(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 104822012 A
(43)申请公布日 2015.08.05

(21)申请号 201410151694.9

(22)申请日 2014.04.15

(30)优先权数据
2014-015102 2014.01.30 JP

(71)申请人 株式会社茉菲莉亚
地址 日本东京品川区西五反田二丁目13番6号

(72)发明人 菅原宽

(74)专利代理机构 广州三环专利代理有限公司 44202
代理人 郝传鑫 梁婷

(51)Int.Cl.
H04N 5/225(2006.01)
H04N 5/232(2006.01)

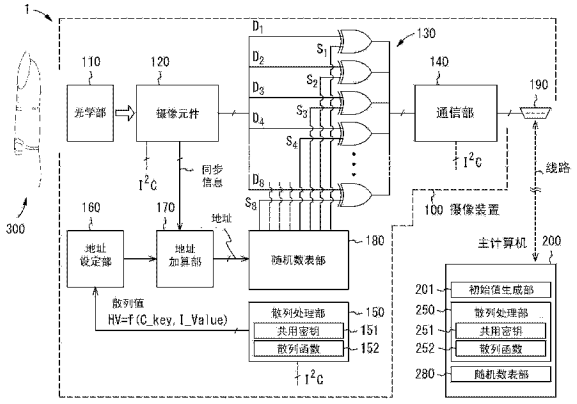
权利要求书2页 说明书9页 附图10页

(54)发明名称

摄像系统以及摄像装置

(57)摘要

本发明提供一种提高图像数据的发送安全性的摄像系统。该摄像系统由主计算机以及摄像装置构成，该摄像装置通过线路连接上述主计算机，拍摄包含指静脉信息的图像并将图像数据发送到上述主计算机；摄像装置具有第1散列处理部以及存储多个随机数值而形成的第1随机数表部，该第1散列处理部基于作为随机值而被赋予的初始值和共用密钥的信息而生成散列值；主计算机具有第2散列处理部以及第2随机数表部，该第2散列处理部以可以进行与上述第1散列处理部相同的处理的方式构成，该第2随机数表部存储与存储于上述第1随机数表部的上述多个随机数值相同的数值而形成。



CN 104822012 A

1. 一种摄像系统，其由主计算机以及摄像装置构成，该摄像装置通过线路连接所述主计算机，拍摄包含指静脉信息的图像并将图像数据发送到所述主计算机；

所述摄像装置具有：

基于作为随机值而被赋予的初始值和共用密钥的信息生成散列值的第 1 散列处理部，以及存储多个随机数值而形成的第 1 随机数表部；

所述主计算机具有：

以可进行与所述第 1 散列处理部相同的处理的方式构成的第 2 散列处理部，以及存储与存储于所述第 1 随机数表部的所述多个随机数值相同的数值而形成的第 2 随机数表部；

所述摄像装置在拍摄包含指静脉信息的图像时，

通过所述第 1 散列处理部生成散列值，

将所述散列值作为地址值，选择存储于所述第 1 随机数表部的随机数值作为用于对构成图像数据的第 1 行数据施加置乱处理的随机数值从而对所述第 1 行数据进行置乱处理，

在所述地址值上依次加算指定的固定值，选择存储于所述第 1 随机数表部的随机数值作为用于对第 2 行以后的数据施加置乱处理的随机数值从而对第 2 行以后的数据进行置乱处理，

将经施加置乱处理的图像数据通过所述线路发送到所述主计算机，

所述主计算机使用所述初始值、所述第 2 散列处理部以及所述第 2 随机数表部对接收到的所述图像数据进行译码处理。

2. 如权利要求 1 所述的摄像系统，其中，所述主计算机在生成随机值的初始值并保持之后，通过所述线路将初始值发送到所述摄像装置，

所述第 1 散列处理部使用接收到的所述初始值生成散列值，

所述主计算机使用所保持的所述初始值进行译码处理。

3. 如权利要求 1 所述的摄像系统，其中，

所述摄像装置进一步具有生成随机值的初始值的初始值生成部，

所述第 1 散列处理部使用所述初始值生成部所生成的初始值生成散列值，

所述摄像装置将经施加置乱处理的图像数据的一部分替换为所述初始值并发送到所述主计算机，

所述主计算机使用从接收到的经施加置乱处理的图像数据中抽出的初始值进行译码处理。

4. 如权利要求 1 至 3 中任一项所述的摄像系统，其中，

所述摄像装置使用通用串行总线连接所述主计算机。

5. 如权利要求 1 至 4 中任一项所述的摄像系统，其中，

所述第 1 随机数表部以及所述第 2 随机数表部以可基于主计算机的指示而更新表格的方式构成。

6. 一种摄像装置，其通过线路连接主计算机，拍摄包含指静脉信息的图像并将图像数据发送到所述主计算机；

所述摄像装置具有：

基于作为随机值而被赋予的初始值和共用密钥的信息生成散列值的第 1 散列处理部，以及存储多个随机数值而形成的第 1 随机数表部；

所述摄像装置在拍摄包含指静脉信息的图像数据时，

通过所述第 1 散列处理部生成散列值，

将所述散列值作为地址值，选择存储于所述第 1 随机数表部的随机数值作为用于对构成图像数据的第 1 行数据施加置乱处理的随机数值从而对所述第 1 行的数据施加置乱处理，

在所述地址值上依次加算特定的固定值，选择存储于所述第 1 随机数表部的随机数值作为用于对第 2 行以后的数据施加置乱处理的随机数值从而对第 2 行以后的数据施加置乱处理，

将经施加置乱处理的图像数据通过所述线路发送到所述主计算机。

7. 如权利要求 6 所述的摄像装置，其中，

所述第 1 随机数表部以可基于主计算机的指示而更新表格的方式构成。

摄像系统以及摄像装置

技术领域

[0001] 本发明涉及一种通过线路与主计算机连接，拍摄包含指静脉信息的图像并将图像数据发送到主计算机的摄像装置，以及由该摄像装置和主计算机所构成的摄像系统。

背景技术

[0002] 近年来，出于安全保护的观点，使用指纹、虹膜以及血管的图形等生物体信息的生物体认证受到关注。生物体认证例如把用于核对的数据事先登记于数据库中，在认证时取得使用者（被检者）的数据，通过比较其与登记于数据库的用于核对的数据是否一致而进行对使用者的认证。

[0003] 尤其是，使用生物体的静脉图形的认证技术除了具有认证精度优良的优点以外，还具有由于使用身体的内部信息所以伪造较困难，而且使用者心理上的抵触感也较少等优点（参考非专利文献 1）。使用静脉图形的认证技术正被引入自动柜员机 (ATM)、进出管理装置 (entry control system)、个人电脑、移动信息终端 (personal digital assistant) 以及移动电话等各种机器。

[0004] 非专利文献 1 ：社团法人日本自动认识系统协会著，《可理解的生物测定学基础》，第 1 版，株式会社 OHM 社，平成 17 年 9 月 5 日，P.47-55。

发明内容

[0005] 为了进行使用静脉图形的认证，需要拍摄包含使用者的指静脉信息的图像而取得图像数据。在 WEB 相机的用途等上被广泛使用的 USB(Universal Serial Bus) 相机等摄像装置被大量生产，价格低廉。因为它降低了认证装置的成本，故也有人考虑使用这样的相机拍摄包含使用者的指静脉信息的图像等。

[0006] 可是，在使用这样的相机的情形下，需要把个人信息的图像数据发送到例如构成认证装置的主计算机一侧。因此，也有人认为第三者会在发送路径的途中夺取图像数据等，进而认为会产生安全问题。

[0007] 因此，本发明的目的在于提供一种可使用廉价的摄像装置，并可防止在图像数据的发送中安全性降低的摄像系统。而且，本发明的目的在于提供一种用于这样的摄像系统的摄像装置。

[0008] 用于达成上述目的的本发明的摄像系统为如下所述的摄像系统 ：

[0009] 该摄像系统由主计算机以及摄像装置构成，该摄像装置通过线路与上述主计算机连接，拍摄包含指静脉信息的图像并将图像数据发送到上述主计算机 ；

[0010] 上述摄像装置具有 ：

[0011] 基于作为随机值而被赋予的初始值和共用密钥 (common key) 的信息，生成散列 (hash) 值的第 1 散列处理部，以及，

[0012] 存储多个随机数值而形成的第 1 随机数表部 ；

[0013] 上述主计算机具有 ：

[0014] 以可以进行与上述第 1 散列处理部同样的处理的方式构成的第 2 散列处理部，以及，

[0015] 存储了与存储于上述第 1 随机数表部的上述多个随机数值同样的数值而构成的第 2 随机数表部；

[0016] 上述摄像装置在拍摄含有指静脉信息的图像时，

[0017] 通过上述第 1 散列处理部生成散列值，

[0018] 把上述散列值作为地址值 (address value)，选择存储于上述第 1 随机数表部的随机数值作为用于对构成图像数据的第 1 行的数据施加置乱 (scramble) 处理的随机数值，从而对上述第 1 行的数据进行置乱处理，

