

# [12] 发明专利申请公开说明书

[21] 申请号 00135387. X

[43] 公开日 2001 年 6 月 13 日

[11] 公开号 CN 1299113A

[22] 申请日 2000. 12. 8 [21] 申请号 00135387. X

[30] 优先权

[32] 1999. 12. 8 [33] JP [31] 348268/1999

[71] 申请人 日本电气株式会社

地址 日本东京都

[72] 发明人 内田薰

[74] 专利代理机构 中国专利代理(香港)有限公司

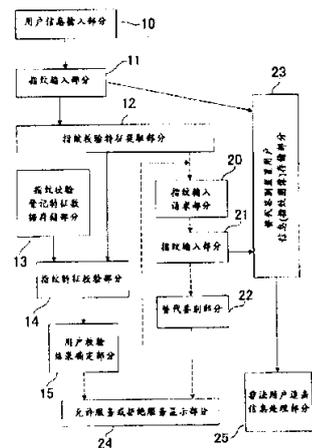
代理人 吴增勇 傅康

权利要求书 3 页 说明书 13 页 附图页数 6 页

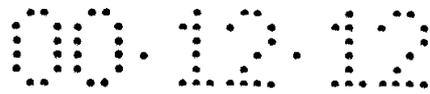
[54] 发明名称 利用生物测量学的用户鉴别设备及用户鉴别方法

[57] 摘要

公开了一种用户鉴别设备,藉此即使在某些用户的生物测量输入数据质量低下,因而不适宜于校验的地方,也能在不因为引入重大的附加硬件而造成成本上升的情况下,提高整个系统的安全性。当指纹校验特征提取部分判定指纹图像的质量不够高时,或当由用户校验结果判定部分基于输入的指纹进行的鉴别失败时,从指纹输入请求部分向用户发出输入指纹的请求。当从指纹输入部分完成需要的指纹输入时,允许用替代鉴别部分进行替代鉴别。



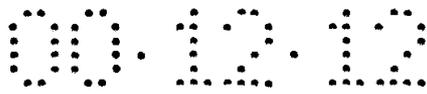
ISSN 1008-4274



## 权 利 要 求 书

---

1. 一种用户鉴别设备，它包括：  
鉴别装置，用来通过校验作为个人所特有的生物特征的用户生物  
5 测量量度来鉴别用户；  
采集装置，可在所述鉴别装置校验生物测量量度的所述鉴别失败  
时工作，用来采集请求所述鉴别的所述用户的生物测量数据；和  
替代鉴别装置，当用所述采集装置采集所述生物测量数据时，用  
来代替所述生物测量量度的校验。
- 10 2. 权利要求 1 的用户鉴别设备，其特征在于还包括：存储装置，  
用来存储所述采集装置所采集的生物测量数据；和处理装置，用来根  
据存储在所述存储装置中的生物测量数据进行对非法用户的搜索和追  
击。
- 15 3. 权利要求 1 的用户鉴别设备，其特征在于还包括：判断装置，  
用来判断为生物测量数据校验而输入的生物测量数据是否具有适合于  
自动校验的质量；和一种可在判定生物测量数据不具有适合于自动比  
较的质量时工作的装置，用来存储所采集的生物测量数据。
- 20 4. 权利要求 3 的用户鉴别设备，其特征在于还包括一种可在判  
定生物测量数据不具有适合于自动比较的质量时工作的装置，用来判  
断所述生物测量数据是否适用于对非法用户的搜索和追击，而且其中  
当判定所述生物测量数据适合于对非法用户的搜索和追击时，允许使  
用所述替代鉴别装置。
- 25 5. 权利要求 4 的用户鉴别设备，其特征在于：所述生物测量数  
据是否适用于对非法用户的搜索和追击的判断是根据输入的生物测量  
数据是否适当、而且是否由用户就地输入的来判断的。
6. 权利要求 5 的用户鉴别设备，其特征在于：测量所述采集装  
置所采集的多个生物测量数据的相关性，以进行所述生物测量数据是  
否由用户就地输入的判断。



