[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04N 1/00 (2006.01)
H04N 1/32 (2006.01)
H04L 9/32 (2006.01)
H04N 101/00 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200710108410.8

[43] 公开日 2007 年 12 月 12 日

[11] 公开号 CN 101087342A

[22] 申请日 2007.6.7

[21] 申请号 200710108410.8

[30] 优先权

[32] 2006. 6. 7 [33] JP [31] 2006 - 159144

[71] 申请人 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 田头信博

[74] 专利代理机构 北京林达刘知识产权代理事务所

代理人 刘新宇

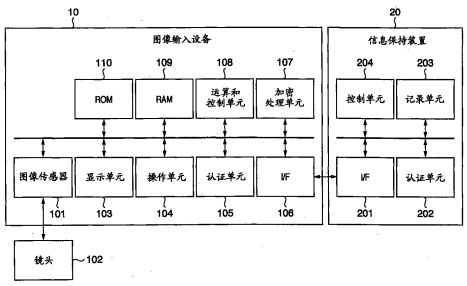
权利要求书 2 页 说明书 17 页 附图 6 页

[54] 发明名称

数据处理设备和方法

[57] 摘要

本发明提供一种数据处理设备和方法。目的是为了实现抗攻击性强、过程简单的装置认证。因此，图像输入设备的认证单元将第一数据发送给信息保持装置的认证单元，并从认证单元接收加密后的密钥信息和根据第一数据生成的第二数据。认证单元基于第一数据和第二数据，认证对方装置。在认证成功的情况下，图像输入设备的认证单元对加密后的密钥信息进行解密以获取密钥信息。然后，图像输入设备使用该密钥信息对数据进行加密，并将加密后的数据发送给对方装置。



1. 一种数据处理设备，其包括：

发送部件，用于将第一数据发送给对方装置；

接收部件，用于从所述对方装置接收加密后的密钥信息和根据所述第一数据生成的第二数据；

认证部件，用于基于所述第一数据和所述第二数据，认证所述对方装置；

解密部件，用于在所述认证成功的情况下，对加密后的所述密钥信息进行解密以获取密钥信息；以及

加密部件，用于使用所述密钥信息对数据进行加密，以将加密后的所述数据发送给所述对方装置。

2. 根据权利要求1所述的数据处理设备，其特征在于，还包括保持部件，所述保持部件用于将解密后的所述密钥信息保持预定的时间段。

3. 根据权利要求1所述的数据处理设备，其特征在于，还包括对方装置。

4. 根据权利要求3所述的数据处理设备，其特征在于，所述对方装置包括用于存储所述密钥信息或加密后的所述密钥信息的存储卡，并且所述对方装置可以存储加密后的所述数据。

5. 根据权利要求1所述的数据处理设备，其特征在于，所述第一数据是随机数，并通过对所述随机数进行加密获得所述第二数据。

6. 一种数据处理设备，其包括：

第一接收部件，用于从对方装置接收第一数据；

生成部件，用于根据所述第一数据生成第二数据；以及

发送部件，用于将所述第二数据和加密后的密钥信息发送给所述对方装置。

7. 根据权利要求6所述的数据处理设备，其特征在于，还

包括第二接收部件，所述第二接收部件用于接收用可通过对加密后的所述密钥信息进行解密而获得的密钥信息加密的数据。

8. 根据权利要求7所述的数据处理设备，其特征在于，还包括存储部件，所述存储部件用于存储所述密钥信息或加密后的所述密钥信息，所述存储部件能够存储由所述第二接收部件接收到的加密后的所述数据。

9. 一种数据处理方法，其包括以下步骤：

将第一数据发送给对方装置；

从所述对方装置接收加密后的密钥信息和根据所述第一数据生成的第二数据；

基于所述第一数据和所述第二数据，认证所述对方装置；

在所述认证成功的情况下，对加密后的所述密钥信息进行解密以获取密钥信息；以及

使用所述密钥信息对数据进行加密，以将加密后的所述数据发送给所述对方装置。

10. 一种数据处理方法，其包括以下步骤：

从对方装置接收第一数据；

根据所述第一数据生成第二数据；以及

将所述第二数据和加密后的密钥信息发送给所述对方装置。

数据处理设备和方法

技术领域

本发明涉及相互连接的设备之间的认证和加密技术。

背景技术

近年来，使用数字照相机的图像拍摄已经普及。这是因为数字照相机所拍摄的图像不会随着时间而劣化，可以容易地存储和搜索该图像，并且可以容易地将该图像发送到远方。

随着半导体工艺的发展，用于记录图像数据的存储卡的容量迅速增加。近年来，甚至千兆字节量级的存储卡也已经开始普及，一个存储卡可以记录大量的图像数据。另一方面，从丢失或被盗的存储卡可能一次泄漏大量的图像数据。从秘密保护的观点出发，大量图像数据的泄漏会造成严重的问题。

作为防止图像数据泄漏的措施，提出了一种在数字照相机内对该数字照相机所拍摄的图像进行加密、并将加密后的图像数据记录在存储卡上的方法。为了使加密有效，必须安全地管理加密所需的密钥信息。以下是可能的管理数字照相机内的密钥信息的方法：

(1)在数字照相机内管理密钥信息的方法；以及

(2)在加密时，从数字照相机外输入密钥信息的方法。

方法(1)被称为“内部密钥方法”，方法(2)被称为“外部密钥方法”。

(1)内部密钥方法

根据加密算法的分类，可将内部密钥方法划分为两种类型：“公用密钥加密模型(common-key cryptographic model)”和“公开密钥加密模型(public-key cryptographic model)”。

根据公用密钥加密模型的内部密钥方法，仅加密侧和解密

侧秘密保持公用密钥。如果该方法假定个人计算机(PC)使用加密后的图像数据，则必须与该PC共享秘密保持在数字照相机中的公用密钥。

公开密钥加密模型的内部密钥方法可以使加密密钥(公开密钥)与解密密钥(秘密密钥)互不相同，并且可以向公众公开加密密钥。数字照相机对加密所需的公开密钥进行管理，由于公开密钥加密模型的特征而使该管理非常容易。然而，公开密钥加密模型产生比公用密钥加密模型更重的处理负荷。数字照相机的处理能力较差，公开密钥加密模型的处理负荷会造成问题。

(2)外部密钥方法

根据用于管理密钥信息的实体，可将外部密钥方法划分为两种类型："人模型"和"装置模型"。

根据人模型的外部密钥方法，加密时，用户向数字照相机输入密钥信息。为了使加密有效，使用至少预定长度的随机密钥信息(例如，至少预定长度的个人识别码(personal identification number，PIN))。然而，数字照相机仅具有包括拨盘和按钮在内的有限的用户界面。因此通过数字照相机的用户界面输入密钥信息在实用上有缺陷。

根据装置模型的外部密钥方法，将保持密钥信息的装置安装在数字照相机中，以在加密时从该装置装载密钥信息。象智能卡(smart card)一样，该方法具有对破坏攻击等的抵抗性，并且可以采用具有管理密钥信息的各种特性并具有处理能力的装置。

