

(12) 发明专利

(10) 授权公告号 CN 1959750 B

(45) 授权公告日 2011.12.07

(21) 申请号 200610143650.7

(22) 申请日 2006.10.31

(30) 优先权数据

315626/2005 2005.10.31 JP

(73) 专利权人 日立欧姆龙金融系统有限公司

地址 日本东京都

(72) 发明人 佐川大介 今井启允 山口章

(74) 专利代理机构 永新专利商标代理有限公司

72002

代理人 陈英俊

(51) Int. Cl.

G07F 19/00 (2006.01)

G07F 7/10 (2006.01)

G06K 9/00 (2006.01)

审查员 李鹏飞

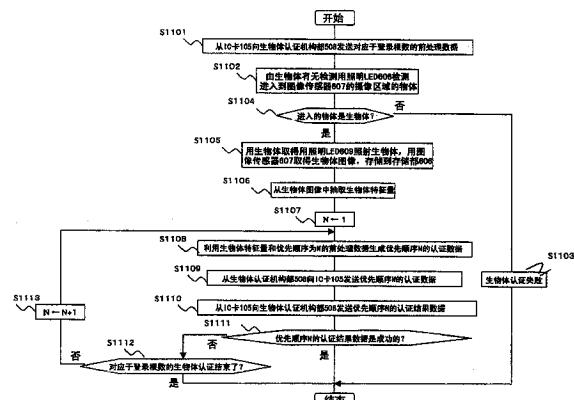
权利要求书 1 页 说明书 15 页 附图 12 页

(54) 发明名称

现金自动存取系统及装置

(57) 摘要

提供一种现金自动存取系统，具有：存储部，存储多个生物体信息；生物体信息取得部，取得利用者的生物体信息；生物体信息对照部，对照由上述生物体信息取得部取得的生物体信息和预先存储在上述存储部的生物体信息是否一致，得到对照结果；以及控制部，对变更处理和对照处理进行控制，所述变更处理是，每当由上述生物体信息对照部实施对照时，计数对照结果的成功次数，根据该对照的成功次数，变更对于预先存储在上述存储部的多个生物体信息的优先顺序；所述对照处理是，对照由上述生物体信息取得部取得的生物体信息和按照优先顺序预先存储在上述存储部的生物体信息。



1. 一种现金自动交易装置,自动地进行现金的交易,其特征在于,具有:

卡机构部,读取 IC 卡的信息;

生物体认证机构部,取得利用上述现金自动交易装置的利用者的生物体特征量;以及控制部,接收由上述卡机构部读取的上述 IC 卡内的附加了优先顺序的、根据生物体特征量经过不可逆变换处理制作的多个前处理数据,并且,向上述生物体认证机构部发送接收的附加了上述优先顺序的多个前处理数据,并且,接收利用发送的附加了上述优先顺序的多个前处理数据中的优先顺序高的前处理数据、和由上述生物体认证机构部取得的生物体特征量经过不可逆变换处理而制作的认证数据,而且,经上述卡机构部向上述 IC 卡发送接收的上述认证数据,执行利用上述 IC 卡对生物体信息的认证处理,

上述控制部利用某种算法对照上述认证数据、以及 IC 卡内存储的根据上述前处理数据和生物体特征量经过不可逆变换处理而制作的登录数据,来执行认证处理。

2. 如权利要求 1 所述的现金自动交易装置,其特征在于,

上述控制部,在上述认证处理的结果是成功时,处理利用者希望的交易,在上述认证处理的结果是失败时,接收利用发送的附加了上述优先顺序的多个前处理数据中的优先顺序其次高的前处理数据、和由上述生物体认证机构部取得的生物体特征量而生成的认证数据,并且,经上述卡机构部向上述 IC 卡发送上述认证数据,执行利用上述 IC 卡对生物体信息的认证处理。

3. 一种现金自动交易装置,自动地进行现金的交易,其特征在于,具有:

卡机构部,读取 IC 卡的信息;以及

控制部,执行变更处理和认证处理,所述变更处理是,每当执行生物体认证处理时,计算认证结果的成功次数,根据该认证成功次数,变更对于预先存储在上述 IC 卡内的、根据生物体特征量经过不可逆变换处理制作的多个前处理数据的优先顺序;所述认证处理是,接收由上述卡机构部读取的上述 IC 卡内的多个前处理数据,向生物体认证机构部发送接收的上述多个前处理数据,并且,接收利用由上述生物体认证机构部取得的生物体特征量、和发送的上述多个前处理数据中遵从优先顺序的前处理数据经过不可逆变换处理而制作的认证数据,而且,经上述卡机构部向上述 IC 卡发送接收的上述认证数据,执行利用上述 IC 卡对生物体信息的认证处理,

上述控制部利用某种算法对照上述认证数据、以及 IC 卡内存储的根据上述前处理数据和生物体特征量经过不可逆变换处理而制作的登录数据,来执行认证处理。

现金自动存取系统及装置

技术领域

[0001] 本发明涉及使用于现金自动存取装置(ATM)等的生物体认证系统。

背景技术

[0002] 过去,在现金自动存取装置(ATM)等进行的生物体认证系统有如下的例子。

[0003] 在专利文献1(特开2002-140707号公报)中记载着生物体测量式个人识别装置中的优先处理装置。该技术的构成是,在数据库中预先登录赋予了优先顺序的多个个人识别信息,按照优先顺序进行对照。并且,认为上次使用的手指在下次使用的可能性最大,基于使用实绩重新排列该优先顺序,同按照固定顺序进行对照相比,能够提高本人认证的速度。

[0004] 但是,在专利文献1的方法中,是基于假设上次使用的手指在下次使用的可能性最高为前提的使用实绩,重新排列该优先顺序的变更技术,所以发生以下问题。

[0005] 预先登录五个生物体信息(五根不同的手指),假设过去的认证成功次数每个手指不同时(认证成功次数:拇指0次、食指70次、中指15次、无名指10次、小指5次),则利用进行了认证登录但过去从没有用于认证的拇指进行认证时,拇指认证前的优先顺序是,第一位食指、第二位中指、第三位无名指、第四位小指、第五位拇指,这些在认证后变更为第一位拇指、第二位食指、第三位中指、第四位无名指、第五位小指。再者,如果利用一般不用于认证的无名指进行认证,那么在无名指认证之后变更为第一位无名指、第二位拇指、第三位食指、第四位中指、第五位小指。然后,如果想利用食指进行认证,在此状况下优先顺序下降到第三位,所以,在到达食指之前进行过去认证成功实绩少的无名指、拇指的对照,耗费时间。

[0006] 即,专利文献1的方法中,如果一旦在认证中使用过去的认证成功次数少的手指,那么下次使用平时使用次数多的手指进行认证时,在平时使用次数多的手指的对照之前必须要进行认证成功次数少的手指的对照,所以不方便。

发明内容

[0007] 本发明是为解决上述问题而做出的,其目的在于提供一种使用了IC卡的生物体认证系统及其方法,实现生物体信息的高隐密性并且缩短认证处理时间。

[0008] 为了解决上述课题,本发明采用如下构成。

[0009] 在现金自动存取系统中,具有:存储部,存储多个生物体信息;生物体信息取得部,取得利用者的生物体信息;生物体信息对照部,对照由上述生物体信息取得部取得的生物体信息和预先存储在上述存储部的生物体信息是否一致,得到对照结果;以及控制部,对变更处理和对照处理进行控制,所述变更处理是,每当由上述生物体信息对照部实施对照时,计数对照结果的成功次数,根据该对照的成功次数,变更对于预先存储在上述存储部的多个生物体信息的优先顺序;所述对照处理是,对照由上述生物体信息取得部取得的生物体信息和按照优先顺序预先存储在上述存储部的生物体信息。

[0010] 本发明在使用了 IC 卡的生物体认证系统、及装置中,对多个生物体信息附加了优先顺序,通过利用优先顺序高的生物体信息实施认证处理,保持了高的安全性,能够在较短的处理时间内进行本人认证。

附图说明

- [0011] 图 1 是生物体信息登录处理系统的概要图的例子。
- [0012] 图 2 是生物体信息登录处理系统的方框图的例子。
- [0013] 图 3 是生物体信息登录处理的说明图。
- [0014] 图 4 是生物体信息登录处理的流程图的例子。
- [0015] 图 5 是生物体认证处理系统的概要图的例子。
- [0016] 图 6 是生物体认证处理系统的方框图的例子。
- [0017] 图 7 是认证控制软件的结构图的例子。
- [0018] 图 8 是生物体认证处理的说明图。
- [0019] 图 9 是包含使用了 IC 卡内认证方式的生物体认证处理的交易流程图的例子。
- [0020] 图 10 是认证交易开始处理的流程图的例子。
- [0021] 图 11 是生物体认证处理的流程图的例子。
- [0022] 图 12 是认证交易结束处理的流程图的例子。
- [0023] 图 13 是表示优先顺序和生物体信息之间关系的数据例子。

具体实施方式

- [0024] 下面,说明使用了本发明的一实施方式。
- [0025] (第一实施例)
 - [0026] 在本实施方式中,大致分为两方面进行说明,其一是生物体信息登录处理,在金融机构的营业店中,在店员(窗口担当)和利用者之间向利用者所有的便携式电子装置、尤其是 IC 卡登录利用者的生物体信息(例如,指静脉);其二生物体认证处理,使用设置在金融机构、便利店等,主要是自动进行涉及现金的交易的现金自动交易装置、现金自动存取机(ATM),并且使用利用者的生物体信息进行认证。利用图 1~图 4 说明生物体信息登录处理,利用图 5~图 12 说明生物体认证处理。
 - [0027] 首先,简单说明生物体信息的登录处理和认证处理的概要。
 - [0028] 在生物体信息登录处理中,从利用者的指静脉抽取特定量来生成前处理数据,并且,还生成登录数据登录到 IC 卡。在该处理过程使用的窗口终端与带有 IC 卡装置的生物体信息登录装置连接着,登录用的生物体信息(前处理数据、登录数据)被加密后,不经由窗口终端,而是从生物体信息登录装置直接传送给 IC 卡,执行写入。
 - [0029] 另一方面,在生物体认证处理中,基于特有的认证、对照技术对来自利用者的指静脉的特征量和登录在 IC 卡的前处理数据、登录数据执行该处理。在该处理过程中,以 ATM 为中心,利用由连接在 ATM 上的生物体认证机构部新取得的生物体信息和从 IC 卡读取的前处理数据,生成认证数据,将其传送给 IC 卡,在 IC 卡内进行认证处理。
 - [0030] 在本发明的说明中,以生物体信息的登录处理使用营业店系统、认证处理使用 ATM 的方式进行说明,但还可以是在营业店系统中也进行认证处理、在 ATM 也进行登录处理

的方式。其中，生物体信息的登录处理最好是在确认了是本人之后，也在有店员在场的营业店系统中执行。而且，作为预先登录生物体信息的介质例举了 IC 卡，但不限定于此，也可以是便携式电话、RFID(Radio-Frequency-Identification) 标签等可以携带的电子介质(便携式电子装置)，希望是当前在利用者中最普及的在银行卡中装载了 IC 芯片的 IC 卡，这样可以抑制系统的变更。

[0031] 图 1 是从金融机构的营业店内店员使用的营业店系统中，特别地删除了与生物体信息的登录有关的生物体信息登录处理系统的概要图。该生物体信息登录系统是将具备生物体信息读取装置 102 的生物体信息登录装置 101、和控制该生物体信息登录装置 101 的登录用终端装置 104 连接而构成。该系统是金融机构的店员(窗口担当)操作登录用终端装置 104，在 IC 卡 105 中登录利用者的生物体信息的机构。具体地说，是窗口担当操作操作部 107，通过显示在显示部 106 的各种菜单进行选择，除了生物体信息的登录之外，还可以进行金融机构的各种交易的机构。

[0032] 窗口担当将 IC 卡 105 插入到作为生物体信息登录装置 101 的一个构成的 IC 卡装置 103，成为可对 IC 卡 105 进行写入的状态。另一方面，利用者沿图示形状将利用者自身的手指放置在生物体信息读取装置 102 上。通过窗口担当者的操作，生物体信息读取装置 102 向放置的手指透过近红外线，由照相机拍摄指静脉图案，并得到该图像。从该图像抽取生物体特征量，对抽出的生物体特征量施加后述的处理，利用 IC 卡装置 103 对 IC 卡 105 进行记录及写入处理。并且，生物体特征量是从手指的静脉数据(指静脉图案)中得到的能够确定个人的数据。

