



(12) 发明专利

(10) 授权公告号 CN 1741449 B

(45) 授权公告日 2011.02.09

(21) 申请号 200510097750.6

审查员 张行素

(22) 申请日 2005.08.24

(30) 优先权数据

2004-244129 2004.08.24 JP

(73) 专利权人 佳能株式会社

地址 日本东京

(72) 发明人 岩村惠市

(74) 专利代理机构 中国国际贸易促进委员会专

利商标事务所 11038

代理人 康建峰

(51) Int. Cl.

H04L 9/32(2006.01)

(56) 对比文件

US 5499294 A, 1996.03.12, 说明书第5栏到第8栏.

US 2004/0030909 A1, 2004.02.12, 说明书第[0020]段到第[0022]段.

CN 1059999 A, 1992.04.01, 全文.

US 2003/0152227 A1, 2003.08.14, 全文.

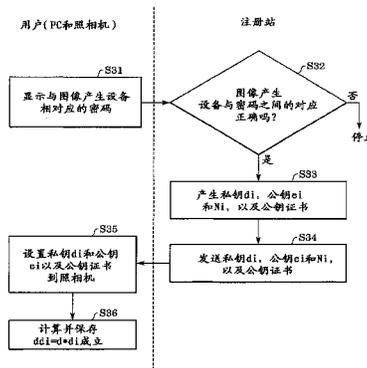
权利要求书 2 页 说明书 9 页 附图 5 页

(54) 发明名称

数据处理系统及其控制方法、计算机程序和可读记录介质

(57) 摘要

本发明公开一种控制合成数字签名信息的数据处理系统和方法。该系统和方法包括保存第一私钥信息,输入第二私钥信息,基于第一私钥信息和第二私钥信息产生第三私钥信息,保存第三私钥信息,基于待验证信息和第三私钥信息产生签名信息,并且输出待验证信息和签名信息。



1. 一种数据处理设备,包括:

保存单元,用于保存在数据处理设备中被管理的第一私钥信息,以使得第一私钥信息被保持为对于用户是保密的;

输入单元,用于输入从一个用户到另一个用户各不相同的第二私钥信息,以及公钥信息;

私钥信息产生单元,用于基于第一私钥信息和第二私钥信息产生第三私钥信息,并且保存第三私钥信息,其中,产生的第三私钥信息和公钥信息在公钥加密系统算法中彼此成对;

签名信息产生单元,用于基于待验证的信息和第三私钥信息产生签名信息;以及
输出单元,用于输出待验证信息、签名信息以及公钥信息。

2. 根据权利要求1的数据处理设备,其中输入单元还输入用于对公钥信息进行身份验证的证书信息。

3. 根据权利要求2的数据处理设备,其中输出单元作为单个文件输出待验证信息、签名信息、公钥信息、以及证书信息。

4. 根据权利要求1的数据处理设备,还包括用于产生待验证信息的产生单元。

5. 根据权利要求1的数据处理设备,还包括图像拾取单元,其中由图像拾取单元拾取的预先确定图像的数据作为待验证信息产生。

6. 一种注册管理中心设备,用于产生用在根据权利要求1所述的数据处理设备中的第二私钥信息,所述注册管理中心设备包括:

数据库,用于保存在用以注册的数据处理设备中提供的保存单元中保存的第一私钥信息;

用于通过参考数据库获取用于用以注册的数据处理设备的第二私钥信息的单元,在数据处理设备中,注册请求经由网络发送,根据预先确定的算法产生第二私钥信息,并且产生与基于第一私钥信息和第二私钥信息产生的第三私钥信息相对应的公钥信息;以及

发送单元,用于发送产生的第二私钥信息和公钥信息到请求源。

7. 一种控制数据处理设备的方法,该数据处理设备包括用于保存在数据处理设备中被管理的第一私钥信息的保存单元,以使得第一私钥信息被保持为对于用户是保密的,在该数据处理设备中,产生待验证信息,该方法包括步骤:

输入从一个用户到另一个用户各不相同的第二私钥信息,以及公钥信息;

基于第一私钥信息和第二私钥信息产生第三私钥信息,并且将第三私钥信息存储在预先确定的存储器中,其中,产生的第三私钥信息和公钥信息在公钥加密系统算法中彼此成对;

基于待验证信息和第三私钥信息以及公钥信息产生签名信息;以及
输出待验证信息和签名信息。

8. 根据权利要求7的控制数据处理设备的方法,其中输入步骤还输入用于对公钥信息进行身份验证的证书信息。

9. 根据权利要求7的控制数据处理设备的方法,其中输出步骤作为单个文件输出待验证信息、签名信息、公钥信息、以及证书信息。

10. 根据权利要求7的控制数据处理设备的方法,还包括产生待验证信息的步骤。

11. 根据权利要求 7 的控制数据处理设备的方法,还包括拾取预先确定图像的步骤,其中拾取的预先确定图像的数据作为待验证信息而产生。

数据处理系统及其控制方法、计算机程序和可读记录介质

技术领域

[0001] 本发明涉及一种数据处理系统以及一种控制该数据处理系统的方法,尤其涉及一种合成数字签名信息的技术。

背景技术

[0002] 近年来,数字照相机迅速普及。由数字照相机拍摄的图像如今在许多领域中使用,因为它们可以作为电子图像数据存储和保存。因此,不像已知的银盐照片,数字照相机的用户不需要显影和印刷由数字照相机拍摄的图像。此外,图像不会老化退化,容易检索,并且可以经由通信线路作为图像数据发送到遥远的地方。

[0003] 在上述领域中,存在其中通过使用事故中涉及的汽车损坏情况的拍摄图像来评估事故的损害保险(non-life insurance)业、其中施工现场被拍摄以确认其进展并且其中建筑物被拍摄以确认其规范的建筑行业,等等。日本的土地、基础设施和运输部(MLIT)已经允许使用数字照相机拍摄的图像来进行土木工程工地的记录。

[0004] 但是,因为由数字照相机获取的拍摄图像可以变成数字数据,下面提及的问题已经出现。也就是,拍摄的图像可以通过使用市场上可买到的 photoretouch 工具容易地在个人计算机(PC)上更改和修改,该工具是一种应用程序。因为数字数据可以容易地处理和/或修改,由数字照相机拍摄的图像的可靠性被认为低于银盐照片图像,特别是在图像用作事故的拍摄证据,或者附加到事故报告的情况下。