7. 权利要求 1 的用户鉴别设备，其特征在于：至少指纹用作所述生物测量量度。

8. 权利要求 1 的用户鉴别设备，其特征在于：在替代鉴别之前存储所述生物测量数据时，在输入指纹时拍摄面部或/和身材的图像。

5 9. 一种用户鉴别方法，它包括以下步骤：

通过校验作为个人所特有的生物特征的生物测量量度来鉴别用户；

当在所述生物测量量度的所述校验中所述鉴别失败时，采集请求鉴别的用户的生物测量数据；以及

10 当用所述采集装置采集所述生物测量数据时进行用来代替生物测量量度的校验的替代鉴别。

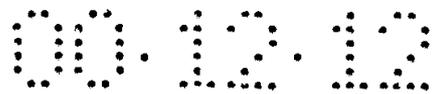
10. 权利要求 9 的用户鉴别方法，其特征在于还包括存储所述采集生物测量数据的步骤中采集的所述生物测量数据，并根据所述存储的生物测量数据进行对非法用户的搜索并追击的步骤。

15 11. 权利要求 9 的用户鉴别方法，其特征在于还包括：判断为准备用来进行生物测量学校验而输入的生物测量数据是否具有适合于自动校验的质量的步骤；和当判断所述生物测量数据不具有适合于自动比较的质量时存储所采集的生物测量数据的步骤。

20 12. 权利要求 11 的用户鉴别方法，其特征在于还包括当判断所述生物测量数据不具有适合于自动比较的质量时判断所述生物测量数据是否具有适用于对非法用户的搜索和追击用的质量的步骤，以及当判断所述生物测量数据适用于对非法用户的搜索和追击时，允许使用替代鉴别。

25 13. 权利要求 12 的用户鉴别方法，其特征在于：所述生物测量数据是否适用于对非法用户的搜索和追击的判断是根据所述生物测量数据是否适当而且是由所述用户就地输入的来判断的。

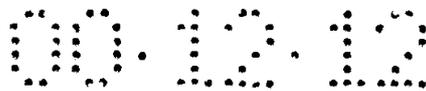
14. 权利要求 13 的用户鉴别方法，其特征在于：测量在所述生物测量数据采集步骤中所采集的多个生物测量数据的相关性，以便判断



断所述生物测量数据是不是由用户就地输入的。

15. 权利要求9的用户鉴别方法，其特征在于：至少指纹用作所述生物测量量度。

16. 权利要求9的用户鉴别方法，其特征在于：在所述替代鉴别  
5 之前存储所述生物测量数据时，在输入指纹时至少拍摄面部和/或身材  
的图像。



## 说明书

### 利用生物测量学的用户 鉴别设备及用户鉴别方法

5

本发明涉及使用生物测量学的用户鉴别设备及用户鉴别设备用的用户鉴别方法，更详细地说，涉及一种方法，其中在门禁的人身通行管理时或在诸如个人计算机等终端上进行信息存取管理时，使用诸如指纹等生物测量学对用户本身进行鉴别。

10

在传统上，用户鉴别方法用来确认管理门禁人身通行等或在诸如个人计算机等终端上管理信息访问权限的用户是否该用户本人。

在用户鉴别方法中，除了根据用户持有诸如磁卡等他所持有的物件或者根据用户是否知道诸如个人标识号码或密码等机密信息来完成鉴别的方法以外，还使用基于生物测量学的鉴别。

15

基于生物测量学的鉴别利用诸如指纹等每一个个人所特有的生物特征。指纹是人类手指头的皮肤图案。已经知道，指纹具有“不同的人指纹不同”和“指纹至死不变”的特征。即使指头的表皮被破坏，从表皮内部的不变的真皮也会使同样的指纹恢复原状。因此，把指纹作为能够准确鉴别个人的生物测量量度，已广为人知。

20

例如，在有人要求进入时的用户鉴别过程中，便要求该个人输入其指纹。输入指纹时，可以按如下方式使用指纹。更详细地说，若指纹与登记的指纹一致，则允许进入，但若指纹与登记的指纹不一致，则判定该个人是非法用户，因而该个人的进入不被允许。

25

在使用基于拥有的物件的鉴别的办法，检到该拥有的物件的不相关的个人就可以使用它。另外，在使用基于知识的鉴别的办法，若一个偷看了或对知识进行随机猜测的人输入该知识，则他将取得非法的进入许可。相反，按照基于生物测量学的方法，可实现真正个人本人才能得到鉴别的功能。