[0033] IC 卡装置 103 除了如上所述地具有向 IC 卡 105 写入信息的功能之外，还具有读取存储在 IC 卡 105 的信息的功能。即具有读取或写入功能，但是，下面利用向 IC 卡 105 写入生物体信息的例子进行说明。

[0034] 图 2 是表示在图 1 说明的生物体信息登录处理系统的一实施例的结构的方框图。

[0035] 生物体信息登录装置 101 包括：控制生物体信息登录装置 101 全体的 CPU201、存储各种信息的主存储部 202、读取生物体信息的生物体信息读取装置 102、向 IC 卡 105 写入生物体信息的 IC 卡装置 103、以及与登录用终端装置 104 连接的通信部 215。

[0036] 主存储部 202 分为存储各种程序的 ROM203、和主要存储数据并且可进行存储数据的重写的 RAM204。在此，说明了由 ROM203、RAM204 构成的主存储部(也称为存储部)202，但是，也可以是由各硬盘、各种半导体存储器构成的结构。ROM203 具备：用于生物体信息的登录处理的登录处理程序 205；用于生成认证时使用的登录数据的登录数据生成程序 206；用于控制生物体信息读取装置 102 的生物体信息读取装置控制程序 207；用于进行向 IC 卡 105 的信息写入处理的 IC 卡装置控制程序 208；以及用于控制通信部 215 的通信控制程序 209。

[0037] 生物体信息读取装置 102 具备：取得生物体图像(指静脉图案)的由 CCD 照相机等构成的图像传感器(图像取得部)210；检测在图像传感器 210 的图像可取得区域是否放置了手指的生物体有无检测用照明 LED211；在生物体图像(指静脉图案)取得时对手指照射近红外线的生物体取得用照明 LED(生物体照射部)212。IC 卡装置 103 具备：向 IC 卡 105 写入信息的 IC 卡写入部 213；用于与 IC 卡 105 连接的触点端子 214。

[0038] IC 卡 105 具备：控制 IC 卡 105 整体的 CPU221；存储与生物体信息有关的数据和涉

及金融交易的程序等的存储部 222；用于与生物体信息登录装置 101 连接的触点端子 223。而且，不局限于利用触点端子连接 IC 卡装置 103 和 IC 卡 105 的接触式，也可以由非接触式构成。

[0039] 登录用终端装置 104 包括：控制登录用终端装置 104 整体的 CPU231；存储数据和程序的主存储器 232；由 CRT 或液晶显示器等构成、显示操作引导的显示部 106；由接受窗口担当者的输入操作的键盘、鼠标等构成的操作部 107；连接生物体信息登录装置 101 和生物体登录用终端装置 104 的通信部 235。并且，主存储部 232 除了存储着用于控制生物体信息登录装置 101 的生物体信息登录装置程序 233，还存储着通过窗口进行交易的各种金融交易用程序。

[0040] 利用图 3 说明在生物体信息登录处理中登录到 IC 卡 105 的登录数据的生成过程。其中，由于安全上的原因，即为了防止信息泄漏引起的伪造，省略了对生成过程中的算法等的说明。在生物体信息的认证处理中也同样。

[0041] 首先，基于由图像传感器 210 得到的生物体图像（指静脉图案），使用某种算法抽取表示其特征的生物体特征量（步骤 301）。然后，利用该生物体特征量进一步使用某种算法生成前处理数据。再者，组合生物体特征量和前处理数据，生成登录数据（步骤 302）。

[0042] 在此，所谓前处理数据，也可以解释成为了生成登录数据而使用的加密密钥。而且，登录数据如上述及附图所示，是不能利用生物体特征量直接生成的数据。而且，前处理数据和登录数据是利用明确表现利用者自身特征的生物体特征量生成的数据，但在该生成过程使用了利用不可逆变换处理的算法。因此，作为利用逆变换的生成处理，不能利用登录数据生成生物体特征量或前处理数据，不能利用前处理数据和登录数据这两个数据生成生物体特征量。而且，希望是如下方式，即前处理数据是抽出了不能确定利用者个人的部分而生成的信息，登录数据是抽出可以确定个人的部分而生成的信息。而且，前处理数据、登录数据都是只有卡持有者才能够得到的特有信息。虽然在后面也叙述，对每个手指存在前处理数据和登录数据，对要登录的根数的手指附加优先顺序，存储在 IC 卡 105。举例的话，如果登录三根手指（按右手食指、右手中指、左右食指的顺序赋予优先顺序）的指静脉，那么如图 13 所示地登录优先顺序为 1 的右手食指的前处理数据及认证数据、优先顺序为 2 的右手中指的前处理数据及认证数据、优先顺序为 3 的左手食指的前处理数据及认证数据。

[0043] 如图 13 所示，附图标记 1301 表示利用者在 IC 卡中登录生物体信息时的优先顺序，是对各手指的种类 1302 设定的值（固定值）。然后，对应于手指的种类 1302，在 IC 卡中分别登录前处理数据 1303、登录数据 1304。再者，作为其他例子，对每个该手指的种类 1302 累积后述的认证时的成功次数，存储在符号 1305。然后，追加根据该认证成功次数 1305 变更优先顺序的优先顺序变更数据的设定值（变更值、未图示），存储到 IC 卡中。

[0044] 最后，向 IC 卡 105 存储生成的前处理数据和登录数据（步骤 303）。存储在 IC 卡 105 的这些数据以加密状态存储，再者，如上所述地，以不能够进行利用逆变换的生成处理的状态存储。由此，假设前处理数据、登录数据由有恶意的人读取，并且，即使解读了两个数据也不可能生成生物体特征量。这样，利用数据的加密和逆变换不可的数据生成这样的双重安全措施来保护 IC 卡内的数据，这也是特征之一。

[0045] 用以下的数学式表示上述数据生成算法。

[0046] 如果设生物体特征量为 x ，则前处理数据 y 使用某函数（相当于算法）表示为 $[y]$

$= f(x)$]。

[0047] 登录数据 z 通过生物体特征量 x 和前处理数据 y 的组合生成, 所以使用某函数 g 表示为 [$x+y \rightarrow z = g(x, y)$]。

[0048] 并且, 由于该生成过程是不可逆的, 所以如 $z = g(x, y) \rightarrow x$, $z = g(x, y) \rightarrow y$, $z = g(x, y) \rightarrow x+y$ 那样, 不能从登录数据复原生物体特征量或前处理数据。

[0049] 图 4 是生物体信息登录装置 101 的 CPU201 执行、或者基于来自 CPU201 的指示由各机构、各部(还包含程序)执行的生物体信息的登录处理的流程图的例子。

[0050] 在 IC 卡装置 103 插入了 IC 卡 105, 成为 IC 卡连接状态(可以向 IC 卡 105 写入数据的状态)。为了实现 IC 卡连接, 需要使 IC 卡 105 的触点端子 223 和 IC 卡装置 103 的触点端子 214 接触。在下面, 说明窗口担当者操作登录用终端装置 104 并且将利用者的生物体信息登录到 IC 卡 105 内的过程, 并且, 说明基于该操作由各机构等执行的处理、控制。而且, 在图 2 说明的通信控制程序 209 尤其在生物体信息登录装置 101 和生物体登录用终端装置 104 之间控制数据的收发, 但在下面省略说明。

[0051] 登录用终端装置 104 在显示部 106 显示菜单画面(引导登录、认证、变更、结束等处理的选择的画面), 由操作部 107 接受窗口担当者的输入操作。当通过操作部 107 从显示的交易项目中选择登录处理时, 登录用终端装置 104 的 CPU231 执行登录处理程序 205、生物体信息登录装置控制程序 233, 向生物体信息登录装置 101 发出登录处理开始的指示。接受了登录处理开始指示的生物体信息登录装置 101 的 CPU201 执行登录处理程序 205, 作为整个系统实施登录处理。

[0052] 在登录用终端装置 104 的显示部 106 显示向生物体信息登录装置 101 插入 IC 卡 105 的引导。当 IC 卡 105 插入到 IC 卡装置 103 时(步骤 401), 使 IC 卡 105 的触点端子 223 和 IC 卡装置 103 的触点端子 214 接触, 进行生物体信息登录装置 101 和 IC 卡 105 的连接(步骤 402)。此时判断插入的 IC 卡 105 的存储部 222 中的与生物体信息有关的程序的有无(步骤 403), 没有程序时(是不能登录数据的卡时), 返回 IC 卡 105(步骤 414)。另一方面, 在插入的 IC 卡 105 的存储部 222 有关于生物体信息的程序时(是可以登录数据的卡时), 设定优先顺序 N 为“1”(步骤 404), 在显示部 106 显示将登录的手指放置在生物体信息读取装置 102 上的引导。对应于此, 利用者在生物体信息读取装置 102 上放置登录的手指。生物体信息登录装置 101 的 CPU201 执行生物体信息读取装置控制程序 207, 向生物体信息读取装置 102 发出生物体信息读取开始的指示。物体(手指)被放置在图像传感器 210 的图像可取得区域时, 生物体信息读取装置 102 通过生物体有无检测用照明 LED211 检测物体(手指)的进入(步骤 405), 调查物体(手指)是否是生物体(步骤 406)。当插入的物体(手指)不是生物体时, 不对 IC 卡 105 写入任何信息就返还 IC 卡 105(步骤 414)。当插入的物体(手指)是生物体时, 由生物体取得用照明 LED212 向物体(手指)照射近红外线, 用图像传感器 210 取得优先顺序 N(N=1) 的生物体图像(指静脉图案), 存储到 RAM204(步骤 407)。接着, 从优先顺序 N(N=1) 的生物体图像(指静脉图案)抽出优先顺序 N(N=1) 的生物体特征量(步骤 408)。然后, 通过执行登录数据生成程序 206, 如图 3 所示地利用优先顺序 N(N=1) 的生物体特征量生成优先顺序 N(N=1) 的前处理数据之后(步骤 409), 利用优先顺序 N(N=1) 的生物体特征量和优先顺序 N(N=1) 的前处理数据, 生成优先顺序 N(N=1) 的登录数据(步骤 410)。接着, 执行 IC 卡装置控制程序 208,

通过 IC 卡写入部 213、进一步通过 IC 卡 105 内的 CPU221 向 IC 卡 105 的存储部 222 存储生成的 RAM204 内的优先顺序 N(N = 1) 的前处理数据和优先顺序 N(N = 1) 的认证数据(步骤 411)。判断要登录根数的手指的登录是否结束(步骤 412),若结束,就结束生物体信息登录,返还 IC 卡 105(步骤 414)。若未结束,将优先顺序 N(N = 1) 加上 1,作为优先顺序 N(N = 2)(步骤 413),再次进到步骤 405 ~ 411,向 IC 卡 105 的存储部 222 存储优先顺序为 N(N = 2) 的手指的前处理数据和优先顺序为 N(N = 2) 的手指的认证数据。这样,重复步骤 405 ~ 411,在要登录根数结束之前,继续进行登录。而且,要登录的手指根数可以是由金融机构侧、或利用者侧自由决定的方式。

[0053] 而且,也可以是,优先顺序不是如图 4 所示地在登录时附加,而是在所有手指的登录之后,通过利用者的申告以任意顺序追加及变更。由此,能够向利用者提供考虑优先顺序的时间。

[0054] 再者,也可以不是在事先登录中附加优先顺序,而是利用者根据使用频度顺序自动地对认证处理实施时使用的手指进行附加及变更。在前处理数据、登录数据上附加使用频度,预先登录在 IC 卡内。如果是使用频度顺序,不但可以节省附加优先顺序的时间,对利用者来说使用更方便。优先顺序的定义,可以考虑使用了数值的降序及升序或字符串等的各种方法。并且,所谓使用频度,可以是如图 13 所示地单纯计数(计算)生物体认证的成功次数,只要能够实现本发明的目的,可以考虑各种统计方法,包含实施生物体认证的全体次数中的手指的使用率等、使用了失败次数的方法。

[0055] 以上,基于存储在各 CPU201、221、231 或存储部的程序的处理、控制,说明了生物体信息的登录处理、控制,各程序可以在转移到登录处理的当初的阶段已经被启动,而且,也可以将这些硬件及软件的结构作为控制部,上述的各种控制、处理是该控制部的功能、手段,这是不言而喻的。而且,对于下面说明的生物体信息的认证处理也相同。

[0056] 当执行生物体信息的认证处理时,以使用通过上述登录处理登录的信息,即存储、登录、写入在 IC 卡 105 中的前处理数据和登录数据进行认证处理为前提进行了说明。