[0019] 在上述地址值上依次加算指定的固定值，选择存储于上述第 1 随机数表部的随机数值作为用于对第 2 行以后的数据施加置乱处理的随机数值，从而对第 2 行以后的数据进行置乱处理，

[0020] 将经施加了置乱处理的图像数据通过上述线路发送到上述主计算机，

[0021] 上述主计算机利用上述初始值、上述第 2 散列处理部以及上述第 2 随机数表部对收到的上述图像数据进行译码处理。

[0022] 本发明的摄像系统可为如下结构：

[0023] 上述主计算机在生成随机值的初始值并保持之后，通过上述线路将初始值发送到上述摄像装置，

[0024] 上述第 1 散列处理部使用收到的上述初始值生成散列值，

[0025] 上述主计算机使用保持的上述初始值进行译码处理。

[0026] 或者，本发明的摄像系统还可为如下结构：

[0027] 上述摄像装置进一步具有生成随机值的初始值的初始值生成部，

[0028] 上述第 1 散列处理部使用上述初始值生成部所生成的初始值生成散列值，

[0029] 上述摄像装置将经置乱处理的图像数据的一部分替换为上述初始值，并发送到上述主计算机，

[0030] 上述主计算机使用从收到的经置乱处理的图像数据中抽出的初始值进行译码处理。

[0031] 在含有上述各种优选结构的本发明的摄像系统中，可以使用周知的线路作为连接上述摄像装置和上述主计算机的线路。例如，可以使用以太网（注册商标）规格、通用串行总线 (Universal Serial Bus)(USB) 规格、IEE1394 规格、ThunderBolt 规格等线路。从拍摄的图像的信息量大小或降低成本的观点出发，上述摄像装置优选使用通用串行总线连接上述主计算机。

[0032] 摄像装置与主计算机可通过线路直接连接，也可以例如通过设于路径上的其他计算机，利用线路间接连接。即，“通过线路连接”除了包括直接连接的结构以外，也包括间接连接的结构。

[0033] 含有上述各种优选结构的本发明的摄像系统可为如下结构：

[0034] 上述第 1 随机数表部以及上述第 2 随机数表部以可基于主计算机的指示而更新表格的方式构成。

[0035] 用于达成上述目的的本发明的摄像装置为如下所述的摄像装置：

[0036] 该摄像装置为通过线路与主计算机连接，拍摄包含指静脉信息的图像并将图像数据发送到上述主计算机的摄像装置；

[0037] 该摄像装置具有：

[0038] 基于作为随机值而被赋予的初始值和共用密钥的信息，生成散列值的第 1 散列处理部，以及，

[0039] 存储多个随机数值而形成的第 1 随机数表部；

[0040] 上述摄像装置在拍摄包含指静脉的信息的图像数据时，

[0041] 通过上述第 1 散列处理部生成散列值，

[0042] 将上述散列值作为地址值，选择存储于上述第 1 随机数表部的随机数值作为用于对构成图像数据的第 1 行的数据施加置乱处理的随机数值，从而对上述第 1 行的数据进行置乱处理，

[0043] 在上述地址值上依次加算指定的固定值，选择存储于上述第 1 随机数表部的随机数值作为用于对第 2 行以后的数据施加置乱处理的随机数值，从而对第 2 行以后的数据进行置乱处理，

[0044] 将经施加了置乱处理的图像数据通过上述线路发送到上述主计算机。

[0045] 上述本发明的摄像装置可为如下结构：

[0046] 上述第 1 随机数表部以可基于主计算机的指示而更新表格的方式构成。

[0047] 用于本发明的摄像系统的摄像装置以及本发明的摄像装置（下面有时仅将它们称作本发明的摄像装置）除了光学滤光器或透镜等光学元件以外，也可使用 CMOS 传感器或 CCD 传感器等周知的摄像元件、运算电路、存储装置（存储器）等周知的电路元件等而构成。只要不对本发明的实施产生障碍，摄像装置的结构没有特别的限定。

[0048] 用于本发明的摄像系统的主计算机以及连接本发明的摄像装置的主计算机的结构只要不对本发明的实施产生障碍，并没有特别的限定。例如，主计算机也可由静脉认证装置构成。主计算机可以使用运算电路、存储装置（存储器）等周知的电路元件等构成。

[0049] 在本发明的摄像系统以及本发明的摄像装置（下面有时仅将它们称作本发明）中，进行在对应第 2 行以后的数据的随机数表部的地址值中，依次加算指定的固定值而参考的处理。加算后结果超过随机数表部的地址值的范围时，基于余数而进行处理即可。而且，从使控制简便等观点出发，指定的加算值优选设为“1”。

[0050] 根据本发明，能够提供一种可使用廉价的摄像装置，并且在发送图像数据时不会在安全性上产生问题的摄像系统。而且，可以提供一种使用于这样的摄像系统的摄像装置。

附图说明

[0051] 图 1 为第 1 实施方式所涉及的摄像系统的模式框图。

[0052] 图 2 为用于说明摄像系统的工作的模式流程图。

[0053] 图 3 为接着图 2 的用于说明摄像系统的工作的模式流程图。

[0054] 图 4 为表示与第 1 随机数表部的地址对应的随机数值的例子的表格。

[0055] 图 5 为摄像元件所拍摄的各行的图像数据与参照第 1 随机数表而进行的置乱处理的对应关系的汇总表。

[0056] 图 6 为用于说明经置乱处理的图像数据的译码工作的模式流程图。

[0057] 图 7 为第 2 实施方式所涉及的摄像系统的模式框图。

[0058] 图 8 为用于说明摄像系统的工作的模式流程图。

[0059] 图 9 为用于说明经置乱处理的图像数据的译码工作的模式流程图。

[0060] 图 10 为第 3 实施方式所涉及的摄像系统的模式框图。

[0061] 图 11 为用于说明随机数表部的更新工作的模式图。

具体实施方式

[0062] 下面参照附图对本发明的摄像系统以及摄像装置进行说明。本发明不限定于实施方式，举例说明了实施方式中的各种数值或构成材料。在以下的说明中，具有同一要素或同一功能的元件使用同一符号，省略重复说明。

[0063] [第 1 实施方式]

[0064] 第 1 实施方式涉及到本发明的摄像系统以及摄像装置。

[0065] 图 1 为第 1 实施方式所涉及的摄像系统的模式框图。

[0066] 第 1 实施方式所涉及的摄像系统 1 由主计算机 200 以及摄像装置 100 构成，该摄像装置 100 通过线路连接主计算机 200，拍摄包含指静脉信息的图像并将图像数据发送到主计算机 200。

[0067] 摄像装置 100 具有基于作为随机值而被赋予的初始值和共用密钥的信息生成散列值的第 1 散列处理部 150 以及存储多个随机数值而形成的第 1 随机数表部 180。

[0068] 第 1 散列处理部 150 包含共用密钥 151 和散列函数 152。将它们设定为预先指定的内容，例如，将该内容写入图中未示出的只读存储装置中。第 1 随机数表部 180 也一样。共用密钥 151 或散列函数 152 的结构以不对散列处理产生障碍的方式，根据规格或设计适当决定即可。

[0069] 主计算机 200 具有以可进行与第 1 散列处理部 150 同样的处理的方式构成的第 2 散列处理部 250，以及存储与存储于第 1 随机数表部 180 的多个随机数相同的数值而形成的第 2 随机数表部 280。

[0070] 摄像装置 100 拍摄包含指静脉信息的图像时，通过第 1 散列处理部 150 生成散列值，将散列值作为地址值，选择存储于第 1 随机数表部 180 的随机数值作为用于对构成图像数据的第 1 行的数据施加置乱处理的随机数值并对第 1 行的数据进行置乱处理；向地址值中依次加算指定的固定值，选择存储于第 1 随机数表部的随机数值作为用于对第 2 行以后的数据施加置乱处理的随机数值，从而对第 2 行以后的数据进行置乱处理，将经置乱处理的图像数据通过线路发送到主计算机 200。

[0071] 主计算机 200 使用初始值、第 2 散列处理部 250 以及第 2 随机数表部 280 对收到的图像数据进行译码处理。

[0072] 根据该结构，每次拍摄时都会改变置乱处理，因此即使图像数据被夺取，也难以类推置乱处理时的随机数值或共用密钥的信息等。因此，即使经施加置乱处理的图像被夺取，亦难以恢复原图像，可以防止图像数据发送过程中安全性降低。

[0073] 第 1 实施方式中，主计算机 200 在生成随机值的初始值并保持之后，通过线路将初始值发送到摄像装置 100，第 1 散列处理部 150 使用收到的初始值生成散列值，主计算机 200 使用所保持的初始值进行译码处理。

[0074] 接着，对摄像装置 100 以及主计算机 200 的结构进行详细说明。

[0075] 摄像装置 100 除了上述第 1 散列处理部 150 和第 1 随机数表部 180 以外，还具有由对使用者（被检者）的手指 300 的图像进行成像的透镜或近红外线滤光器等构成的光学部 110、通过光学部 110 拍摄图像的摄像元件 120、施加置乱处理的置乱电路部 130、进行与外部的通信的通信部 140、保持第 1 随机数表部 180 中的初始地址值的地址设定部 160、根据图像的水平扫描而加算地址值的地址加算部 170。