[0005] 虽然银盐照片的图像可以改变,这种改变很难进行,因为进行改变的成本显著高于改变获得的补偿,或者改变的结果不自然,这使得银盐照片适合用作证据。因此,存在由数字照相机拍摄的图像的上述缺陷将是未来损害保险业和建筑行业的大问题的担忧。随后,配置以解决上述问题的系统已经被需要。

[0006] 当前,通过使用由加密技术合成的数字签名数据检测图像数据中的改变的在美国专利 5,499,294 号中公开。

[0007] 上述系统包括配置以合成图像数据的图像产生设备(照相机),以及配置以验证图像数据完整性的图像验证设备。在图像产生设备中,预先确定的计算基于图像产生设备唯一的私有信息以及关于由图像产生设备拍摄和数字化的图像的数据来执行,从而作为用于识别图像数据(检测图像中的变化)的信息的数字签名数据(随后描述)被合成。然后,数字签名数据和关于由图像产生设备拍摄并数字化的图像的数据从图像产生设备向外部发送。图像验证设备通过比较对图像数据执行预先确定的计算而获得的数据与通过对数字签名数据执行数字签名数据合成时执行的计算的逆而获得的数据来执行验证。此外,在美国专利 5,499,294 号的情况下,散列函数(压缩函数)和公钥加密系统被使用,来合成数字签名数据。

[0008] 这里,配置以通过使用数字签名来检测图像中的改变的考虑,其中系统用于图像合成单元例如照相机。数字签名允许通过使用私钥来合成签名数据,像上述已知技术的情况一样。私钥可以根据下面两种方法来设置。

- [0009] 1. 照相机的用户合成私钥并且将它设置到照相机。
- [0010] 2. 照相机的制造商合成私钥并且将它设置到照相机。
- [0011] 随之而来的是会产生下面的问题。
- [0012] 1. 因为用户知道私钥, 并且是设置私钥的特别的人, 图像数据仅可以由用户改变。因此, 不存在由照相机拍摄的图像还没有改变的保证, 即使上述已知技术已经成功地提供保证。
- [0013] 2. 如果制造商设置私钥, 用户不能知道私钥, 使得高度的安全性获得。但是, 给照相机设置私钥使得每个私钥对与其相对应的照相机是唯一的, 使得制造照相机的步骤变得复杂。因此, 完全相同的私钥应当对所有照相机而设置。但是, 在那种情况下, 如果一个照相机的私钥被解析, 其他照相机的私钥可以被解析。

发明内容

- [0014] 因此, 本发明提供一种技术, 其允许减少制造商的工作量以及私钥的泄漏。此外, 即使私钥被解析, 本发明允许防止其他设备因解析而损坏。
- [0015] 根据本发明一方面, 提供一种数据处理设备, 包括排列以保存第一私钥信息的保存单元, 排列以输入第二私钥信息的输入单元, 排列以基于第一私钥信息和第二私钥信息产生第三私钥信息, 并且保存第三私钥信息的私钥信息产生单元, 排列以基于待验证的信息和第三私钥信息产生签名信息的签名信息产生单元, 排列以输出待验证信息和签名信息的输出单元。
- [0016] 本发明的更多特征将从参考附随附图的下面示例实施方案的详细描述中变得明白。

附图说明

- [0017] 图 1 说明根据本发明实施方案的图像验证系统的实例配置。
- [0018] 图 2 是说明根据实施方案的图像产生设备的配置的框图。
- [0019] 图 3 显示根据实施方案的图像验证设备的功能配置。
- [0020] 图 4 显示根据实施方案的注册管理中心的功能配置。
- [0021] 图 5 是说明根据实施方案的私钥分发处理的流程图。
- [0022] 图 6 是说明由根据实施方案的图像产生设备执行的数字签名合成处理的流程图。
- [0023] 图 7 是说明由根据实施方案的图像验证设备执行的数字签名验证处理的流程图。

具体实施方式

- [0024] 在下文中, 本发明的实施方案将参考附随附图详细描述。在实施方案中公开的组成部分作为实例提供。随后, 组成部分将不对本发明的范围做任何限制。
- [0025] 第一实施方案
- [0026] 首先, 数字签名将详细描述。
- [0027] 数字签名表示身份验证技术。也就是, 数据 (待验证数据) 和与其对应的数字签名数据从发送方发送, 并且用于验证的数据通过使用数字签名数据在接收方验证, 从而数据的有效性被确认。

[0028] 通常,散列 (hash) 函数和公钥加密系统用于确认数据有效性,以便合成数字签名数据。这里,公钥加密系统的私钥和公钥分别定义为 K_s 和 K_p ,这将在下面描述。

[0029] 在发送方,明文 (plain-text) 数据 (待验证数据) M 通过使用散列函数 $H()$ 压缩,使得预先确定长度的输出 h 被计算。也就是,计算 $H(M) = h$ 被执行。接下来,输出 h 通过使用私钥 K_s 转换,使得数字签名数据 s 被合成。也就是,计算 $D(K_s, h) = s$ 被执行。然后,数字签名数据 s 和明文数据 M 发送到验证方。

[0030] 在验证方,数字签名数据 s 通过使用公钥 K_p 转换。也就是,计算 $E(K_p, s) = E(K_p, D(K_s, h)) = h'$ 被执行。此外,发送的明文数据 M' 通过使用与发送方相同的散列函数来压缩,使得输出 h'' 被计算。也就是,计算 $H(M') = h''$ 被执行。当输出 h' 和 h'' 彼此一致时,确定明文数据 M' 是有效的 ($M' = M$)。

[0031] 当明文数据 M 在发送方和验证方之间改变时,由计算 $E(K_p, s) = E(K_p, D(K_s, h))$ 获得的输出 h' 与通过使用与发送方相同的散列函数压缩发送的存文本数据 M' 所获得的输出 h'' 不一致。因此,确定明文数据 M 改变。如果数字签名数据 s 根据明文数据 M 中的改变而改变时,改变不能被检测。但是,为了制造上述改变,明文数据 M 必须根据输出 h 获得,这因为散列函数的单向特性是不可能的。

