(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 101118586 B
(45)授权公告日 2011.12.07

(21)申请号 200710143174.3
(22)申请日 2007.08.03
(30)优先权数据
2006-213944 2006.08.04 JP
2007-181450 2007.07.10 JP
(73)专利权人 佳能株式会社
地址 日本东京都大田区下丸子 3-30-2
(72)发明人 须贺祐治
(74)专利代理机构 北京林达刘知识产权代理事务所(普通合伙) 11277
代理人 刘新宇
(51)Int.Cl.
G06F 21/00(2006.01)
H04N 5/913(2006.01)
(56)对比文件
CN 1556449 A,2004.12.22, 权利要求 1-12, 附图 1-10.
审查员 苏珊珊

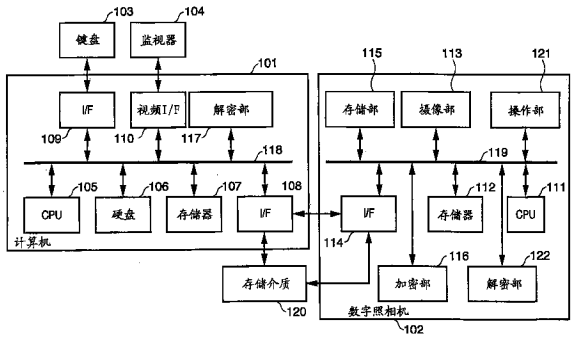
权利要求书 2 页 说明书 13 页 附图 11 页

(54)发明名称

数据处理设备和数据处理方法

(57)摘要

本发明涉及一种数据处理设备和数据处理方法。本发明的目的是当内容持有者与内容创建者不一致时,保护内容持有者的权利,而不必使用结合了版权保护机制的特殊的存储介质。输入用于生成加密密钥的信息;根据用于生成加密密钥的信息生成加密密钥;从存储介质中获取加密密钥检验数据,以及基于检验数据来认证生成的加密密钥的有效性;生成要存储在存储介质中的数据;通过使用在所述认证中认证为有效的加密密钥来加密所生成的数据;以及将加密的数据存储在存储介质中。



CN 101118586 B

1. 一种数据处理设备，包括：

输入部，用于输入用于生成加密密钥的信息；

密钥生成器，用于根据用于生成加密密钥的所述信息生成第一加密密钥；

认证器，用于从预先存储有加密密钥检验数据的存储介质中获取该加密密钥检验数据，并基于所述检验数据来认证用于生成加密密钥的所述信息的有效性，从而认证由所述密钥生成器生成的所述第一加密密钥的有效性；

图像数据生成器，用于生成要存储在存储介质中的图像数据；

会话密钥生成器，用于基于由所述认证器认证为有效的所述第一加密密钥，生成会话密钥；

第一加密部，用于使用由所述会话密钥生成器生成的所述会话密钥来加密由所述图像数据生成器生成的图像数据；

二次图像数据生成器，用于生成由所述图像数据生成器生成的图像数据的二次图像数据；

第二加密密钥生成器，用于使用由所述数据处理设备秘密保持的信息来生成第二加密密钥；

第二加密部，用于使用由所述第二加密密钥生成器生成的第二加密密钥来加密由所述二次图像数据生成器生成的二次图像数据；以及

控制器，用于将由所述第一加密部加密了的图像数据和由所述第二加密部加密了的二次图像数据存储在存储介质中，

其中，所述会话密钥生成器首先使用所述第一加密密钥和单向函数生成会话密钥，接下来使用前次生成的会话密钥和所述单向函数生成下一个会话密钥，并且破坏所述前次生成的会话密钥。

2. 根据权利要求 1 所述的数据处理设备，其特征在于，所述检验数据是用于生成加密密钥的所述信息的消息认证码。

3. 根据权利要求 1 所述的数据处理设备，其特征在于，所述检验数据是所述加密密钥的消息认证码。

4. 根据权利要求 1 所述的数据处理设备，其特征在于，所述二次图像数据是由所述图像数据生成器生成的图像数据的缩略图图像数据。

5. 根据权利要求 1 所述的数据处理设备，其特征在于，如果所述认证器认证所述第一加密密钥失败，则所述控制器将由所述图像数据生成器生成的图像数据存储在所述存储介质中，而不加密。

6. 一种数据处理设备的数据处理方法，所述方法包括下列步骤：

输入用于生成加密密钥的信息的输入步骤；

根据用于生成加密密钥的所述信息生成第一加密密钥；

从预先存储有加密密钥检验数据的存储介质中获取该加密密钥检验数据，以及基于所述检验数据来认证用于生成加密密钥的所述信息的有效性，从而认证所生成的第一加密密钥的有效性的认证步骤；

生成要存储在所述存储介质中的图像数据；

基于在所述认证步骤中认证为有效的所述第一加密密钥生成会话密钥的会话密钥生

成步骤；

通过使用所述会话密钥来加密所生成的图像数据的第一加密步骤；

生成图像数据的二次图像数据；

使用由所述数据处理设备秘密保持的信息来生成第二加密密钥；

使用所述第二加密密钥来加密所述二次图像数据；以及

将加密的图像数据和加密的二次图像数据存储在所述存储介质中，

其中，在所述会话密钥生成步骤中，首先使用所述第一加密密钥和单向函数生成会话密钥，接下来使用前次生成的会话密钥和所述单向函数生成下一个会话密钥，并且破坏所述前次生成的会话密钥。

数据处理设备和数据处理方法

技术领域

[0001] 本发明涉及信息处理设备和方法以及数据处理设备和方法，尤其涉及一种保护存储于存储介质中的数据的持有者的权利的技术。

[0002] 背景技术

[0003] 计算机和网络的快速增长和发展促进了例如文本数据、图像数据以及音频数据等各种信息的数字化和这些数字数据的发布。然而，通过例如因特网的广域网来发布数字数据充满了被第三方在传送路径上偷听或窃听的危险。不仅传送路径上的数据，而且存储在存储介质中的数字数据也是不安全的，这是因为没有访问权的未授权的第三方可能复制并非法使用并泄漏该数据。为了保证安全的传送路径或在便携式存储介质中安全地存储数据，通常对数字数据加密。

[0004] 数字数据很容易复制、编辑和修改。复制、编辑和修改的容易对于用户是有利的，但是同时也引入了保护数字数据不被第三方非法篡改的必要性。存在添加反篡改数据来检验存在 / 不存在对数字数据的篡改的数字签名和消息认证码 (MAC)。数字签名不仅有篡改检验功能，而且还具有防止欺骗和拒认 (repudiation) 的功能。

[0005] 下面将说明实现上述机制的密码术。

[0006] 哈希 (hash) 函数

[0007] 哈希函数与数字签名处理一起使用，以缩短对要签名的有损压缩数据添加签名的处理时间。也就是，哈希函数具有处理任意长度的数据 M 以生成具有预定长度的输出数据的功能。将 哈希函数的输出 H(M) 称为普通可读文本 (plaintext) 数据 M 的哈希值。

[0008] 尤其是，按照计算量，给定数据 M 的单向哈希函数很难计算满足 H(M') = H(M) 的普通可读文本数据 M'。单向哈希函数的例子是 MD2(消息摘要 2，Message Digest 2)、MD 5(消息摘要 5) 以及 SHA-1(安全哈希算法 1，Secure Hash Algorithm)。

[0009] 公共密钥密码系统

[0010] 作为使用两个不同密钥的公共密钥密码系统的特有特征，由其中一个密钥加密的数据只能由另一个密钥来解密。这两个密钥其中的一个被称为公共密钥，并可以对公众开放。另一个密钥称为私有密钥，只由被授权的人持有。根据该特有特征，可以对公众开放一个密钥 (公共密钥)。因此，可以容易地传送该密钥，因为不必将其秘密地送给通信对方。公共密钥密码系统的例子是 RSA 加密和 El Gamal 加密。

[0011] 数字签名

[0012] 使用公共密钥加密系统的数字签名的例子是 RSA 签名、DSA 签名以及 S chnorr 签名。

[0013] 消息认证码

[0014] 数字签名是一种通过使用公共密钥加密系统来保证文档创建者的权利的消息认证系统。另一种使用通用密钥密码系统或哈希函数来代替公共密钥密码系统的消息认证系统被称为消息认证码 (MAC)。

[0015] MAC 与数字签名很大的不同在于：发送方 (MAC 值创建者) 和接收方 (认证

者）共享保密数据（在消息认证码用密钥哈希法(HMAC，keyed-hashing for message authentication code)中的密钥K)。因为计算量小于数字签名，所以它是有利的。然而，因为认证者也持有该保密数据，所以第三方就不可能证明MAC 的创建者，即发送方或接收方。使用例如SHA-1的标准哈希函数的MAC被用于安全性协议，例如网络中的IPSec(IP安全性协议，IP Security protocol)或SSL(安全套接层，Secure SocketLayer)。

[0016] 数字照相机中的图像数据保护

[0017] 使用上述密码系统或数字签名能够保护数字照相机拍摄的图像数据不受例如偷听、窃听、篡改和欺骗的威胁。

[0018] 在日本特开第2005-18914号公报中公开的技术的目的是：保护便携式存储介质中记录的数据并实现复制保护和数据加密。更具体地说，可以由计算机激活的数据记录程序和数据再现程序被预先写入便携式存储介质中。也就是，存在一种对便携式存储介质给予版权保护功能的技术。

[0019] 包括图像数据的内容不总是通过使用便携式存储介质来发布。在另一种方法中，内容被通过网络自由发布。在日本特开第2004-118327号公报中公开的技术使得指定的服务器管理员来控制对例如通过网络获取的内容的利用。也就是，假定要使用该内容的装置连接到网络，则存在一种版权保护技术，其使得装置与服务器通信并获得使用内容的许可。

[0020] 通常，作为内容创建者的摄影者可以自由地删除或传输他／她使用例如数字照相机所拍摄的图像数据。然而，摄影者不总是内容的持有者。例如，内容持有者可以是发行公司，摄影者是与该公司签订合同的摄影师。在这种情况下，摄影者可能错误地或有意地将拍摄的图像数据传送给第三方（合同方之外）。为了防止这种情况，有必要建立一种机制，用来使不同于摄影者的实体（内容持有者）保护图像数据的版权。

[0021] 在日本特开第2005-18914号公报中公开的技术通过使用特殊存储介质来加密图像数据。这种方法在两点上是不利的：特殊存储介质的购买费用和现有存储介质的不可使用性。日本特开第2004-118327号公报中公开的技术需要网络连接来使用内容。这对于内容使用者来说不总是方便的。

[0022] 为了设置远处地点的照相机中的权利保护，必须将照相机从该地点带到内容持有者所在的地方。为了避免这种情况，需要这样一种机制：该机制将远处地点的照相机的存储卡注册为能够进行权利保护的介质，从而保护拍摄后存储在存储卡中的图像数据。