例如，在日本公开特许公报 No.33065/1992 公开了如上所述这样的技术。

在上述传统的用户鉴别方法中，在使用一个其中输入诸如指纹等生物测量量度并将其与登记的校验特征比较来确认个人本身的系统的地方，不能忽视存在这样的用户：当指纹图像的质量由于手指干燥或手指受损等而下降时其登记或校验不能顺利通过。

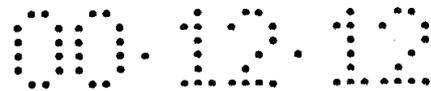
当指纹登记或校验不能顺利通过时，例如，一般采用诸如输入密码等代替另一种鉴别方法的规避办法。按照这种方法，输入指纹，而若它不具有足以允许进行自动校验的质量，则放弃基于指纹的自动校验方法，从键盘输入密码作为替代措施。但是，在使用密码的地方，如上所述，不相关的个人可以通过偷看等装扮成个人本人。这成了整个系统的安全漏洞，这是上述方法的缺点。

很自然，在指纹不适用于自动鉴别的方面，例如，另外使用基于诸如虹膜等某些其他的生物测量量度的校验是一种可能的主意。但是，在这种情况下，安装和操作诸如照相机等虹膜图像输入设备、获得稳定的图像用的照明系统等需要额外费用，因而无法避免成本增大。

本发明的一个目的是提供一种用户鉴别方法和用户鉴别设备，藉此即使在某些用户的生物测量输入数据，诸如指纹等质量低下因而不适用于校验的地方，整个系统的安全也可以提高，而不会因为引入重要的附加硬件而造成成本上升。

为了达到上述目的，按照本发明的一个方面，提供一种用户鉴别设备，它包括：鉴别装置，用来通过校验作为个人所特有的生物特征的用户生物测量量度来鉴别用户；采集装置，可在鉴别装置校验生物测量量度鉴别失败时工作，用来采集请求鉴别的用户的生物测量数据；和替代鉴别装置，当用采集装置采集生物测量数据时，用来代替生物测量量度的校验。

按照本发明的另一个方面，提供一种用户鉴别方法，它包括以下



步骤：通过校验作为个人所特有的生物特征的生物测量量度来鉴别用户；当在生物测量量度的校验中所述鉴别失败时，采集请求鉴别的用户的生物测量数据；以及当用采集装置采集生物测量数据时进行替代鉴别，用来代替生物测量量度的校验。

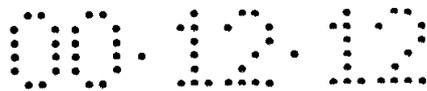
5            用户鉴别方法最好还包括存储采集生物测量数据的步骤中采集的生物测量数据，以及根据所存储的生物测量数据进行对非法用户的搜索和追击。

10           作为替代方案，用户鉴别方法还包括：判断为准备用来进行生物测量量度校验而输入的生物测量数据是否具有适合于自动校验的质量的步骤；和当判别生物测量数据不具有适合于自动比较的质量时存储所采集的生物测量数据的步骤。所述用户鉴别方法还可以包括当生物测量数据被判定为不具有适合于自动比较的质量时判断生物测量数据是否具有适用于对非法用户的搜索和追击用的质量的步骤，而且其中当生物测量数据被判定为适用于对非法用户的搜索和追击时，允许使用替代鉴别。生物测量数据是否适用于对非法用户的搜索和追击的判断可以根据所述生物测量数据是否适当以及是否由用户在使用地点输入的判断。可以测量在生物测量数据采集步骤中采集的多个生物测量数据的相关性，以便进行所述生物测量数据是否由用户就地输入的判断。

20           至少指纹可以用作生物测量量度。

             在替代鉴别之前存储生物测量数据时，在可以输入指纹时至少拍摄面部和/或身材的图像。

25           在用户鉴别设备和用户鉴别方法中，若通过生物测量学校验的鉴别失败，则采集请求鉴别的用户的生物测量数据，并在采集了用户的生物测量数据之后替换生物测量学的校验。因此，当后来发现进行门禁管理的非法通行或计算机系统的非法登录时，便可以详细描述非法装扮的个人。因此，用户鉴别设备和用户鉴别方法的优点是，即使在某些用户的生物测量输入数据、例如指纹的质量低下，因而不适合于