[0057] 图 5 是生物体认证处理系统的概要图。生物体认证系统是将具备读取生物体信息的功能和对 IC 卡 105 的信息的读取(或写入)功能的现金自动交易、或存取装置(ATM)501,和存储与金融商品有关的交易所需信息的服务器 502 连接而构成。ATM501 是自动执行存款、支付、汇款等利用者希望的各种交易的装置,利用者向卡 / 明细表机构部 504 插入 IC 卡 105,通过操作部 503 输入希望的交易和金额,由生物体认证机构 508 实现认证来进行交易。尤其,在现金交易中,执行纸币输入输出机构部 506 的纸币的存款或取款,硬币输入输出机构部 507 的硬币的存款或取款,ATM501 进行利用者希望的现金交易。而且,在利用者希望打印存折时,可以由存折机构部 505 在存折上记录、打印交易内容。而且,在本实施方式中说明的生物体认证系统使用于现金自动交易、或存取装置,所以作为整体也可以称为现金自动交易、或存取系统。

[0058] 图 6 是表示生物体认证处理系统的一实施例的结构的方框图。ATM501 具有:控制 ATM 整体的 CPU601;操作部 503,由进行交易项目的画面显示、键盘输入的检测,具体地说接受利用者的操作、用手指按下的键输入的触摸屏等构成;卡 / 明细表机构部 504,具有卡的插入及排出动作、对卡的磁条或 IC 卡 105 的读 / 写动作、卡压花部分的图像的读取、或在明细表上打印交易内容并从装置内排出的功能;存折机构部 505,具有利用者存折的插入 / 排

出动作、磁条的读 / 写动作、对存折的打印部的打印功能等。

[0059] 再者,还包括:纸币输入输出机构部 506,具有纸币的鉴别及输送、收纳功能等,进行纸币的存款或取款处理;硬币输入输出机构部 507,具有硬币的鉴别及输送、收纳功能等,进行硬币的存款或取款处理;生物体认证机构部 508(还称为生物体信息取得部),取得生物体信息,支持其认证;存储数据和程序的主存储部(还简略称为存储部)602;以及与服务器 502 连接的通信部 610。

[0060] 而且,在图 1、图 2 说明的登录用终端装置 104 的操作部 107 是在窗口担当者向 IC 卡 105 登录利用者的生物体信息时进行输入操作的单元,所以由键盘、鼠标等构成;另一方面,图 5、6 的 ATM501 的操作部 503 是利用者在 ATM501 上交易时进行输入操作的单元,所以由触摸屏等构成,这两个是相同的操作部,但结构和用途不同。

[0061] 卡 / 明细表机构部 504 具备:读取 IC 卡 105 的信息的 IC 卡读取部 603;在明细表上打印交易内容的明细表打印部 604;及用于与 IC 卡连接的触点端子 605。

[0062] 生物体认证机构部 508 具备:存储各种数据等的存储部 606;取得利用者的生物体图像(指静脉图案)且由 CCD 照相机等构成的图像传感器(图像取得部)607;检测手指是否放置在图像传感器 607 的图像可取得区域的生物体有无检测照明 LED608;在取得生物体图像(指静脉图案)时向手指照射近红外线的照明 LED(生物体照射部)609。即,生物体认证机构部 508 具有取得与图 1、图 2 所示的生物体信息读取装置 102 大致相同的生物体信息的功能。

[0063] 主存储部(单纯称为存储部)602 在硬件上包括存储各种程序的 ROM620、和主要存储数据且可以重写存储数据的 RAM621。如上述登录处理中说明的那样,也可以是分别由硬盘或各种半导体存储器构成的结构,还可以称为第一、二存储部。而且,ROM620 具备按照 CPU601 等的指示进行下面说明的生物体图像的取得、认证等处理,用于控制生物体认证机构部 508 的认证控制软件 622。另外,虽然未图示,还存储向 ATM501 的操作部 503 的画面数据,ATM501 的现金交易、汇款交易等所需的程序、软件。经由通信网同 ATM501 连接的服务器 502,包括控制服务器 502 整体的 CPU611、存储部 612、及与 ATM501 连接的通信部 613。

[0064] 图 7 图示了以认证控制软件 622 为中心的、与主存储部 602、生物体认证机构部 508、卡 / 明细表机构部 504 内的 IC 卡 105 有关的控制模块(软件构成),该认证控制软件 622 用于 ATM501 中的生物体信息的认证所涉及的控制、尤其是生物体认证机构部 508 的控制。

[0065] 认证控制软件 622 大致分为认证控制应用程序 701 和认证控制中间件 702,可以分别称软件为软件、应用程序为应用、中间件为中间。认证控制应用程序 701 是指具有导入搭载生物体认证机构部 508 的 ATM501 的金融机构等的个别功能的程序,其认证顺序、方式、认证时的画面显示等在各个金融机构制作其式样,并变更。尤其,本认证控制应用程序 701 对认证中间件 702 进行认证处理开始指示等。

[0066] 认证控制中间件 702 是指即使金融机构不同、生物体信息不同也具有认证处理所需的共同功能的程序,是负担控制生物体认证机构部 508 的生物体认证机构部控制程序 703、从 IC 卡 105 进行卡和数据的交换、并且控制 IC 卡 105 内程序的执行的 IC 卡控制程序 704 这样的生物体信息的认证所涉及的各种程序的控制、处理的程序。

[0067] 而且,由认证控制中间件 702 执行、且得到的数据暂时存储在 RAM621。RAM621 具

有用于进行生物体认证机构部 508 和 IC 卡 105 之间数据的交换的缓冲区域,即认证结果数据缓冲存储器 705、认证数据缓冲存储器 706、前处理数据缓冲存储器 707 这样的各数据缓冲存储器。可以说,这些数据在硬件上暂时存储在 RAM621,在软件上存储在认证控制软件 622、尤其是认证控制中间件 702。

[0068] 而且,认证控制中间件 702 根据来自认证控制应用程序 701 的指示,经由驱动器(未图示)使卡 / 明细表机构部 504、生物体认证机构部 508 动作。然后,如上所述,这些各部位由 ATM501 的 CPU601 控制其处理。并且,驱动器是指用于利用计算机周边设备及装置(器件)的控制用软件。

[0069] 由认证控制软件 622 控制的生物体认证机构部 508 的存储部 606,具有用于生成认证数据的认证数据生成程序 709、用于根据认证结果数据判断认证的成功与否的认证结果判断程序 710。而且,卡 / 明细表机构部 504 具有用于实施认证处理的认证程序 711。

[0070] 利用图 8 说明生物体认证处理中的认证的方式及数据的交换。还作为下述的图 11 的生物体认证流程的说明的补充而使用。也可以说,下面动作的主体是从认证控制应用程序 701 接受了执行命令的认证控制中间件 702,但由于认证控制应用程序 701 和认证控制中间件 702 共同进行,所以通过认证控制软件 622 动作。而且,还可以将接收、发送分别称为输入、输出。

[0071] 当 ATM501 的交易中执行了生物体信息的认证时,预先存储在 IC 卡 105 中的前处理数据和登录数据中的前处理数据被发送给认证控制中间件 702。认证控制中间件 702 从 IC 卡 105 接收前处理数据,在 RAM621(包含认证控制软件 622、认证控制中间件 702) 的前处理数据缓冲存储器 707 暂时存储后,向生物体认证结构部 508 发送(步骤 801)。另一方面,生物体认证机构部 508 从认证控制软件 622 接收前处理数据,之后或并行地取得利用者的生物体信息,从生物体信息抽取生物体特征量。然后,组合接收的前处理数据和取得并抽取的生物体特征量,生成认证数据(步骤 802)。

[0072] 这样,在生物体信息的认证处理中,前处理数据具有作为用于生成认证数据的加密密钥的功能。而且,即使假设能够取得该认证数据,也不能从该数据直接生成生物体特征量。认证数据虽然是从生物体特征量生成的数据,但在该生成过程使用了基于不可逆变换处理的算法,所以,相反地从认证数据不能生成生物体特征量,再者,不能利用前处理数据和认证数据这两个数据生成生物体特征量。前处理数据是抽出了不能确定个人的部分而生成的信息,认证数据是抽出可以确定个人的部分而生成的信息。

[0073] 在此,与生物体信息登录时相同地用数学式表示上述的数据生成算法。

[0074] 由生物体认证机构部 508 认证时得到的信息,即新得到的生物体特征量设为 x' 。然后,前处理数据 y 与登录时没有变化,所以是 $[y = f(x)]$ 。

[0075] 认证数据 z' 是通过生物体特征量 x' 和前处理数据 y 的组合而生成的,所以使用某函数 g 表示为 $[x' + y \rightarrow z' = g(x', y)]$ 。然后,由于此生成过程是不可逆过程,所以如 $z' \rightarrow x'$, $z' \rightarrow y$, $z' \rightarrow x' + y$ 那样不能从登录数据复原生物体特征量和前处理数据。

[0076] S802 的认证数据生成之后,根据认证控制软件 622 的指示、控制在认证数据缓冲存储器 706 暂时存储由生物体认证机构部 508 生成的认证数据,然后向 IC 卡 105 发送(步骤 803)。IC 卡 105 接收认证数据,利用某种算法对照存储在 IC 卡 105 的登录数据和认证数据(也称为生物体认证处理),生成认证结果数据(步骤 804)。再者,向认证控制中间件

702 发送生成的认证结果数据。认证控制中间件 702 从 IC 卡 105 接收认证结果数据，在认证控制软件 622 的认证结果数据缓冲存储器 705 暂时存储之后，向生物体认证机构部 508 发送。然后，生物体认证机构部 508 在生物体认证机构部 508 内进行认证结果数据的判断（分析）（步骤 805），向认证控制中间件 702 通知认证结果数据和认证成功部位及认证失败原因（步骤 806），结束生物体认证处理。

[0077] 这样，在生物体认证处理中具有如下特征：与利用者的生物体信息最接近的生物体特征量未存储在 IC 卡 105 内，而且由生物体认证机构部 508 取得并抽出生物体特征量，但是从生物体认证机构部不向外部输出。

[0078] 而且，还具有如下特征：经认证控制软件 622、或基于其控制，在 IC 卡 105 和生物体认证机构部 508 之间进行交换的数据是前处理数据、认证数据、认证结果数据这三个，但是，如上所述，不论如何组合这些数据也不能生成生物体特征量。

[0079] 而且，具有如下特征：在涉及生物体信息的各数据的生成等生物体认证处理中，IC 卡 105、生物体认证机构部 508 分别分担着得到认证结果。因此，设计成即使 IC 卡或生物体认证机构部被盗，而且解读了其内部也不能执行生物体认证处理。即，虽然在理论上可以利用在认证时由生物体认证机构部 508 取得的生物体特征量新生成前处理数据，利用该前处理数据和生物体特征量生成认证数据，但是在本实施方式中没有那么做，是利用存储在 IC 卡 105 的前处理数据和生物体特征量生成认证数据，所以保持着较高的安全性。

[0080] 而且，希望是如下的方式，即认证控制中间件 702 将前处理数据存储在生物体认证机构部 508 内，生成认证数据之后删除即可，在需要认证时，随时从前处理数据缓冲存储器 707 向生物体认证机构部 508 发送的方式。即，在 ATM501 的交易结束之前，在认证控制软件 622 内的前处理数据缓冲存储器 707 中存储前处理数据。通过这样做，与从 IC 卡 105 发送前处理数据相比，从认证控制软件 622 内的前处理数据缓冲存储器 707 发送时具有能实现更快处理的效果。

[0081] 而且，如上所述地在 IC 卡 105 内实施生物体认证处理，所以将 IC 卡 105 本身或 IC 卡 105 的 CPU221 还称为生物体信息对照部、或生物体认证处理部。

[0082] 使用图 9～12 说明在现金自动交易装置、现金自动存取装置（ATM）501 使用 IC 卡 105 实施包含利用 IC 卡内认证方式的生物体认证处理的支付交易时的处理。

[0083] 图 9 是表示 ATM501 的 CPU601、认证控制软件 622 等（控制部）执行的、特别是通过使用了 IC 卡内认证方式的生物体认证处理进行的 ATM 上的交易的流程图。

[0084] 在进行生物体认证处理之前，进行交易选择、密码输入、卡插入等为了执行 ATM501 上的交易而必要的处理。从 ROM620 读取存款、支付、查询余额、汇款等的交易选择引导并显示在操作部 503，从利用者接受交易的选择（步骤 901）。在选择了生物体认证所需的交易、例如支付交易等时，显示向操作部 503 插入 IC 卡的引导，提醒 IC 卡 105 的插入。当利用者向卡 / 明细表机构部 504 插入了 IC 卡 105 时，则检测出该插入（步骤 902），由卡 / 明细表机构部 504 的 IC 卡读取部 603 从 IC 卡 105 读取账号。并且，IC 卡 105 也可以是具备磁条的，此时，也可以从 IC 卡 105 的磁条读取生物体信息以外的账号等的数据。