[0076] 近红外光对生物体组织的穿透性较高。一方面，特定波长 (800 纳米左右) 的近红外光表现出被静脉的血液中的还原血红蛋白吸收的特性。因此，如果拍摄透过生物体的近红外光，静脉图形以阴影的方式出现，因此可以得到包含静脉图形的图像。

[0077] 构成摄像装置 100 的各构成部分，例如可通过 I^2C(I 平方 C) 等总线，利用未图示的控制部来控制工作。为方便作图，图 1 中限定了一部分的构成元件，模式性地表示了 I^2C 总线的连接。

[0078] 摄像装置 100 通过通信部 140 连接于主计算机 200。

[0079] 在此，假定摄像装置 100 使用通用串行总线连接于主计算机 200 来进行说明。符号 190 模式性地表示摄像装置 100 的 USB 连接器部。

[0080] 主计算机 200 中，第 2 散列处理部 250 包含共用密钥 251 以及散列函数 252。它们具有与共用密钥 151 以及散列函数 152 同样的结构。借此，第 2 散列处理部 250 以进行与第 1 散列处理部 150 相同的处理的方式工作。而且，第 2 随机数表部 280 具有与第 1 随机数表部 180 同样的结构。

[0081] 第 2 随机数表部 280 以与随机数表部 180 同样的结构被预先存储于主计算机 200。另外，根据情况，也可考虑通过使主计算机 200 经由线路而读取第 1 随机数表部 180 的数值从而生成第 2 随机数表部。

[0082] 在第 1 实施方式中，主计算机 200 进一步具有用于生成作为随机值而被赋予的初始值的初始值生成部 201。初始值生成部 201 以例如生成 8 比特范围的数值的方式构成。初始值生成部 201 可安装为硬件，亦可安装为软件。

[0083] 以上，对摄像装置 100 以及主计算机 200 的结构进行了说明。下面，对摄像系统 1 的工作进行说明。

[0084] 图 2 以及图 3 为用于说明摄像系统 1 的工作的模式流程图。参照附图，对生成经置乱处理的图像数据的工作进行说明。

[0085] 开始拍摄时，主计算机 200 在生成随机值的初始值并保持后 (图 2 的步骤 S2101)，通过线路将初始值发送到摄像装置 100(步骤 S2102)。通过 USB 规格的线路，在摄像装置 100 和主计算机 200 之间进行发送。

[0086] 第 1 散列处理部 150 基于收到的初始值和共用密钥而生成散列值 (步骤 S1101)。如果将共用密钥表示为“C_key”、初始值表示为“I_Value”、散列函数表示为“f”、散列值表示为“HV”，则可表示 HV = f(C_key、I_Value)。散列函数的构成没有特别的限定，相对初始值“I_Value”生成唯一的值即可。

[0087] 下面，保持所生成的散列值 (步骤 S1102)。在图 1 所示的结构中，散列值 HV 被保持于地址设定部 160 内。

[0088] 之后，将水平扫描帧中的第 1 行时所参照的第 1 随机数表部 180 的地址值设定为

散列值（步骤 S1103）。

[0089] 摄像元件 120 拍摄由 N×M 个像素组成的图像。在 VGA 的情况下，N=640、M=480。

[0090] 对摄像元件 120 所拍摄的水平扫描第 1 行时的图像数据施加基于对应于地址值的第 1 随机数表部 180 的值的置乱处理（参照图 3 的步骤 S1104）。为方便说明，设定图像数据为 8 比特的值。在图 1 的实施方式中，使用水平扫描数据和第 1 随机数表部 180 的值求异或，由此进行置乱处理。关于置乱处理的详细情况，参照下述图 4 以及图 5，在后面进行详细说明。

[0091] 之后，在地址值上加算指定的固定值 (S1105)，对下一行的水平扫描数据施加基于对应于地址值的第 1 随机数表部 180 的值的置乱处理 (S1106)。在图 1 所示的结构中，通过地址加算部 170 在地址值上加算指定的固定值。以下，把指定的固定值设为“1”进行说明。重复步骤 S1105 以及步骤 S1106（步骤 S1107）直到帧中最后一行的处理结束为止。

[0092] 在拍摄 1 帧的静止图像的情况下，摄像处理结束。当要拍摄例如像动画那样连续的、具有下一帧的图像时，返回到图 2 的步骤 S1103，进行相同处理即可（图 3 的步骤 S1108）。

[0093] 根据上述的步骤，可以得到经置乱处理的图像数据。另外，上述的步骤需要在摄像元件 120 水平扫描或垂直扫描时同步进行。因此，如图 1 所示，可以结合摄像元件 120 的水平 / 垂直的同步信息，使地址加算部 170 等工作。

[0094] 经施加置乱处理的图像数据，例如按帧存储于图中未示出的缓冲存储器，通过通信部 140 发送到主计算机 200。

[0095] 图 4 为表示与第 1 随机数表部 180 的地址对应的随机数值的例子的表。只要能够对图像施加充分的置乱处理，随机数值的个数没有特别的限定。出于控制的观点，优选设为 64、128、256 等 2 的幂数个。在此，随机数的个数为 (U+1) 个，第 1 随机数表部 180 的地址值为 0 至 U，随机数值设定为 0 到 255 范围内的值。将地址值为“u”（其中，u=0，1……，U) 时所对应的随机数值表示为 RT(u)。

[0096] 图 5 为摄像元件 120 所拍摄的各行的图像数据与参照第 1 随机数表部 180 进行的置乱处理的对应关系的汇总表。

[0097] 摄像元件 120 拍摄的第 n 列（其中，n=1，2……，N)、第 m 行（其中，m=1，2……，M) 的图像数据用符号 vd(m，n) 来表示，构成第 m 行的图像数据组用符号 VD(m) 来表示。

[0098] 根据上述工作，对第 1 行的图像数据组 VD(1)，从第 1 随机数表部 180 中选择与地址值 HV 对应的随机数 RT(HV)，通过取异或进行置乱处理。该处理表示为 [VD(1)xor RT(HV)]。第 2 行的置乱处理表示为 [VD(2)xor RT(HV+1)]。因此，第 m 行的置乱处理基本表示为 [VD(m)xor RT(HV+(m-1))]。

[0099] 另外，根据第 1 随机数表部 180 的规模或摄像装置 100 拍摄的行数的设定，可能发生 [HV+(M-1) ＞ U] 的情况。该情况下，根据余项参照第 1 随机数表部 180 即可。因此，如果将第 m 行的置乱处理一般化表示的话，有 [VD(m)xor RT((HV+(m-1))mod(U+1))]。

[0100] 以上，对关于生成经置乱处理的图像数据的工作进行了说明。下面，对关于主计算机 200 的处理进行说明。

[0101] 图 6 为用于说明经置乱处理的图像数据的译码工作的模式流程图。

[0102] 主计算机 200 接收经置乱处理的图像数据（步骤 S2103)，保持于例如图中未示出

的缓冲存储器。

[0103] 主计算机 200 的第 2 散列处理部 250 基于图 2 所示的步骤 S2101 中所保持的初始值和主计算机 200 所具有的共用密钥 251，生成散列值。

[0104] 第 2 散列处理部 250 以能够进行与摄像装置 100 的第 1 散列处理部 150 相同的处理的方式构成，因此生成与摄像装置 100 中第 1 行的图像数据组 VD(1) 所对应的地址值 HV 相同的散列值。而且，主计算机 200 中具有存储与存储于第 1 随机数表部 180 的多个随机数值相同的数值而形成的第 2 随机数表部 280。

[0105] 由此，主计算机 200 可以通过参照第 2 随机数表部 280 从而确定对第 m 行的图像数据组施加置乱处理时所使用的随机数值。使用该经参照的随机数值，通过解除置乱，可以复原图像数据（步骤 S2105）。

[0106] 以上，对主计算机 200 的处理进行了说明。

[0107] 根据上述的摄像系统 1 的操作，每次拍摄图像时都会变更用于置乱的随机数值，因此即使置乱图像被夺取，也难以类推随机数表或共用密钥。因此，可以防止图像数据的发送过程中安全性降低。

[0108] [第 2 实施方式]

[0109] 第 2 实施方式也涉及本发明的摄像系统以及摄像装置。

[0110] 图 7 为第 2 实施方式所涉及的摄像系统的模式框图。

[0111] 构成第 2 实施方式所涉及的摄像系统 2 的摄像装置 100A 与图 1 所示的摄像装置 100 相比，在进一步具有生成随机值的初始值的初始值生成部 101 这一点上不同。对应该点，主计算机 200A 形成从图 1 所示的主计算机 200 中省略初始值生成部 201 后的结构。初始值生成部 101 可安装为硬件，亦可安装为软件。