[0032] 接下来,散列函数将被描述。散列函数用于增加合成上述数字签名的速度。散列函数具有处理任意长度的明文数据 M 并合成预先确定长度的输出 h 的功能。这里,输出 h 称作明文数据 M 的散列值 (或者消息摘要或数字指纹)。散列函数应当是单向和抗冲突的。当散列函数是单向时,明文数据 M 的计算变得难以按照计算量来执行,其中表达式 $h = H(M)$ 成立。此外,当散列函数是抗冲突时,并且当明文数据 M 已知时,明文数据 M' ($M \neq M'$) 的计算变得难以按照计算量执行,其中等式 $H(M) = H(M')$ 成立。此外,明文数据 M 和明文数据 M' 的计算变得难以按照计算量执行,其中等式 $H(M) = H(M')$ 且 $M \neq M'$ 成立。

[0033] 散列函数 MD-2, MD-4, MD-5, SHA-1, RIPEMD-128, RIPEMD-160 等已知并且其算法公共可见。

[0034] 接下来,公钥加密系统将被描述。公钥加密系统用于加密方法,其中编码密钥 (公钥) 和解码密钥 (私钥) 彼此不同,并且编码密钥是公共可见的,而解码密钥保持秘密。公钥加密系统具有下面的特性。

[0035] (a) 因为编码密钥不同于解码密钥并且编码密钥可以公开,编码密钥可以不保密发送,这使得容易执行密钥传输。

[0036] (b) 因为每个用户的编码密钥公开的,用户必须仅保密地记住他 / 她自己的解码密钥。

[0037] (c) 身份验证功能,其允许接收方确认通信语句从其发送的发送方不是伪造的,并且通信语句没有改变。

[0038] 例如,当通过使用公钥 K_p 加密明文数据 M 的操作确定为 $E(K_p, M)$ 且通过使用私钥 K_s 解密明文数据 M 的操作确定为 $D(K_s, M)$ 时,公钥加密系统算法满足下面两个条件。

[0039] (1) 当公钥 K_p 已知时,计算 $E(K_p, M)$ 可以容易地执行。当私钥 K_s 已知时,计算 $D(K_s, M)$ 可以容易地执行。

[0040] (2) 当私钥 K_s 未知时,按照计算量确定明文数据 M 变得困难,即使计算公钥 K_p 和 $E()$ 的步骤,以及 $C (= E(K_p, M))$ 已知。

[0041] 此外,下面的条件 (3) 进一步根据上述条件 (1) 和 (2) 设置,使得私有通信可以执行。

[0042] (3) $E(K_p, M)$ 可以对每个明文数据 M 确定,使得等式 $D(K_s, E(K_p, M)) = M$ 成立。也就是说,即使任何人可以执行计算 $E(K_p, M)$,因为公钥 K_p 是公开的,仅拥有私钥 K_s 的用户可以通过执行计算 $D(K_s, E(K_p, M))$ 获得明文数据 M 。另一方面,下面的条件 (4) 进一步根据上述条件 (1) 和 (2) 设置,使得身份验证通信可以执行。

[0043] (4) $D(K_s, M)$ 可以对每个明文数据 M 而定义,使得等式 $E(K_p, D(K_s, M)) = M$ 成立。也就是说,仅拥有私钥 K_s 的用户可以执行计算 $D(K_s, M)$ 。如果另一个人通过使用假的私钥 K_s' 执行计算 $D(K_s', M)$,并且伪装成拥有私钥 K_s 的用户,计算结果变成 $E(K_p, D(K_s, M)) \neq M$ 。因此,确认发送的信息在接收方无效。此外,如果 $D(K_s, M)$ 改变,计算结果变成 $E(K_p, D(K_s, M)') \neq M$,使得确定发送的数据在接收方无效。

[0044] 此外,当明文数据 M 的有效性被确认时,仅拥有私钥 K_s 的人可以合成 $D(K_s, M)$ 。随后,确认拥有私钥 K_s 的用户签名明文数据 M 。

[0045] RSA 编码, R 编码等已知,作为允许执行上述私有通信和身份验证通信的实例。

[0046] 这里,近来最频繁使用的 RSA 编码、签名合成以及签名验证的加密和解码由下面的表达式实现。

[0047] 加密:加密密钥 (e, n)

[0048] 加密转换 $C = M^e \pmod n$

[0049] 解码:解码密钥 (d, n)

[0050] 解码转换 $M = C^d \pmod n$

[0051] 签名合成:签名密钥 (d, n)

[0052] 签名合成: $S = M^d \pmod n$

[0053] 签名验证:签名验证密钥 (e, n)

[0054] 签名验证 $M = S^e \pmod n$

[0055] 这里,等式 $n = p \cdot q$ 成立,其中 p 和 q 表示彼此不同的大质数。此外, e 和 d 是满足下面等式的整数。

[0056] $e \cdot d = 1 \pmod L$

[0057] $L = \text{LCM}((p-1), (q-1))$

[0058] 这里, $\text{LCM}(a, b)$ 表示 a 和 b 的最小公倍数。

[0059] 图 1 显示根据第一实施方案的系统的配置。如该附图中所示,系统包括配置以合成用于身份验证的图像信息及其数字签名信息的图像产生设备 11,可以与图像产生设备 11 通信的注册管理中心 12,以及图像验证设备 13。

[0060] 图像产生设备 11 具有设置用于合成数字签名的私钥的功能,合成图像数据并拍摄图像的功能,合成与被合成图像数据相对应的数字签名的功能,合成辅助参数(照相机以该参数使用,例如,拍摄时间,焦距, f 数目, ISO 感光度,计量模式,图像文件大小,摄影者信息等)的功能,用数字签名合成图像文件(包括图像数据,数字签名,辅助参数等)的功能,以及与注册管理中心 12 执行通信的功能。此外,图像产生设备 11 可以是,但不局限于图像拾取设备例如数字照相机,数字摄像机,扫描仪等,以及包括照相机单元的电子装备。为了简单起见,在下文中,图像产生设备 11 用于数字静止照相机。

[0061] 注册管理中心 12 具有验证用户的功能,根据从有效用户发送的请求合成彼此成对的对有效用户唯一的私钥以及公钥的功能,添加公钥证书到公钥并且发送公钥和公钥证书到有效用户的功能,通知并释放注册管理中心 12 的公钥的功能。此外,在本实施方案中,注册管理中心 12 提供作为可以经由网络执行通信的个人计算机 (PC)。注册管理中心 12 并不局限于该实现,并且将能够实践本发明的任何实体是可应用的。