[0023] 发明内容

[0024] 在一方面，一种数据处理设备包括：输入部，用于输入用于生成加密密钥的信息；密钥生成器，用于根据用于生成加密密钥的信息生成第一加密密钥；认证器，用于从预先存储有加密密钥检验数据的存储介质中获取该加密密钥检验数据，并基于检验数据来认证用于生成加密密钥的信息的有效性，从而认证由密钥生成器生成的第一加密密钥的有效性；图像数据生成器，用于生成要存储在存储介质中的图像数据；会话密钥生成器，用于基于由认证器认证为有效的第一加密密钥，生成会话密钥；第一加密部，用于使用由会话密钥生成器生成的会话密钥来加密由图像数据生成器生成的图像数据；二次图像数据生成器，用于生成由图像数据生成器生成的图像数据的二次图像数据；第二加密密钥生成器，用于使用由数据处理设备秘密保持的信息来生成第二加密密钥；第二加密部，用于使用由第二加密密钥生成器生成的第二加密密钥来加密由二次图像数据生成器生成的二次图像数据；以及

控制器，用于将由第一加密部加密了的图像数据和由第二加密部加密了的二次图像数据存储在存储介质中，其中，会话密钥生成器首先使用第一加密密钥和单向函数生成会话密钥，接下来使用前次生成的会话密钥和单向函数生成下一个会话密钥，并且破坏前次生成的会话密钥。

[0025] 在另一方面，一种信息处理设备包括：密钥生成器，用于根据通过上述数据处理设备中的输入部所输入的用于生成加密 密钥的信息，生成当外部装置将数据存储在存储介质中时使用的加密密钥；检验数据生成器，用于生成认证加密密钥的有效性的检验数据，并将检验数据存储在存储介质中；以及解密部，用于通过使用加密密钥来解密存储于存储介质中的数据。

[0026] 在另一方面，一种数据处理设备的数据处理方法包括下列步骤：输入用于生成加密密钥的信息的输入步骤；根据用于生成加密密钥的信息生成第一加密密钥；从预先存储有加密密钥检验数据的存储介质中获取该加密密钥检验数据，以及基于检验数据来认证用于生成加密密钥的信息的有效性，从而认证所生成的第一加密密钥的有效性的认证步骤；生成要存储在存储介质中的图像数据；基于在认证步骤中认证为有效的第一加密密钥生成会话密钥的会话密钥生成步骤；通过使用会话密钥来加密所生成的图像数据的第一加密步骤；生成图像数据的二次图像数据；使用由数据处理设备秘密保持的信息来生成第二加密密钥；使用第二加密密钥来加密二次图像数据；以及将加密的图像数据和加密的二次图像数据存储在存储介质中，其中，在会话密钥生成步骤中，首先使用第一加密密钥和单向函数生成会话密钥，接下来使用前次生成的会话密钥和单向函数生成下一个会话密钥，并且破坏前次生成的会话密钥。

[0027] 在另一方面，一种信息处理方法包括以下步骤：根据在上述数据处理方法的输入步骤中所输入的用于生成加密密钥的信息，生成当外部装置将数据存储在存储介质中时使用的加密密钥；生成认证加密密钥的有效性的检验数据，并将检验数据存储在存储介质中；以及通过使用加密密钥来解密存储于存储介质中的数据。

[0028] 根据这些方面，即使当内容持有者与内容创建者不一致的时候，也有可能保护内容持有者的权利，而不需要结合版权保护机制的特殊存储介质。

[0029] 根据下面参考附图对典型实施例的说明，本发明的进一步特征将变得明显。

[0030] 附图说明

[0031] 图 1 是示出根据实施例的信息处理系统的框图；

[0032] 图 2 是示出图 1 中所示信息处理系统使用便携式存储介质的例子的框图；

[0033] 图 3 是示出解密部的结构的框图；

[0034] 图 4 是示出加密部的结构的框图；

[0035] 图 5 是用于示意性说明五个阶段的序列图；

[0036] 图 6 是示出计算机中的预设置过程的流程图；

[0037] 图 7 是示出计算机中的另一个预设置过程的流程图；

[0038] 图 8 是示出数字照相机中的预处理过程的流程图；

[0039] 图 9 是示出计算机中的加密图像数据解密过程的流程图；

[0040] 图 10 是示出包括附加处理的图 9 中所示处理的流程图，所述附加处理为当接收到加密密钥检验数据以及加密的图像数据时，检验加密密钥检验数据与加密的图像数据之间

的关联是否正确的处理；

[0041] 图 11 是用于说明为每个图像数据生成会话密钥的加密处理的流程图；

[0042] 图 12 是用于说明通过为每个图像数据生成会话密钥来加密缩略图图像的处理的流程图；

[0043] 图 13 是用于说明浏览数字照相机中的加密缩略图图像的解密方法的流程图。

具体实施方式

[0044] 下面将参考附图详细说明根据本发明实施例的信息处理设备和方法以及数据处理设备和方法。下面将说明这样的例子：内容持有者请求数字照相机使用者进行拍照。在这种情况下，摄影者，即数字照相机使用者，对应于内容创建者。然而，在本发明中，内容创建者不限于数字照相机使用者（摄影者）。任何根据来自内容持有者的请求来创建内容的人对应于本发明的内容创建者，而与创建的内容的类型无关。

[0045] 第一实施例

[0046] 图 1 是示出根据本实施例的信息处理系统的框图，所述信息处理系统包括计算机 101 和数字照相机 102。

[0047] 计算机的设置

[0048] 由微处理器形成的 CPU 105 通过将包括在存储器 107 中的 RAM（随机存取存储器）用作工作存储器，来执行存储于硬盘 106 和包括在存储器 107 中的 ROM（只读存储器）中的程序。CPU105 通过系统总线 118 来控制稍后说明的设置，并执行各种处理。

[0049] 硬盘 106 存储驱动软件以控制数字照相机 102，例如文本、图形和照片数据的图像数据以及各种用于生成、编辑和修改图像数据的软件程序。

[0050] CPU 105 执行各种软件程序并通过视频 I/F 110 在监视器 104 上显示用户接口。CPU 105 通过连接到例如 USB（通用串行总线）的接口 (I/F) 109 的键盘或鼠标 103 来接收用户指令。

[0051] I/F 108 是串行总线接口，例如 USB 或 IEEE 1394 或网络接口。例如数字照相机 102 或打印机、存储卡读 / 写器、或网络电缆的图像输入 / 输出装置被连接到该 I/F 108。

[0052] CPU 105 通过 I/F 108、通过网络从数字照相机 102 或从附到存储卡读 / 写器的存储介质中直接接收图像数据，并将数据存储于硬盘 106 的预定区域。如果图像数据被加密或具有数字签名，则 CPU 105 通过控制解密部 117 来执行解密或认证。

[0053] 数字照相机的设置

[0054] CPU 111 通过将包括在存储器 112 中的 RAM 用作工作存储器来执行存储于包括在存储器 112 中的 ROM 中的程序。CPU105 通过系统总线 119 来控制稍后说明的设置，并执行各种处理。

[0055] 具有例如 C CD 的传感器的摄像部 113 拍摄被摄体并生成对应于该被摄体的静止图像或运动图像的图像数据。CPU 111 将摄像部 113 所拍摄的图像数据存储在存储器 112 的 ROM 中，执行必要的数据处理、加密以及数字签名添加，然后将数据存储在存储部 115 中。加密部 116 用于加密数据或为数据添加数字签名。

[0056] 操作部 121 包括快门按钮和用于设定各种摄影条件的命令拨盘和键，并能够输入对于加密处理和数字签名处理所必须的各种设置信息。也就是，用户使用操作部 121 来例

如输入密码，以生成对于加密处理所必须的密钥信息。

[0057] I/F 114 是串行总线接口，例如 USB 或 IEEE 1394 或网络接口。例如计算机 101 或打印机、读存储卡 / 写器、或网络电缆的各种装置可被连接到 I/F 114。

[0058] 图像数据的输入

[0059] 为了从数字照相机 102 的存储部 115 接收图像数据，CPU 105 执行驱动软件或应用软件中描述的指令。图像数据请求被通过 I/F 108 和 114 发送到 CPU 111。响应于该请求，CPU 111 从存储部 115 中读出图像数据，并通过 I/F 114 和 108 将其提供给计算机 101。CPU 105 将接收的图像数据存储到硬盘 106 的预定区域中。

[0060] 可选择地，如图 2 中所示，数字照相机 102 可以通过使用便携式存储介质 120 将图像数据提供给计算机 101。在这种情况，CPU 111 根据来自操作部 121 的指令，将从存储部 115 中读出的图像数据写入连接到 I/F 114 的存储卡读 / 写器所附的存储介质 120 中。CPU 105 根据通过用户接口接收的用户指令，从连接到 I/F 108 的存储卡读 / 写器所附的存储介质 120 中读出图像数据。

[0061] 解密部

[0062] 图 3 是示出解密部 117 或 122 的结构的框图。

[0063] 加密密钥生成器 301 生成用于将图像数据存储到存储介质 120 或硬盘 106 的加密密钥。存储器 107 或 112 存储由加密密钥生成器 301 所生成的加密密钥。

[0064] 数据解密部 302 使用存储于存储器 107 或 112 中的加密密钥来解密存储于存储介质 120 或硬盘 106 中的加密的图像数据。解密的图像数据被存储在硬盘 106 的预定区域中。

[0065] 加密密钥检验数据生成器 303 生成加密密钥检验数据，以检验与存储在存储介质 120 或硬盘 106 中的加密图像数据相对应的加密密钥是否有效。存储介质 120 或硬盘 106 存储由加密密钥检验数据生成器 303 生成的加密密钥检验数据。稍后将说明使用加密密钥检验数据的处理。

[0066] 加密部

[0067] 图 4 是示出加密部 116 的结构的框图。

[0068] 加密密钥检验数据获取部 401 通过 I/F 108 和 114 从存储介质 120 中获取加密密钥检验数据。

[0069] 预加密密钥数据输入部 402 输入作为用于生成加密密钥的信息的预加密密钥数据。预加密密钥数据例如对应于密码，并从计算机 101 的键盘 103 或数字照相机 102 的操作部 121 输入。

[0070] 加密密钥生成器 403 根据预加密密钥数据生成加密密钥。用于根据预加密密钥数据生成加密密钥的算法，或由该算法使用的密钥数据是保密的。加密密钥的生成是在具有篡改抵抗力的存储器上完成的。也就是，即使当第三方知道预加密密钥数据时，他 / 她既不能通过使用他 / 她自己的装置来导出加密密钥，也不能解密加密的图像数据。

[0071] 加密密钥检查部 404 基于加密密钥检验数据来确认由加密密钥生成器 403 生成的加密密钥是否正确。稍后将说明使用加密密钥检验数据的处理。

[0072] 数据加密部 405 通过使用加密密钥对存储在存储器 112 中的图像数据加密，并将加密的数据存储到存储部 115 或存储介质 120 中。

[0073] 密钥破坏器 407 例如生成加密图像数据所使用的会话密钥。

[0074] 图像数据的加密和解密

[0075] 下面将以五个阶段来说明以下一系列处理：加密由数字照相机 102 生成的图像数据、将图像数据存储在存储介质 120 中、将加密的图像数据从存储介质 120 加载到计算机 101、以及解密图像数据以使其可处理。

[0076] 图 5 是用于示意性说明这五个阶段的序列图。内容持有者（下文中有时称为“持有者”）持有计算机 101。摄影者持有数字照相机 102。

[0077] 阶段 1：持有者通过操作计算机 101 的键盘 103 来输入密码（预加密密钥数据），生成加密密钥和加密密钥检验数据 (S 501)，并将加密密钥检验数据设置到存储介质 120 中 (S502)。持有者将存储介质 120 给予摄影者，请求摄影，并秘密地使摄影者知道密码 (S511)。在这种情况下，内容持有者不同于摄影者。