[0112] 第 2 实施方式涉及的摄像系统 2 中，如下各点与第 1 实施方式不同：摄像装置 100A 进一步具有生成随机值的初始值的初始值生成部 101；第 1 散列处理部 150 使用初始值生成部 101 所生成的初始值生成散列值；摄像装置 100A 将被施加置乱处理的图像数据的一部分替换为初始值，发送到主计算机 200A；主计算机 200A 使用从接收到的经施加置乱处理的图像数据中抽出的初始值进行译码处理。

[0113] 以上对摄像装置 100A 以及主计算机 200A 的结构进行了说明。下面，对摄像系统 2 的工作进行说明。

[0114] 图 8 以及图 9 为用于说明摄像系统 2 的工作的模式流程图。参照图，对生成经置乱处理的图像数据的工作进行说明。

[0115] 首先，参照图 8，对摄像装置 100A 的工作进行说明。开始拍摄时，初始值生成部 101 生成随机值的初始值并保持（图 8 的步骤 S1201）。

[0116] 接着，第 1 散列处理部 150 基于从初始值生成部 101 接收到的初始值和专用密钥，生成散列值（步骤 S1101）。下面，由于到步骤 S1104 为止的处理已经在前面参照图 2 以及图 3 进行了说明，因此此处省略说明。

[0117] 然后，将被施加了置乱处理的图像数据一部分替换为初始值。第 2 实施方式中，进行将经置乱处理的第 1 行的图像数据的起始值替换为初始值的处理（步骤 S1202）。之后，进行已参照图 3 进行了说明的步骤 S1105 以后的处理过程。此处省略对这些的说明。

[0118] 接着，参照图 9 对主计算机 200A 的处理进行说明。

[0119] 主计算机 200A 接收经置乱处理的图像数据（步骤 S2103）并将其保持于例如图中未示出的缓冲存储器内。

[0120] 主计算机 200A 将图像数据的第 1 行的起始数据作为初始值抽出（步骤 S2103A）。

[0121] 主计算机 200A 的第 2 散列处理部 250 基于被抽出的初始值和主计算机 200A 所具有的共用密钥 251，生成散列值（步骤 S2104）。

[0122] 主计算机 200A 可以通过参照第 2 随机数表部 280 来确定对第 m 行的图像数据组施加置乱处理时所使用的随机数值。使用该经参照的随机数值，通过解除置乱，可以复原图像数据（步骤 S2105）。

[0123] 以上，对主计算机 200A 的处理进行了说明。

[0124] 根据上述的摄像系统 2 的工作，由于图像数据内嵌入了初始值，因此不需要进行从主计算机 200A 侧向摄像装置 100A 侧发送初始值等的步骤。

[0125] [第 3 实施方式]

[0126] 第 3 实施方式也涉及本发明的摄像系统以及摄像装置。

[0127] 图 10 为第 3 实施方式所涉及的摄像系统的模式图。

[0128] 第 3 实施方式所涉及的摄像系统 3 为第 1 实施方式所涉及的摄像系统 1 的变形例，主要在以下点上不同 ：第 1 随机数表部以及第 2 随机数表部以基于主计算机的指示而可以更新表格的方式构成。

[0129] 当经施加置乱处理的图像数据被大量夺取，担心基于这些图像数据可以推定随机数表的值时，通过更新表格，可以恢复发送的安全性。

[0130] 图 10 为第 3 实施方式所涉及的摄像系统的模式框图。

[0131] 构成第 3 实施方式所涉及的摄像系统 3 的摄像装置 100B 与图 1 所示的摄像装置 100 相比，在如下点上不同 ：第 1 随机数表部 180B 以表格可更新的方式构成。此外，构成第 3 实施方式所涉及的摄像系统 3 的主计算机 200B 与图 1 所示的主计算机 200 相比，在如下点上不同 ：第 2 随机数表部 280B 以表格可更新的方式构成，以及进一步具有用于进行表格更新的随机数表更新部 290。

[0132] 第 1 随机数表部 180B 或第 2 随机数表部 280B 可通过可改写的存储装置，例如，闪存等周知的存储装置构成。

[0133] 随机数表更新部 290，例如，基于系统操作者的指示等，以基于适当的随机数种子而生成构成随机数表的随机数的方式而构成。随机数表更新部 290 例如可通过伪随机数生成程序等而构成。

[0134] 图 11 为用于说明随机数表部的更新工作的模式图。

[0135] 例如，如果系统操作者指示主计算机 200B 进行表的更新，则随机数表更新部 290 基于适当的随机数种子而生成构成随机数表的随机数。而且，通过主计算机 200B 的工作，基于生成的随机数的值更新第 2 随机数表部 280B 的内容的同时，通过线路更新摄像装置 100B 的第 1 随机数表部 180B 的内容。

[0136] 根据上述摄像系统 3，当担心随机数表的值被推定时，可以通过更新表格来恢复发送的安全性。

[0137] 另外，为方便说明，作为第 1 实施方式的变形例对第 3 实施方式所涉及的摄像系统进行了说明，但也可作为第 2 实施方式的变形例而构成。

[0138] 以上基于优选的实施方式对本发明进行了说明，但本发明不限定于该实施方式。实施方式中的生物体认证系统的构成要素的具体构成、构造如举例所示，亦可进行适当变更。

[0139] 符号说明

[0140] 1,2,3 摄像系统

[0141] 100,100A,100B 摄像装置

[0142] 101 初始值生成部

[0143] 110 光学部

[0144] 120 摄像元件

[0145] 130 置乱电路部

[0146] 140 通信部

[0147] 150 第 1 散列处理部

[0148] 151 共用密钥

[0149] 152 散列函数

[0150] 160 地址设定部

[0151] 170 地址加算部

[0152] 180,180B 第 1 随机数表部

[0153] 190USB 连接器部

[0154] 200,200A,200B 主计算机

[0155] 201 初始值生成部

[0156] 250 第 2 散列处理部

[0157] 251 共用密钥

[0158] 252 散列函数

[0159] 280,280B 第 2 随机数表部

[0160] 290 随机数表更新部

[0161] 300 使用者（被检者）的手指

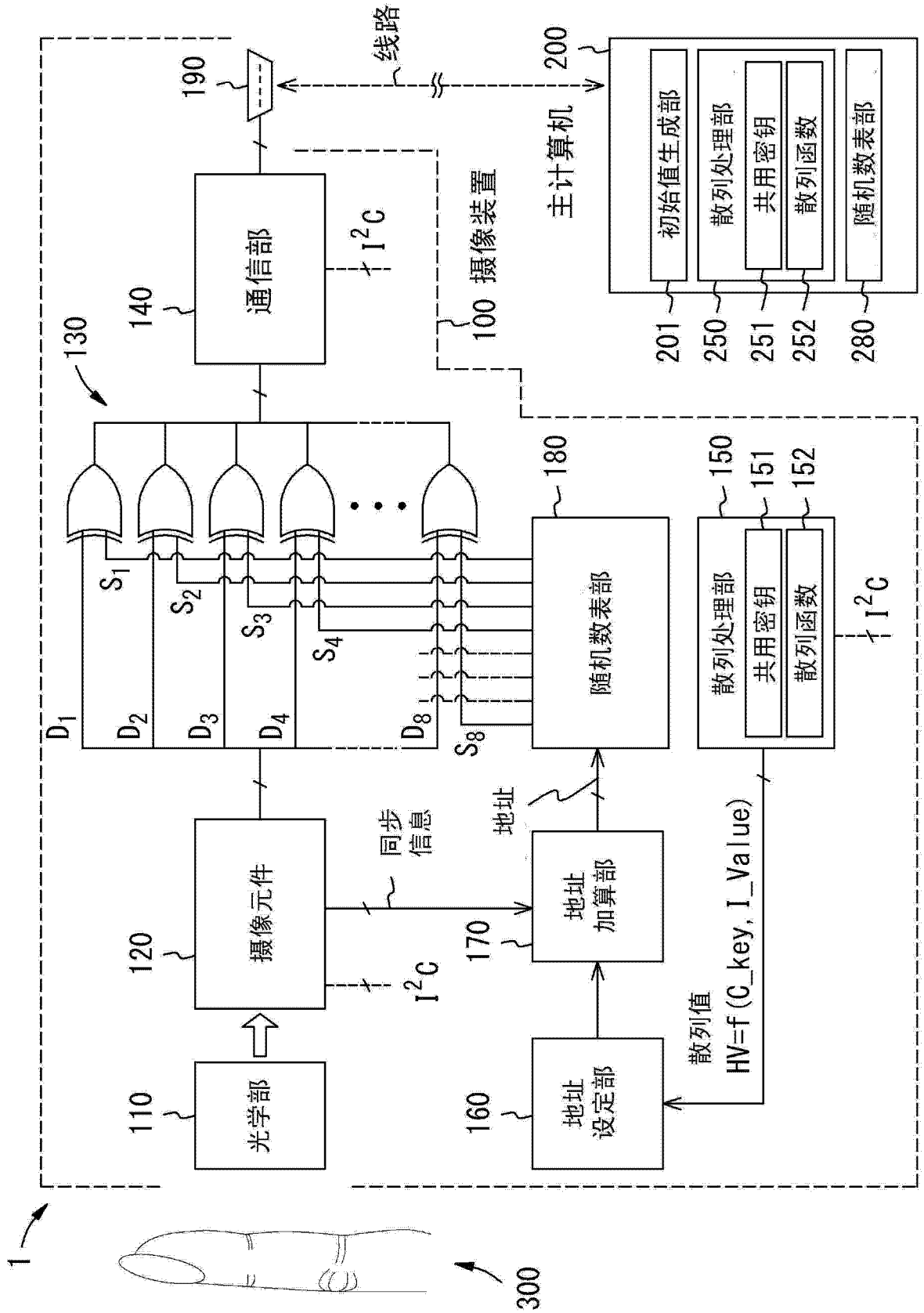

1
300
光学部
110
摄像元件
120
通信部
140
130
190
线路
200
主计算机
初始值生成部
201
散列处理部
250
共用密钥
251
散列函数
252
随机数表部
280
100 摄像装置
I²C
S1
S2
S3
S4
S8
D1
D2
D3
D4
D8
180
随机数表部
150
151
152
散列处理部
共用密钥
散列函数
I²C
同步信息
地址
地址加算部
170
I²C
地址设定部
160
散列值
HV=f(C_key, I_Value)