[0062] 图像验证设备 13 具有分离添加数字签名的图像文件的功能,验证从图像数据中分离的数字签名的功能,以及产生验证结果的显示图像的功能。此外,图像验证设备 13 可以是,但并不局限于,配置以存储数据的 web 服务器,配置以分发数据的 PC,或者包括 CPU、内存等的小装置。为了简单起见,在下文中,图像验证设备 13 将被描述为 PC。

[0063] 图 2 是显示根据第一实施方案的图像产生设备 11 的配置的框图。在该附图中,图像拾取单元 25 包括光学透镜和图像拾取元件,并且密钥保存单元 21 包括可写非易失性存储器。计算单元 23 根据从配置以控制整个系统的控制单元 24 发送的请求执行预先确定的计算,并且图像文件产生单元 26 基于拾取的图像以预先确定的格式合成图像文件并且将图像文件写入可移动存储卡(没有显示)中。操作单元 22 包括配置以确认拾取图像并且产生各种菜单、开关、和按钮的显示图像的显示单元(液晶显示器等)。操作单元 22 用作系统与用户之间的接口。此外,配置以计算散列值的散列产生单元 27,和数字签名产生单元 28 被提供。

[0064] 图 3 是说明根据第一实施方案的图像验证设备 13 功能的框图。如上所述,图像验证设备 13 形成为 PC。因为 PC 的配置与本发明的实践无关,图 3 仅显示配置以用作验证设备的程序执行的实例。也就是,图 3 中所示每个功能单元形成为 CPU,和配置以执行 CPU 处理的程序。

[0065] 图 3 显示配置以从图像文件中分离图像数据和签名数据的图像文件分离单元 62,散列产生单元 63,以及配置以产生验证结果(例如数据是否改变)的显示图像的显示单元 65。图 3 还包括配置以发送用于验证的图像文件的输入单元 61,其中当图像文件经由网络等传输时,输入单元 61 用作网络 I/F,以及用于从记录介质例如存储卡中读取图像文件的读卡器(没有显示)。附图还包括配置以控制整个系统的控制单元 66,签名验证单元 64,以及判断单元 67。

[0066] 图 4 是显示根据第一实施方案的注册管理中心 12 配置的功能框图。图 4 包括连接到因特网、用于与拥有图像产生设备 11 的用户的 PC 通信的通信单元 71,配置以合成密钥信息和随后将描述的公钥证书 P 的密钥数据产生单元 72,配置以存储下面更详细描述、由每个图像产生设备 11 的制造商存储并保存在图像产生设备 11 中的私钥 d,并且存储当用户试图访问注册管理中心 12 时用于进行用户有效性检查的数据的数据库 73。图 4 还包括配置以控制整个注册管理中心 12 的控制单元 74。

[0067] 在上述系统中,分发数字签名私钥给每个用户的处理根据图 5 的流程图描述。这里,图像产生设备 11 具有执行与注册管理中心 12 安全通信的技术。例如,加密通信软件程序作为图像产生设备 11 的捆绑软件程序而提供,并且密码添加到每个图像产生设备 11,其中密码对于图像产生设备 11 是唯一的。此外,图像产生设备 11 在制造过程期间安装的密钥保存单元 21(例如可写非易失性存储器)中保存预先确定的私有信息 d。私有信息 d 对由图像产生设备的制造商提供的所有图像产生设备 11 共有。注册管理中心 12 也将私有信

息 d 保存在数据库 73 中,使得图像产生设备 11 的用户不被通知私有信息 d 的存在。

[0068] 在本发明中,每个私有信息 d 和说明符 e_i , d_i 和 N_i 指示数值,其设置为具有预先确定长度数值。

[0069] 转向图 5,在步骤 S31 中,用户安装捆绑软件到用户的 PC 上,提供 PC 与注册管理中心 12 之间的安全通信路径,并且将与图像产生设备 11 的 ID 相对应的密码提供到注册管理中心 12。接下来,在步骤 S32 中,注册管理中心 12 将图像产生设备 11 的 ID 与密码之间的一系列对应关系存储在数据库 73 中,并且确认密码的有效性。如果确定密码是无效的,注册管理中心 12 停止处理。否则,流程继续到步骤 S33,其中注册管理中心 12 控制密钥数据产生单元 72 使得用户“i”合成满足等式 (1) 和 (2) 之间关系的私钥 d_i ,公钥 e_i 和 N_i ,以及公钥证书 P:

$$[0070] \quad d_i \times d \times e_i = \text{lmod} \Phi(N_i) \quad \text{等式 (1)}$$

$$[0071] \quad \Phi(N_i) = \text{LCM}((p-1)(q-1)) \quad \text{等式 (2)}$$

[0072] 这里,p 和 q 表示质数。此外,公钥证书 P 证明用户公钥的有效性。这里密钥证书 P 通过使用注册管理中心 12 的私钥来签名。

[0073] 然后,在步骤 S34 中,私钥 d_i ,公钥 e_i 和 N_i ,以及公钥证书 P 通过安全通信路径发送到用户。发送到具有相同类型并且由相同制造商提供的图像产生设备 11 的上述信息项彼此不同。随后,私钥 d_i ,公钥 e_i 和 N_i ,以及公钥证书 P 被合成,使得等式 (1) 和 (2) 之间的关系满足。此外,私钥 d_i ,公钥 e_i 和 N_i ,以及公钥证书 P 基于,但不局限于随机数,用户的名字和地址,由用户使用的、应用到注册管理中心 12 的密码等合成。

[0074] 当接收到以上述方式从注册管理中心 12 发送的各种信息项时,安装在用户 PC 上的应用程序产生基于十六进制系统显示的信息项的显示图像,从而消息包括提示用户设置到图像产生设备 11 的发送信息的信息。

[0075] 在步骤 S35 中,用户通过操作图 2 中所示的操作单元 22,设置私钥 d_i 、公钥 e_i 、以及公钥证书 P 到密钥保存单元 21。结果,控制单元 24 通过使用存储在密钥保存单元 21 中并且没有发布给用户的私钥 d,以及发送的私钥 d_i 在计算单元 23 执行计算 $dd_i = d \times d_i$ 。然后,在步骤 S36 中,控制单元 24 存储计算结果在密钥保存单元 22 中。

[0076] 密钥保存单元 21 作为没有数据可以从其中读取并发送到除计算单元 23 和数字签名产生单元 30 之外的任何外部单元的存储器而提供,以便防止密钥信息的泄漏。计算单元 23 包括至少 CPU, RAM, ROM, 专用 IC 芯片,并且执行预先确定的计算。