进行校验的地方，整个系统的安全便得以提高，而不会由于引入重要的附加硬件而使成本提高。

从结合附图而作的以下的描述和后附的权利要求书中，本发明的上述和其他目的、特征和优点将变得显而易见，附图中类似的部分或要素用类似的标号表示。

图 1 是表示采用本发明的用户鉴别设备的配置的方框图；

图 2 和 3 是举例说明图 1 的用户鉴别设备的操作的流程图；

图 4 是表示采用本发明的另一种用户鉴别设备的配置的方框图；

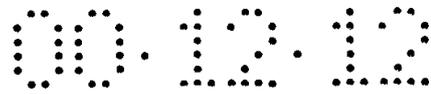
图 5 和 6 是举例说明图 4 的用户鉴别设备的操作的流程图。

首先参见图 1，其中示出采用本发明的用户鉴别设备的配置。在本实施例的用户鉴别设备中，使用指纹作为生物测量量度。应该指出，图 1 中虚线表示处理程序(控制)的流程，而实线表示诸如指纹等数据的流程。

用户鉴别设备包括用户信息输入部分 10、指纹输入部分 11、指纹校验特征提取部分 12、指纹校验登记特征数据存储部分 13、指纹特征校验部分 14、用户校验结果确定部分 15、指纹输入请求部分 20、指纹输入部分 21、基于输入密码的替代鉴别部分 22、替代鉴别装置用户信息存储部分 23、服务允许或拒绝显示部分(此后简称显示部分)24 和非法用户追击信息处理部分 25。

图 2 和 3 举例说明图 1 的用户鉴别设备的操作，参照图 1 至 3 描述该用户鉴别设备的操作。应该指出，举例示于图 2 和 3 的处理操作可以通过用户鉴别设备的执行存储在用户鉴别设备的未示出的控制存储器中的程序的组件来实现。控制存储器可以是 ROM(只读存储器)、IC(集成电路)存储器或类似的存储器。

从用户信息输入部分 10 输入请求鉴别以便请求提供服务的用户的用户姓名(图 2 的步骤 S1)。输入用户姓名时，从 0~9 数字键输入用户号码或从键盘输入用户识别符或者不然可以为这样的输入使用磁性 ID(标识号码)卡等。



为了输入用户的指纹图像,当用户的手指触及指纹传感器(未示出)时,指纹输入部分 11 拍摄用户的指纹图像。指纹输入部分 11 还把指纹图像的图像数据转换成数字图像数据,以便能够进行用户鉴别设备后来的处理(图 2 的步骤 S2)。

5 作为指纹传感器的配置简图,使用光学系统,其中一般从 LED(发光二极管)发射出来的光被棱镜反射,然后利用 CCD(电荷耦合器件)转换成数字图像。所述转换利用沿放置在棱镜反射面外侧的手指隆起线(ridge)的隆起部分和凹部之间反射系数不同这一事实。

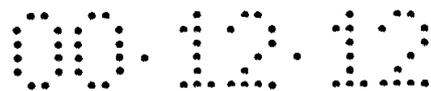
10 指纹校验特征提取部分 12 接收从指纹输入部分 11 获得的指纹图像,并执行从指纹图像提取识别指纹用的特征的处理过程(图 2 的步骤 S4)。

例如,在 the Transactions of The Institute of Electronics,Information, and Communication Engineers of Japan, Vol. J72-D-II, No.5, May, 1989, pp.724-732 “利用特征点网络(minutiae-network)特征的自动指纹识别-特征提取方法-”一文中 Hiroshi Asai, Yukio Hoshino 和 Kazuo Kiji 公开了实现指纹识别用的特征的提取方法。

15 按照该文献公开的方法,通过二进制数字化处理和薄化(thinning)处理从包括隆起线的可变密度图像中提取隆起线图案,并检测任何一条隆起线的终点和分支点的位置。然后,对连接终点和分支点的线段上相交隆起线的数目进行计数,并用数字数据代表关系图,用作校验用的指纹特征。