图 1

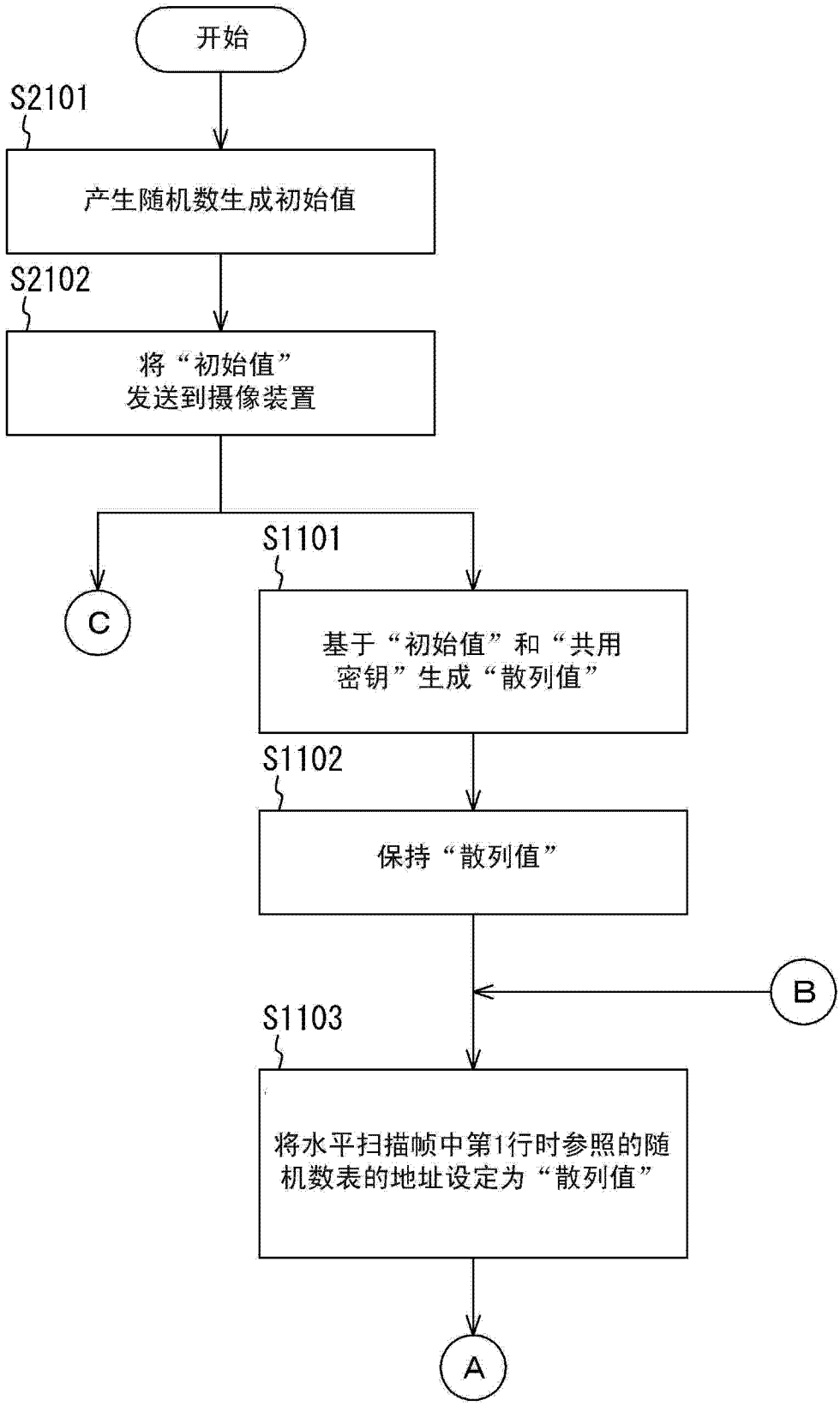

开始
S2101
产生随机数生成初始值
S2102
将“初始值”
发送到摄像装置
C
S1101
基于“初始值”和“共用
密钥”生成“散列值”
S1102
保持“散列值”
B
S1103
将水平扫描帧中第1行时参照的随
机数表的地址设定为“散列值”
A