例如，存在被称为MOPASS(mobile passport，移动口令)卡的装置。MOPASS卡是闪存和智能卡的集成卡，并具有与闪存相同的物理形状。MOPASS卡可用作不向数字照相机提供新的物理接口而具有与智能卡相同的抗攻击性的装置。通过使用

具有这种抗攻击性的装置，可认为保持在该装置中的密钥信息是安全的。

●装置认证

从一套数字照相机和装置的观点出发，重要的是安装在数字照相机内的装置是否保持了所期望的密钥信息。对此，一个解决方案是基于ISO/IEC9798系列的装置认证(或对方认证)。根据装置认证，当通过将保持密钥信息的装置安装在数字照相机中来使用该装置时，数字照相机确认该装置是否是保持所期望的密钥信息的经认证的装置，该装置确认数字照相机是否应当接收密钥信息。也就是说，数字照相机和装置进行相互认证。

考虑到在许多情况下数字照相机不连接到网络而使用。因此，认证不能利用第三方。基于ISO/IEC9798系列的认证方法中不使用第三方的相互认证方法如下：

使用公用密钥加密模型的二次通过(two-pass)认证方法(ISO/IEC9798-2)

实体A和B共享秘密密钥K。实体A将通过秘密密钥K加密的消息M(E_K(M))发送给实体B。实体B对加密消息E_K(M)进行解密，并验证消息M的确定性以对实体A进行认证。实体A通过逆向执行相同的过程对实体B进行认证。

使用公用密钥加密模型的三次通过(three-pass)认证方法(ISO/IEC9798-2)

实体A和B共享秘密密钥K。实体A通过询问-应答(challenge-response)方法对实体B进行认证。实体B使用秘密密钥K和公用密钥加密模型生成应答。实体B通过逆向执行相同的过程对实体A进行认证。当从实体B向实体A发送回应答时，可通过增加询问来削减一次通过。

使用公开密钥加密模型的二次通过认证方法

(ISO/IEC9798-3)

实体A将添加过数字签名的消息M发送给实体B。实体B通过实体A的公开密钥验证消息M的数字签名以对实体A进行认证。实体A通过逆向执行相同的过程对实体B进行认证。

使用公开密钥加密模型的三次通过认证方法(ISO/IEC9798-3)

除使用数字签名生成应答之外，该方法同样基于与使用公用密钥加密模型的三次通过认证方法(ISO/IEC9798-2)相同的询问-应答方法。

使用MAC的二次通过认证方法(ISO/IEC9798-4)

除了生成MAC(Message Authentication Code，消息认证码)代替加密消息$E_K(M)$之外，该认证方法与使用公用密钥加密模型的二次通过认证方法(ISO/IEC9798-2)相同。

使用MAC的三次通过认证方法(ISO/IEC9798-4)

除了使用MAC生成应答以外，该认证方法同样基于与使用公用密钥加密模型的三次通过认证方法(ISO/IEC9798-2)相同的询问-应答方法。

●数字照相机的问题

在通过装置模型的外部密钥方法与装置认证的简单组合在数字照相机内对图像进行加密的方法中，仍有以下未解决的问题。

第一，装置认证产生问题。更具体地，必须执行两次认证(相互认证)：数字照相机对保持密钥的装置进行认证，并且该装置对数字照相机进行认证。也就是说，数字照相机和装置二者都必须具有认证功能。结果，处理过程和功能安装可能变得冗长。

第二，数字照相机需要从外部接收密钥信息的功能。与第一个问题类似，处理过程和功能安装可能变得复杂。

●装置认证的问题

当与传统方法简单组合时，装置认证遇到以下问题。

二次通过认证方法实质上不能抵抗重放攻击(replay attack)。例如，在使用公用密钥加密模型的二次通过认证方法(ISO/IEC9798-2)中，攻击者窃听实体A和B之间的通信路径，获取加密消息$E_K(M)$，并将该加密消息$E_K(M)$发送回实体B。这样将攻击者伪装成实体A。

三次通过认证方法花费较长时间进行三次通过消息交换(过程)直到完成装置认证为止。

发明内容

在一个方面，一种数据处理设备包括：发送部件，用于将第一数据发送给对方装置；接收部件，用于从对方装置接收加密后的密钥信息和根据第一数据生成的第二数据；认证部件，用于基于第一数据和第二数据，认证对方装置；解密部件，用于在认证成功的情况下，对加密后的密钥信息进行解密以获取密钥信息；以及加密部件，用于使用密钥信息对数据进行加密，以将加密后的数据发送给对方装置。

在另一方面，一种数据处理设备包括：第一接收部件，用于从对方装置接收第一数据；生成部件，用于根据第一数据生成第二数据；以及发送部件，用于将第二数据和加密后的密钥信息发送给对方装置。

在另一方面，一种数据处理方法包括以下步骤：将第一数据发送给对方装置；从对方装置接收加密后的密钥信息和根据第一数据生成的第二数据；基于第一数据和第二数据，认证对方装置；在认证成功的情况下，对加密后的密钥信息进行解密以获取密钥信息；以及使用密钥信息对数据进行加密，以将加

密后的数据发送给对方装置。

在另一方面，一种数据处理方法包括以下步骤：从对方装置接收第一数据；根据第一数据生成第二数据；以及将第二数据和加密后的密钥信息发送给对方装置。

根据这些方面，实现了抗攻击性强、过程简单的装置认证。

通过以下参考附图对典型实施例的说明，本发明的其它特征将显而易见。

附图说明

图1是示出具有装置认证功能的图像处理设备的配置的框图；

图2是示出认证单元的配置的框图；

图3是示出由认证单元执行的装置认证处理的流程图；

图4是示出输入图像的加密处理的流程图；

图5是示出第二实施例中的认证单元的配置的框图；以及

图6是示出第三实施例中具有装置认证功能的图像处理设备的配置的框图。

具体实施方式

下面参考附图详细说明根据本发明的信息处理设备和方法。

第一实施例

认证系统的结构

图1是示出具有装置认证功能的图像处理设备的配置的框图。

该图像处理设备包括数字照相机等图像输入设备10和智能卡等抗攻击信息保持装置20。在实现图像处理设备时，无需使

用图1所示的全部构件。由图像输入设备10感测到的图像不局限于静止图像，还包括运动图像。

●图像输入设备

在图像输入设备10中，CCD或CMOS传感器等图像传感器101将通过镜头102输入的光转换成电信号。显示单元103在液晶监视器和多个显示面板上显示图像数据以及图像输入设备10的各种设置值和状态。操作单元104包括各种按钮、设置拨盘等，并允许图像输入设备10的用户输入各种指示。

运算和控制单元108使用RAM 109作为工作存储器，并执行存储在ROM 110中的程序以控制图像输入设备10的各单元。运算和控制单元108将从图像传感器101输出的电信号转换成数字信号，并执行数字信号的编码和压缩等图像处理，从而生成所拍摄图像的图像数据。

使用由认证单元105所保持的密钥信息作为加密密钥，加密处理单元107对由运算和控制单元108所生成的图像数据进行加密。加密算法可以采用AES(Advanced Encryption Standard，高级加密标准)等各种公用密钥加密模型。