[0077] 接下来,由根据第一实施方案的图像产生设备 11 执行的正常图像拾取处理将被描述。这里,图像产生设备 11 用于照相机,使得 AF 处理过程和 AE 处理过程被执行。因为 AF 和 AE 处理过程与本发明没有直接关系,其详细内容将不描述。但是,操作单元 22 的快门按钮按下之后执行的处理过程将根据图 6 中所示流程图来描述。

[0078] 首先,在步骤 S41 中,操作单元 22 被操作使得图像拾取单元 25 合成拾取的图像数据 D。然后,在步骤 S42 中,图像文件产生单元 26 将拾取的图像数据 D 转换成由基于已知 JPEG 标准的压缩和编码处理压缩并编码的文件。

[0079] 流程然后继续到步骤 S43,关于压缩图像文件的数据发送到散列产生单元 27 使得散列值 h 产生并且数字签名产生单元 28 通过使用存储在密钥保存单元 21 中的私钥 dd_i 来执行计算并且合成数字签名 s。接下来,在步骤 S44 中,控制单元 24 将合成的数字签名 S、

公钥 e_i 、以及公钥证书 P 插入到由图像文件产生单元 26 合成的图像文件的预先确定区域（例如标题部分），并且将图像文件存储在存储卡中（没有显示）。也就是说，在步骤 S44，生成图像 D、数字签名 S、公钥 e_i 、以及公钥证书 P，作为单个文件。

[0080] 这里，图像拾取单元 25 包括光学传感器例如电荷耦合器件 (CCD) 并且根据发送到操作单元 22 的指令合成对象的图像数据和辅助参数。此外，由图像文件产生单元 26 合成的图像文件可以基于 JPEG 文件交换格式 (JFIF)，标签图像文件格式 (TIFF)，图形交换格式 (GIF)，通过扩展上述格式而获得的格式，或者其他图像文件格式中任何一种。此外，通常已知的散列函数例如 MD5，SHA1，RIPEMD 等用作由散列产生单元 27 使用的散列函数 H。数字签名产生单元 28 包括配置以通过使用上述 RSA 编码执行签名合成处理的 CPU，以及配置以存储由 CPU 所需的密钥信息的存储器，包括 RAM，ROM 等。控制单元 24 控制上述处理过程。

[0081] 接下来，由图像验证设备 13 执行的数字签名验证将根据图 7 中所示流程图来描述。

[0082] 图 1 显示从图像产生设备 11 延伸到图像验证设备 13 的双向箭头，其指示图像文件经由通信和 / 或记录介质在其间传送。

[0083] 返回图 7，首先，在步骤 S51，包括图像 D、数字签名、公钥 e_i 、以及公钥证书 P 的图像文件从输入单元 61 中读取。然后，在步骤 S52，图像文件分离单元 62 从读取的图像文件中分离图像 D、数字签名、公钥 e_i 、以及公钥证书 P。

[0084] 接下来，在步骤 S53 中，散列产生单元 63 从图像 D 中合成散列值 H。

[0085] 流程然后继续到步骤 S54，其中图像验证设备 13 在签名验证单元 64 中通过使用由注册管理中心 12 发布的公钥来测试分离的公钥证书 P。

[0086] 如果验证结果不正确，指示公钥证书 P 验证失败的消息等的显示图像产生，从而数字签名验证终止。

[0087] 如果验证结果正确，流程继续到步骤 S55，其中分离的数字签名 S 通过使用公钥 e_i 由签名验证单元 64 解码。然后，在步骤 S56 中，在步骤 S53 计算的散列值 H 由判断单元 66 与在步骤 S55 解码的值 M 相比较。当散列值 H 与值 M 一致时，流程继续到步骤 S57，在那里确定不存在改变。否则，流程继续到步骤 S58，在那里确定存在改变。最后，在步骤 S59 中，判断结果的显示图像在显示单元 65 例如监视器上产生。例如，当判断单元 66 确定不存在改变时，显示图像“没有改变”产生，并且当判断单元 66 确定存在改变时，显示图像“被改变”产生。

[0088] 因此，根据第一实施方案，当图像产生设备 11 的用户发送注册请求到注册管理中心 12 时，对用户唯一的私钥 d_i 以及公钥 e_i 和 N_i ，和公钥证书 P 被发送，并且结果设置到图像产生设备 11。那时，用户被通知私钥 d_i 。图像产生设备 11 的控制单元 24 根据由制造商预先准备的私钥 d 和 d_i 来合成私钥 dd_i ，使得私钥 dd_i 用于合成数字签名。因此，仅注册管理中心 12 知道私钥 dd_i 。

[0089] 如果具有其型号和制造商与上述图像产生设备 11 相同的图像产生设备 11 的第三方发送注册请求到注册管理中心 12，私钥 d_j ，公钥 e_j 和 N_j ，以及公钥证书 P 发送到第三方。由图像产生设备 11 合成的私钥由说明符 dd_j 指示，使得私钥 dd_i 和 d_i 保密。

[0090] 本发明的第一实施方案允许减少制造商的工作量和私钥的泄漏。此外，即使私钥被解析，第一实施方案允许防止其他设备受解析影响。

[0091] 其他实施方案

[0092] 其他实施方案将在下面描述。根据第一实施方案,数字签名仅对关于对象的图像数据而合成。但是,数字签名数据可以对信息例如图像数据的元数据而合成,例如包括拍摄时间、焦距、f 数目、ISO 感光度、计量模式、图像文件大小、拍摄者信息等的辅助参数。在那种情况下,数字签名数据也可以由与图像数据的情况相同的机制合成,并且数字签名验证也可以对辅助参数执行。

[0093] 因为图像数据和元数据的每个是二进制数据,数字签名验证可以通过用元数据代替图像数据来实现。也就是说,数字签名验证可以通过发送元数据到散列产生单元 27 代替图像数据来实现。该数据改变由控制单元 24 实现。因此,图 6 和 7 中描述的图像 D 应当用辅助参数来代替。随后,变得能够检测不仅图像数据中的改变,而且关于图像的元数据中的改变。

[0094] 在第一实施方案中,为了简单起见,公钥证书 P 由注册管理中心 12 发出。但是,基于广泛已知的公钥基础结构 (PKI) 建立的证书认证中心可以发出公钥证书 P。