[0078] 阶段 2：摄影者将接收的存储介质 120 安装到数字照相机 102 上，并通过操作数字照相机 102 的操作部 121 输入从持有者接收的密码 (S503)。数字照相机 102 通过使用存储介质 120 中设置的加密密钥检验数据来检查输入的密码的有效性 (S504)。这将在后面详细说明。

[0079] 阶段 3：当完成密码检查时，数字照相机通过使用根据密码导出的加密密钥对所摄图像数据加密，并将图像数据存储到数字照相机 102 中 (S505)。如上所述，只有持有者知道如何导出加密密钥。该方法对于包括摄影者的第三方是保密的。稍后将详细说明密钥的导出。

[0080] 阶段 4：摄影者可以浏览拍摄的图像数据 (S506)。摄影者将存储有加密的图像数据的存储介质 120 给予持有者，或通过 I/F114 输出加密的图像数据，并通过例如因特网的广域网将它们发送给持有者 (S507)。为了将从 I/F 114 输出的加密的图像数据发送给持有者，不仅可以采用通过广域网传送，还可以使用许多其它方法。

[0081] 阶段 5：持有者通过操作计算机 101 的键盘 103 来输入密码 (S508)。计算机 101 通过使用存储在例如硬盘 106 中的加密密钥检验数据来检查输入的密码的有效性 (S509)。当完成密码检查时，计算机 101 根据密码生成加密密钥，并通过使用该加密密钥来解密接收的或存储在存储介质 120 中的图像数据，从而使得可以使用（例如浏览、复制或编辑）该图像数据 (S510)。

[0082] 阶段 1

[0083] 在阶段 1，使用计算机 101，持有者在由摄影者在拍摄中使 用的存储介质 120 中执行预设置 (S501 和 S502)。图 6 是示出预设置程序的流程图。该处理是在 CPU 105 的控制下执行的。

[0084] CPU 105 判断是否通过键盘 103 输入了密码（预加密密钥数据）(S601)。预加密密钥数据可以是任意类型，只要它可以通过数字照相机 102 的操作部输入。如果在预定时间内没有输入密码（预加密密钥数据），或输入了生成预加密密钥数据的指令，则 CPU 105 生成预加密密钥数据并将其显示在监视器 104 上 (S602)。

[0085] CPU 105 通过控制解密部 117 的加密密钥生成器 301 来基于预加密密钥数据生成加密密钥 (S603)。CPU 105 可以通过使用例如上述哈希函数或 MAC 来导出加密密钥。例如，当计算机 101 和数字照相机 102 分别在硬盘 106 和存储部 115 中持有相同的系统密钥

Ksys 时，通过将 Ksys 用作密钥并输入预加密密钥数据来执行的 HMAC 处理的输出被设置为加密密钥 Kenc。如果不存在系统密钥 Ksys，通过输入预加密密钥数据来执行的 SHA-1 哈希处理的输出被设置为加密密钥 Kenc。可选择地，使用公共密钥密码系统的单向函数可以被用于替代 SHA-1 哈希函数。

[0086] 接下来，CPU 105 通过控制加密密钥检验数据生成器 303 来生成加密密钥检验数据，并临时将生成的加密密钥检验数据存储到例如存储器 107 中 (S605)。加密密钥检验数据是从加密密钥或预加密密钥数据中导出的。生成方法是基于上述加密密钥导出方法。例如，当计算机 101 和数字照相机 102 分别在硬盘 106 和存储部 115 中持有相同的系统密钥 Ksys 时，通过将 Ksys 用作密钥并输入加密密钥 Kenc 来执行的 HMAC 处理的输出被设置为加密密钥检验数据。如果不存在系统密钥 Ksys，可以通过使用公共密钥密码系统添加数字签名来生成加密密钥检验数据。更具体地说，添加使用仅由持有者持有的 RSA 私有密钥的 RSA 签名，并将签名的数据设置为加密密钥检验数据。

[0087] CPU 105 通过控制 I/F 108 将存储在存储器 107 中的加密密钥检验数据存储在存储介质 120 中 (S606)。代替临时将加密密钥检验数据保存于存储器 107 中，可以将其直接存储在存储介质 120 中。在这种情况下，步骤 S606 被省略。

[0088] 图 7 是示出另一个预设置程序的流程图。与图 6 中相同的步骤号在图 7 中表示相同的处理，且不重复对其进行详细说明。

[0089] 如果没有输入密码 (预加密密钥数据)，或输入了加密密钥生成指令，CPU 105 通过控制加密密钥生成器 301 来生成加密密钥 (S607)。CPU 105 生成对应于所生成的加密密钥的预加密密钥数据，并将其显示在监视器 104 上 (S608)。处理前进到步骤 S 605。通过使用例如基于公共密钥密码系统的陷门 (trapdoor) 单向函数来生成预加密密钥数据。例如，使用私有密钥的 RSA 加密处理被用于将加密密钥转换为预加密密钥数据。根据该方法，数字照相机 102 可以通过使用 RSA 公共密钥来根据预加密密钥数据导出加密密钥。

[0090] 图 6 中所示的处理与图 7 中所示的很大不同在于 :加密密钥和预加密密钥数据 (密码) 中的哪一个首先存在。图 6 中所示的处理中预加密密钥数据首先存在，该处理可以通过使用通用密钥密码系统或哈希函数来导出加密密钥，而不用使用公共密钥加密系统。另一方面，图 7 所示的处理中加密密钥首先存在，该处理必须保证这样的机制 :只允许私有密钥的持有者通过使用基于例如 RSA 加密的公共密钥密码系统的陷门单向函数，来根据预加密密钥数据导出加密密钥。

[0091] 公共密钥和私有密钥可以被相反地使用。也就是，用数字照相机 102 的公共密钥进行的 RSA 加密处理被用于将加密密钥转换为预加密密钥数据。在这种情况下，数字照相机 102 通过使 用 RSA 私有密钥来根据预加密密钥数据导出加密密钥。注意 :数字照相机具有与其它数字照相机所持有的私有密钥不同的自己的私有密钥。该方法允许指定能够使用存储介质 120 的数字照相机。然而，需要将数字照相机的私有密钥预先存储在具有篡改抵抗力的存储器中。

[0092] 阶段 2

[0093] 在阶段 2 中，数字照相机 102 执行预处理 (S503 和 S504)，检查其是否具有对连接到 I/F 114 的存储介质 120 的写数据权。图 8 是示出预处理程序的流程图。该处理由 CPU 111 执行。

[0094] CPU 111 通过控制加密密钥检验数据获取部 401 来从存储介质 120 中获取加密密钥检验数据 (S801)。如果没有获取到加密密钥检验数据 (S802)，则 CPU 111 判断为该数字照相机没有对存储介质 120 的写数据权，并且该处理结束。

[0095] CPU 111 通过控制预加密密钥数据输入部 402 来输入预加密密钥数据（密码）(S803)。应该由摄影者通过操作操作部 121 来输入的密码（预加密密钥数据）是由持有者给定的密码。要输入的密码取决于数字照相机 102 的用户接口。该密码可以是人可读的密码、手写在触摸面板上的密码、或对开关和快门按钮的操作的组合。操作部 121 可以通过在监视器上显示虚拟键盘并使得用户在触摸面板上选择字母和数字，或通过设置密码输入模式并使得用户按下多个按钮的组合来输入密码。因此，计算机 101 的 CPU 105 有时将获取的或生成的密码转换为摄影者可以通过数字照相机 102 的用户接口来输入的操作程序。

[0096] CPU 111 通过控制加密密钥生成器 403 来基于预加密密钥数据生成加密密钥，并将生成的加密密钥存储在存储器 112 中 (S804)。加密密钥生成器 403 提供用于根据密码导出单独的加密密钥的机制，该密码例如是人可读的密码、手写在触摸面板上 的密码、或对开关和快门按钮的操作的组合。该加密密钥生成方法符合阶段 1 的步骤 S603 中说明的方法。也就是，使用了与计算机 101 的生成方法相同的生成方法。

[0097] 可以将加密密钥生成方法说明为获取的加密密钥检验数据的一部分。例如，加密密钥生成方法被预先注册为对应于指定 URI（统一资源标识符，Uniform Resource Identifier) 的服务器的存储区。通过基于被说明为加密密钥检验数据的一部分的 URI 参考注册的信息，可以从多个加密密钥生成方法中选择预定的加密密钥生成方法。

[0098] 接下来，CPU 111 通过控制加密密钥检查部 404 来认证加密密钥检验数据的有效性 (S805)。该检验方法符合阶段 1 的步骤 S605 中说明的方法。如果该有效性是不可靠的，则结束处理。也就是，加密密钥检验数据可以被用于检测预加密密钥数据是否已经被无误的输入。

[0099] 当加密密钥检验数据的有效性是可靠的时，CPU 111 将存储介质 120 的记录注册到存储部 115 中存储的介质列表（未示出）中 (S806)。该记录包括存储介质 120 的 ID、加密密钥检验数据或其哈希值（摘要）、以及预加密密钥数据或根据加密密钥导出的数据的组合。可以将计数器信息或 salt 存储在相同的记录中作为关于用于阶段 3 的图像加密的密钥信息的元数据。稍后将结合阶段 3 详细说明。

[0100] 步骤 S 806 的过程不是必须的，但是对于提供预加密密钥数据（密码）缓存功能是有效的。也就是，即使当存储介质 120 被频繁交换，当在数字照相机 102 和存储介质 120 之间完成预处理时，CPU 仅需要参考介质列表，从而节省了用于获取预加密密钥数据（密码）的时间和精力。

[0101] 阶段 3

[0102] 在阶段 3 中，数字照相机 102 使数据加密部 405 通过使用在阶段 2 生成的加密密钥来加密所摄图像数据，并将数据存储在存储介质 120 中 (S505)。加密密钥可以直接用于使用通用密钥密码系统的加密。可选择地，可以为每个图像数据导出会话密钥，并用作加密密钥。为了导出会话密钥，使用哈希函数或 HMAC。更具体地说，该方法与上述使用 HMAC 处理或 SHA-1 哈希处理的方法是相同的。

[0103] 下面说明两个作为导出方法的详细例子。(1) 当持有系统密钥 Ksys 时，第一会话

密钥Kenc(0)是加密密钥Kenc，并将通过使用Ksys作为密钥并输入会话密钥Kenc(i-1)执行的HMAC处理的输出设置为会话密钥Kenc(i)。(2)如果不存在系统密钥Ksys，则第一会话密钥Kenc(0)是加密密钥Kenc，且通过输入会话密钥Kenc(i-1)来执行的SHA 1-1哈希处理的输出被设置为会话密钥Kenc(i)。

[0104] 在这两种情况下，都需要将计数器信息i存储在例如存储部115中。可以通过将计数器信息i存储在步骤S 806中说明的介质列表的记录中来管理计数器信息i。对HMAC处理或SHA-1哈希处理的输入还可以包括包含随机数据的salt信息。即使在这种情况下，也需要存储并管理上述介质列表的记录中的salt信息。在任何一种情况下，计数器信息（和salt信息）对于解密都是必要的。因此，加密的图像数据必须具有计数器信息（和salt信息）作为元数据。当为计数器信息（和salt信息）生成了例如MAC的加密密钥检验数据，并与加密的图像数据一起发送该加密密钥检验数据时，可以防止持有者通过使用错误的密钥来解密数据。