[0085] 接着，在操作部 503 显示输入密码的提示。当由利用者在操作者输入了密码时，检测该输入（步骤 903），经通信部 610、613 向服务器 502 发送读取的账号和输入的密码。另一方面，服务器 502 的 CPU611 经通信部 610、613 接收输入的密码，进行输入的密码和预先

登录在存储部 612 的对应账号的密码的对照,经通信部 610、613 向 ATM501 发送其对照结果。ATM501 经通信部 610、613 接收对照结果,检验密码的正确与否(步骤 904),在输入的密码不正确时,计数密码的输入次数(步骤 905)。若此时的密码输入次数在规定次数以内,则向利用者催促密码的再输入。若密码的输入次数超过规定次数,则中止交易(步骤 906)。

[0086] 在 S904 中,在输入的密码正确时,判断插入的 IC 卡 105 是否是生物体认证对象卡(步骤 907)。此时的生物体认证对象卡是指,具有为了实施生物体认证而必要的信息和程序的卡。

[0087] 然后,在插入的 IC 卡 105 不是生物体认证对象卡时,不进行生物体认证处理,接着执行支付等交易(步骤 915)。在插入的 IC 卡 105 是生物体认证对象卡时,作为生物体认证处理的事先准备,进行认证交易开始处理(步骤 908)。使用后述的图 10 详细说明认证交易开始处理。

[0088] 当认证交易开始处理结束时,ATM501 的 CPU601 将认证控制软件 622 取入到 RAM621 并展开。接着,ATM501 的 CPU601 执行认证控制应用程序 701。由此,认证控制应用程序 701 对认证控制中间件 702 发出登录信息取得指示。接受了登录信息取得指示的认证控制中间件 702 执行 IC 卡控制程序 704,从 IC 卡 105 取得进行由认证控制应用程序 701 指示的处理所必要的信息(登录者信息)(步骤 909)。在处理所必要的信息中,包含账号、支店号、科目等交易信息,和利用者姓名、驾驶证、保险证等的可以确认本人的证件的有无这样的利用者信息等。而且,此时,认证控制中间件 702 除了取得由认证控制应用程序 701 指示取得的信息之外,还取得预先登录在 IC 卡 105 的前处理数据,存储到前处理数据缓冲存储器 707。这是因为,通过与认证控制应用程序 701 指定的信息一起,还取得前处理数据,降低对 IC 卡 105 存取的次数,提高处理时间。此数据被发送给认证控制中间件 702,并存储在前处理数据缓冲存储器 707。如此地,ATM501 的 CPU501 成为主体,执行认证控制软件 622 内的各种程序,进行各种处理,在下面,为了简化说明而省略了该过程,以认证控制中间件 702 为主体进行说明。而且,如上所述地,将这些也称为控制部(单元)的控制、处理。

[0089] 从 IC 卡 105 取得登录信息后,认证控制中间件 702 执行生物体认证机构部控制程序 703 进行生物体认证处理(步骤 910)。即,向生物体认证机构部 508 发送存储在前处理数据缓冲存储器 707 的前处理数据,并且,向生物体认证机构部 508 指示生物体信息取得。使用图 8 说明了该生物体认证处理,但在后述的图 11 中也详细说明。

[0090] 接着,检验生物体认证的成功与否(步骤 911),在此,生物体认证失败时,计数生物体认证的实施次数(步骤 912)。如果此时的生物体认证的实施次数在规定次数以内,就向生物体认证机构部 508 再次发送存储在 RAM621 或程序中的前处理数据,在 ATM501 的操作部 503 显示再认证开始画面等,使利用者再次实施生物体认证(步骤 917)。若生物体认证的实施次数超过规定次数,就中止交易(步骤 913)。而且,此时,为了提高安全性,删除存储在 RAM621 的前处理数据等。然后,在 S911 中,当生物体认证成功时,作为生物体认证处理的事后处理进行认证交易结束处理(步骤 914)。使用后述的图 12 详细说明该认证交易结束处理。

[0091] 当认证交易结束处理结束时,就执行利用者希望的交易、即在 S901 选择的交易(步骤 915)。具体地说,若利用者希望的交易是支付交易,由操作部 503 接受支付金额的输入。当由利用者进行了支付金额输入时,在操作部 503 显示输入的金额及提醒按下金额是

否正确的确认键的消息。当操作部 503 的确认键被按下时,与服务器 502 进行交易数据的通信。通信后,ATM501 的 CPU601 从纸币输入输出机构部 506、硬币输入输出机构部 507 分别排出所要求金额的纸币、硬币,在卡 / 明细表机构部 504 的明细表打印部 604 进行交易数据的打印。然后,从卡 / 明细表机构部 504 返回 IC 卡 105,并且在明细表上打印交易数据并送出,结束交易(步骤 916)。

[0092] 而且,若利用者希望的交易是查询余额,则与服务器 502 进行交易数据的通信,通信之后,在操作部 503 显示存款或借入的余额。显示后,向利用者提示要结束交易、还是接着实施其它交易。要结束交易时,从卡 / 明细表机构部 504 返回 IC 卡 105,并且根据利用者的请求在明细表上打印交易数据并送出,结束交易(步骤 916)。利用者希望实施其它交易,进行以下的处理。

[0093] 在查询余额之后,接着希望进行上述支付交易等的需要生物体认证的交易时,再次实施生物体认证,只有在生物体认证成功时执行交易。还可以想到当利用者在查询余额时确认了存款及借入余额没取出 IC 卡 105 就离开 ATM 时,由第三者进行交易的情况,通过在每次交易时实施生物体认证,能够排除这样的危险,可以实现安全性高的 ATM 系统。

[0094] 并且,在此流程中,输入密码之后实施了生物体认证,但也可以取相反的顺序,在生物体认证实施后输入密码。在先输入密码时,利用者与通常的交易相同地插入卡后,在最初的交易选择之后立刻输入密码,所以,具有在之后进行生物体认证,其操作流程也接近现状而容易操作装置的优点。另一方面,在利用密码的认证之前实施生物体认证的情况下,在本人以外进行生物体认证而导致生物体认证失败并拒绝交易时,不经过密码输入就结束交易,所以可以不必进行用于密码对照的、与服务器的无用的通信,具有减轻服务器的负担的优点。

[0095] 利用图 10 说明图 9 的 S908 中的认证交易开始处理。从认证控制应用程序 701 接受了认证交易开始指示的认证控制中间件 702,执行 IC 卡控制应用程序 704,进行与 IC 卡 105 的连接(步骤 1001)。这样,如上所述,使来自 IC 卡 105 的数据的读取成为可能的状态。但是,在 IC 卡 105 中不存在关于生物体信息的数据,是不对应 IC 卡内认证的 IC 卡时,例如希望只通过利用上述密码的认证处理也可以进行 ATM 上的期望的交易时,可以在与图 9 的 S902 等的卡插入几乎相同时刻,由认证控制中间件 702 以外的其他 ATM 软件来执行 IC 卡控制程序 704,至少要在 S908 的处理之前结束与 IC 卡 105 的连接。

[0096] 而且,在插入到卡 / 明细表机构部 504 的 IC 卡 105 中,通过图 1 的生物体信息登录装置 101 预先登录有利用者固有的登录数据及前处理数据,在 IC 卡 105 内装载并存储了用于进行认证的认证程序 711。此认证程序 711 是事先且用不可重写的形式在 IC 卡 105 写入的应用程序,是按照特定的算法对预先登录在 IC 卡中的登录数据和由 ATM 控制部得到的认证数据进行匹配及对照的程序。

[0097] 当在 S1001 卡 / 明细表机构部 504 和 IC 卡 105 的连接成功时,认证控制中间件 702 取得登录在 IC 卡 105 的支持认证方式(或支持认证信息)(步骤 1002)。支持认证方式是指,预先登录在 IC 卡 105 的、能够唯一地确定用哪个控制步骤认可对证数据、生物体特征量等信息实施认证处理的信息。例如,在指静脉认证中,支持在生物体认证机构部 508 内进行认证(对照)的装置内认证处理和在 IC 卡 105 内进行认证的 IC 卡内认证处理,通过从 IC 卡 105 取得支持认证方式,切换认证控制顺序,用一个认证控制程序就可以进行两

个认证方式。

[0098] 如该支持认证方式取得这样的、使用唯一地确定登录在 IC 卡等中的认证方式、认证控制顺序的信息,来切换认证控制的顺序和方式的方法,在 ATM 等生物体认证装置搭载终端上搭载了多个认证装置(例如手指、手掌的静脉认证装置、眼睛的虹彩认证装置等)时,也能够通过切换认证控制程序的控制方式,来对应多个生物体认证装置的控制。

[0099] 接着,判断在步骤 1002 得到的认证方式是否是 IC 卡内认证(步骤 1003),在不是 IC 卡内认证时,不进行交易处理,返还 IC 卡 105(步骤 916)。另一方面,是 IC 卡内认证方式时,进行 ATM501 和 IC 卡 105 之间的相互认证,结束认证交易开始处理(步骤 1004)。相互认证是,用于确认位于生物体认证机构部 508 的认证数据生成程序 709、搭载在 IC 卡 105 的认证程序 711 等是否被非法改写成不正当的程序,在 ATM501 和 IC 卡 105 确认相互的程序正当性的处理。

[0100] 利用图 11 说明图 9 的 S908 的生物体认证处理。如图 8 说明的那样,该生物体认证处理是最终进行预先记录在 IC 卡 105 内的登录数据、和在生物体认证处理时新生成的认证数据的认证(对照),并得到其对照结果的处理,其特征是,涉及认证自身的根本的处理在 IC 卡 105 内进行。

[0101] 在图 9 的 S909 由 IC 卡 105 接收数据,在该生物体认证时,同该数据一起,从 IC 卡 105 向认证控制中间件 702 发送预先存储的对应于登录根数的前处理数据。认证控制中间件 702 接收存储在 IC 卡 105 的前处理数据,存储到前处理数据缓冲存储器 707。再者,向生物体认证机构部 508 发送存储在前处理数据缓冲存储器 707 的对应于该登录根数的前处理数据(步骤 1101)。当生物体认证机构部 508 接收到对应于登录根数的前处理数据时,接着作为并行处理,读取利用者的生物体信息。

[0102] 图 11 的步骤 1102 ~ 步骤 1106 的处理,执行与图 4 的步骤 405 ~ 步骤 408 几乎相同的处理,得到生物体特征量。在图像传感器 607 的图像取得可能区域放置了手指时,由生物体有无检测用照明 LED608 检测放置了物体(手指)的情况(步骤 1102),调查物体(手指)是否是生物体(步骤 1103)。当插入的物体(手指)不是生物体时,生物体认证失败(步骤 1104)。当插入的物体(手指)是生物体时,由生物体取得用照明 LED609 向生物体照射近红外线,由图像传感器 607 取得生物体图像(指静脉图案),存储在存储部 606 中(步骤 1105)。

[0103] 接着,从生物体图像(指静脉图案)抽出表示特征性数据的生物体特征量(步骤 1106)。在此,将优先顺序 N 设定为 [1](步骤 1107)。然后,通过用认证控制中间件 702 的指示来执行认证数据生成程序 709,生成在图 8 说明的优先顺序 N(N = 1) 的认证数据(步骤 1108)。然后,向认证控制中间件 702 发送生成的优先顺序 N(N = 1) 的认证数据,存储在认证数据缓冲存储器 706。

[0104] 认证控制中间件 702 执行 IC 卡控制程序 704,向 IC 卡 105 发送存储在认证数据缓冲存储器 706 的优先顺序 N(N = 1) 的认证数据,同时向 IC 卡 105 内的认证程序 711 发出生物体认证指示(步骤 1109)。另一方面,IC 卡 105 执行存储在卡内的认证程序 711,对照预先登录在 IC 卡 105 中的优先顺序 N(N = 1) 的登录数据、和存储在上述认证控制中间件 702 的认证数据缓冲存储器 706 的优先顺序 N(N = 1) 的认证数据,进行生物体认证处理,生成优先顺序 N(N = 1) 的认证结果数据。

[0105] 然后, IC 卡 105 向认证控制中间件 702 发送优先顺序 N(N = 1) 的认证结果数据, 认证控制中间件 702 存储到认证控制中间件 702 内(作为硬件是 RAM 内)的认证结果数据缓冲存储器 705。在此地由认证控制中间件 702 实施的生物体认证机构部 508 和 IC 卡 105 之间的数据收发控制中, 从生物体图像(指静脉图案)取得的生物体特征量不会输出到生物体认证机构部 508 的外部, 而且, 登录在 IC 卡 105 中的认证数据也不会输出到外部。由此, 可以防止个人信息泄漏到装置外部, 所以保护了个人信息的保密性并提高了安全性。