20 在所述方法中,还计算指纹图像中图像质量高到足以进行特征提取的区域的面积、通过所述特征提取获得的诸如终点和分支点等特征的数目、通过所述自动特征提取处理而加在每一个特征上的可靠性信息以及其他必要的信息,作为附加信息。

25 另外,指纹校验特征提取部分 12 根据特征提取结果判断输入的指纹是否具有适合于使用自动指纹校验的鉴别的质量(图 2 的步骤 S5)。为了允许进行自动指纹校验,指纹隆起线之间的凸的和凹的几何



形状的对比度必须足够大。但是，尤其是当皮肤干燥或者因为皮肤的排汗、损伤、磨损等时，有时不能获得具有要求的质量的指纹图像。在这样的情况下，指纹图像被判断为质量不够高。

5 在实现该判断的现有方法中，一般判断质量高到足以进行特征提取的区域的面积、从特征提取中获得的诸如终点和分支点等各个特征的数目、通过所述自动特征提取处理而加在各个特征的可靠性信息等等指纹校验特征提取部分 12 所获得的一切是否分别地或以组合的形式高于预先为它们确定的阈值。

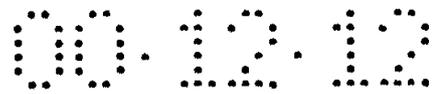
10 指纹校验登记特征数据存储部分 13 把校验用的指纹特征信息和有关作为指纹拥有者的用户的用户特有信息以彼此对应的关系存储起来。用户特有信息包括识别用户的信息和允许向该用户提供的服务的类型、范围等等。

15 若指纹校验特征提取部分 12 判断指纹图像具有足够高的质量，则指纹特征校验部分 14 校验指纹图像，以便检测有关该用户的登记特征是否与输入的指纹特征彼此一致，就是说，是否足够地彼此类似(图 2 的步骤 S6)。

20 指纹特征校验部分 14 接收从用户这次由指纹校验特征提取部分 12 输入的指纹所确定的指纹特征 S。另外，指纹特征校验部分 14 从指纹校验登记特征数据存储部分 13 接收与输入的用户姓名对应的指纹特征信息 F 作为来自此前存储的指纹特征信息范围内的用户信息。然后，指纹特征校验部分 14 把指纹特征信息 F 与指纹特征 S 彼此比较，并计算代表相似性的得分，当这两种类型的信息来自同一手指时所述相似性得分具有高值。

25 指纹特征校验部分 14 把所述得分与预先为此而设置的阈值加以比较，以判断给出该指纹特征 S 的用户与登记的用户是否同一人(图 2 的步骤 S7)。若得分高于阈值，则指纹特征校验部分 14 输出“指纹一致”的识别结果。

例如，在 the Transactions of The Institute of Electronics, Information,



and Communication Engineers of Japan, Vol. J72-D-II, No.5, May, 1989, pp.733-740 “利用特征点网络(minutiae-network)特征的自动指纹识别--校验方法--”一文中 Hiroshi Asai, Yukio Hoshino 和 Kazuo Kiji 公开了实现如上所述地利用指纹校验留下指纹的个人的身份的典型方法。

5           按照此文献所公开的方法，对于校验用的两个指纹中的每一个，对与连接隆起线终点和分支点的线段相交的隆起线数目进行计数，并以数字数据代表。数字数据用于指纹的彼此相对定位，评价它们之间的相似性以实现校验。

10           当校验结果表示输入的指纹与有关该用户的存储的指纹特征足够相似时，用户校验结果确定部分 15 鉴定输入了用户信息的用户是合法用户，并在显示部分 24 上显示允许服务(图2的步骤 S8)。另一方面，当指纹不一致时，用户校验结果确定部分 15 判定鉴别结果失败，拒绝服务，而且指纹输入请求部分 20 随后执行进行替代鉴别的处理。

15           上述处理操作是在指纹校验特征提取部分 12 判定所述质量足以进行自动校验时执行的。但是，另一方面，当指纹校验特征提取部分 12 判定质量不够高时，或者当用户校验结果确定部分 15 进行的输入指纹鉴定得出失败的结果时，指纹输入请求部分 20 向该用户多次发出向指纹传感器输入指纹的请求(图3的步骤 S9 至 S11)。之所以要多次发出输入指纹的请求，理由是意在以此找出和排除伪造指纹的输入。