[0095] 此外,根据第一实施方案,在步骤 S35 中将私钥 d_i 、公钥 e_i 、以及公钥证书 P 设置到密钥保存单元 21 中。但是,也可以仅将私钥 d_i 设置到密钥保存单元 21 中。在这种情况下,在步骤 S44 中,将生成的数字签名 S 插入到所生成的图像文件的预先确定的区域,以便生成包括图像 D 和数字签名 S 的图像文件。

[0096] 另外,根据第一实施方案,在步骤 S51 中读出包括图像 D、数字签名、公钥 e_i 、以及公钥证书 P 的图像文件。但是,也可以配置为读出包括图像 D 和数字签名 S 的图像文件。在这种情况下,在步骤 S54 测试的公钥证书 P 以及在步骤 S56 使用的公钥 e_i 可以从外部设备(证书认证中心、注册管理中心等等)获得。此外,在步骤 S51 中读出包括图像 D 和数字签名 S 的图像文件时,在步骤 S52 中将该图像文件分离成图像 D 和数字签名 S。

[0097] 到此,已经描述了本发明的实施方案。在第一和其他实施方案中,图像产生设备 11(数字静止照相机)已经作为配置以合成验证信息的设备来描述。但是,本发明不仅用于上述设备。也就是,本发明可以用于配置以通过使用上述私钥 d_i 合成数字签名数据的任何设备,当用于验证的数据合成时,或者当设备合成用于验证的数据时。

[0098] 上述设备的实例将在下面描述。

[0099] 存储卡作为存储私钥 d 的 USB 设备而准备。存储在存储卡中的私钥 d 由设备制造商设置,使得用户不能访问私钥 d 。

[0100] 然后,当文档由 PC 产生时,用于合成数字签名 S 的应用程序被启动。应用程序通过使用私钥 d 和从注册管理中心 12 发送的私钥 d_i 来合成私钥 d_i ,并且合成关于文档文件和单个文件的签名数据。

[0101] 此外,上述实施方案已经基于图像产生设备 11 的用户具有 PC 的前提描述。但是,当图像产生设备 11 具有网络连接功能时,本发明并不局限于上述实施方案。例如,移动电话等可以用于获取密钥信息等。

[0102] 因此,即使包括存储卡等的硬件是必需的,本发明可以用于运行在 PC 上的应用程序。通常,应用程序存储在计算机可读记录介质例如 CD-ROM 中,设置到计算机,并且拷贝并安装到系统上,以便可执行。因此,上述计算机可读记录介质在本发明的范围内。