[0106] 认证控制中间件 702 执行生物体认证机构部控制程序 703, 向生物体认证机构部 508 发送存储在认证结果数据缓冲存储器 705 的优先顺序 N(N = 1) 的认证结果数据(步骤 1110), 并且向认证结果判定程序 710 发出认证结果判定指示。接着, 执行认证结果判定程序 710, 根据在 IC 卡 105 内进行的认证结果、即存储在认证结果数据缓冲存储器 705 的优先顺序 N(N = 1) 的认证结果数据, 判断生物体认证是成功还是失败。

[0107] 在此, 作为输出, 生物体认证机构部 508 在认证成功时, 向认证控制中间件 702 通知在生物体的哪一部位认证成功了。例如, 如果生物体认证的部位是指静脉、指纹等, 就向认证控制中间件 702 通知在哪个手指(例如、右手中指等)认证成功了, 如果是手掌的静脉, 则通知是右手还是左手, 如果是眼睛的彩虹, 则通知是在右眼和左眼的哪一个认证成功了。另一方面, 认证失败时, 用认证结果判定程序 710 判断在 IC 卡内认证失败的原因, 并通知给认证控制中间件 702。作为原因, 例如附加手指放置方法是否不好、是否放置了登录的其它手指等的信息, 向认证控制中间件 702 通知, 基于此希望由认证控制应用程序 710 在操作部 503 显示其原因, 由此, 可以提供操作性良好的装置。这样, 利用生物体认证机构部 508 判别认证结果的例子作了说明, 但也可以是 IC 卡内的认证程序 711、或者取得了认证结果数据的认证控制中间件 702 进行认证处理的成功与否、认证成功部位、认证失败原因等认证结果的判别的方式。

[0108] 接着, 认证控制中间件 702 向认证控制应用程序 701 发送优先顺序 N(N = 1) 的登录数据和优先顺序 N(N = 1) 的认证数据的匹配及对照结果, 即优先顺序 N(N = 1) 的认证结果数据。认证控制应用程序 701 判断优先顺序 N(N = 1) 的认证结果数据是成功还是失败(步骤 111)。若认证结果数据是成功, 结束生物体认证处理。若认证结果数据是失败, 则判断登录在 IC 卡 105 的对应于根数的生物体认证是否结束(步骤 1112)。若对应于登录根数的生物体认证已经结束, 则结束生物体认证处理。若对应于登录根数的生物体认证没有结束, 则在优先顺序 N(N = 1) 加上 1, 作为优先顺序 N(N = 2)(步骤 1113), 再次转移到步骤 1108 ~ 步骤 1112, 判断优先顺序 N(N = 2) 的手指的认证结果数据是成功还是失败, 若是失败, 则判断对应于登录根数的生物体认证是否结束。这样, 重复步骤 1108 ~ 步骤 1112, 按照优先顺序高的顺序, 继续进行认证, 直到登录的根数结束。此时, 希望认证控制中间件 702 在前处理数据缓冲存储器 707 继续保存由 IC 卡 105 的登录信息取得处理取得的前处理数据, 可以省略 IC 卡 105 的登录信息取得处理, 所以提高认证处理时间。为了进行从查询余额到支付交易这样的仅一次来店时需要连续的本人确认的交易, 而执行多次的认证处理的情况下, 同样地通过不从前处理数据库 707 删除从 IC 卡 105 取得的前处理数据, 省略 IC 卡 105 的登录信息取得处理, 可以执行连续交易时的认证处理。

[0109] 在此, 作为在上述步骤 111 认证结果数据是成功的例子, 说明了图 13 的优先顺序不变更的例子。再者, 如在生物体登录处理中也说明的那样, 还可以在图 13 的数据上附加

表示认证成功次数的数据。此时,在上述认证结果数据是成功时,作为一次的计数来计数该成功次数(计数、算账),将其追加到图13的认证成功次数1305,根据认证控制中间件702的指示执行并控制变更优先顺序的变更处理。由此,对于优先顺序完全不变更的例(只使用图13的1301时),还可以构筑使用方便的装置、系统。但是,在成为认证成功次数完全相同的状态时,基于最初登录的一方的优先顺序1301进行认证处理。

[0110]而且,在本实施方式中,不显示“请放入右手食指”、“用右手食指认证已成功”、“用右手食指认证已失败。接着请放入右手中指。”等指定了手指种类的指示及结果,而是显示“请放入手指”、“认证已成功”、“认证已失败。请再次放入手指。”等不涉及手指种类的指示及结果,来实施认证。然后,在认证控制应用程序701接受到认证失败的结果时,按优先顺序高的顺序自动地指定不同的登录手指,再次向认证控制中间件702请求认证处理,在所有的登录手指的认证失败时,首次向利用者发出认证失败的通知。由此,在操作部503的画面上不显示用于认证的手指的种类,所以万一不是卡主人的第三者以伪造等犯罪为目的想知道登录了哪一手指时,可以进行防止。

[0111]但是,也可以在操作部503的画面上显示包含手指种类的指示、认证结果。若这样做,利用者可以经常确认登录了哪一手指、在认证时使用哪一手指进行操作,所以对利用者来说使用方便,成为心理上可以安心的结构。

[0112]利用图12说明图9的S914所示的认证交易结束处理。

[0113]若认证结果数据是认证成功,认证控制应用程序701向认证控制中间件702发出认证交易结束指示。认证控制中间件702执行IC卡控制程序704,执行与IC卡105的切断处理。与IC卡105的切断是指,不能对IC卡105进行访问的状态。与IC卡105切断后,在来自认证控制中间件702的指示下,生物体认证装置控制程序703从所有存储部删除位于生物体认证机构部508的生物体特征量等使用于生物体认证的个人信息、和基于此生成的涉及认证的信息。

[0114]这是为了防止个人信息等向外部泄漏,提高安全性的有效的特征。清除了生物体认证机构508内的数据后,认证控制中间件702删除存储在自身具有的认证结果数据缓冲存储器705、认证数据缓冲存储器706、前处理数据缓冲存储器707的信息(除去连续交易),防止信息泄漏。当认证交易结束处理结束时,进行支付金额的输入、与服务器502的通信,结束支付交易。

[0115]以上,如使用图1~4说明了生物体信息的登录处理、使用图5~12说明了生物体信息的认证处理的那样,例如,在硬件上通过CPU601、主存储部602的控制及处理,执行生物体信息的认证,在软件上通过认证控制软件622、认证控制应用程序701、认证控制中间件702的控制及处理,执行生物体信息的认证。由此,如上所述,汇总这些可以称为控制部、控制单元的控制及处理,还可以用LSI等硬件来实现各程序的功能。而且,图7的各种程序不仅在其处理所需时开始启动、执行,在ATM启动时启动各程序,在各处理中执行必要的程序,这样做可以缩短处理时间。

[0116]而且,在图3中,说明了从生物体特征量生成前处理数据,利用该生成的前处理数据和生物体特征量来生成认证时使用的登录数据的方式,但是,也可以是,前处理数据的生成与生物体特征量完全无关联,或者独立地生成。如上所述,在生物体信息的登录时,前处理数据具有用于生成登录数据的密码密钥(或算法)的功能,在生物体认证时,具有用于生

成认证数据的密码密钥的功能及作用。因此,如果从生物体特征量生成前处理数据,即成为对应各个利用者的数据,可以构成安全性高的数据生成算法,但是,另一方面,如果与生物体特征量相独立地生成前处理数据,还可以预先制作具有密码密钥的作用的前处理数据自身,作为整体成为简易的程序构成,所以减少时间,缩短登录及认证的处理时间。

[0117] 而且,在一个阶段从生物体特征量生成了前处理数据,但是,也可以在几个阶段生成。由此,即使第三者要解析前处理数据生成过程,但因生成过程复杂,所以不容易解析,而且,还具有需要解析时间的效果。

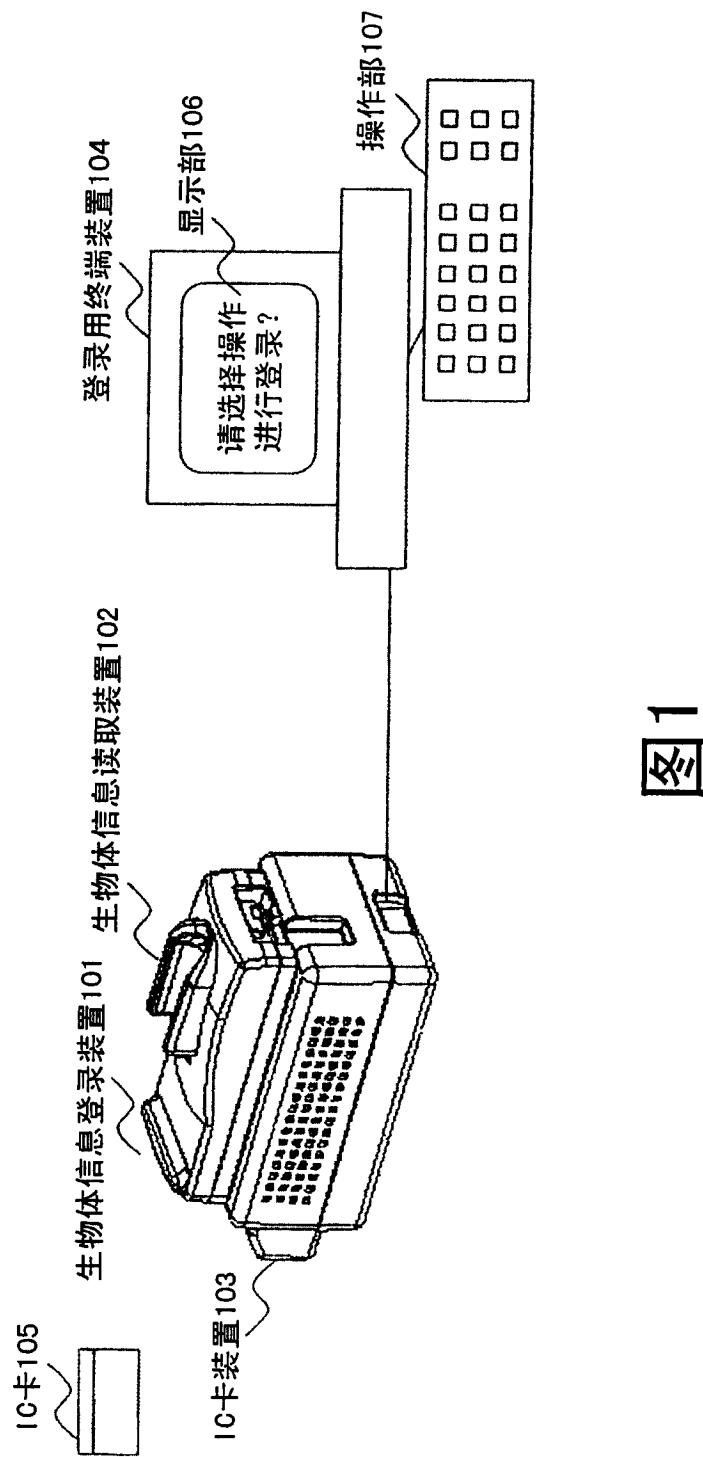
[0118] 而且,前处理数据、登录数据、认证数据(包含认证失败或连续交易时生成的认证数据)原本是从利用者的手指等生物体特征量(包含图像图案)制作并生成的信息,可以称为第一、第二、…(生物体)信息。即,这些第一、第二、…(生物体信息)也可以说是从包含生物体特征量的概念、即生物体信息得到的信息。