[0105] 对于使用公共密钥密码系统加密的加密密钥是持有者的公共密钥，并且因此，直接通过使用该加密密钥来完成加密。在这种情况下，会话密钥Kenc(i)在每次图像被加密时改变。从Kenc(i)到Kenc(i-1)的反向计算是困难的。因此，被使用过一次的会话密钥被认为实际上每次都被破坏了。这使得可以应付对于CPU 111或存储器112的读攻击，并提高了系统的安全水平。

[0106] 图11是用于说明为每个图像数据生成会话密钥的加密处理的流程图。该处理由加密部116执行。

[0107] 加密部116的加密密钥生成器403确定计数器信息i是否被设置在存储器112中、或设置在存储于存储部115或存储介质120中的介质列表中(S1101)。这个确定过程的执行是为了检查之前是否已经生成了会话密钥。如果设置了计数器信息i，处理前进到步骤S1102。否则，处理前进到步骤S1111。

[0108] 如果没有设置计数器信息i，加密密钥生成器403将加密密钥Kenc作为初始会话密钥Kenc(0)存储于存储器112中(S1111)。加密密钥生成器403将存储于存储器112或存储介质120中的计数器信息i设置为0(S1112)。处理前进到步骤S1102。

[0109] 数据加密部405从例如存储部115接收要被加密的图像数据(S1102)。加密密钥生成器403增加计数器信息i(i = i+1)(S1103)。

[0110] 密钥破坏器407生成要用于图像数据加密的会话密钥(S1104)。例如，通过将系统密钥Ksys(例如存储在存储器112中的系统密钥Ksys)用作密钥并输入会话密钥Kenc(i-1)来执行的HMAC处理的输出被设置为会话密钥Kenc(i)，并覆盖会话密钥Kenc(i-1)。在步骤S 1104的操作中，通过使用单向函数，将会话密钥Kenc(i-1)转换为会话密钥Kenc(i)。从Kenc(i)到Kenc(i-1)的反向计算是困难的。因此，会话密钥Kenc(i-1)被认为实际上被破坏了。该会话密钥生成方法将被称为“每次密钥破坏方案”。

[0111] 接下来，数据加密部405通过使用会话密钥Kenc(i)来加密图像数据(S1105)，并将计数器信息i作为元数据添加到加密的图像数据中(S1106)。存储部115或存储介质120存储带有元数据的加密的图像数据(S1107)。在步骤S1106种，不仅计数器信息，salt信息有时也被作为元数据添加到加密的图像数据中。

[0112] 在某些情况下，所摄图像数据（原始图像数据）的二次图像数据（例如缩略图图

像）被添加到图像数据中。缩略图图像通常是不加密的，尽管它可以被加密。如果未加密的缩略图图像被作为元数据持有，可以从阶段 4 中显示所摄图像的列表。

[0113] 为了加密缩略图图像，与用于原始图像数据的会话密钥相同的会话密钥或另一个会话密钥是有用的。前者不能应付每次密钥破坏方案。后者被通过相同的方法导出而作为缩略图的会话密钥，它不同于用于加密原始图像数据的密钥。如果对步骤 S806 中说明的介质列表的记录提供了一种在缩略图之前导出会话密钥的机制，加密的缩略图图像可以在阶段 4 中被显示。

[0114] 阶段 4

[0115] 在阶段 4 中，数字照相机 102 根据摄影者的指令显示存储于存储介质 120 中的图像数据以用于浏览 (S506)。解密后的加密图像数据是不可浏览的，但缩略图图像是可以浏览的。在阶段 3 禁止加密缩略图图像使得可以浏览存储于存储介质 120 中的图像。

[0116] 自然地，即使在阶段 3 被加密的缩略图图像也可以通过解密而变成可浏览的。在这种情况下，提供了一种使图像仅在将加密图像数据存储在存储介质 120 中的数字照相机 102 中是可浏览的机制。更具体地，通过使用“仅由数字照相机 102 知道的保密信息”来加密缩略图图像。“仅由数字照相机 102 知道的保密信息”被存储在步骤 S 806 中说明的介质列表的记录中。由 HMAC 处理或 SHA-1 处理从加密密钥 Kenc 中导出缩略图的第一会话密钥 Kthum(0)，并将其作为“仅由数字照相机 102 知道的保密信息”存储在介质列表的记录中。对于解密，例如通过执行 i 次对于 Kthum(0) 的 SHA-1 处理来导出对于第 i 个缩略图图像的会话密钥 Kthum(i)。可以通过计算 SHA-1(Kthum(0)||i) 或 SHA-1(Kthum(0)||SHA-1(i)) 来导出缩略图的会话密钥 Kthum(i)。注意“‖”指示数据的连接 (concatenation)。在任何一种情况下，实现安全密钥管理都是可能的，因为不能从缩略图的第一会话密钥 Kthum(0) 导出加密密钥 Kenc。

[0117] 图 12 是用于说明通过为每个图像数据生成会话密钥来加密缩略图图像的处理的流程图。该处里由加密部 116 来执行。

[0118] 加密密钥生成器 403 判断是否在例如存储器 112 中设置了缩略图的会话密钥 (S1201)。如果设置了缩略图的会话密钥，则处理前进到步骤 S1202。否则，处理前进到步骤 S1211。

[0119] 如果没有设置缩略图的会话密钥，加密密钥生成器 403 将加密密钥 Kenc 作为缩略图的初始会话密钥 Kthum(0) 存储在介质列表的记录中 (S1211)。加密密钥生成器 403 将存储在存储器 112 或存储介质 120 中的计数器信息 i 设置为 0(S1212)。处理前进到步骤 S 1202。计数器信息 i 对于用于加密原始图像数据的计数器信息可以是共用的 (S1103 ～ S1106)。

[0120] 数据加密部 405 从例如存储部 115 接收要加密的缩略图图像数据 (S1202)。加密密钥生成器 403 增加计数器信息 i(S1203)。

[0121] 加密密钥生成器 403 生成要用于缩略图图像数据加密的缩略图的会话密钥 (S1204)。例如，通过例如对缩略图的初始会话密钥 Kthum(0) 执行 i 次 SHA-1 处理来导出缩略图的会话密钥 Kthum(i)。可以通过计算 SHA-1(Kthum(0)||i) 或 SHA-1(Kthum(0)||SHA-1(i)) 来导出缩略图的会话密钥 Kthum(i)。

[0122] 接下来，数据加密部 405 通过使用缩略图的会话密钥 Kthum(i) 来加密缩略图图

像，并将计数器信息 i 作为元数据添加到加密的缩略图图像中 (S1206)。存储部 115 或存储介质 120 存储带有元数据的加密的缩略图图像 (S1207)。

[0123] 图 13 是用于说明浏览数字照相机中的加密的缩略图图像的解密方法的流程图。该处理由解密部 122 执行。

[0124] 解密部 122 的数据解密部 302 从存储部 115 或存储介质 120 中获取带有元数据的加密的缩略图图像 (S1301)，并分离出添加到加密的缩略图图像的用作元数据的计数器信息 i(S1302)。

[0125] 加密密钥生成器 301 根据计数器信息 i 和存储在例如介质列表中的缩略图的初始会话密钥 Kthum(0) 导出缩略图的会话密钥 Kthum(i)(S1303)。该密钥生长方法与步骤 S1204 中一致。例如通过对缩略图的初始会话密钥 Kthum(0) 执行 i 次 SHA-1 处理来生成对缩略图的会话密钥 Kthum(i)。

[0126] 数据解密部 302 通过使用缩略图的会话密钥 Kthum(i) 来解密加密过的缩略图图像 (S1304)，并将缩略图图像显示在例如操作部 121 的监视器上 (S1305)。

[0127] 阶段 5

[0128] 在阶段 5 中，计算机 101 允许使用存储在存储介质 120 中的加密的图像数据 (S510)。摄影者将存储介质 120 给予持有者。可选择地，计算机 101 通过网络接收加密的图像数据。下面将说明对于这两种情况通用的处理程序。

[0129] 图 9 是示出计算机 101 中的加密图像数据的解密程序的流程图。该处理是在 CPU 105 的控制下执行的。

[0130] CPU 105 通过例如键盘 103 接收密码 (预加密密钥数据)(S901)。CPU 105 通过控制解密部 117 的加密密钥生成器 301 来基于预加密密钥数据生成加密密钥 (S902)。该加密密钥生成 方法与阶段 1 中说明的方法一致。然后，CPU 105 通过控制数据解密部 302 使用加密密钥来解密加密的图像数据 (S903)。

[0131] 图 10 是示出包括附加处理的图 9 中所示处理的流程图，该附加处理当接收到加密密钥检验数据和加密的图像数据时，检验加密密钥检验数据和加密的图像数据之间的关联是否正确。该处理是在 CPU 105 的控制下执行的。

[0132] CPU 105 获取加密密钥检验数据 (S900)。之后，CPU 105 接收预加密密钥数据 (S901)，生成加密密钥 (S902)，并认证加密密钥检验数据的有效性 (S904)。有效性认证采用与数字照相机 102 的加密密钥检查部 404 的处理相同的方式。如果认证了加密密钥检验数据的有效性，则加密的图像数据被解密 (S903)。如果有效性未通过认证，则处理结束。当加密密钥检验数据的有效性未通过认证时，可以节省用于无意义的加密图像数据的解密的时间和精力。

[0133] 如上所述，即使当摄影者将拍摄的图像数据错误地或有意地传输给第三方 (除内容持有者之外)，摄影者和第三方都不能解密该加密的图像数据。传输包括通过网络的传送和复制在存储介质 120 中存储的图像数据。因此即使当摄影者与内容持有者不一致时，也可以保护内容持有者的权利，而不需要结合了版权保护机制的特殊的存储介质。

[0134] 实施例的变形

[0135] 在第一实施例中，当数字照相机 102 不能获取在加密密钥检验数据获取 (S801) 或加密密钥生成 (S804) 中的加密所必须的信息时，处理停止。如果处理停止了，则摄影者不

能拍摄图像。这有损摄影者的便利，因此需要一些解决办法。

[0136] 如果数字照相机 102 不能获取加密所需的信息，代替停止该处理，将未加密的图像数据存储在存储介质 120 中。另外，如果 因为数字照相机不能获取加密密钥检验数据而使得加密密钥检验数据的有效性未通过认证（验证失败），则基于预加密密钥数据来生成加密密钥 (S804)。然后，处理跳到验证处理 (S805)，并将加密的图像数据存储在存储介质 120 中。

[0137] 当存储介质 120 允许加密的图像数据与未加密的图像数据共同存在时，如上所述，提高了摄影者的便利。

[0138] 第一实施例没有考虑从存储介质 120 的非法数据删除。为了防止这点，在存储介质 120 中设置仅给予指定用户访问权限的访问控制机制。还可以通过使用仅允许写入的介质，即一次写入介质，来防止数据删除。