认证单元105对信息保持装置20的合法性进行认证。当认证单元105对信息保持装置20进行认证时，其对从信息保持装置20接收到的加密后的密钥信息进行解密，并临时保持解密后的密钥信息，稍后对其进行详细说明。

密钥信息保持期可被设置成等于认证合法性维持期。例如，认证单元105可以在加密处理单元107的每个处理周期进行认证，保持密钥信息，并在使用该密钥信息后删除它。可选地，每当信息保持装置20连接到图像输入设备10(或安装在图像输入设备10中)时，认证单元105可以进行认证并保持密钥信息。在这种情况下，认证单元105可以一直保持密钥信息，直到信息

保持装置20从图像输入设备10断开连接(或卸下)为止。当密钥信息包含用于验证完整性的信息(例如，校验和或散列值)时，认证单元105还可以验证密钥信息的完整性，对信息保持装置20的合法性进行认证，并且当验证了解密后的密钥信息的完整性时，临时保持该密钥信息。

接口(I/F)106提供与信息保持装置20的接口，并具有与信息保持装置20相对应的物理形状、连接器等。如果信息保持装置20未直接安装在图像输入设备10中，则I/F 106可以是USB(universal serial bus，通用串行总线)或IEEE1394等串行总线接口，或者是有线、无线、或红外通信接口。

•信息保持装置

信息保持装置20的控制单元204控制记录单元203和I/F 201。记录单元203是用于保持图像数据等的非易失性存储器。认证单元202向图像输入设备10证明信息保持装置20的合法性，稍后对此进行详细说明。此外，认证单元202对其所保持的密钥信息进行加密，并将加密后的密钥信息发送到图像输入设备10。I/F 201是与图像输入设备10的I/F 106相对应的接口。

用于装置认证的配置

图2是示出图1所示的认证单元105和202的配置的框图。

认证单元105的随机数生成单元111生成随机数RND，并将该随机数RND临时保持在随机数生成单元111内。此外，随机数生成单元111通过I/F 106将随机数RND作为询问数据CHA发送到认证单元202。

运算单元112根据随机数生成单元111临时保持的随机数RND生成验证数据f(RND)。生成验证数据的函数f()是与运算单元211秘密共享的函数，并且可以根据输入数据生成特定的输出数据以对对方进行认证。例如，可以使用在图像输入设备10

和信息保持装置20之间共享的系统密钥Ks，通过MAC(消息认证码)或加密函数来实现函数f()。

比较单元113验证信息保持装置20的合法性。更具体地，比较单元113将从认证单元202接收到的应答数据RES与运算单元112所生成的验证数据f(RND)进行比较。当这两个数据相互一致时，比较单元113判断为成功验证了信息保持装置20的合法性，并运行解密单元115。如果RES和f(RND)相互不一致，则比较单元113判断为信息保持装置20的合法性的验证失败，并且不运行解密单元115。

解密单元115对从认证单元202接收到的加密后的密钥信息$E_{Ks}(Ki)$进行解密，获得用于加密图像数据的密钥信息Ki。用于解密的密钥是系统密钥保持单元116所保持的系统密钥Ks。加密算法可以采用与认证单元202的加密单元212所采用的加密算法相对应的AES等各种通用密钥加密模型。解密单元115还可以在密钥信息包含用于验证完整性的信息(例如，校验和或散列值)时验证完整性。

密钥信息临时保持单元114临时保持由解密单元115所获得的密钥信息Ki。系统密钥保持单元116保持在图像输入设备10与信息保持装置20之间共享的系统密钥Ks。勿庸置疑，系统密钥Ks必须秘密且完整地保持。系统密钥Ks是具有依赖于加密单元212和解密单元115的加密算法的格式的密钥信息。例如，当加密算法是AES时，系统密钥Ks是128位的密钥信息。

认证单元202的运算单元211通过I/F 201从认证单元105接收询问数据CHA。运算单元211生成应答数据RES(=f(CHA))，并通过I/F 201将该应答数据发送到认证单元105。生成应答数据的函数f()与运算单元112用来生成验证数据的函数f()相同。

密钥信息保持单元213保持用于加密图像数据的密钥信息

Ki。勿庸置疑，密钥信息Ki必须秘密且完整地保持。密钥信息保持单元213可以通过在密钥信息中设置校验和或散列值来验证密钥信息的完整性。

加密单元212对密钥信息保持单元213所保持的密钥信息Ki进行加密。用于加密的密钥是系统密钥保持单元214所保持的系统密钥Ks。加密算法对应于认证单元105的解密单元115所使用的加密算法。

与系统密钥保持单元116类似，系统密钥保持单元214保持在图像输入设备10与信息保持装置20之间共享的系统密钥Ks。可以通过配置系统密钥保持单元214以保持加密后的密钥信息$E_{Ks}(Ki)$，来省略加密单元212。

装置认证

图3是示出由认证单元105和202执行的装置认证处理的流程图。

在认证单元105中，随机数生成单元111生成作为询问数据CHA的随机数RND，并将该随机数RND发送到运算单元112和认证单元202(S11)。运算单元112根据所接收到的随机数RND生成验证数据f(RND)(S12)。

在认证单元202中，运算单元211根据从认证单元105接收到的询问数据CHA生成应答数据RES(S21)。加密单元212使用系统密钥保持单元214所保持的系统密钥Ks作为密钥，对密钥信息保持单元213所保持的密钥信息Ki进行加密(S22)。认证单元202将在步骤S21中生成的应答数据RES和在步骤S22中生成的加密后的密钥信息$E_{Ks}(Ki)$发送到认证单元105(S23)。

认证单元105接收应答数据RES和加密后的密钥信息$E_{Ks}(Ki)$(S13)。然后，比较单元113将在步骤S12中生成的验证数据f(RND)与所接收到的应答数据RES进行比较(S14)。如果

这两个数据相互不一致，则处理结束。

如果验证数据f(RND)和应答数据RES相互一致(步骤S15中为“是”)，即验证成功，则解密单元115使用系统密钥保持单元116所保持的系统密钥Ks作为密钥，对所接收到的加密后的密钥信息E_{Ks}(Ki)进行解密(S16)。密钥信息临时保持单元114临时保持通过解密获得的密钥信息Ki(S17)。

当密钥信息保持单元213保持加密后的密钥信息E_{Ks}(Ki)时，可以跳过步骤S22。

图像输入

下面说明当图像输入设备10输入图像时的加密。图4是示出输入图像的加密处理的流程图。

当图像输入设备10的用户按下操作单元104上的快门按钮(或者可以经由PC通过远程控制操作快门)时，运算和控制单元108控制图像传感器101等，并执行图像处理以生成图像数据(S31)。RAM 109存储该图像数据。

认证单元105开始与上述装置认证有关的处理(S32)，并从认证单元202接收加密后的密钥信息E_{Ks}(Ki)等(S33)。如果认证单元105成功认证了信息保持装置20(S34)，则认证单元105对加密后的密钥信息E_{Ks}(Ki)进行解密以获取密钥信息Ki(S35)。