[0103] 换句话说,实施方案的前述描述已经给出,仅用于说明目的,而不解释为在各个方

面实行限制。

[0104] 因此,本发明的范围将单独由下面的权利要求确定,而不由说明书的文本所限制,并且与权利要求范围等价的范围内进行的更改落入本发明的实际本质和范围内。

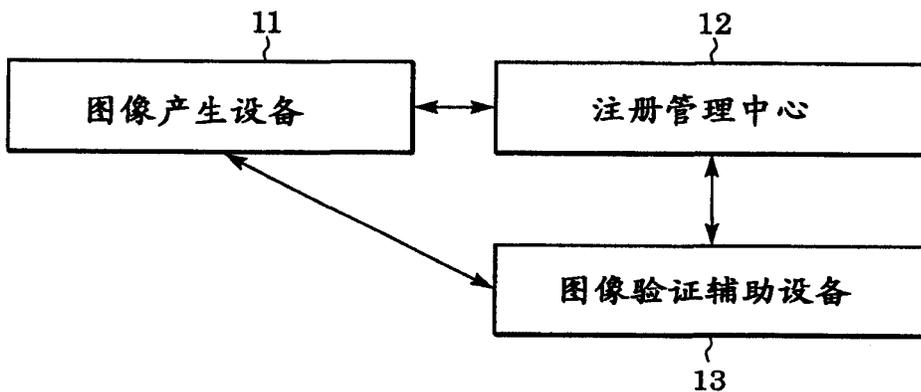


图 1

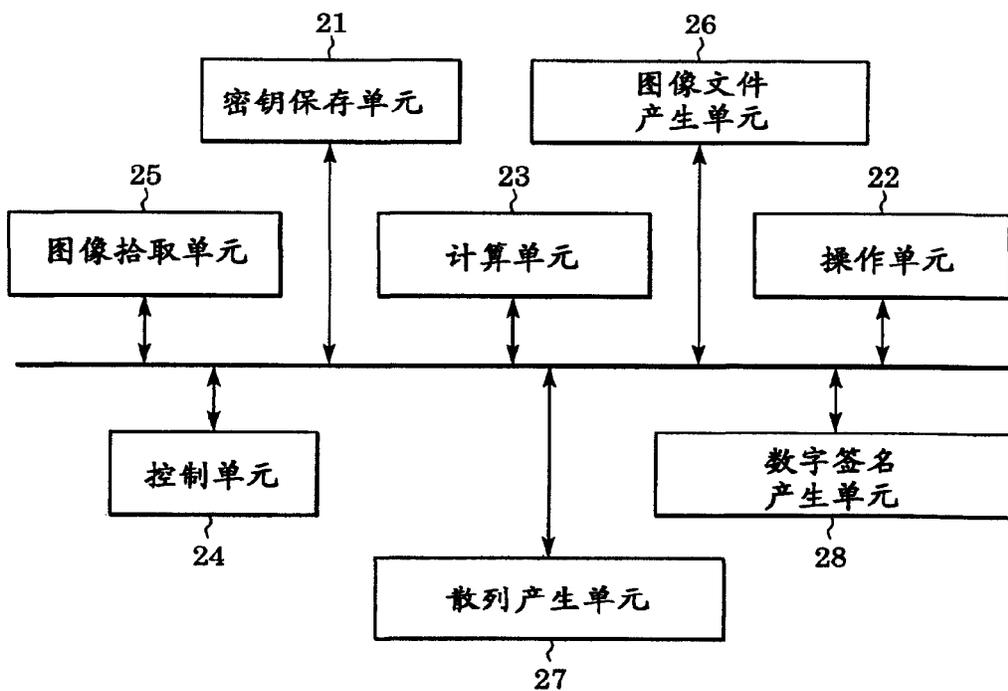


图 2