[0139] 上面举例了将计算机 101 连接到数字照相机 102 的信息处理系统。然而，本发明不限于此，并且还可以用于连接多个任意的信息处理装置的信息处理系统，这些信息处理装置例如是计算机、打印机、数字照相机、扫描仪、视频游戏播放机、便携式信息终端以及便携式电话。本发明还可以用于连接多个相同类型的信息处理装置的信息处理系统，例如多个计算机。

[0140] 对于加密密钥检验数据生成和认证方法，不仅可以应用包括 RSA 签名的公共密钥密码系统，还可以应用通用密钥密码系统和 MAC（消息认证码）生成方案的密码系统。作为密码系统，不仅可以应用包括 RSA 签名的公共密钥密码系统（保密），还可以应用通用密钥密码系统。也就是，任何其它的加密算法都可以应用于第一实施例的配置中。

[0141] 典型实施例

[0142] 本发明可以应用于由多个装置（例如主计算机、接口、读取器、打印机）构成的系统，或应用于包括单独装置（例如，复印机、传真机）的设备。

[0143] 而且，本发明可以提供一种存储用于执行上述对计算机系 统或设备（例如个人计算机）的处理的程序代码的存储介质，由计算机系统或设备的 CPU 或 MPU 从该存储介质中读取程序代码，然后执行该程序。

[0144] 在这种情况下，从存储介质中读取的程序代码实现根据这些实施例的功能。

[0145] 而且，该存储介质可以被用于提供程序代码，存储介质例如：软盘、硬盘、光盘、磁光盘、CD-ROM、CD-R、磁带、非易失性存储卡以及 ROM。

[0146] 而且，除了可以通过执行由计算机读出的程序代码来实现上面实施例的上述功能，本发明还包括这种情况：在计算机上运行的 OS（操作系统）等根据该程序代码的指示来执行部分或全部处理，并实现根据上述实施例的功能。

[0147] 而且，本发明还包括这种情况：当将从存储介质读出的程序代码写入插入到计算机中的功能扩展卡或连接到计算机的功能扩展单元中设置的存储器中后，该功能扩展卡或单元中包括的 CPU 等根据程序代码的指示来执行部分或全部处理，并实现根据上述实施例的功能。

[0148] 在本发明被应用到前述的存储介质中的情况下，该存储介质存储对应于这些实施例中说明的流程图的程序代码。

[0149] 虽然参考典型实施例说明了本发明，应该理解本发明不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，从而包括了全部变形、等同结构功能。

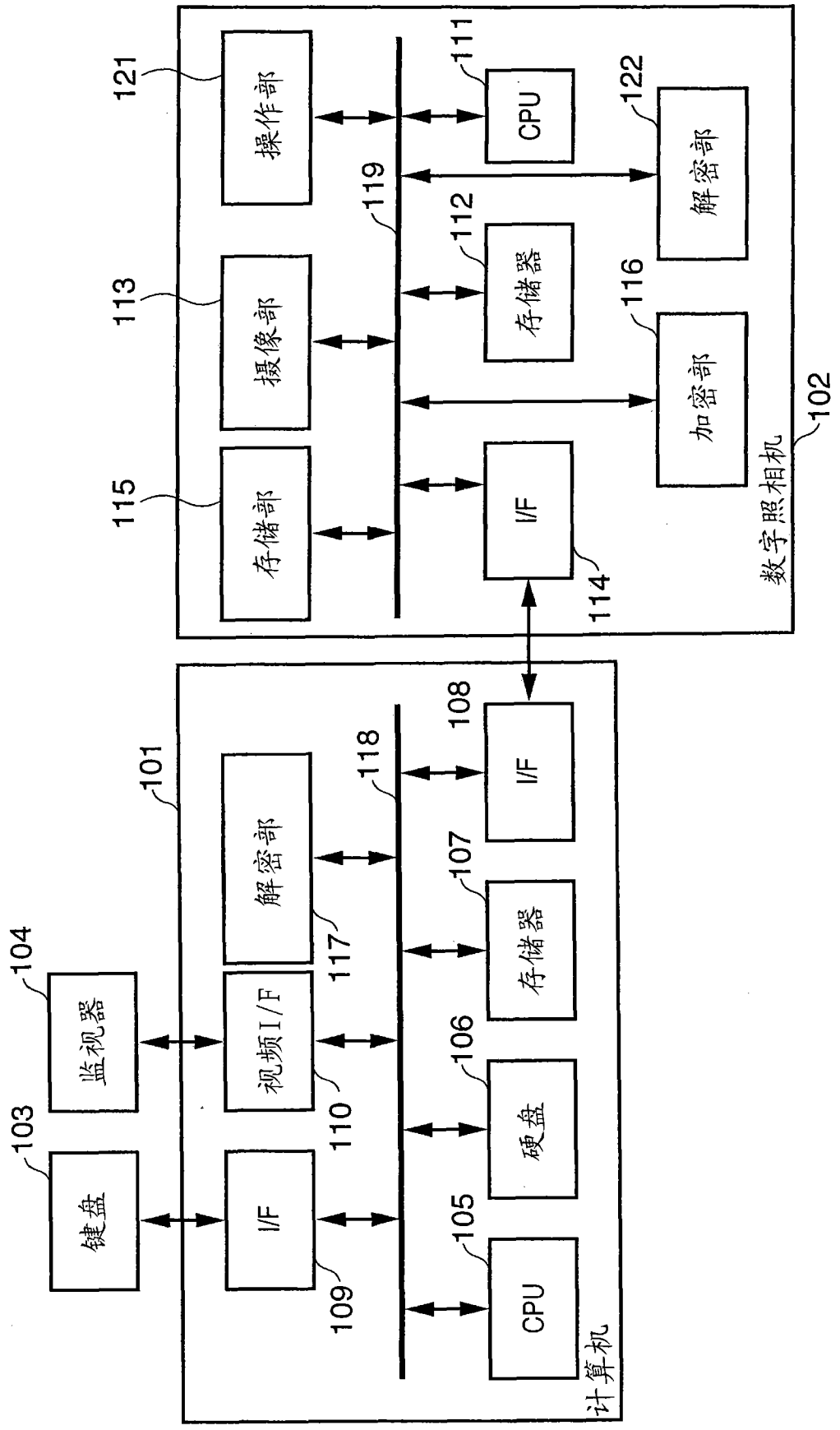

计算机
101
CPU
105
硬盘
106
存储器
107
I/F
108
I/F
109
视频I/F
110
解密部
117
118
键盘
103
监视器
104
数字照相机
102
I/F
114
存储部
115
摄像部
113
操作部
121
CPU
111
存储器
112
加密部
116
解密部
122
119

图 1

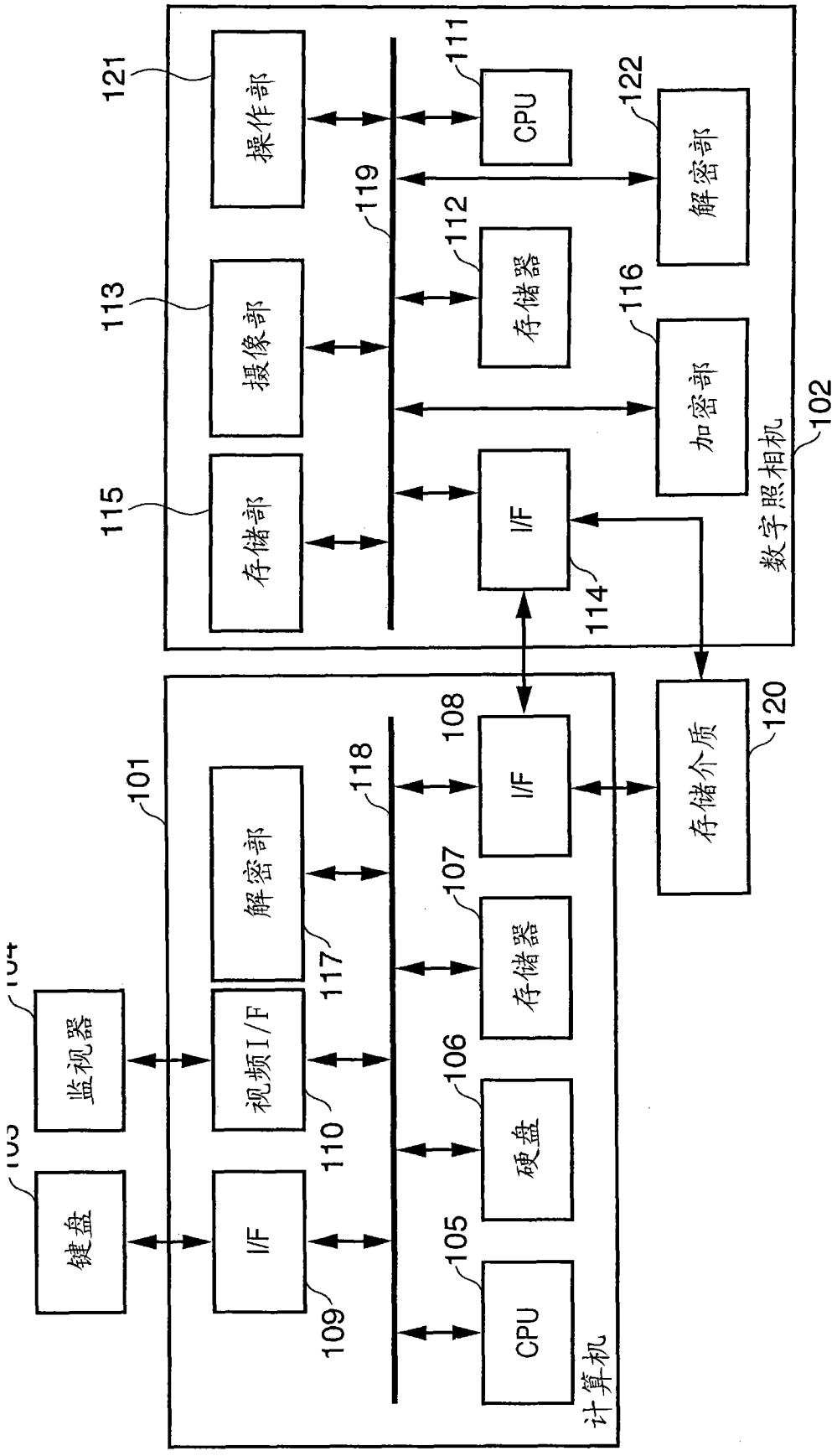

数字照相机
102
121
操作部
111
CPU
122
解密部
113
摄像部
112
存储器
116
加密部
115
存储部
I/F
114
119
101
计算机
118
解密部
108
I/F
117
107
存储器
120
存储介质
视频I/F
106
硬盘
110
I/F
105
CPU
109
103
键盘
104
监视器