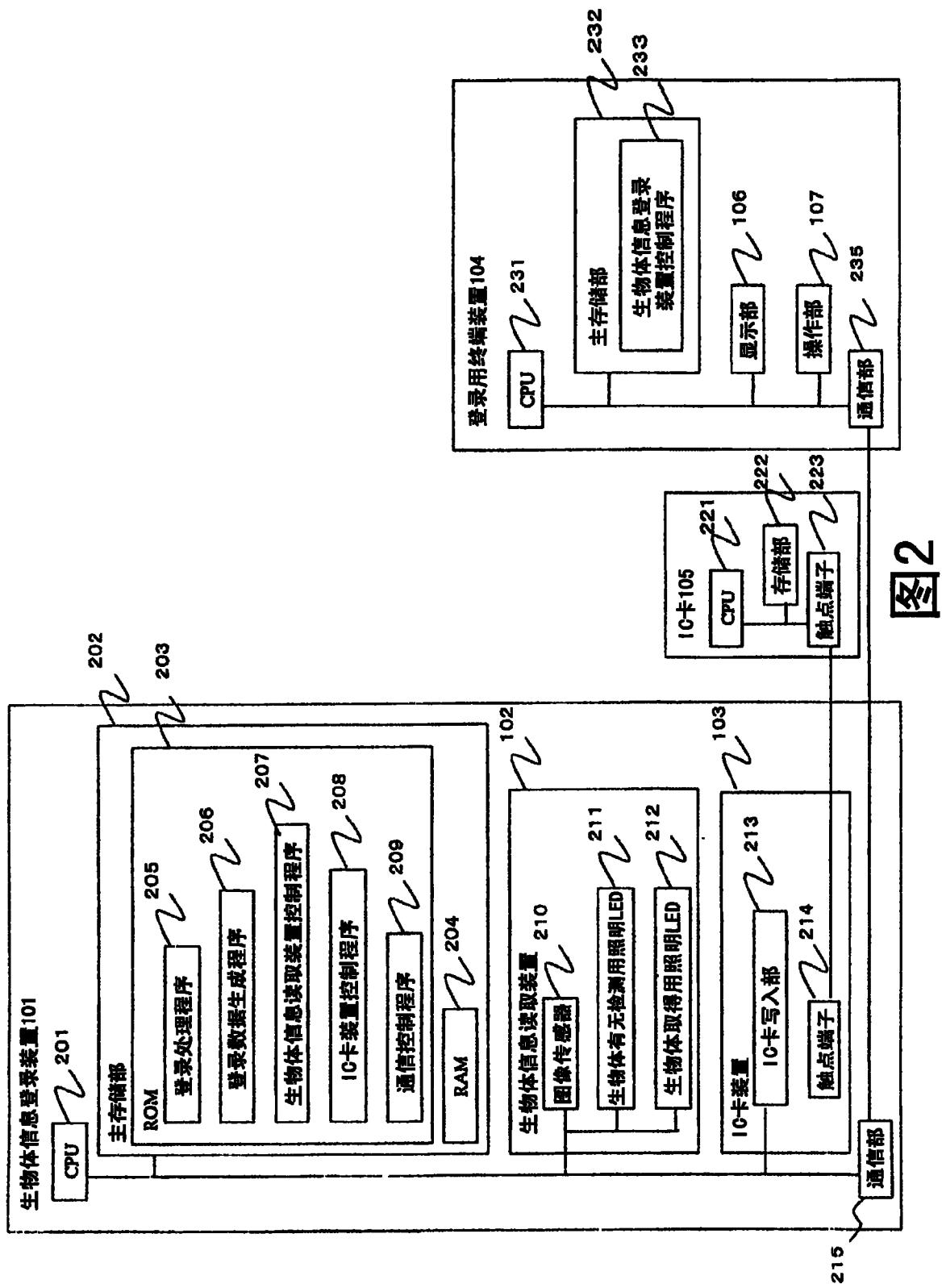
[0119] 如以上说明,在本发明的IC卡内认证方式中,登录在IC卡内的可以确定个人信息、和由认证装置取得的生物体信息(生物体特征量),不会被取入到认证装置搭载终端,所以保护了个人信息的隐秘性,能够实现安全性高的生物体认证成。

[0120] 并且,在本发明的登录生物体信息优先顺序附加认证方式中,利用者对预先登录的多个生物体信息附加优先顺序,通过按照优先顺序高的顺序执行认证处理,可以缩短认证处理。

[0121] 而且,在此前的生物体信息附加优先顺序的生物体认证中,具有基于上次使用的手指在下次使用的可能性最高的使用实绩来重新排列该优先顺序的优先顺序变更技术。但是,在该变更技术中登录了五个生物体信息(五根不同的手指),并且过去的认证成功次数对每根手指不同时(认证成功次数:拇指0次、食指70次、中指15次、无名指10次、小指5次),如果一旦在认证中使用过去的认证成功次数少的手指(拇指等),则在下次使用通常使用次数多的手指(食指等)进行认证时,在通常使用次数多的手指的对照前必须进行认证成功次数少的手指的对照,所以不方便。

[0122] 与此相比,即使是与上述的课题中例举的状况相同的状况(认证成功次数:拇指0次、食指70次、中指15次、无名指10次、小指5次),本发明基于认证成功次数附加优先顺序,所以在拇指认证前后、无名指认证前后,始终是第一位食指、第二位中指、第三位无名指、第四位小指、第五位拇指的顺序。在此,如果下一次要用食指进行认证,则优先顺序是第一位,所以不必进行无用的手指的对照,可以在短时间实施认证。





总2

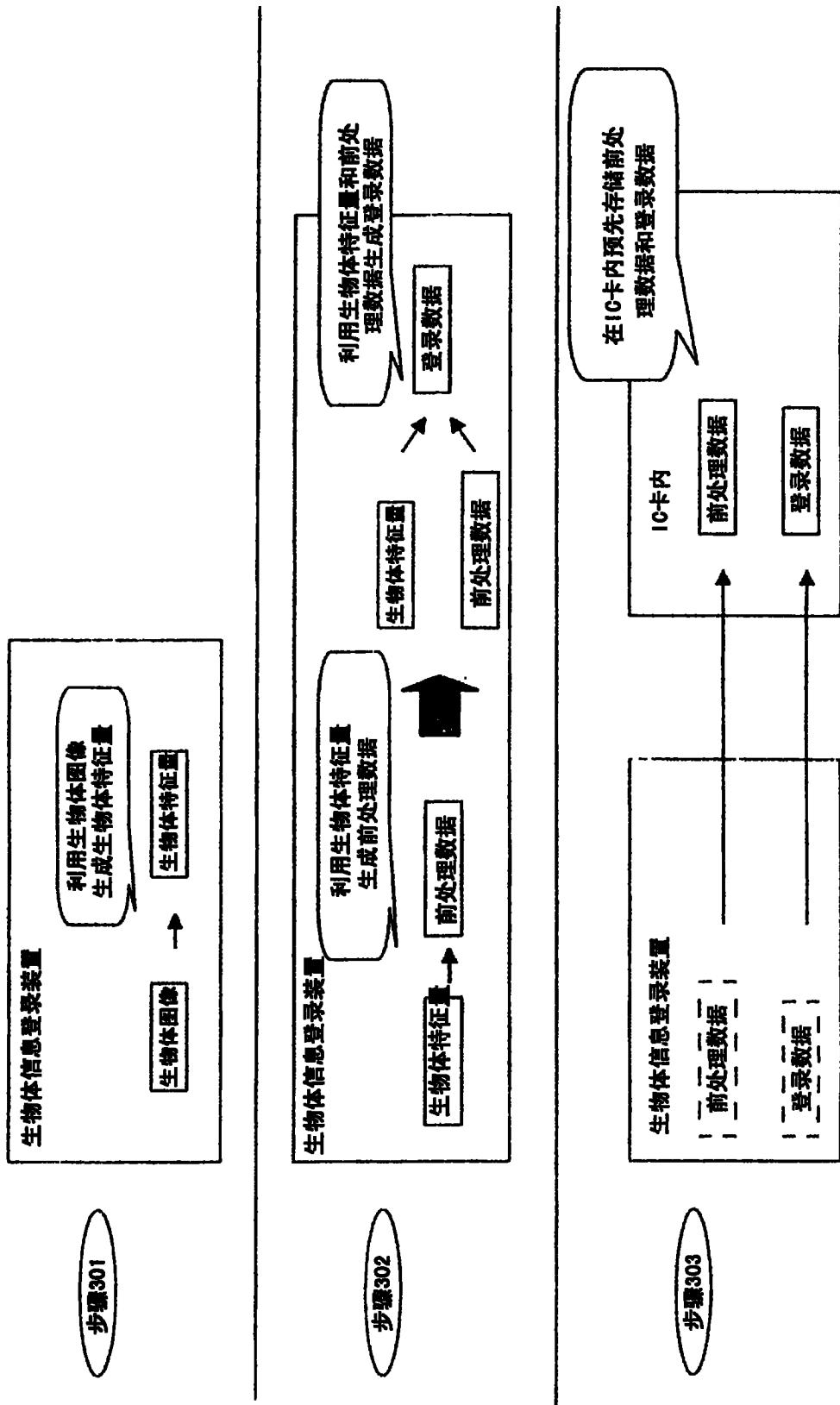
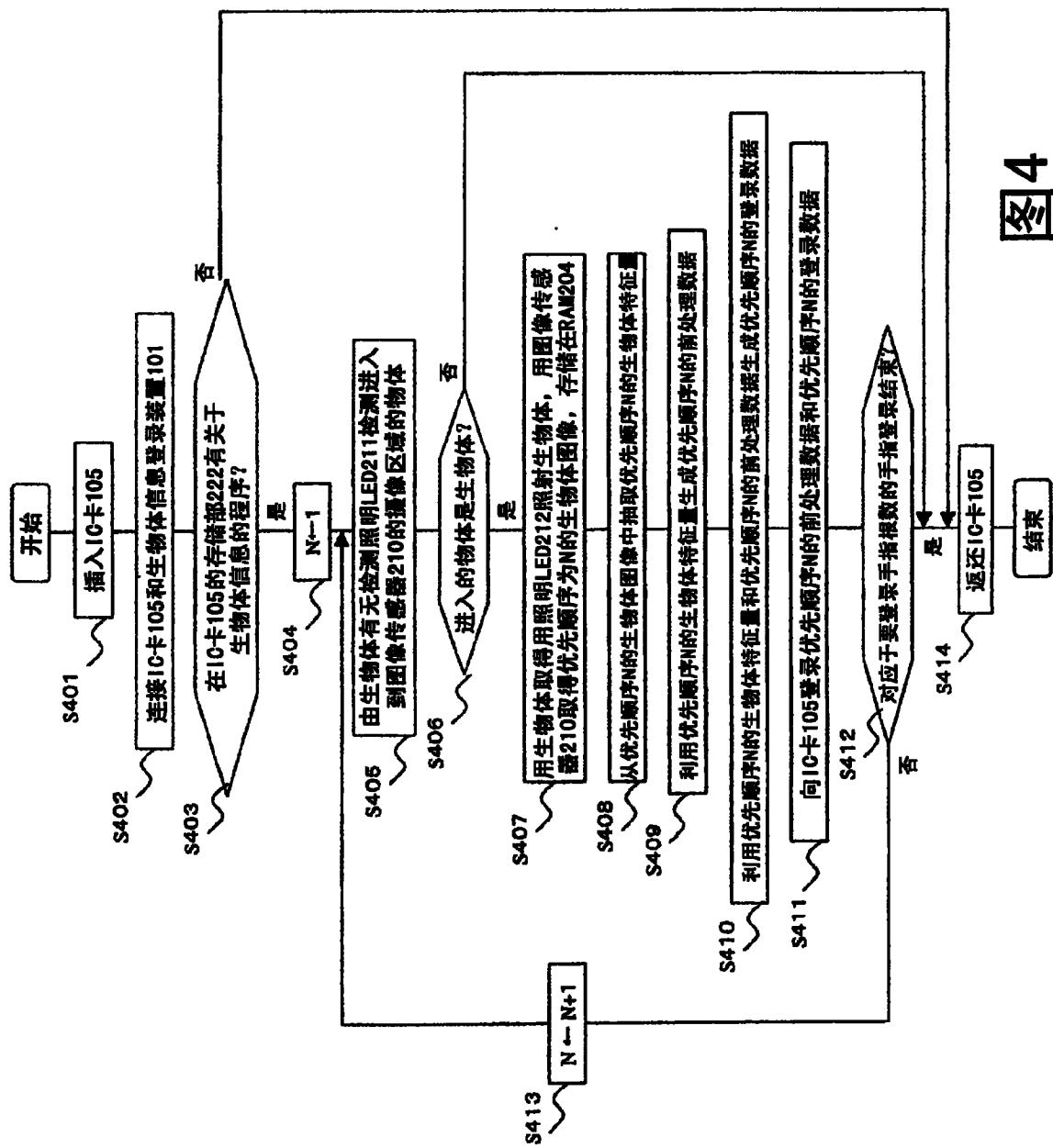