图 2

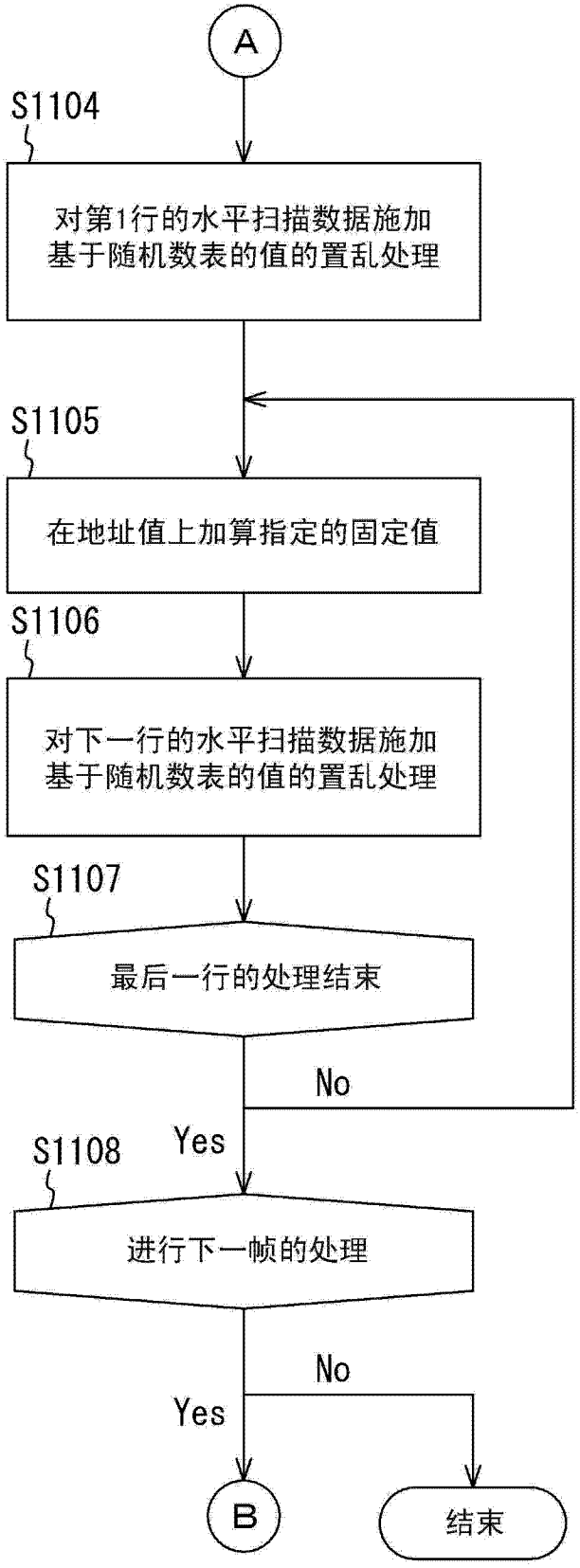
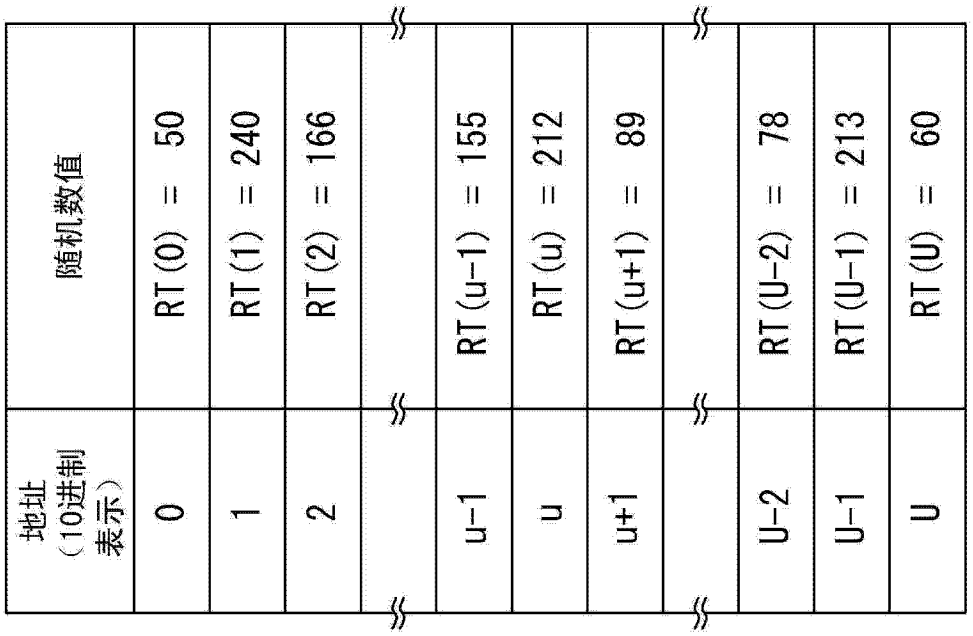
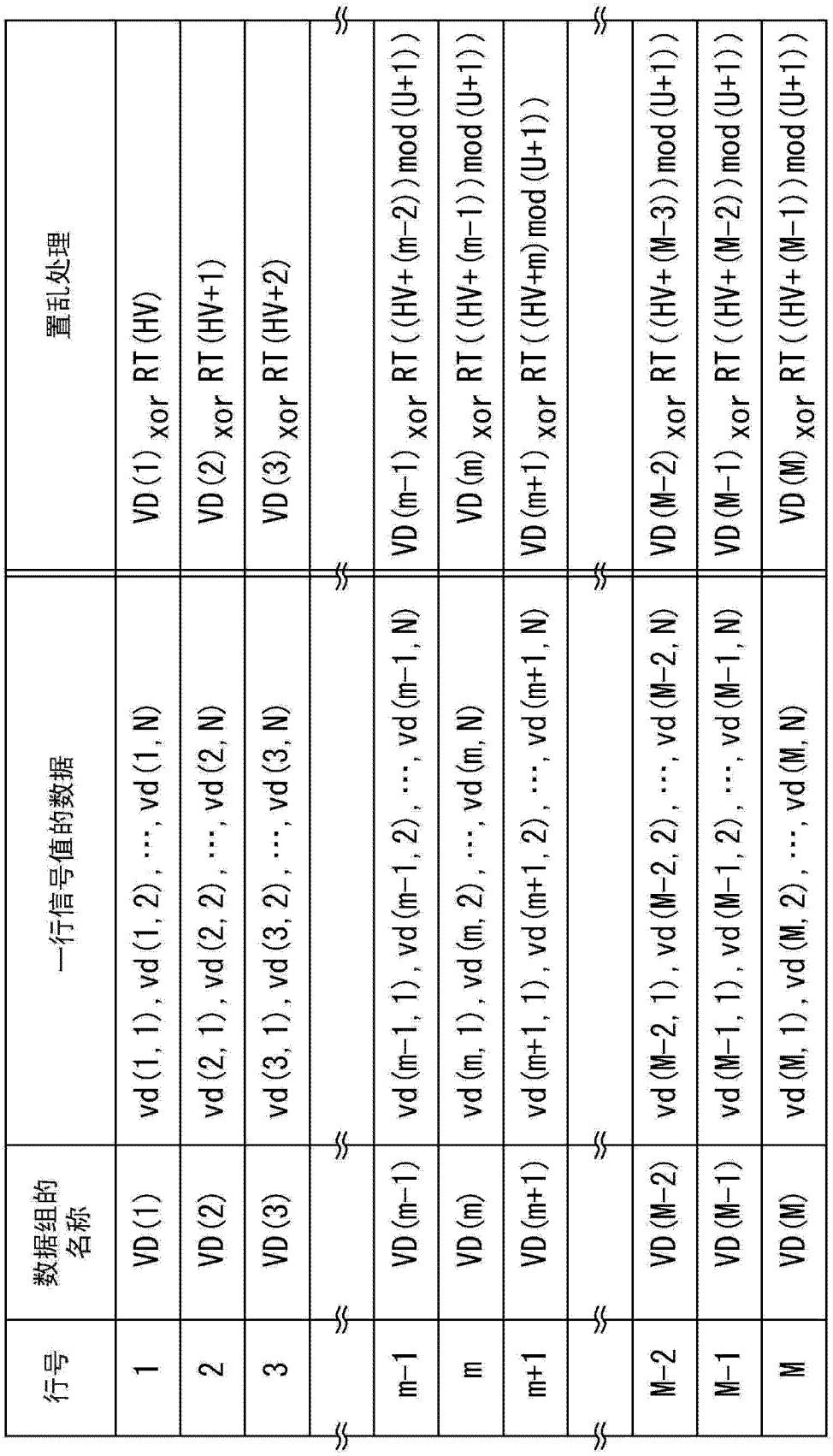

A
S1104
对第1行的水平扫描数据施加
基于随机数表的值的置乱处理
S1105
在地址值上加算指定的固定值
S1106
对下一行的水平扫描数据施加
基于随机数表的值的置乱处理
S1107
最后一行的处理结束
No
Yes
S1108
进行下一帧的处理
No
Yes
B
结束

图 3



地址（10进制表示）	随机数值
0	RT(0) = 50
1	RT(1) = 240
2	RT(2) = 166
u-1	RT(u-1) = 155
u	RT(u) = 212
u+1	RT(u+1) = 89
U-2	RT(U-2) = 78
U-1	RT(U-1) = 213
U	RT(U) = 60

图 4



行号	数据组的名称	一行信号值的数据	置乱处理
1	VD(1)	vd(1,1), vd(1,2), …, vd(1,N)	VD(1) xor RT(HV)
2	VD(2)	vd(2,1), vd(2,2), …, vd(2,N)	VD(2) xor RT(HV+1)
3	VD(3)	vd(3,1), vd(3,2), …, vd(3,N)	VD(3) xor RT(HV+2)
m-1	VD(m-1)	vd(m-1,1), vd(m-1,2), …, vd(m-1,N)	VD(m-1) xor RT((HV+(m-2))mod(U+1))
m	VD(m)	vd(m,1), vd(m,2), …, vd(m,N)	VD(m) xor RT((HV+(m-1))mod(U+1))
m+1	VD(m+1)	vd(m+1,1), vd(m+1,2), …, vd(m+1,N)	VD(m+1) xor RT((HV+m)mod(U+1))
M-2	VD(M-2)	vd(M-2,1), vd(M-2,2), …, vd(M-2,N)	VD(M-2) xor RT((HV+(M-3))mod(U+1))
M-1	VD(M-1)	vd(M-1,1), vd(M-1,2), …, vd(M-1,N)	VD(M-1) xor RT((HV+(M-2))mod(U+1))
M	VD(M)	vd(M,1), vd(M,2), …, vd(M,N)	VD(M) xor RT((HV+(M-1))mod(U+1))