20           指纹输入部分 21 利用类似于指纹输入部分 11 的类似的方法进行指纹的输入和采集。只有在按照指纹输入请求部分 20 的请求从指纹输入请求部分 21 进行必要的指纹输入时，用户才能进到利用替代鉴别部分 22 进行替代鉴别的下一步骤(图3的步骤 S12)。

25           作为使用替代鉴别部分 22 的替代鉴别方法，一般有从 0~9 数字键或键盘输入个人标识号码或密码的方法，和另一种从磁卡读入以证实持有人身份的方法。若由一个替代鉴别方法判定该用户是合法用户(图3的步骤 S13),则与由上述生物测量学自动校验鉴定出该用户是合法用户时类似，鉴别输入了用户信息的用户是合法用户，因而在显示

部分 24 上显示允许服务(图 3 的步骤 S14)。在其他任何情况下判定鉴别结果失败,因而在显示部分 24 上显示拒绝服务(图 3 的步骤 S15)。

替代鉴别装置用户信息存储部分 23 存储首先从指纹输入部分 11 输入的图像和从指纹输入请求部分 20 发出请求之后从指纹输入部分 21 输入的图像(图 2 的步骤 S3 和图 3 的步骤 S10)。存储的图像在以后需要时由非法用户追击信息处理部分 25 用来搜索和追击非法用户。

现将参见图 4,其中示出应用本发明的另一种用户鉴别设备的配置。按照本实施例的用户鉴别设备具有类似于图 3 中所示的用户鉴别设备的配置,但又与之不同:它还包括输入图像性能判别部分 26。公共组件以与第一实施例的用户鉴别设备相似的方式操作,故对其描述从略,不再赘述。

图 5 和 6 举例说明图 4 的用户鉴别设备的操作,现将参考图 4 至 6 描述该用户鉴别设备的操作。应该指出,举例示于图 5 和 6 的处理操作可以用该用户鉴别设备中执行存储在该用户鉴别设备的未示出的控制存储器的程序的组件来实现。所述控制存储器可以是 ROM、IC 存储器或类似的存储器。

在举例示于图 5 和 6 的处理操作中,步骤 S21 至 S30 和 S33 至 S37 的操作分别与图 2 的步骤 S1 至 S8 以及图 3 的步骤 S9 至 S15 相似。于是,按照第二实施例的用户鉴别设备的不同的和具有特点的操作描述如下。

在按照本实施例的用户鉴别设备中,类似于按照第一实施例的用户鉴别设备,当用户鉴别结果判定部分 15 判定根据输入的指纹的鉴别失败,而请求用替代鉴别部分 22 进行的替代鉴别时,从指纹输入请求部分 20 向用户发出把指纹输入到指纹传感器的请求。因此,指纹输入部分 21 采集指纹图像(图 6 的步骤 S29)。

输入图像性能判断部分 26 判断从输入传感器输入的指纹图像是否当前请求鉴别以求服务的用户适当地呈上的手指的指纹图像(图 6 的步骤 S30 和 S31)。

就像下面给出的这样的图像应该由输入图像性能判断部分 26 的判断加以判断和排除。详细地说应该排除(1)由用户呈上的指纹以外的生物要素的图像，例如，诸如指纹以外的手指的一部分、手掌的一部分或者其他某些部分的皮肤的一部分，和(2)由用户呈上的生物部分以外的但模仿指纹的成分的图像，例如，诸如一种用诸如橡胶或硅等类似于人体的材料制成的模仿手指而且此外还在其表面上加有无关人员的指纹的成分。

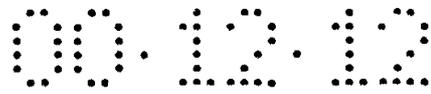
为了排除呈上基于上述模仿手指之类图像的可能性，输入图像性能判断部分 26 首先评估该图像与指纹的相似性，并利用指纹相似性高于阈值作判据。为了评估指纹的相似性，采用这样一种方法，即把图像划分成小区域，并对每一个小区域使用二维富里叶变换等，以确定频率分布。