图 2

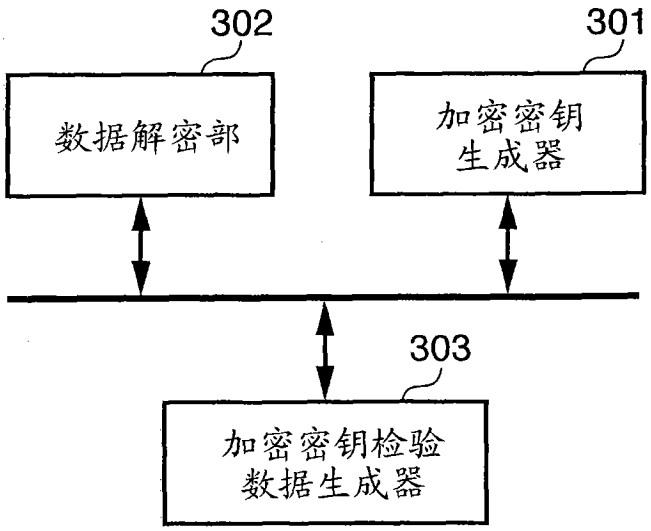

302
301
数据解密部
加密密钥
生成器
303
加密密钥检验
数据生成器

图 3

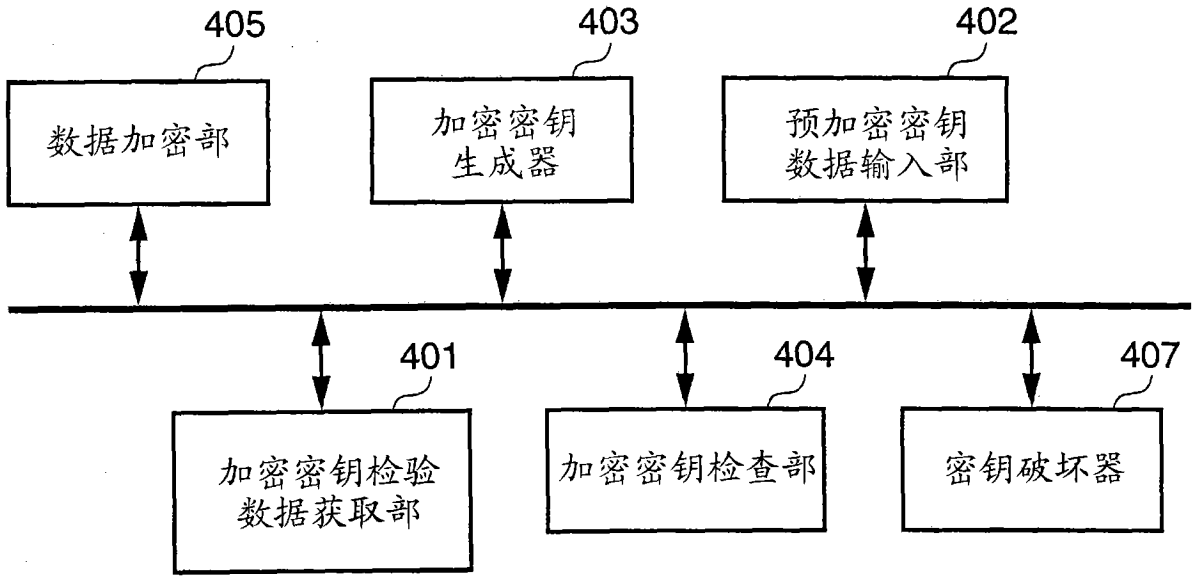

405
403
402
数据加密部
加密密钥
生成器
预加密密钥
数据输入部
401
404
407
加密密钥检验
数据获取部
加密密钥检查部
密钥破坏器

图 4

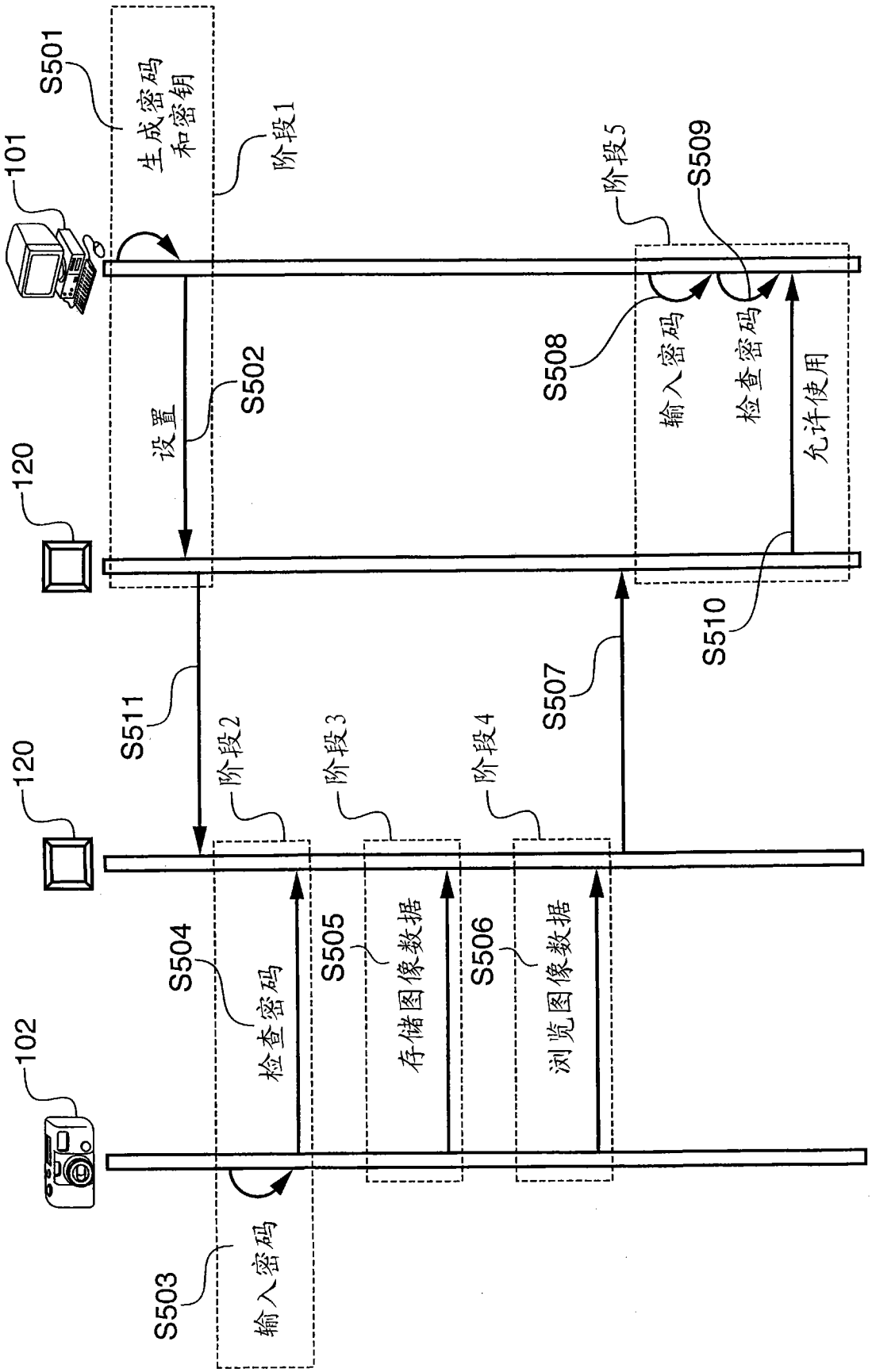

101
102
120
120
120
S501
生成密码和密钥
阶段1
S502
设置
S503
输入密码
S504
检查密码
S505
存储图像数据
S506
浏览图像数据
S507
S508
输入密码
阶段5
S509
检查密码
允许使用
S510
S511
阶段2
阶段3
阶段4

图 5

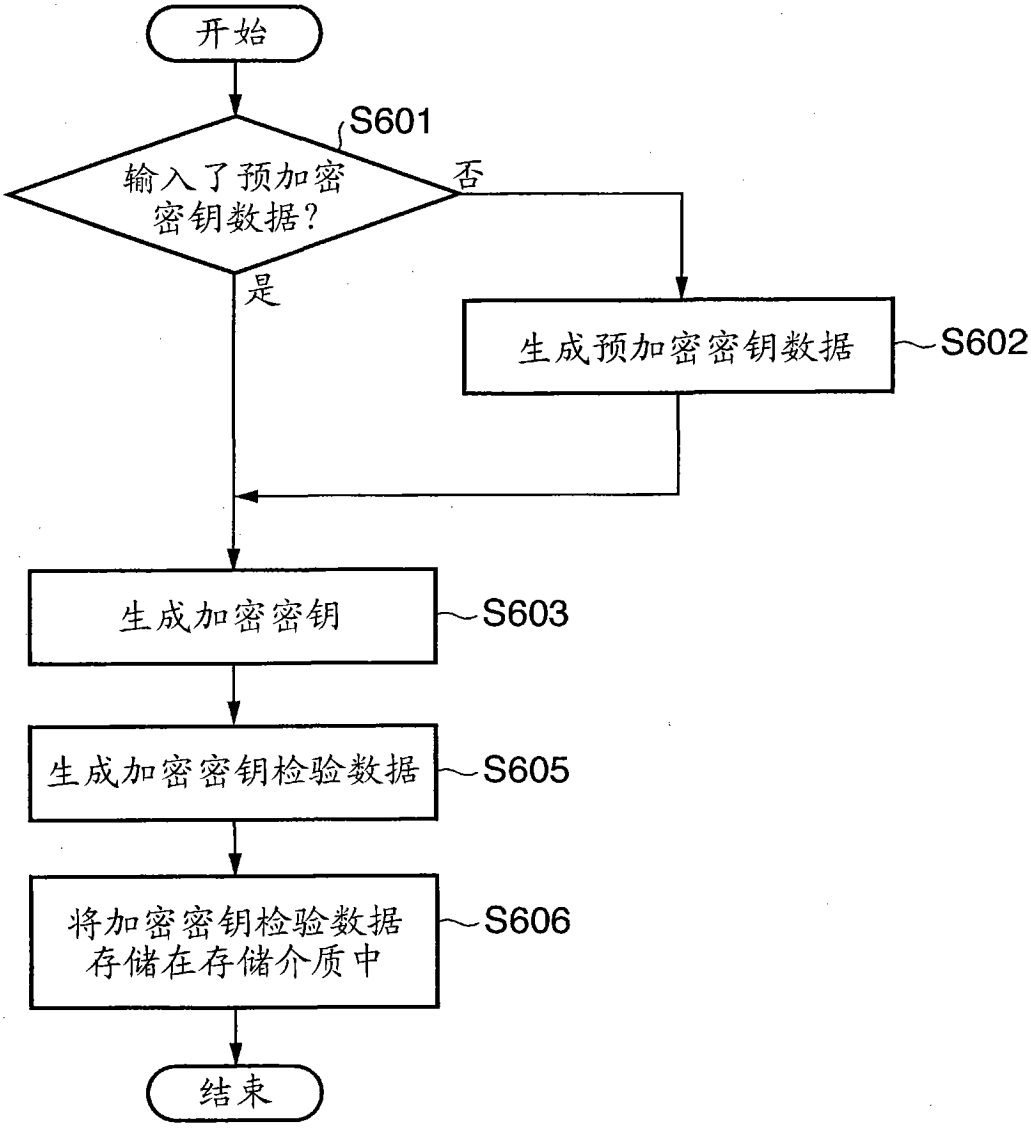

开始
S601
输入了预加密密钥数据?
否
是
生成预加密密钥数据
S602
生成加密密钥
S603
生成加密密钥检验数据
S605
将加密密钥检验数据存储在存储介质中
S606
结束