图 5

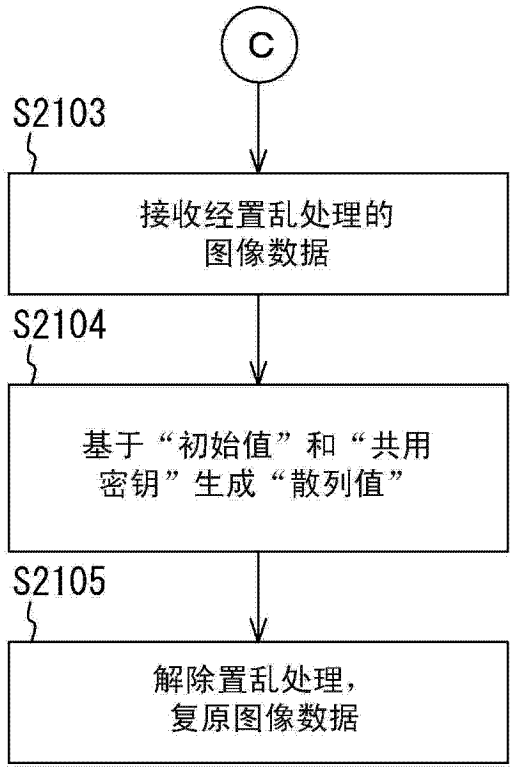

C
S2103
接收经置乱处理的
图像数据
S2104
基于“初始值”和“共用
密钥”生成“散列值”
S2105
解除置乱处理，
复原图像数据

图 6

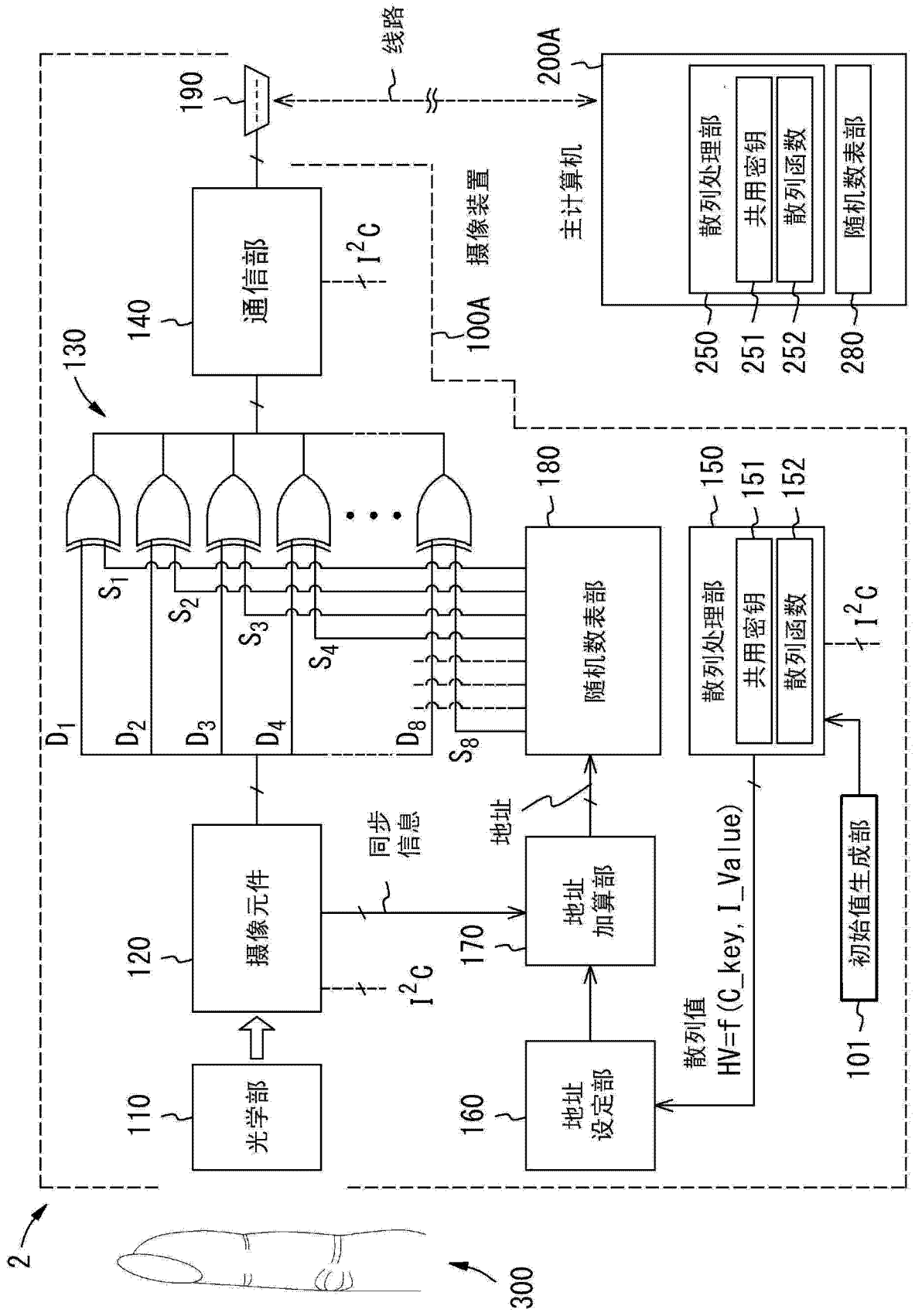

线路
190
200A
主计算机
散列处理部
共用密钥
散列函数
随机数表部
250
251
252
280
通信部
140
I2C
摄像装置
100A
130
180
150
151
152
S1
S2
S3
S4
S8
D1
D2
D3
D4
D8
随机数表部
散列处理部
共用密钥
散列函数
I2C
同步信息
地址
摄像元件
120
地址加算部
170
I2C
散列值
HV=f(C_key, I_Value)
初始值生成部
101
光学部
110
地址设定部
160
2
300

图 7

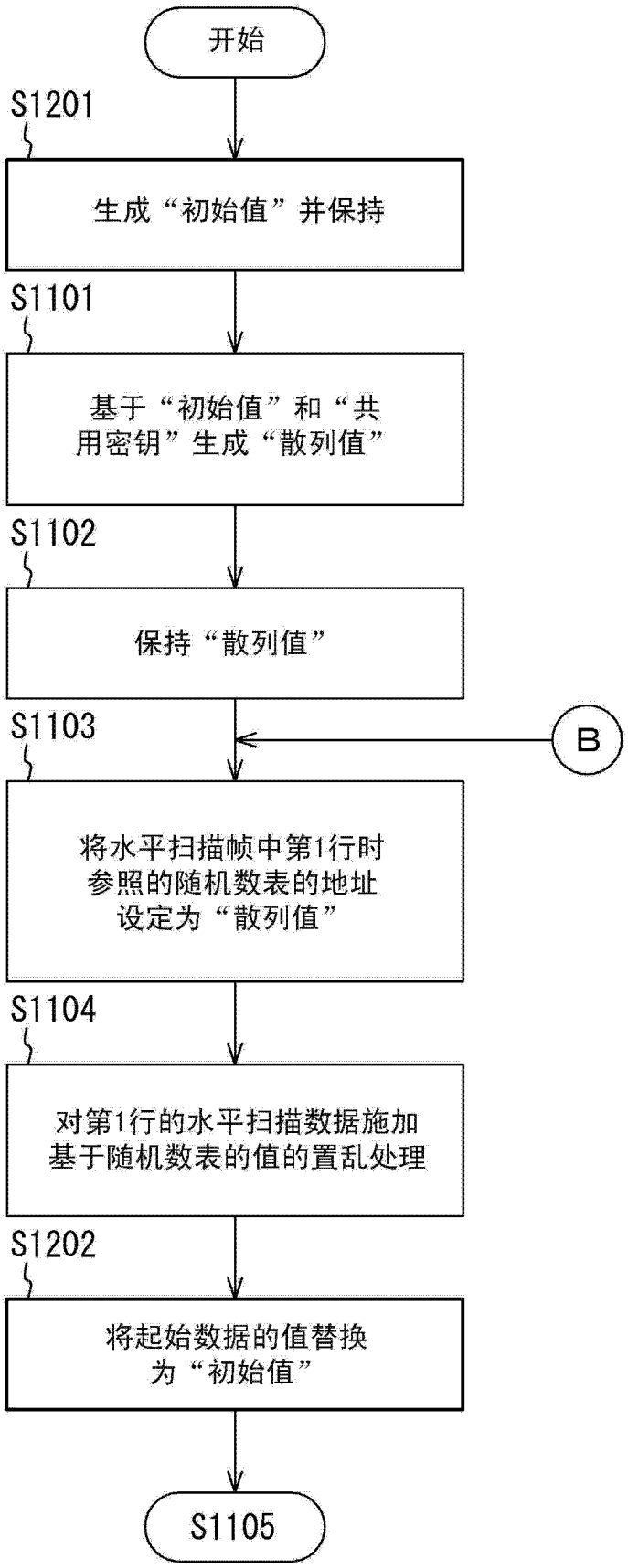

开始
S1201
生成“初始值”并保持
S1101
基于“初始值”和“共用密钥”生成“散列值”
S1102
保持“散列值”
S1103
B
将水平扫描帧中第1行时参照的随机数表的地址设定为“散列值”
S1104
对第1行的水平扫描数据施加基于随机数表的值的置乱处理
S1202
将起始数据的值替换为“初始值”
S1105

图 8

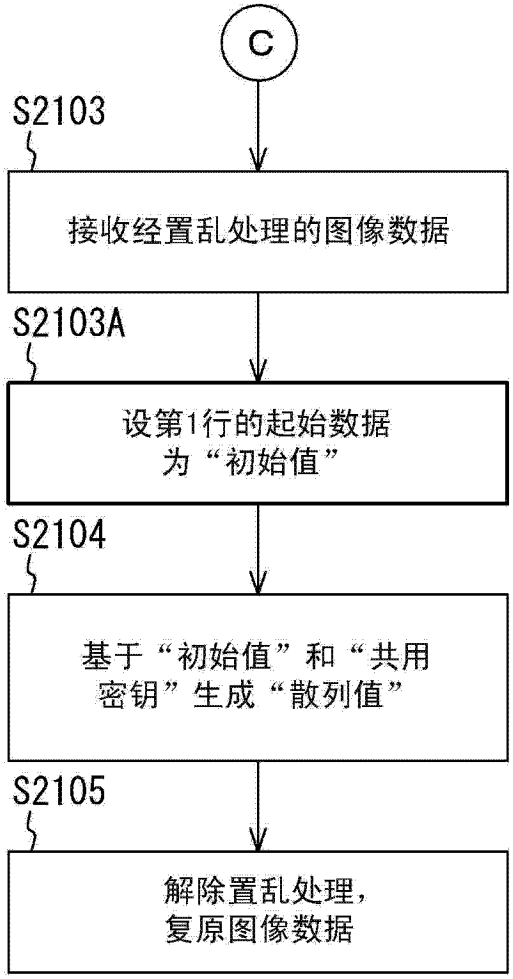

C
S2103
接收经置乱处理的图像数据
S2103A
设第1行的起始数据为“初始值”
S2104
基于“初始值”和“共用密钥”生成“散列值”
S2105
解除置乱处理，复原图像数据