人类指纹的隆起线具有条形图案，后者具有限制在某种程度上的间距分布，而这一点可以通过评估频率分布中的峰值分布来确认。即使指纹由于该部分破损或干燥而部分地具有不适合于自动校验的质量，但指纹必定具有较宽的其中可以观测到条形图案的区域。指纹和其他部分可以用刚才描述的方法彼此区分。

为了确认呈上的成分是活体的手指，使用一种检查多个输入图像之间的相似性的方法。人类的手指具有弹性，而且每次按压时手指变形不同的可能性大。若多次按压的图像连细节都彼此一致，则有理由肯定，呈上的是其弹性不同于活体手指的仿制物品(复制品)，而且不是适当的压痕。

因此，若多个指纹图像通过平行移动和旋转相对定位时他们之间的隆起线图案的位置相关性相当高，则估计该图像的来源是一个具有某种程度刚性的物体。于是，通过评估该程度，即可把该物体与手指皮肤区分开，手指皮肤具有弹性的而且每次按压时必定呈现不同的变形方式。

另外还可以在手指在输入传感器上开始按压输入之后按压面积



变宽，然后按压完成时变窄的过程中拍摄动画，并评估弹性所引起的手指变形程度，然后从所获得的在时间方向上的一系列图像区分出与手指弹性不匹配的输入。还可以使用检查在指纹图像上是否存在汗腺孔的方法。因为汗腺孔在隆起线上具有非常细致的结构，故可认为在复制品上模仿它们是相当困难的。

只有当输入图像性能判断部分 26 这样的判断判定输入的图像是合法的指纹输入时，用户才可以进到使用替代鉴别部分 22 进行替代鉴别的步骤。

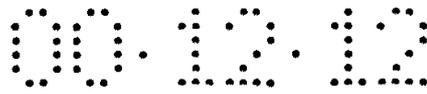
作为替代鉴别部分 22 的替代鉴别方法，一般可用从 0~9 数字键或键盘或从证实持有人身份用的磁卡读出的另一种方法输入个人标识号码或密码的方法。若通过一种替代鉴别方法判定该用户是合法用户，则和用生物测量学自动校验鉴别出该用户是合法用户时相似，鉴别出输入用户信息的用户是合法用户。因而允许提供服务。而在其他任何情况下，判定鉴别结果失败，拒绝提供服务。

替代鉴别装置用户信息存储部分 23 存储指纹输入请求部分 20 发出请求之后输入的图像(图 6 的步骤 S30)。以后必要时，非法用户追击信息处理部分 25 可以用所述存储图像来搜索和追击非法用户。

上面描述了本发明第一和第二实施例的组件的配置和操作，下面将描述它们的应用实例。本发明一般应用于重要设施进门的通行管理(人身通行控制)、包含重要信息的计算机系统的登录管理等等。

例如，在人身通行控制的应用中，请求通行的用户从 0~9 数字键等输入证实用户本身身份用的号码 N 等，并从指纹传感器输入指纹 S。系统判断指纹 S 和利用输入的用户标识号码 N 从其中存储的多个登记指纹中间识别的指纹 F 之间的一致性。在实际的校验中，评估从指纹 S 与指纹 F 提取的校验用的特征的相似性，而若相似性高于阈值，则判定它们彼此一致。

校验处理自动进行，而当输入指纹的质量不够高时，它无法足够可信地判断这些指纹是否同一手指的指纹。当像刚才描述那样用户输



入质量这样低的指纹时，传统上一般使用这样的方法，即其中确定“无法通过自动校验过程进行鉴别”，并作为替代措施，发出输入特殊的个人标识号码或密码的请求。然后，若输入个人标识号码或密码与登记的一致，则判定鉴别结果成功。

5            在本系统中，当自动校验因为输入指纹图像质量不高而得不到成功结果时，首先把输入的指纹图像存入替代鉴别装置用户信息存储部分 23，并在允许替代鉴别之前再次发出输入指纹的请求。