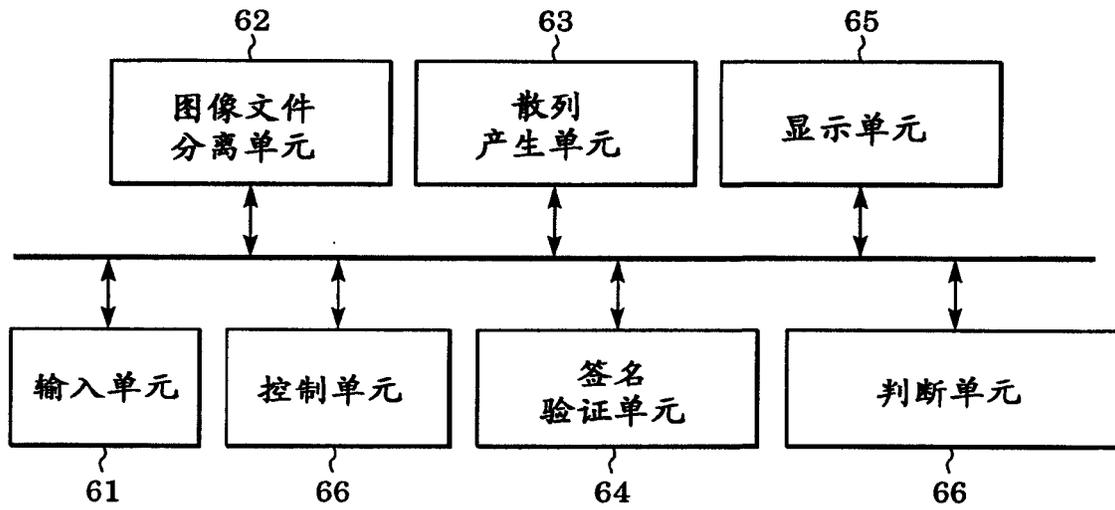


图 3

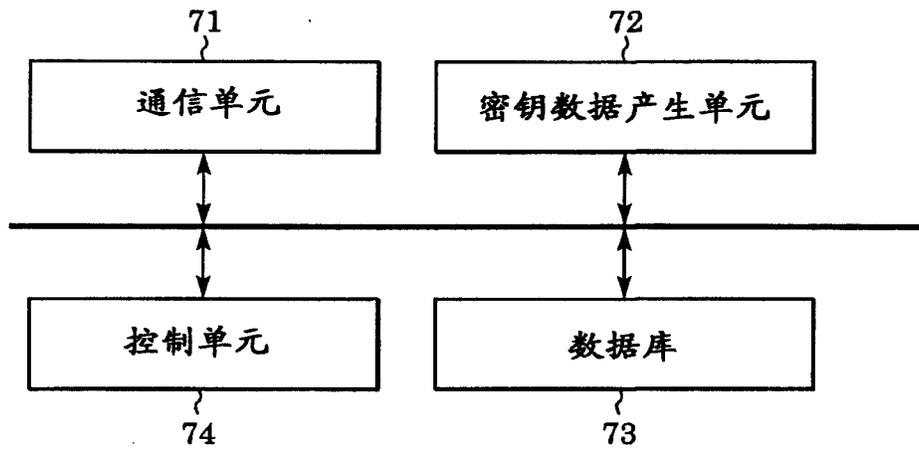


图 4

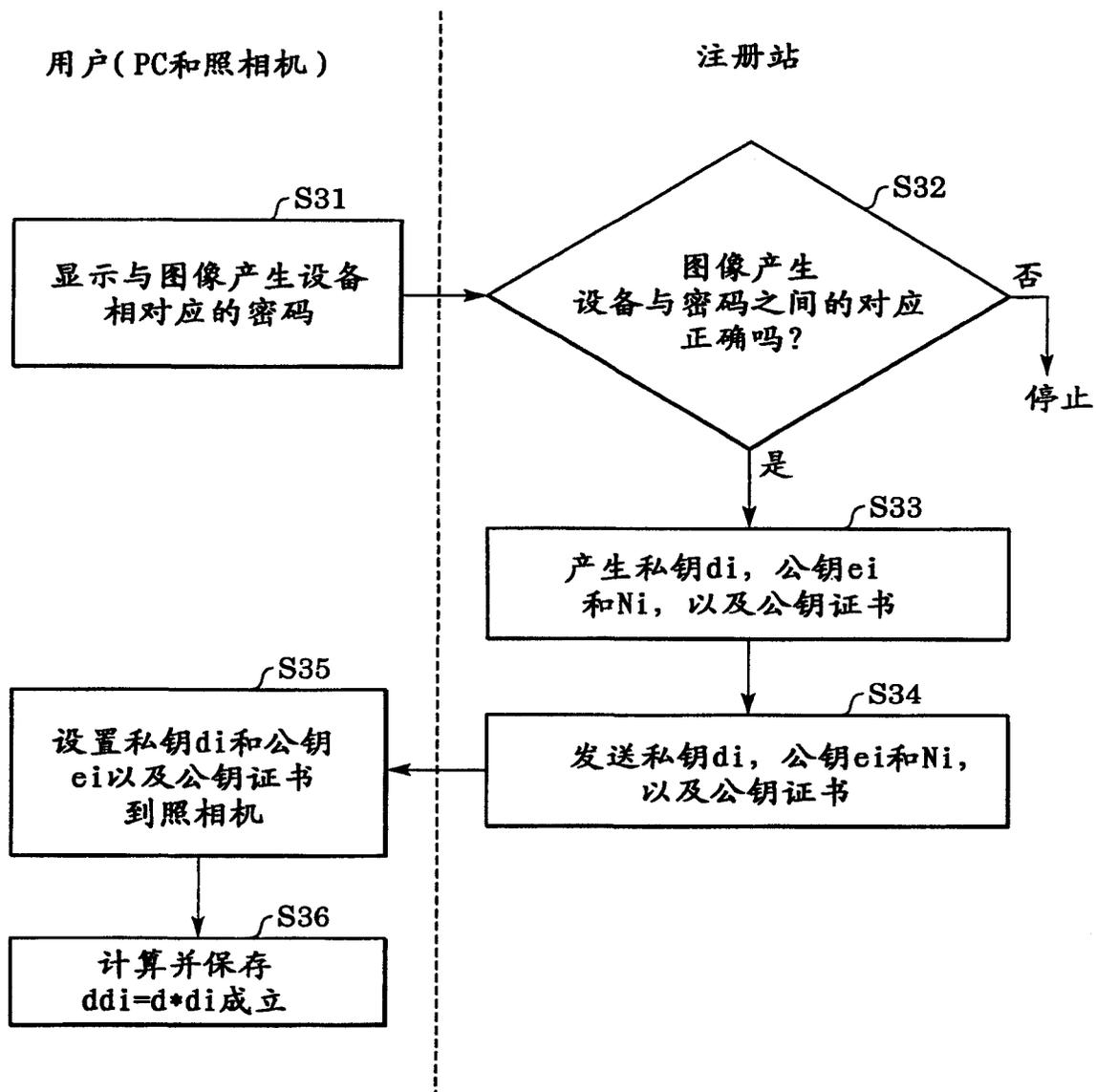


图 5

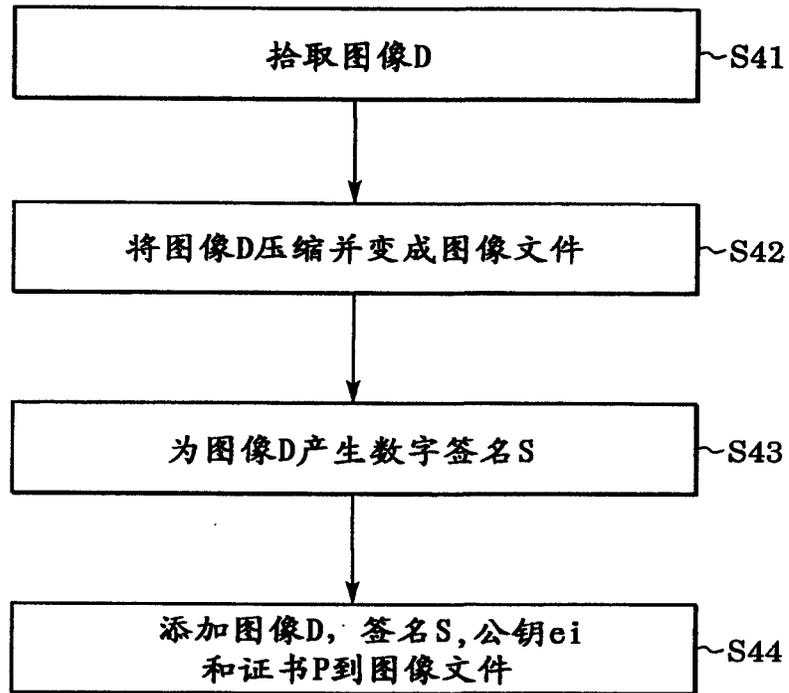


图 6

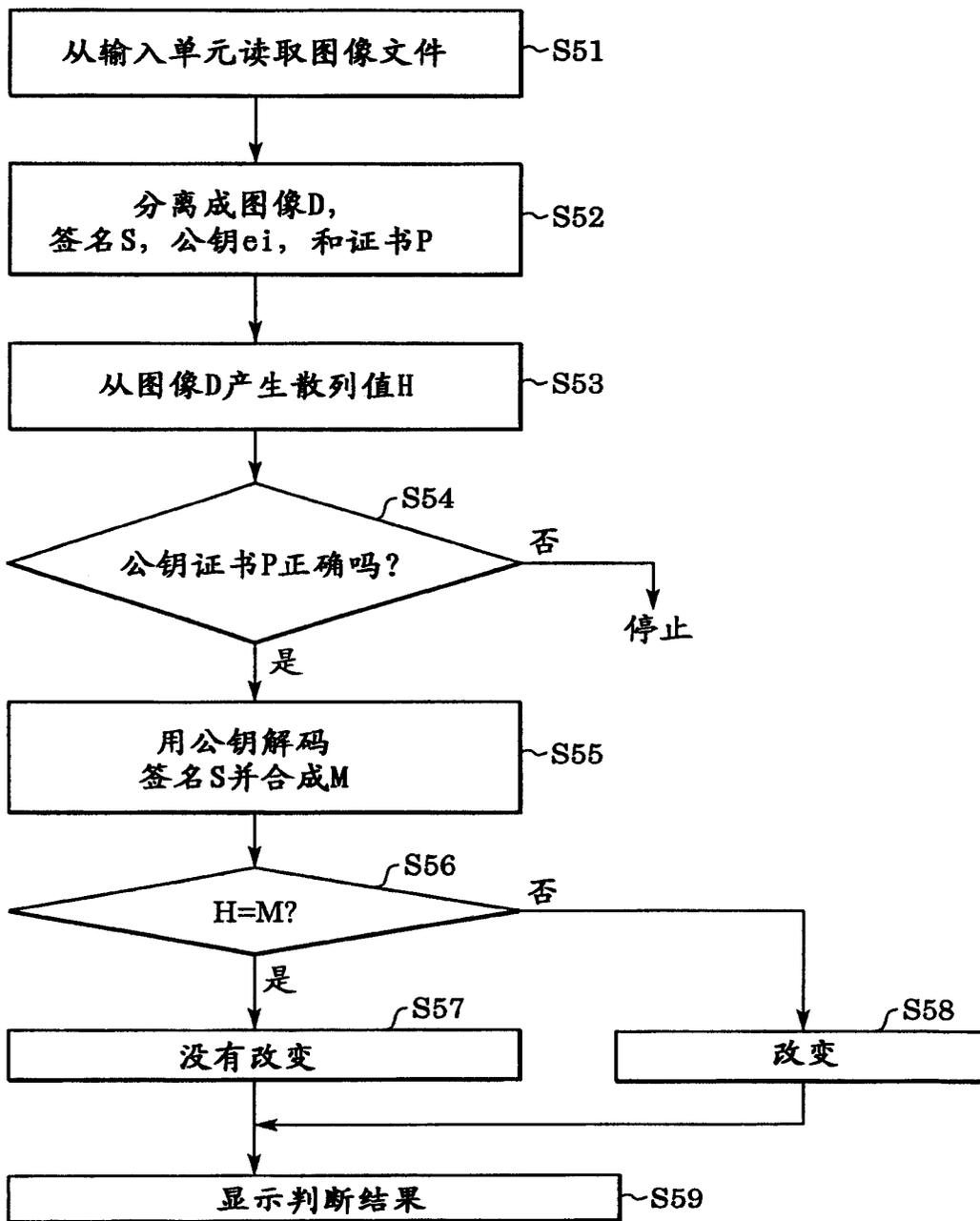


图 7