图 6

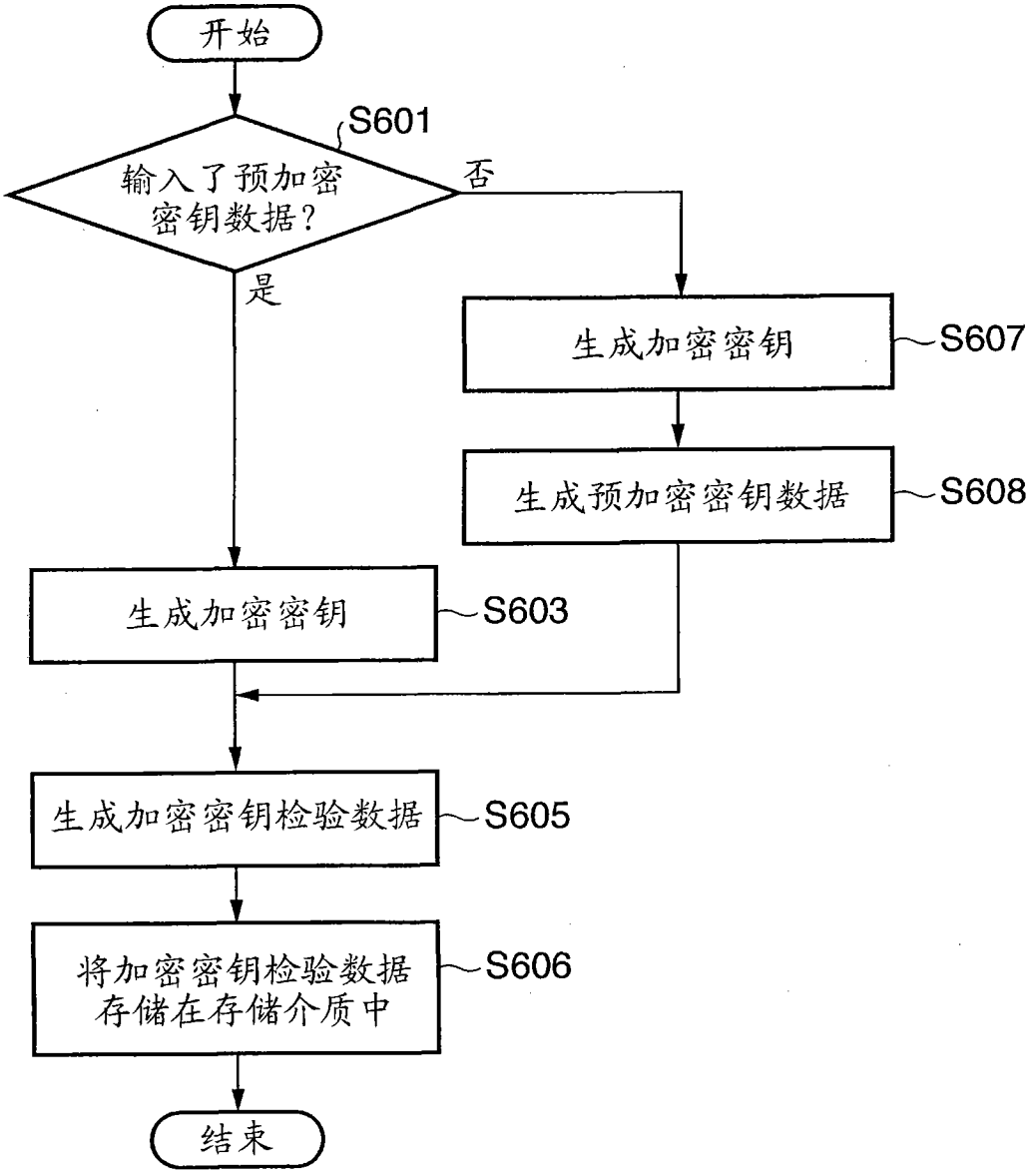

开始
S601
输入了预加密密钥数据？
否
是
生成加密密钥
S607
生成预加密密钥数据
S608
生成加密密钥
S603
生成加密密钥检验数据
S605
将加密密钥检验数据存储在存储介质中
S606
结束

图 7

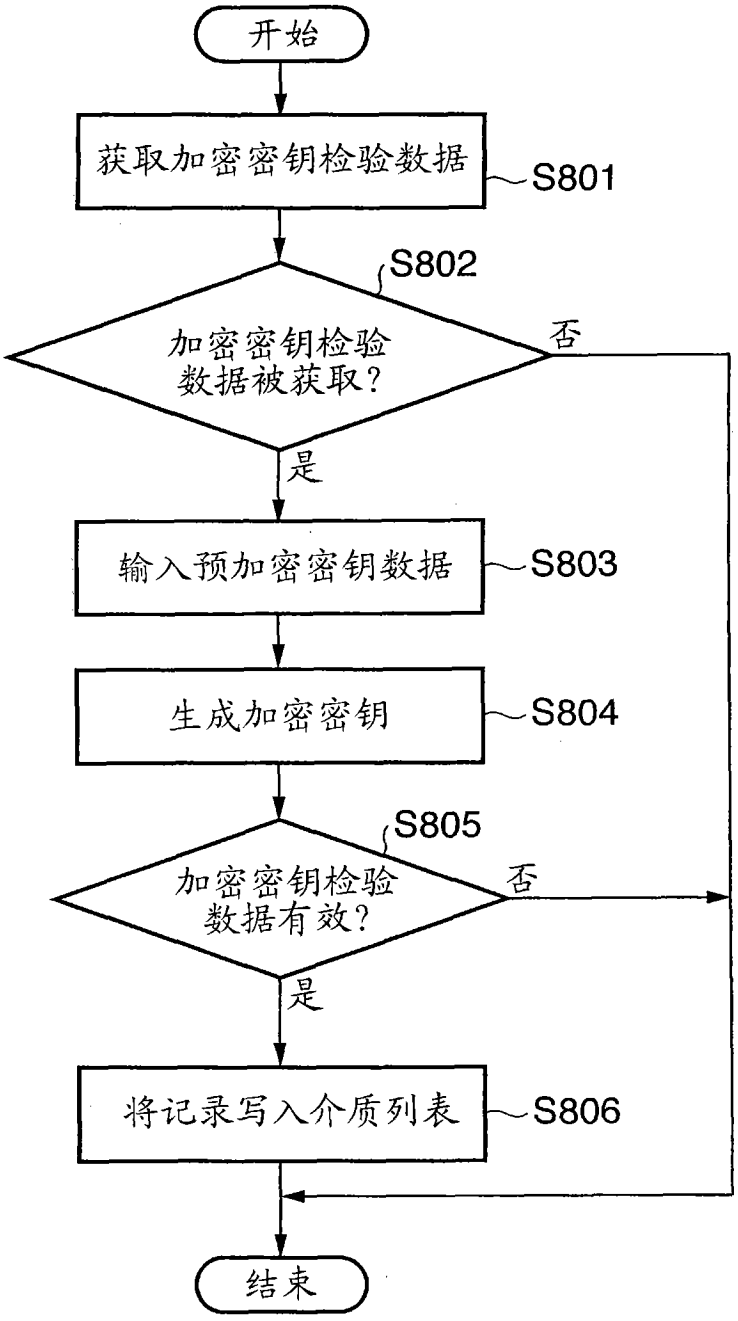

开始
获取加密密钥检验数据
S801
S802
加密密钥检验数据被获取?
否
是
输入预加密密钥数据
S803
生成加密密钥
S804
S805
加密密钥检验数据有效?
否
是
将记录写入介质列表
S806
结束

图 8

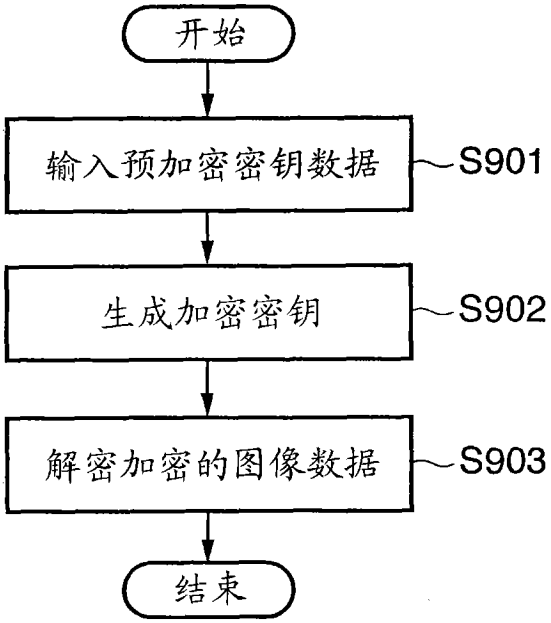

开始
输入预加密密钥数据
S901
生成加密密钥
S902
解密加密的图像数据
S903
结束

图 9

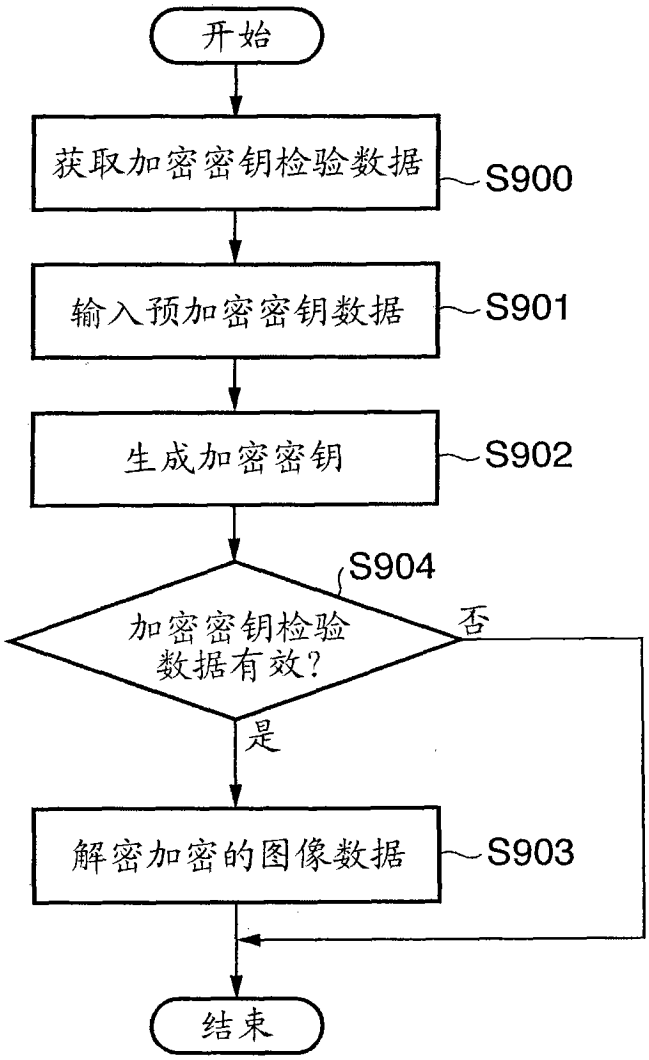

开始
获取加密密钥检验数据
S900
输入预加密密钥数据
S901
生成加密密钥
S902
S904
加密密钥检验数据有效?
否
是
解密加密的图像数据
S903
结束

