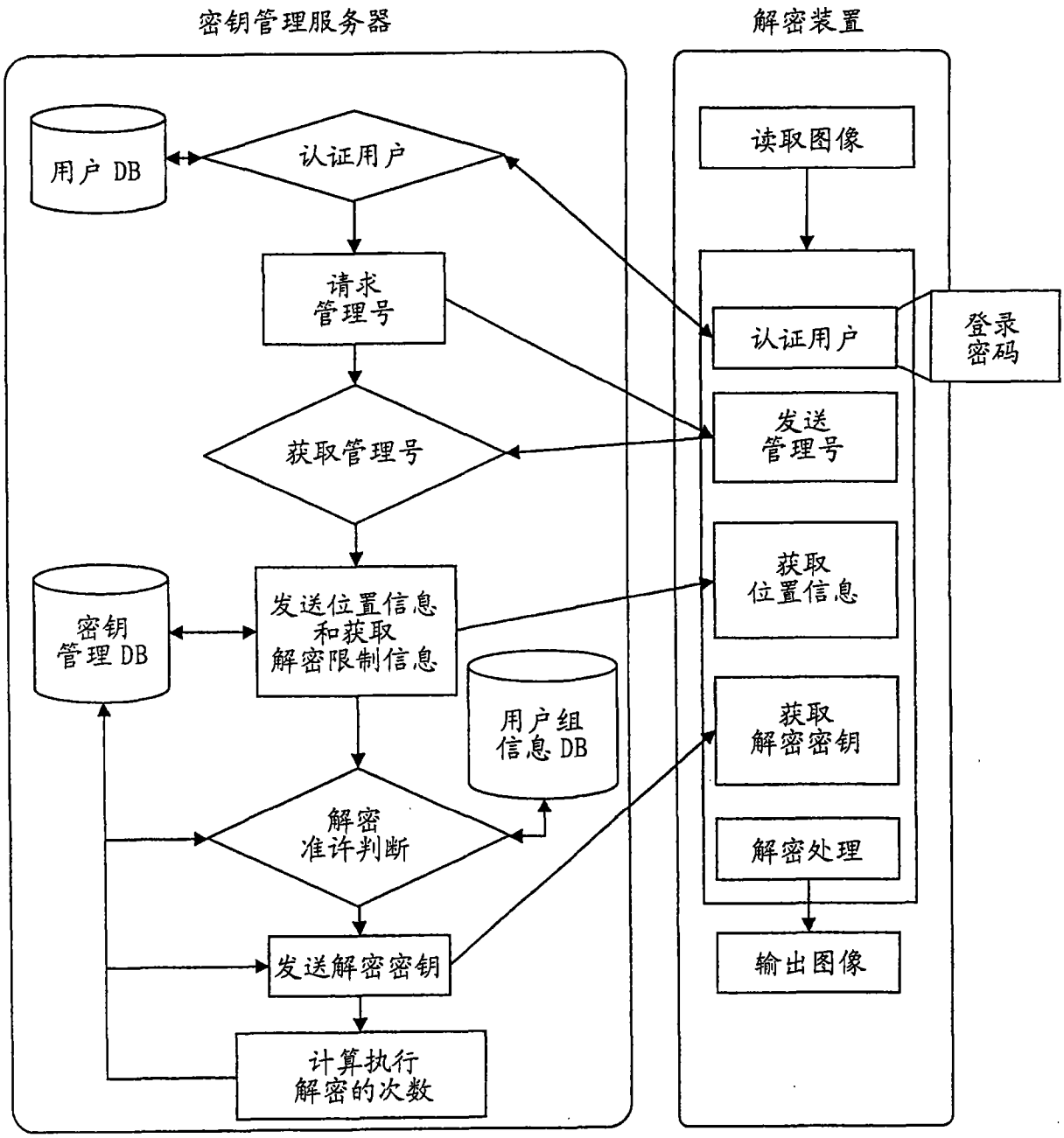

密钥管理服务器
解密装置
用户 DB
认证用户
请求
管理号
获取管理号
密钥
管理 DB
发送位置信息
和获取
解密限制信息
用户组
信息 DB
解密
准许判断
发送解密密钥
计算执行
解密的次数
读取图像
认证用户
登录
密码
发送
管理号
获取
位置信息
获取
解密密钥
解密处理
输出图像

图 19

管理号	位置信息	用户 ID	准许解密的次数	执行解密的次数	解密密钥
1996040103	(20, 1502)・(40, 1720)	AB1234	5	1	AD8CX65Y
1996040103	(20, 1502)・(40, 1720)	EF9977	5	0	AD8CX65Y
1996040103	(20, 1502)・(40, 1720)	CD5678	5	3	AD8CX65Y
2001100102	(356, 2498)・(396, 2742)	GH9021	5	5	2BV5ZMUE
2001100102	(356, 2498)・(396, 2742)	ZT3974	20	12	2BV5ZMUE
2001100102	(356, 2498)・(396, 2742)	JD2970	100	52	2BV5ZMUE

图 20