图3



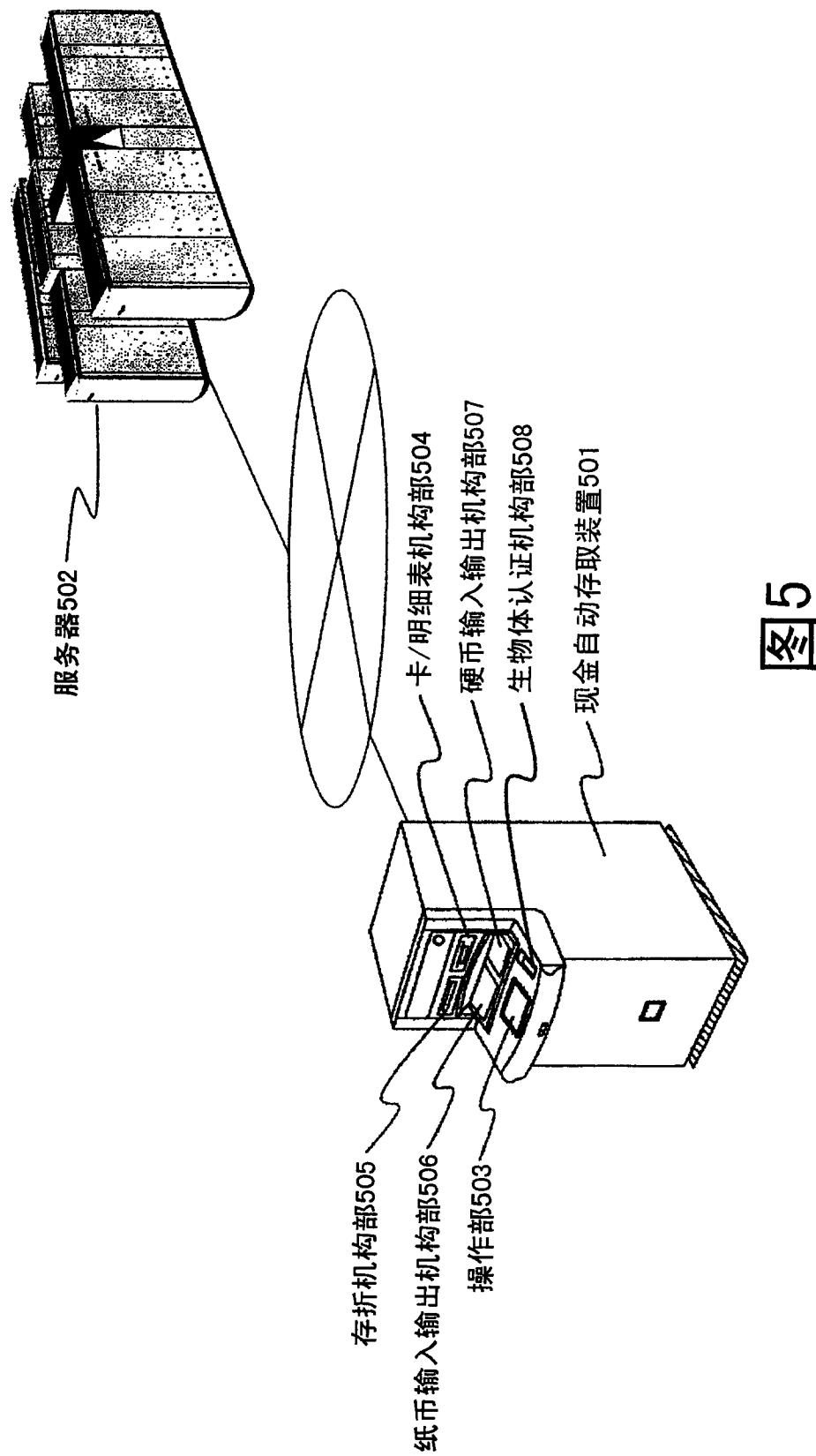


图 5

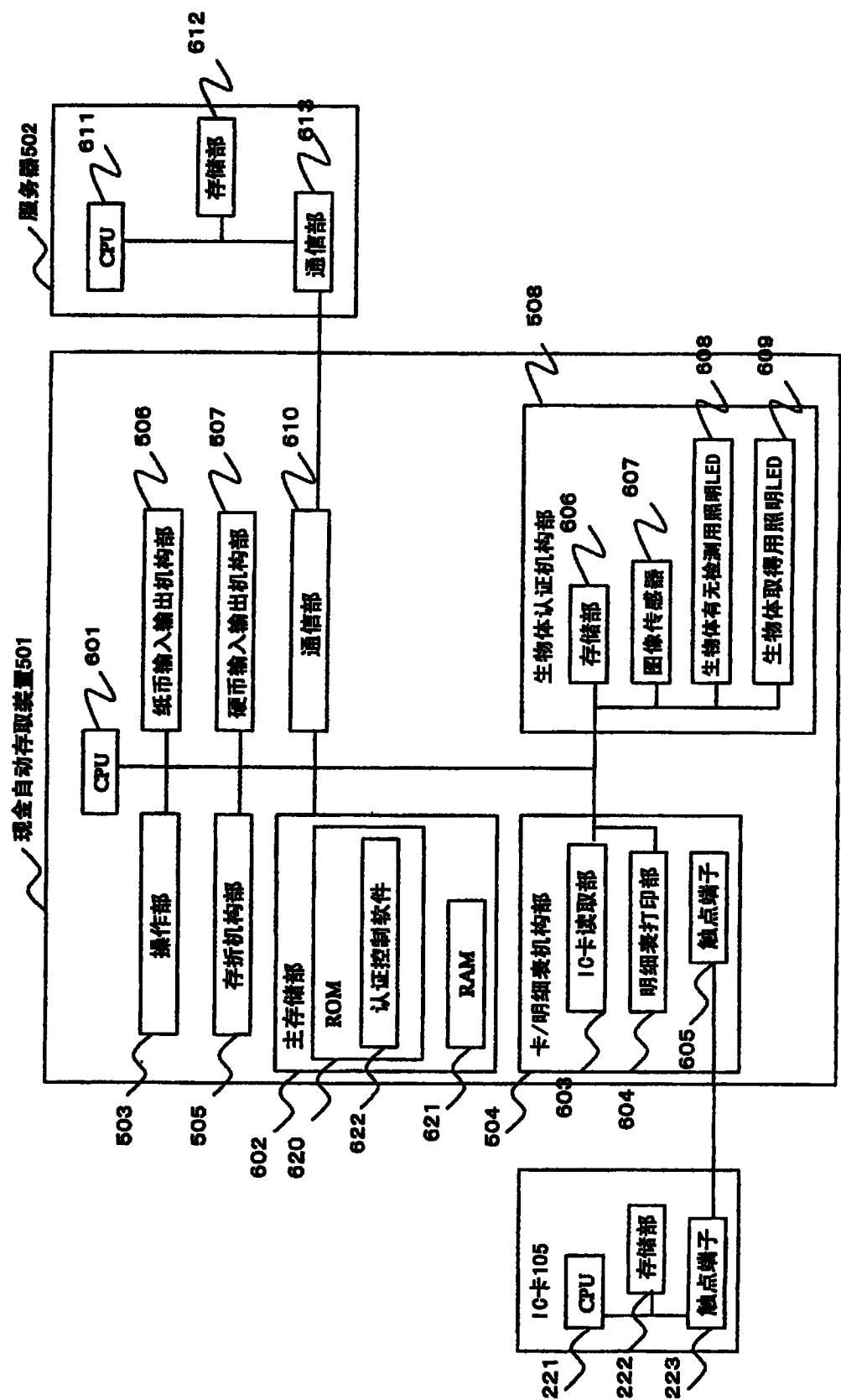
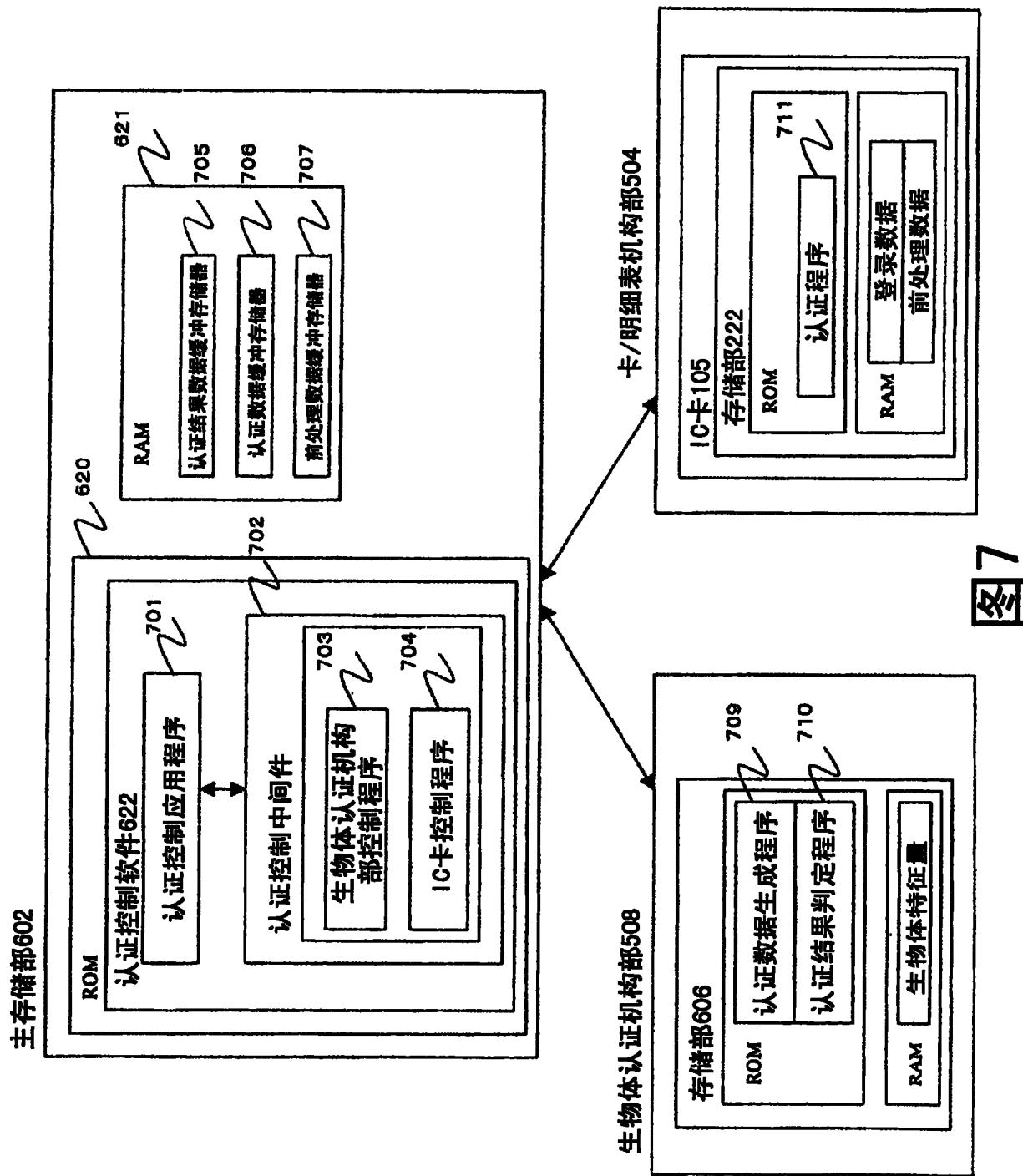