加密处理单元107使用认证单元105所保持的密钥信息Ki，对存储在RAM 109中的图像数据进行加密(S36)。如果装置认证失败并且认证单元105没有保持任何密钥信息，则加密处理单元107不执行任何加密。RAM 109存储加密后的图像数据。

运算和控制单元108通过I/F 106将存储在RAM 109中的加密后的图像数据输出到信息保持装置20(S37)。在从图像输入设备10接收到加密后的图像数据时，信息保持装置20的控制单元204将该数据存储在记录单元203中。如果加密处理单元107

在加密时由于例如认证单元105没有保持密钥信息而失败，则运算和控制单元108可以输出未加密的图像数据，或者可以不输出图像数据。采用这两种处理中的哪一种处理取决于图像输入设备10的控制策略或安全策略。

每次进行快门按钮操作(图像输入指示)，图4中的处理就执行装置认证。如上所述，密钥信息保持期可被设置为各种期间，例如当信息保持装置20连接到图像输入设备10(或安装在图像输入设备10中)时的期间。例如，当信息保持装置20连接到图像输入设备10时，认证单元105执行装置认证并保持密钥信息。认证单元105一直保持密钥信息，直到信息保持装置20从图像输入设备10断开连接(或卸下)为止。每次进行图像输入指示时，保持密钥信息的认证单元105不进行装置认证。当在信息保持装置20安装在图像输入设备10中的情况下打开图像输入设备10的电源时，而不是当连接或安装信息保持装置20时，认证单元105才可以执行认证。类似地，认证单元105可以一直保持密钥信息，直到关闭图像输入设备10的电源而不是从信息保持装置20断开连接(或卸下)为止。换句话说，在打开图像输入设备10的电源时，密钥信息可以由认证单元105保持。

在以上例子中，信息保持装置20的记录单元203存储加密后的图像数据。然而，不需要保存加密后的图像数据和密钥信息Ki的组。因此，除信息保持装置20之外，可以将各种存储卡用作加密后的图像数据的输出目的地。然而，保持密钥信息Ki的信息保持装置20对使用加密后的图像数据来说是不可缺少的。

以上说明与图像传感器101所感测到的图像数据的加密有关。然而，本发明不局限于图像传感器101所感测到的图像数据，还可应用于例如作为数据文件从其它装置输入的图像数据。根据本发明的装置认证和密钥获取方法不局限于加密，还可应用

于解密、MAC生成等。

通过这种方式，第一实施例着眼于装置认证后的处理是将密钥信息从信息保持装置20发送到图像输入设备10的情况。第一实施例通过使用图像输入设备10认证信息保持装置20的询问-应答认证方法和信息保持装置20认证图像输入设备10的消息认证方法，同时实现了相互认证和密钥信息的传送。消息认证方法是通过共享的系统密钥Ks加密密钥信息并发送加密后的密钥信息的方法。

此外，询问-应答认证方法的消息交换包含消息认证方法的消息。因此，第一实施例可以防止重放攻击，并通过二次通过消息交换实现相互认证。

更具体地，在根据第一实施例的装置认证中，图像输入设备10在处理前根据询问-应答方法认证信息保持装置20(单向认证)。然后，信息保持装置20通过消息认证方法将用于加密的密钥Ki提供给图像输入设备10。换句话说，此时共享密钥。因此，仅经认证的信息保持装置20可以使用(解密)处理过的数据(加密后的图像数据)。这样，实现了图像输入设备10的认证(相互认证)。

通常，高效的相互认证方法必须抵抗相同的威胁，因而两个设备必须执行相同的认证方法。在作为不同认证方法的简单组合的相互认证方法中，不同认证方法的特征之间的差异可能导致脆弱性。然而，第一实施例专用于认证之后的处理，从而可以组合不同的认证方法。通过连接由不同的认证方法所发送的消息，第一实施例可以防止作为消息认证方法中的缺点的重放攻击，并且可以减少作为询问-应答认证方法中的缺点的消息交换处理的次数。

第二实施例

以下说明根据本发明第二实施例的信息处理。在第二实施例中，与第一实施例中相同的附图标记表示相同的部件，不重复对其的详细说明。

在第一实施例的认证过程中，从认证单元202发送到认证单元105的数据是应答数据RES和加密后的密钥信息$E_{Ks}(Ki)$。每次认证时该数据作为整体而改变。每次认证时应答数据RES根据作为随机数的询问数据CHA而改变。然而，根据具有固定值的密钥信息Ki和系统密钥信息Ks生成的加密后的密钥信息取固定值。第二实施例着眼于该情况，下面说明不将加密后的密钥信息设置为固定值的方法。

用于装置认证的配置

图5是示出第二实施例中的认证单元105和202的配置的例子的框图。

认证单元202的加密单元212使用通过对询问数据CHA和系统密钥保持单元214所保持的系统密钥Ks进行逻辑异或(exclusive-OR)而获得的数据作为密钥，生成加密后的信息$E_{Ks}(Ki)$。认证单元105的解密单元115使用通过对询问数据CHA和系统密钥保持单元116所保持的系统密钥Ks进行逻辑异或而获得的数据作为密钥，对加密后的信息$E_{Ks}(Ki)$进行解密。

生成解密单元115和加密单元212所使用的密钥的方法必须是成对的方法，以便解密单元115和加密单元212获得相同的密钥。然而，也可以使用其它方法，只要能获得相同的密钥即可。根据上述方法，对系统密钥Ks和询问数据CHA进行逻辑异或以生成密钥。然而，可以使用各种二输入函数，包括对数据进行逻辑与(AND)的方法以及连接数据以获得散列值的方法。

不仅可以通过使用系统密钥Ks和询问数据CHA，而且还可以通过使用系统密钥Ks和应答数据RES，或者使用三个数据输

入即系统密钥Ks、询问数据CHA和应答数据RES，来生成密钥。尤其在使用应答数据RES时，应答数据RES受认证单元105的随机数生成单元111的输出和认证单元202的运算单元211的输出的影响。这可以防止改变一方装置的密钥固定。

如上所述，第二实施例可获得与第一实施例相同的效果。另外，由于每次认证时从认证单元202发送到认证单元105的加密后的密钥信息变成不同的数据，因此第二实施例可以比第一实施例更可靠地防止重放攻击。

第三实施例

以下说明根据本发明第三实施例的信息处理。在第三实施例中，与第一和第二实施例中相同的附图标记表示相同的部件，不重复对其的详细说明。

第一和第二实施例已经说明了在图像输入设备10和信息保持装置20之间进行装置认证的系统。该系统不是仅适用于生成图像数据的图像输入设备。第三实施例将说明将该系统应用于使用图像数据的图像阅览设备的例子。

认证系统的结构

图6是示出具有装置认证功能的图像处理设备的配置的框图。

该图像处理设备包括信息保持装置20和PC等图像阅览设备30。在实现该图像处理设备时，无需使用图6所示的全部构件。可在图像阅览设备30中阅览(再现)的图像不局限于静止图像，还可包括运动图像。