图 10

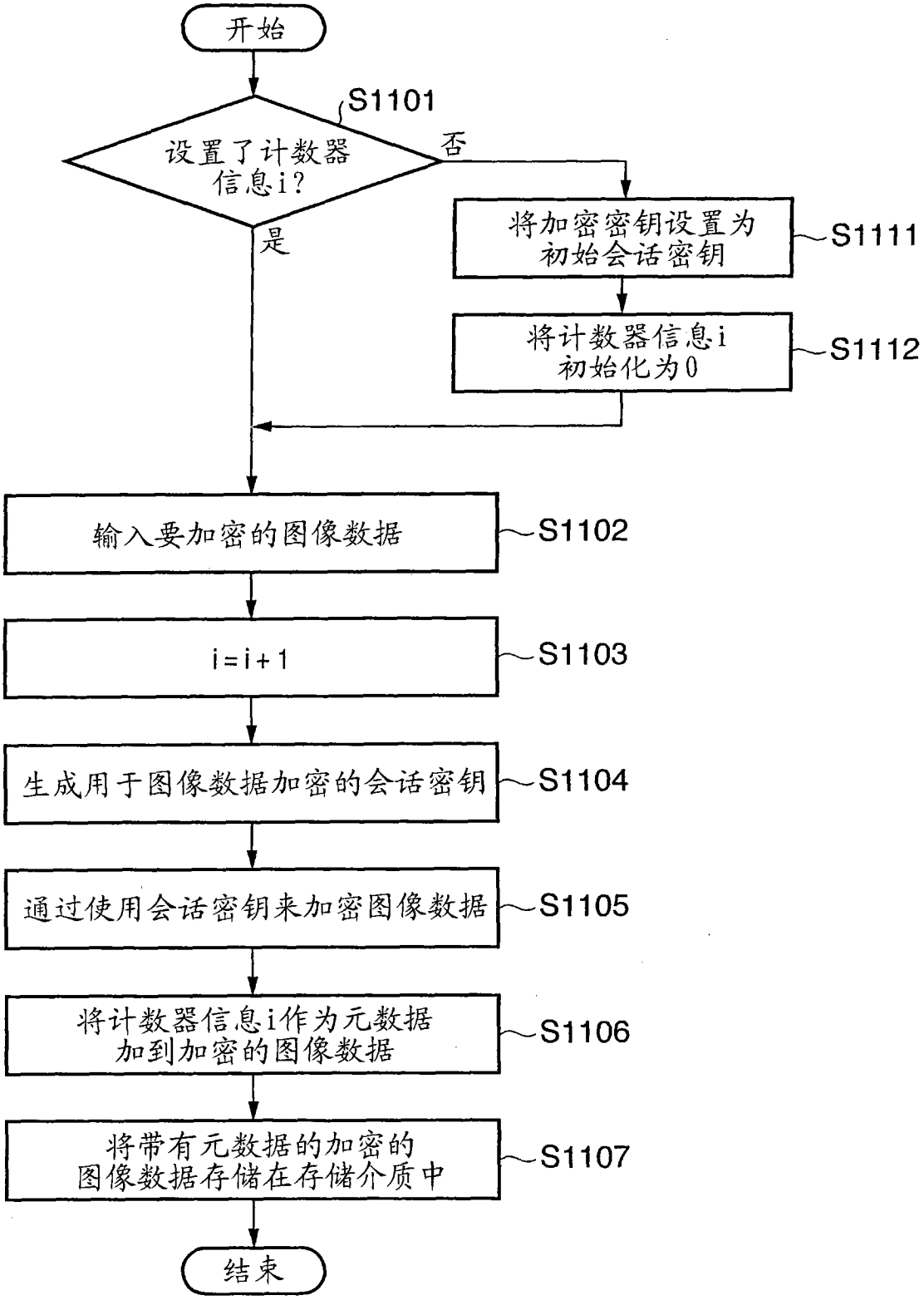

开始
S1101
设置了计数器信息i?
否
是
将加密密钥设置为初始会话密钥
S1111
将计数器信息i初始化为0
S1112
输入要加密的图像数据
S1102
i=i+1
S1103
生成用于图像数据加密的会话密钥
S1104
通过使用会话密钥来加密图像数据
S1105
将计数器信息i作为元数据加到加密的图像数据
S1106
将带有元数据的加密的图像数据存储在存储介质中
S1107
结束

图 11

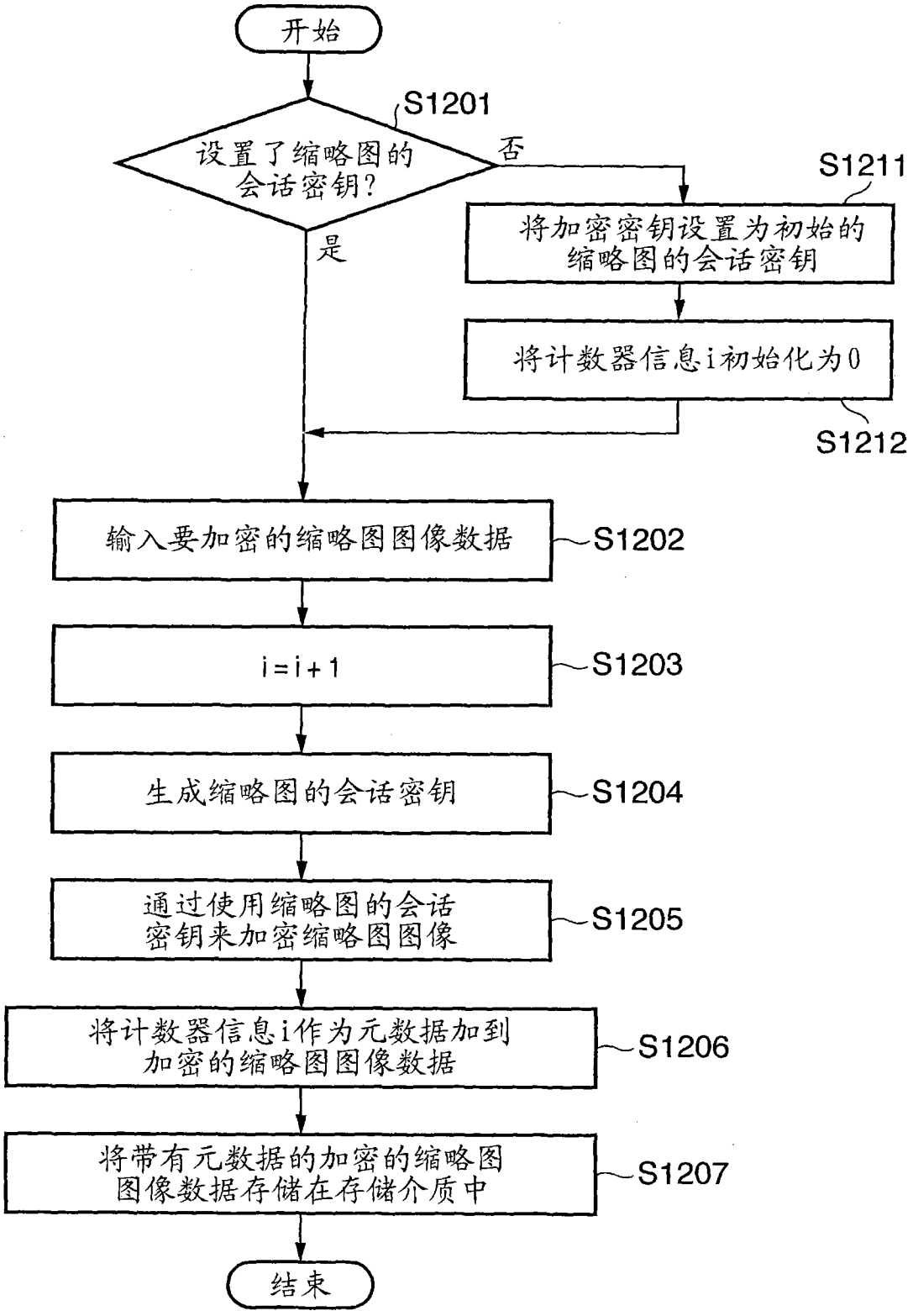

开始
S1201
设置了缩略图的会话密钥?
否
是
S1211
将加密密钥设置为初始的缩略图的会话密钥
将计数器信息i初始化为0
S1212
输入要加密的缩略图图像数据
S1202
i=i+1
S1203
生成缩略图的会话密钥
S1204
通过使用缩略图的会话密钥来加密缩略图图像
S1205
将计数器信息i作为元数据加到加密的缩略图图像数据
S1206
将带有元数据的加密的缩略图图像数据存储在存储介质中
S1207
结束

图 12

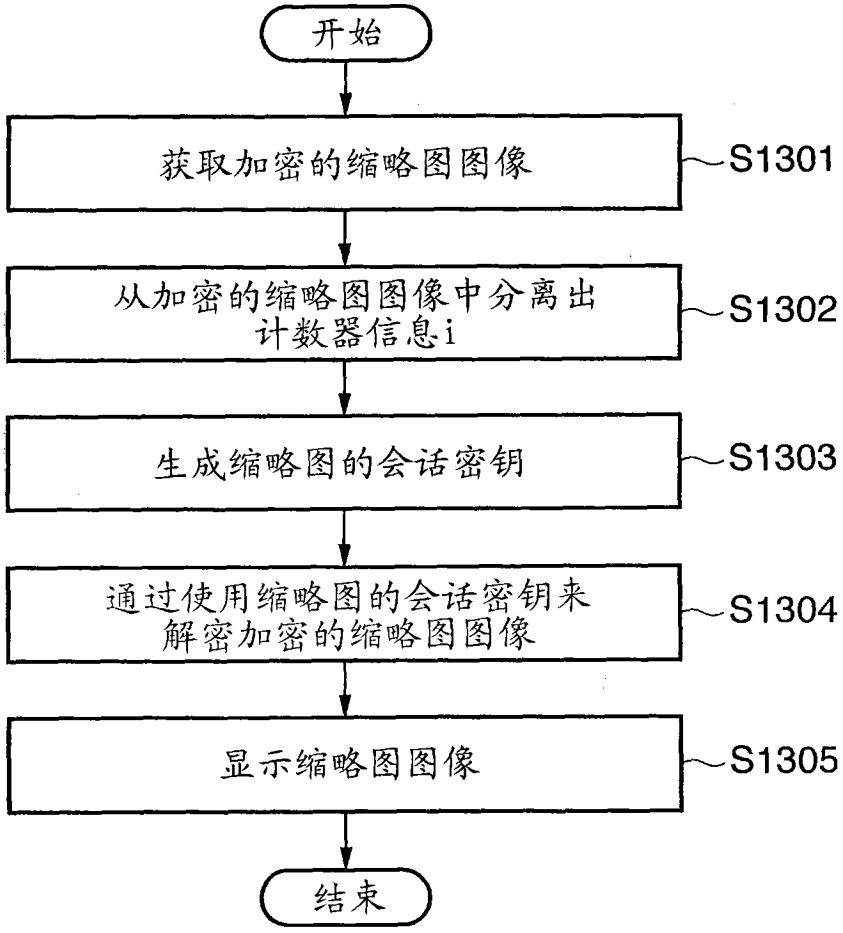

开始
获取加密的缩略图图像
S1301
从加密的缩略图图像中分离出
计数器信息i
S1302
生成缩略图的会话密钥
S1303
通过使用缩略图的会话密钥来
解密加密的缩略图图像
S1304
显示缩略图图像
S1305
结束

图 13