图 6



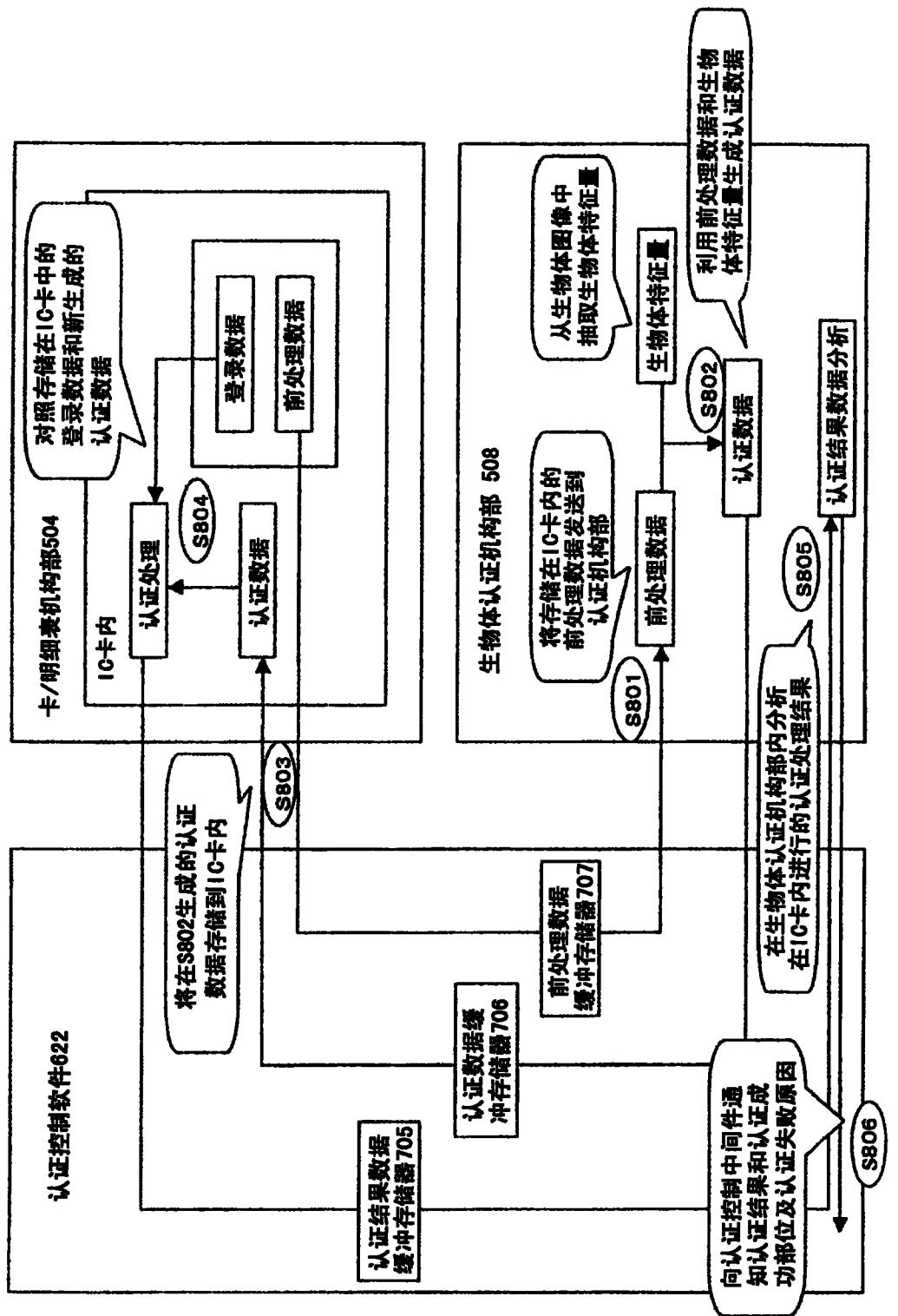
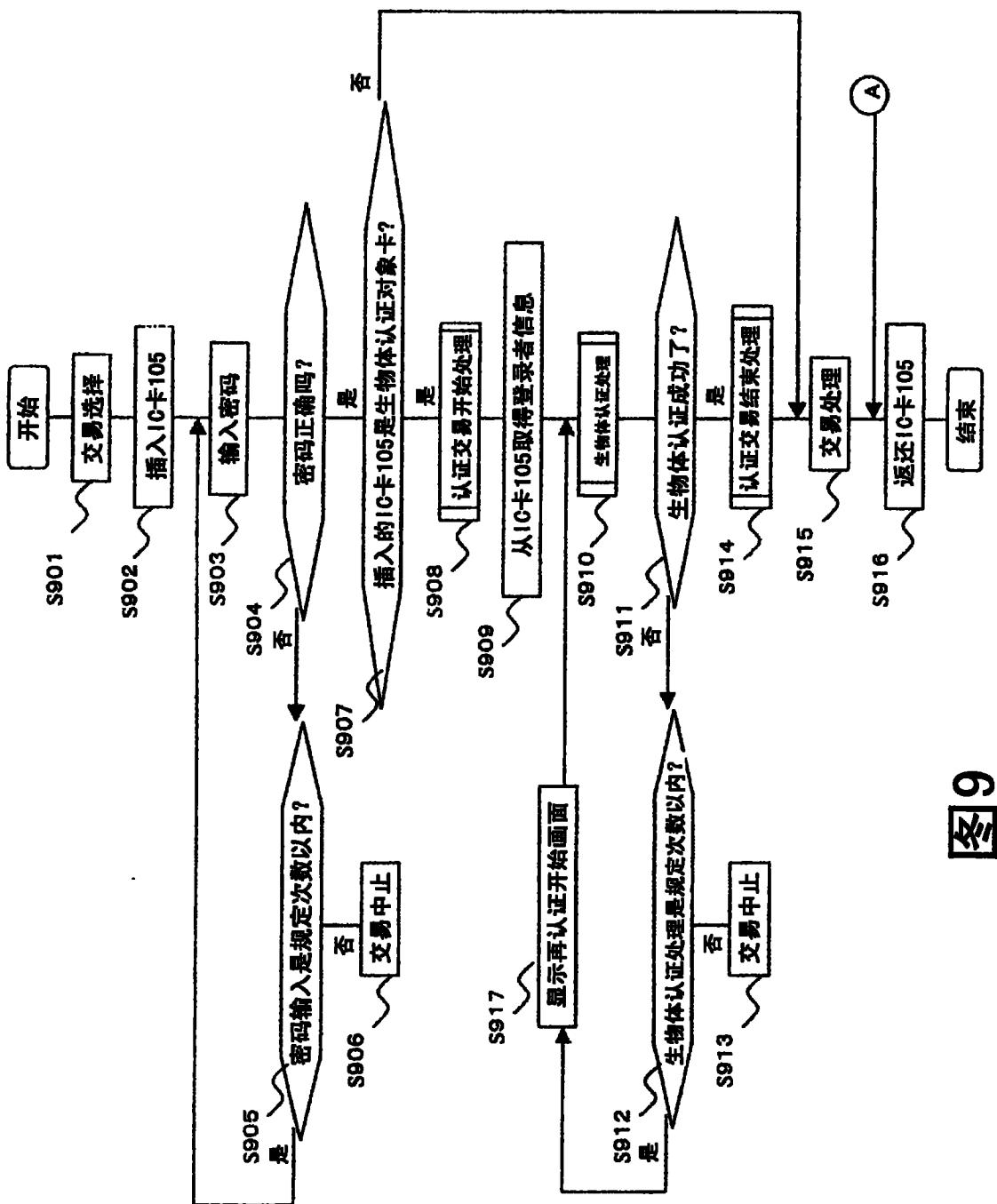


图8



卷9

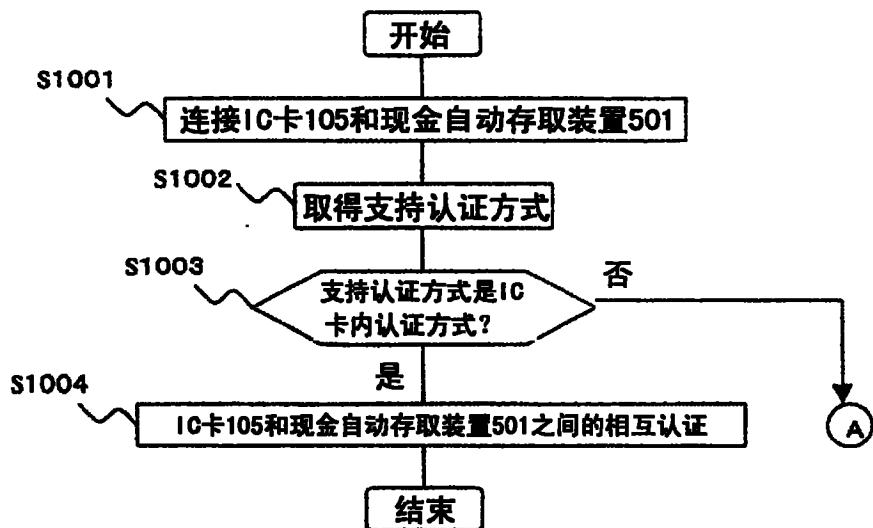
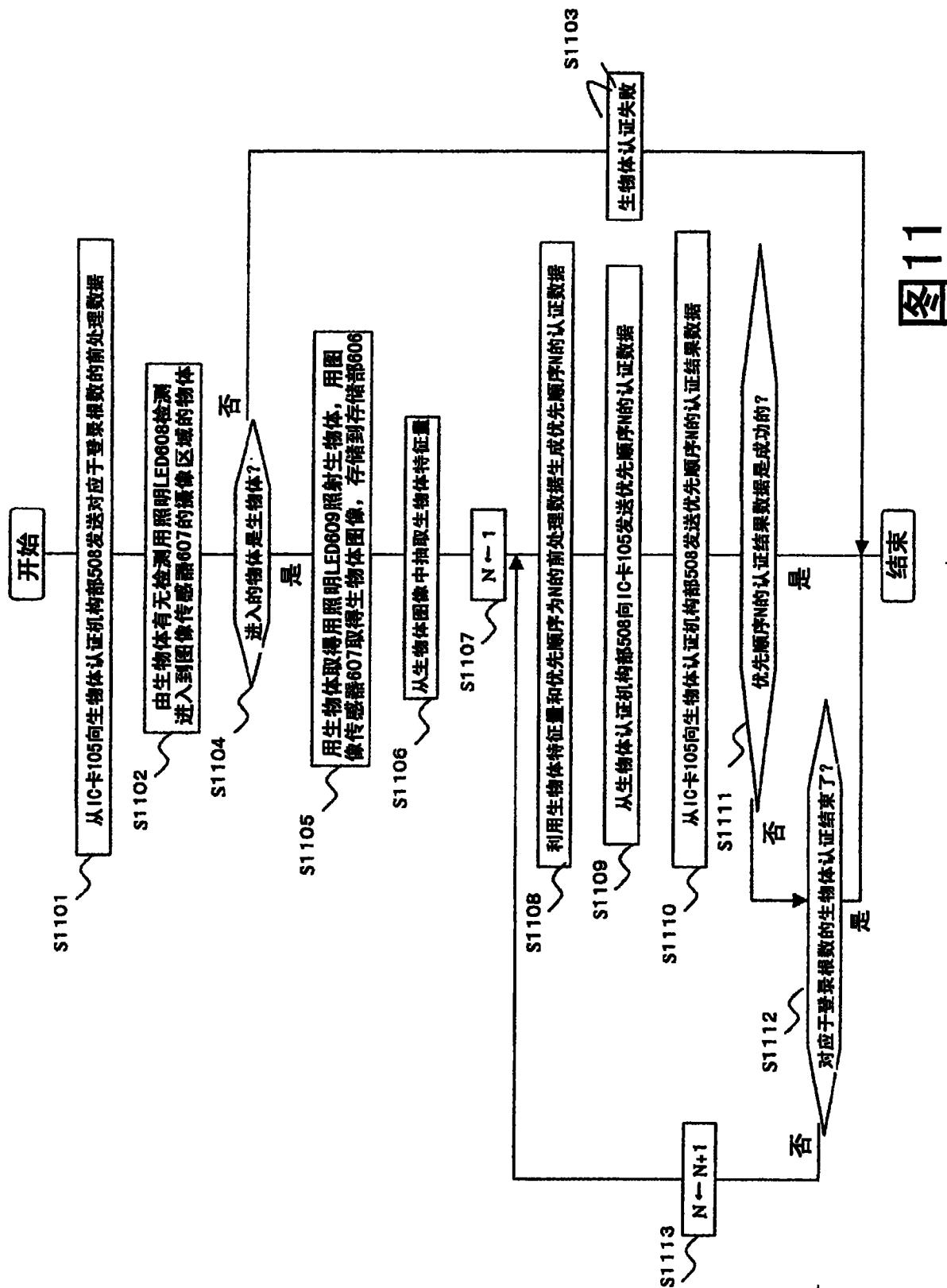


图10



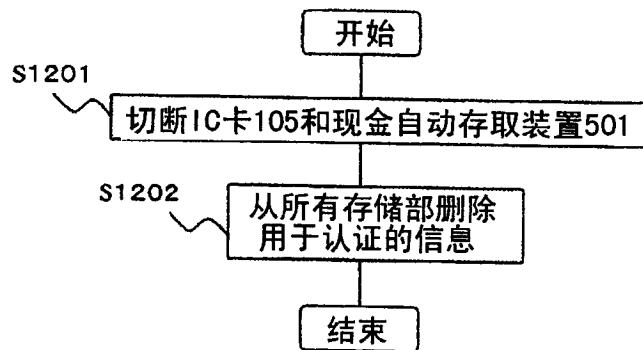


图12

优先顺序	手指种类	前处理数据	登录数据	认证成功次数
1	右手 食指	前处理数据	登录数据	15
2	右手 中指	前处理数据	登录数据	5
3	右手 无名指	前处理数据	登录数据	2
4	左手 食指	前处理数据	登录数据	1
5	左手 中指	前处理数据	登录数据	0
6	左手 无名指	前处理数据	登录数据	0

图13