•图像阅览设备

在图像阅览设备30中，运算和控制单元306使用RAM 307作为工作存储器，并执行存储在ROM 308中的程序以控制图像阅览设备30的各单元。

加密处理单元305使用认证单元303所保持的密钥信息作为解密密钥对加密后的图像数据进行解密。加密算法可以采用AES等各种通用密钥加密模型。

认证单元303对信息保持装置20的合法性进行认证。与第一实施例类似，当认证单元303认证信息保持装置20时，认证单元303对通过I/F 304从信息保持装置20接收到的加密后的密钥信息进行解密，并临时保持解密后的密钥信息。

通过该结构，加密处理单元305对从信息保持装置20的记录单元203加载的加密后的图像数据进行解密，并将其存储在RAM 307中。运算和控制单元306对存储在RAM 307中的图像数据进行必要的图像处理(压缩数据的解压缩处理、视频信号处理等)，并将再现的图像数据显示在显示单元301上。图像阅览设备30的用户操作操作单元302以输入待显示的图像和显示方法等各种指示。

在第一和第二实施例中，待处理的数据是从图像传感器101输入的图像数据，加密处理单元107的操作是加密。相反，在第三实施例中，待处理的数据是从信息保持装置20输入的加密后的图像数据，加密处理单元305的操作是解密。然而，装置认证、获取加密或解密密钥的方法等是相同的。

与第一和第二实施例类似，第三实施例可以在图像阅览设备中同时实现装置认证和密钥传送。第三实施例可以防止重放攻击，并通过二次通过实现消息交换。

典型实施例

本发明可应用于由多个装置(例如，主计算机、接口、读取器、打印机)构成的系统，或者应用于包含单个装置(例如，复印机、传真机)的设备。

本发明可应用于除了三次通过认证方法(ISO/IEC9798-2)

之外的询问-应答方法。

此外，本发明可向计算机系统或设备(例如，个人计算机)提供存储用于进行上述处理的程序代码的存储介质，计算机系统或设备的CPU或MPU从该存储介质读取该程序代码，然后执行该程序。

在这种情况下，从存储介质读取的程序代码实现了根据实施例的功能。

此外，可以使用软盘、硬盘、光盘、磁光盘、CD-ROM、CD-R、磁带、非易失型存储卡和ROM等存储介质来提供该程序代码。

而且，除了根据可通过执行计算机读取的程序代码来实现的以上实施例的上述功能以外，本发明还包括以下情况：运行在计算机上的OS(操作系统)等根据该程序代码的指定进行至少一部分处理，并实现根据以上实施例的功能。

而且，本发明还包括以下情况：在将从存储介质读取的程序代码写入插入计算机中的功能扩展卡或与计算机连接的功能扩展单元中设置的存储器中之后，包含在该功能扩展卡或单元中的CPU等根据该程序代码的指定进行至少一部分处理，并实现以上实施例的功能。

在将本发明应用于上述存储介质的情况下，该存储介质存储与实施例中所述的流程图相对应的程序代码。

尽管参考典型实施例说明了本发明，但是应该理解，本发明不局限于所公开的典型实施例。所附权利要求书的范围符合最宽的解释，从而包含全部这类变形及等同结构和功能。

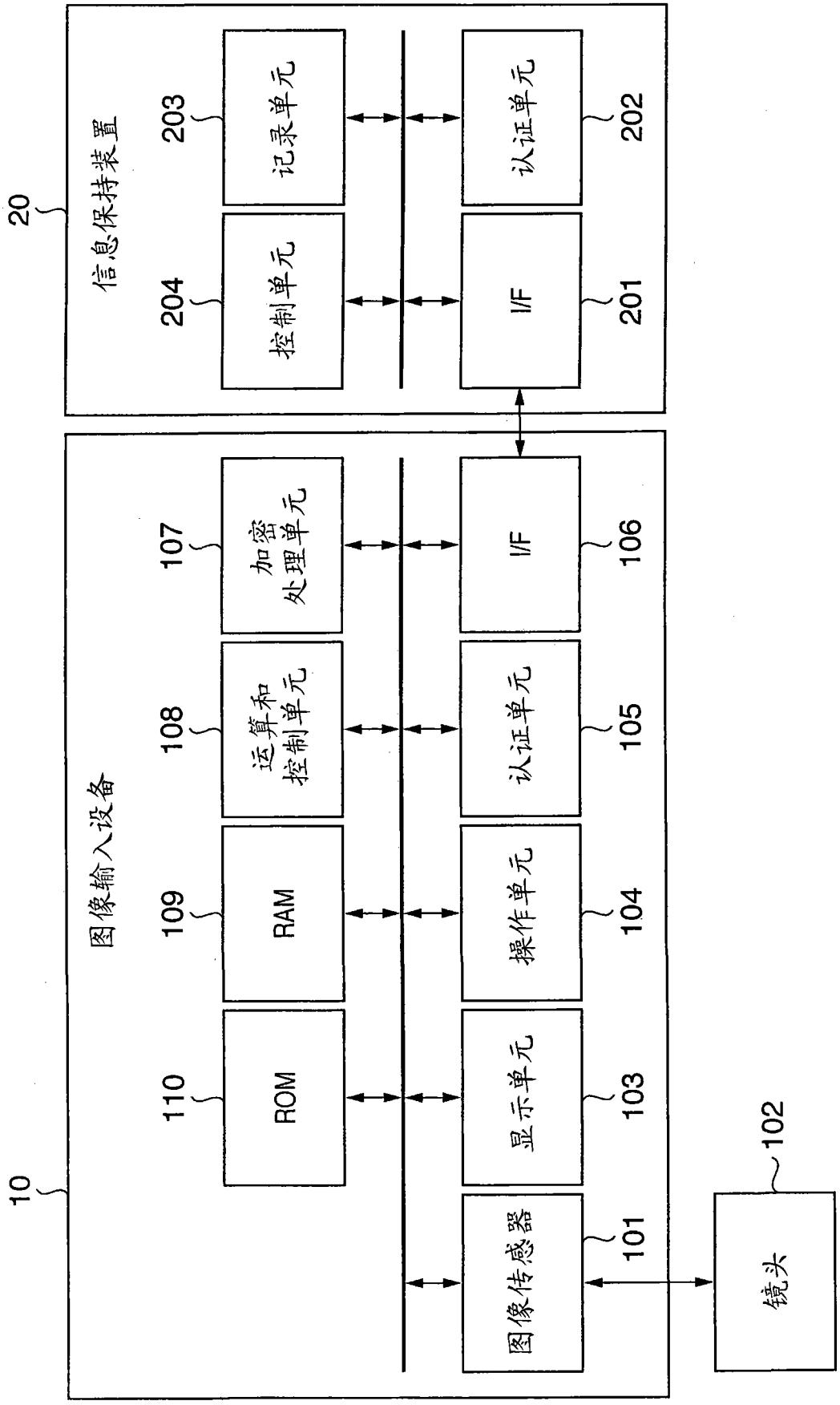

20
信息保持装置
203
记录单元
202
认证单元
204
控制单元
201
I/F
10
图像输入设备
107
加密处理单元
106
I/F
108
运算和控制单元
105
认证单元
109
RAM
104
操作单元
110
ROM
103
显示单元
101
图像传感器
102
镜头