图 9

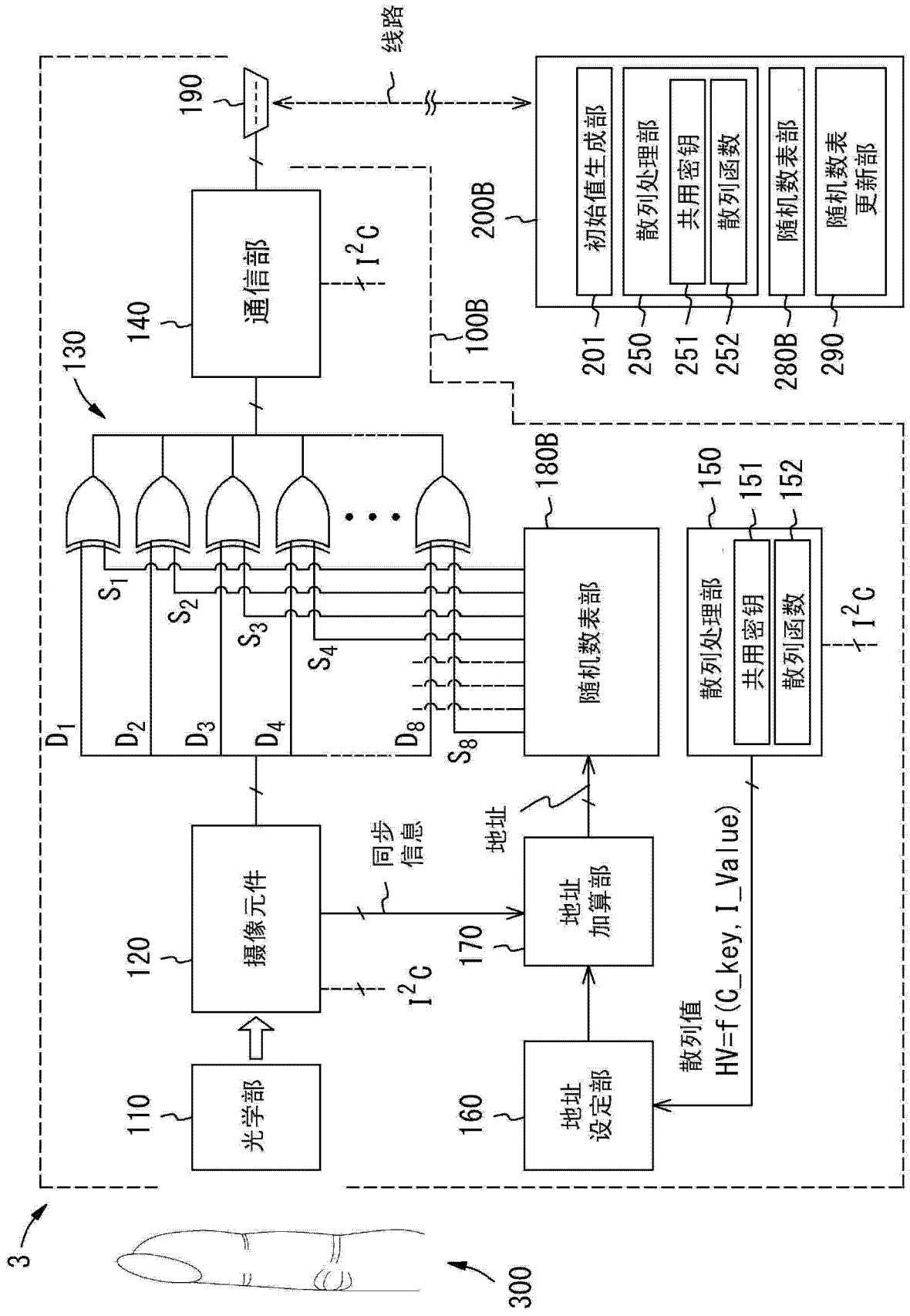

线路
190
通信部
140
130
100B
200B
初始值生成部
散列处理部
共用密钥
散列函数
随机数表部
随机数表更新部
201
250
251
252
280B
290
I²C
180B
随机数表部
150
151
152
散列处理部
共用密钥
散列函数
I²C
D1
D2
D3
D4
D8
S1
S2
S3
S4
S8
同步信息
地址
摄像元件
120
I²C
地址加算部
170
光学部
110
地址设定部
160
散列值
HV=f(C_key, I_Value)
3
300

图 10

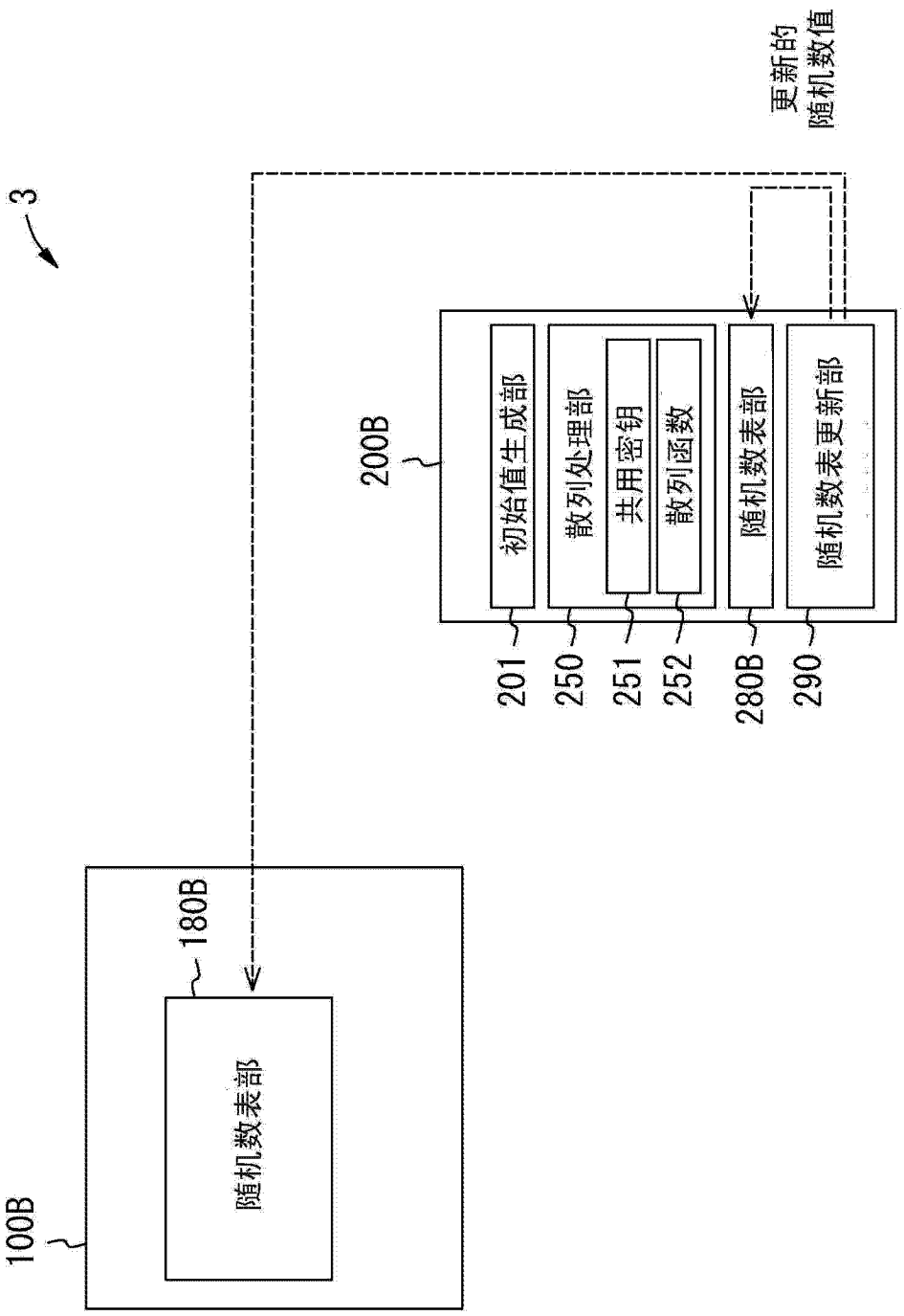

3
更新的
随机数值
200B
初始值生成部
散列处理部
共用密钥
散列函数
随机数表部
随机数表更新部
201
250
251
252
280B
290
180B
随机数表部
100B

图 11