图 1

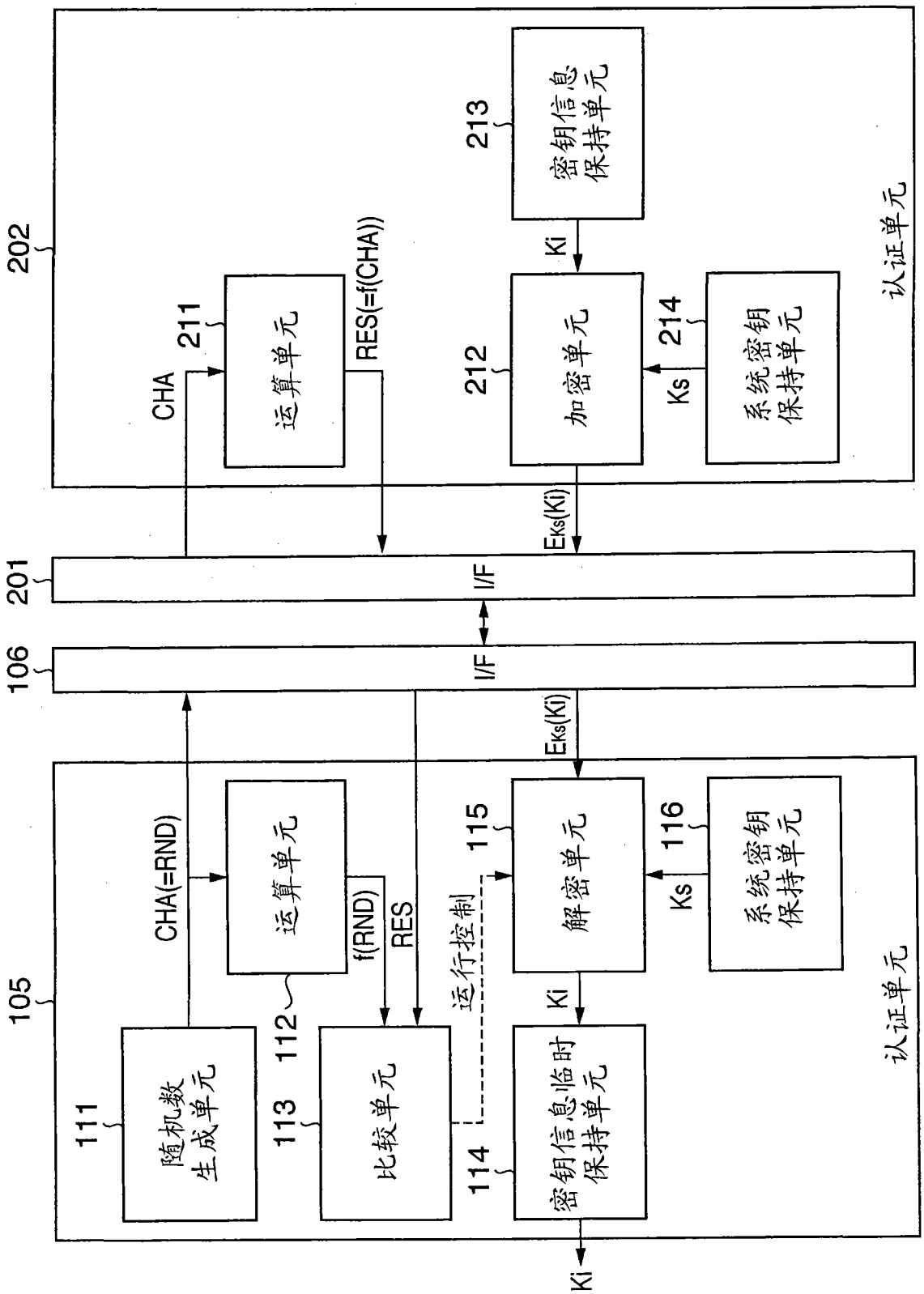

105
106
201
202
111
随机数
生成单元
112
运算单元
113
比较单元
114
密钥信息临时
保持单元
115
解密单元
116
系统密钥
保持单元
认证单元
CHA(=RND)
f(RND)
RES
运行控制
Ki
Ks
Eks(Ki)
I/F
211
运算单元
212
加密单元
213
密钥信息
保持单元
214
系统密钥
保持单元
认证单元
CHA
RES(=f(CHA))

图 2

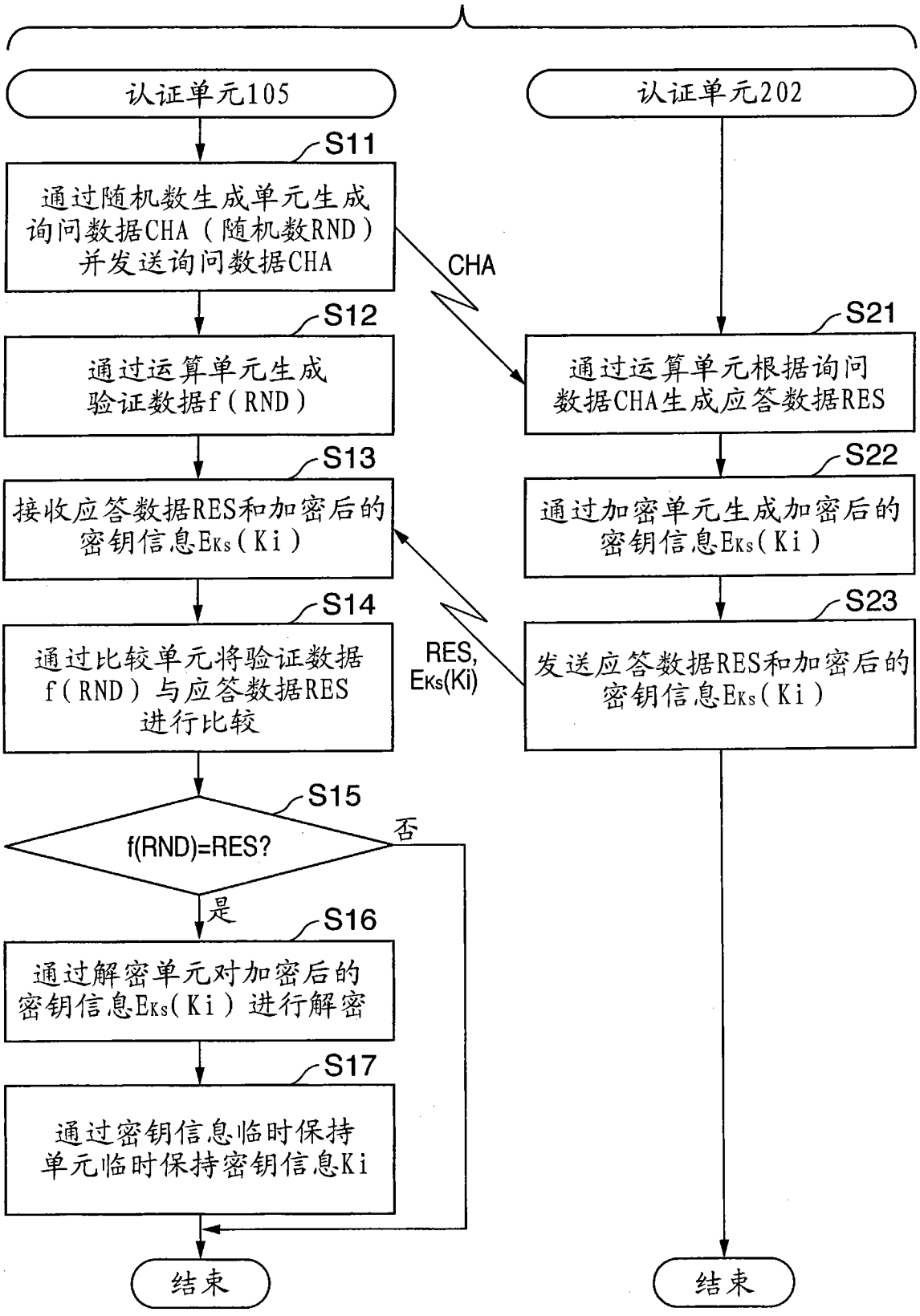

认证单元105
认证单元202
S11
通过随机数生成单元生成询问数据CHA（随机数RND）并发送询问数据CHA
CHA
S12
通过运算单元生成验证数据f（RND）
S21
通过运算单元根据询问数据CHA生成应答数据RES
S13
接收应答数据RES和加密后的密钥信息EKs（Ki）
S22
通过加密单元生成加密后的密钥信息EKs（Ki）
S14
通过比较单元将验证数据f（RND）与应答数据RES进行比较
RES, EKs(Ki)
S23
发送应答数据RES和加密后的密钥信息EKs（Ki）
S15
f(RND)=RES?
否
是
S16
通过解密单元对加密后的密钥信息EKs（Ki）进行解密
S17
通过密钥信息临时保持单元临时保持密钥信息Ki
结束
结束

图 3

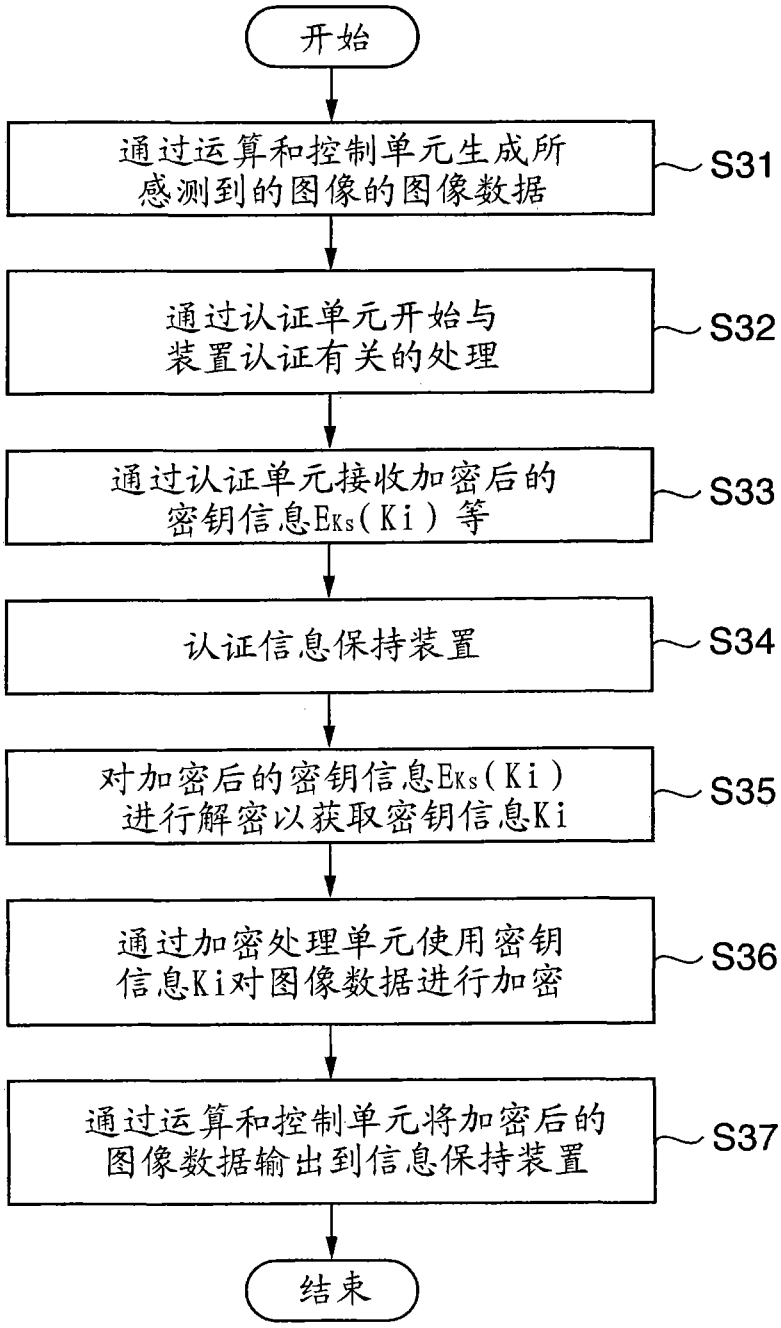

开始
通过运算和控制单元生成所感测到的图像的图像数据
S31
通过认证单元开始与装置认证有关的处理
S32
通过认证单元接收加密后的密钥信息EKs(Ki)等
S33
认证信息保持装置
S34
对加密后的密钥信息EKs(Ki)进行解密以获取密钥信息Ki
S35
通过加密处理单元使用密钥信息Ki对图像数据进行加密
S36
通过运算和控制单元将加密后的图像数据输出到信息保持装置
S37
结束

图 4

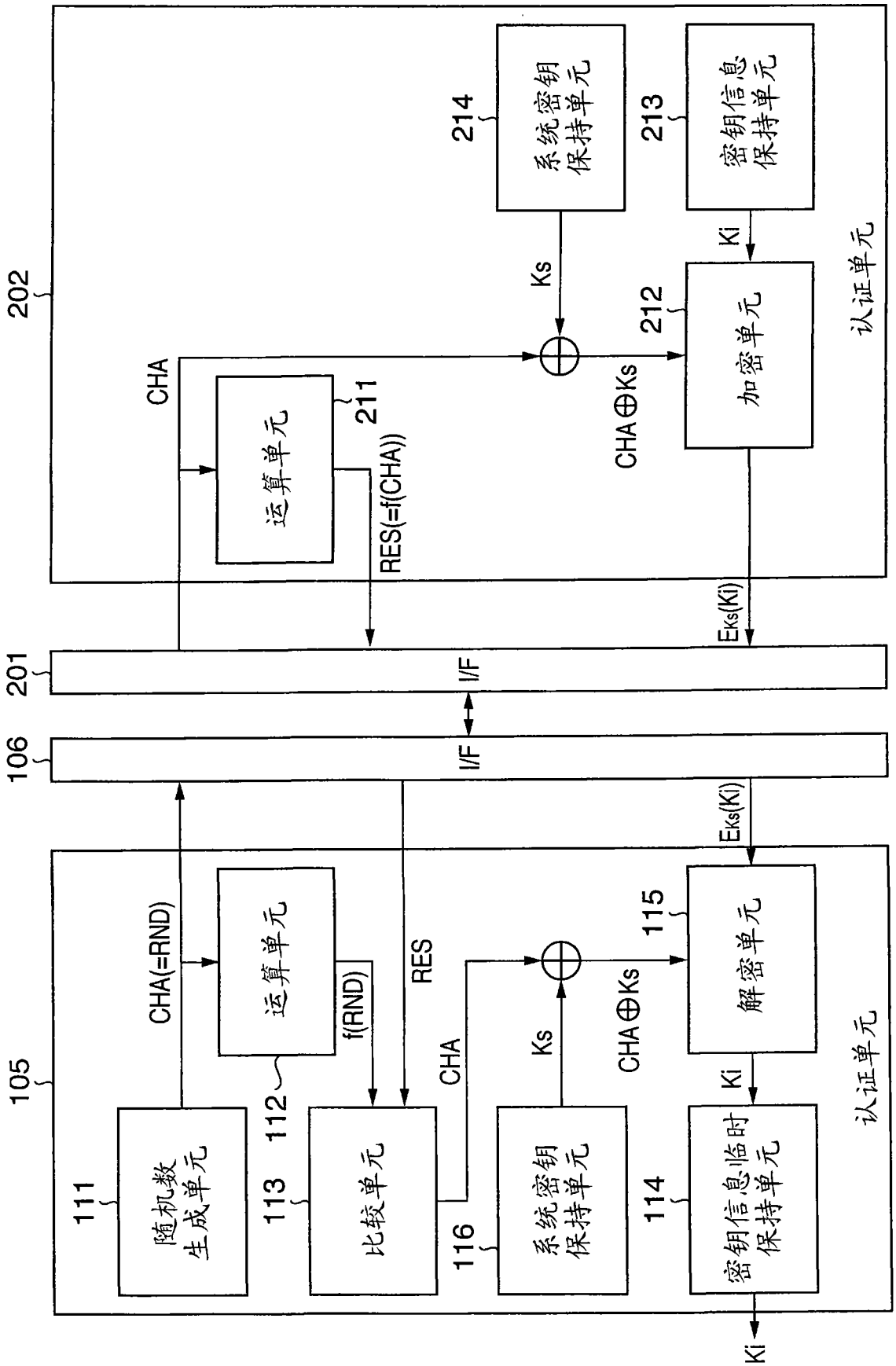

202
认证单元
214
系统密钥保持单元
213
密钥信息保持单元
Ks
Ki
212
加密单元
CHA⊕Ks
CHA
211
运算单元
RES(=f(CHA))
Eks(Ki)
201
I/F
106
I/F
105
CHA(=RND)
运算单元
112
f(RND)
RES
CHA
Ks
CHA⊕Ks
115
解密单元
Ki
111
随机数生成单元
113
比较单元
116
系统密钥保持单元
114
密钥信息临时保持单元
Ki

图 5

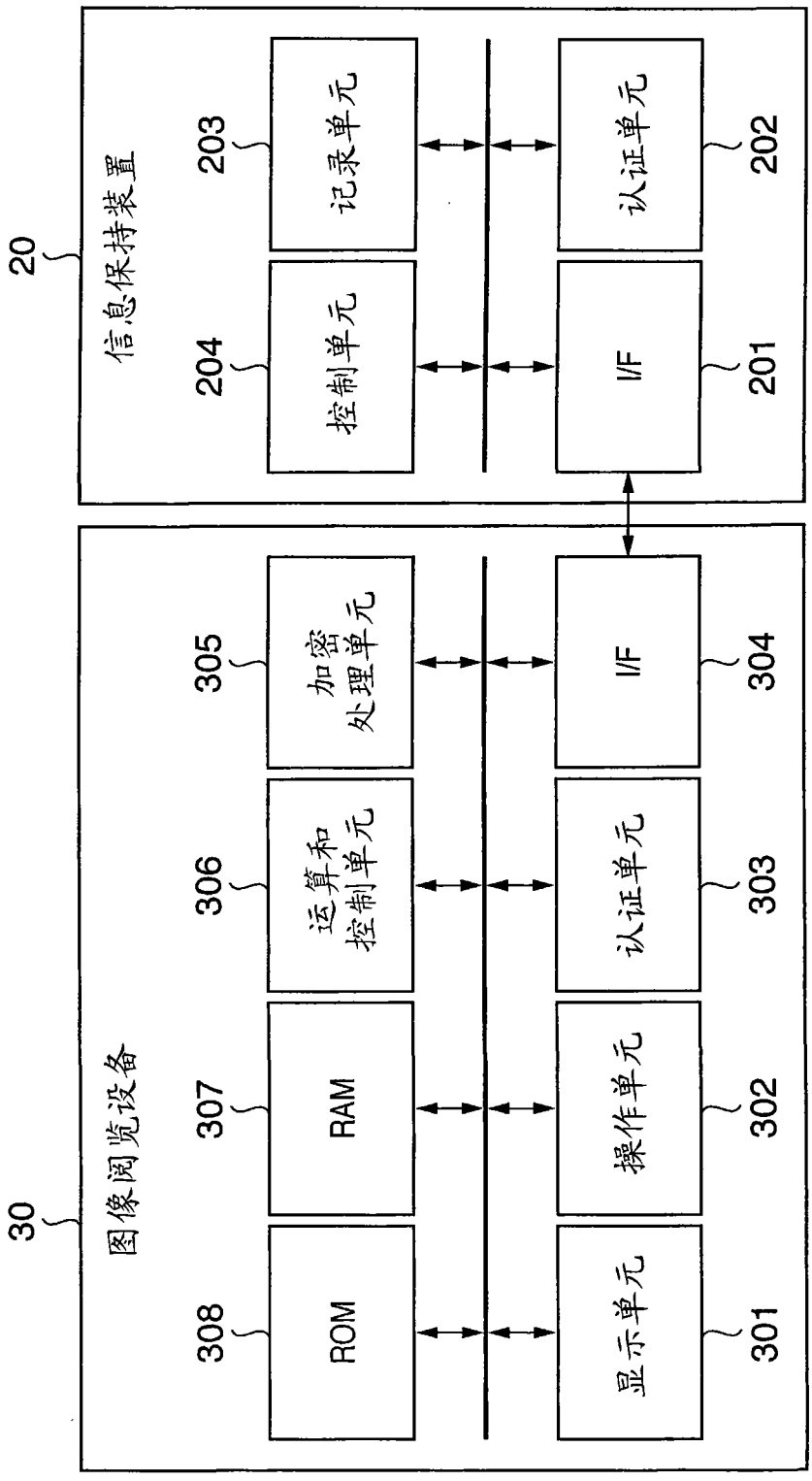

20
信息保持装置
203
记录单元
204
控制单元
202
认证单元
201
I/F
30
图像阅览设备
305
加密处理单元
306
运算和控制单元
307
RAM
308
ROM
304
I/F
303
认证单元
302
操作单元
301
显示单元

图 6