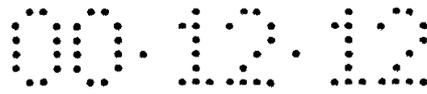
10           之所以以这样的方式多次发出输入指纹的请求，理由是想要防止给出伪造手指的图像并原样存储。为了防止存储这种伪造的手指，把多个指纹图像彼此比较，或如前所述地利用从记录指纹按压过程的动画获得的图像的时间序列。由输入图像性能判断部分 26 判断输入的多个图像或图像的时间序列的特征，而若图像不是活体的指纹，则不允许替代鉴别。

15           若输入的图像是适当的图像，则将其存入替代鉴别装置用户信息存储部分 23，而过程进到用替代鉴别部分 22 进行的基于密码输入的替代鉴别。若输入的密码或个人标识号码与登记的一致，则判定该用户被适当鉴别，该用户可以享受服务。

20           即使是无关的个人，也可以通过推测、偷看等从 0~9 数字键、键盘等输入替代鉴别用的密码或个人标识号码，这会使装作合法用户的个人非法进入。当以后发现非法进入门禁管理或执行计算机非法登录时，本系统提供详细描述非法伪装的个人的措施。

25           详细地说，存储在替代鉴别装置用户信息存储部分 23 中的图像包括利用替代鉴别部分 22 的用户的指纹信息，并能用来由通过视觉观察图像的管理者等搜索和追击非法用户。因为在大多数情况下这样一种系统用户的范围是有限的，通过用视觉把用户的指纹和存储的图像彼此比较即可获得许多追击用的信息。这可以用来发现和追击非法用户。

            尽管在以上的描述中，描述了使用单只手指的指纹作为生物测量



数据的方法，自然可以通过输入多只手指来提高安全性，并利用多只手指来更严格地鉴别输入图像的性能(用户是否适当地呈上活手指)，通过存储多只手指的指纹图像并用来追击非法用户。

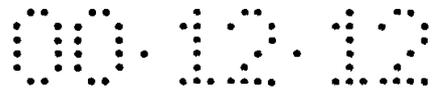
5 另外，尽管描述了这样的实例，其中在输入指纹之前从用户信息输入部分 10 输入用户标识信息，但这并不一定是实质性的。在指纹由指纹输入部分 11 进行输入，而不输入用户标识信息的地方，可以采取以下程序。首先，从输入的指纹提取特征。然后，指纹特征校验部分 14 依次利用存储在指纹校验登记特征数据存储部分 13 中的所有指纹特征数据校验所获得的特征。另外，指纹特征校验部分 14 允许向指纹  
10 具有最高相似性得分的登记用户提供服务。

尽管本发明第一和第二实施例以指纹作为生物测量量度的实例进行描述，但是，若指纹传感器用接收自动校验用的其他类型的生物测量量度(个人所特有的生物特征)的结构代替，则可代之以使用诸如掌纹、面孔、虹膜、视网膜血管图案、拳头、笔迹和声波纹等其他生物测量量度。  
15

还可以在普通生物测量学鉴别中使用指纹，但在替代鉴别之前在生物测量数据的存储中不用指纹而使用其他一些生物测量量度或与指纹一起使用其他一些生物测量量度。例如，可以在替代鉴别时拍摄面部图像或在输入指纹时拍摄身材图像。在指纹输入过程中用另一个摄像机拍摄图像，可以在用输入图像性能判断部分 26 判断指纹是否适当地输入的性能时加以利用。这是存储以后在追击非法用户的处理中表现其效用的信息的有效方法。  
20

用这样的方法，在搜索伪装成有关人员使用服务请求并对鉴别构成威胁的对系统的攻击者中，存储的指纹图像可以用作替代鉴别器。

25 即使存储的指纹图像的质量不足以用于自动校验登录，它们还是提供了对手工搜索攻击者有用的信息。因为输入图像性能判断部分 26 排除用伪造手指进行的欺骗，所以图像表示有关攻击者本人的线索或证据。另外，在输入密码时还要求个人本人的指纹图像，对伪装攻击



有制止作用，对提高整个系统的安全性是有效的。

尽管已经用特定的术语描述了本发明的最佳实施例，但是，这样的描述只是为了举例说明的目的的，因而可以理解，在不脱离以下权利要求书的精神和范围的情况下，可以做出变化和改变。

说明书附图

图 1

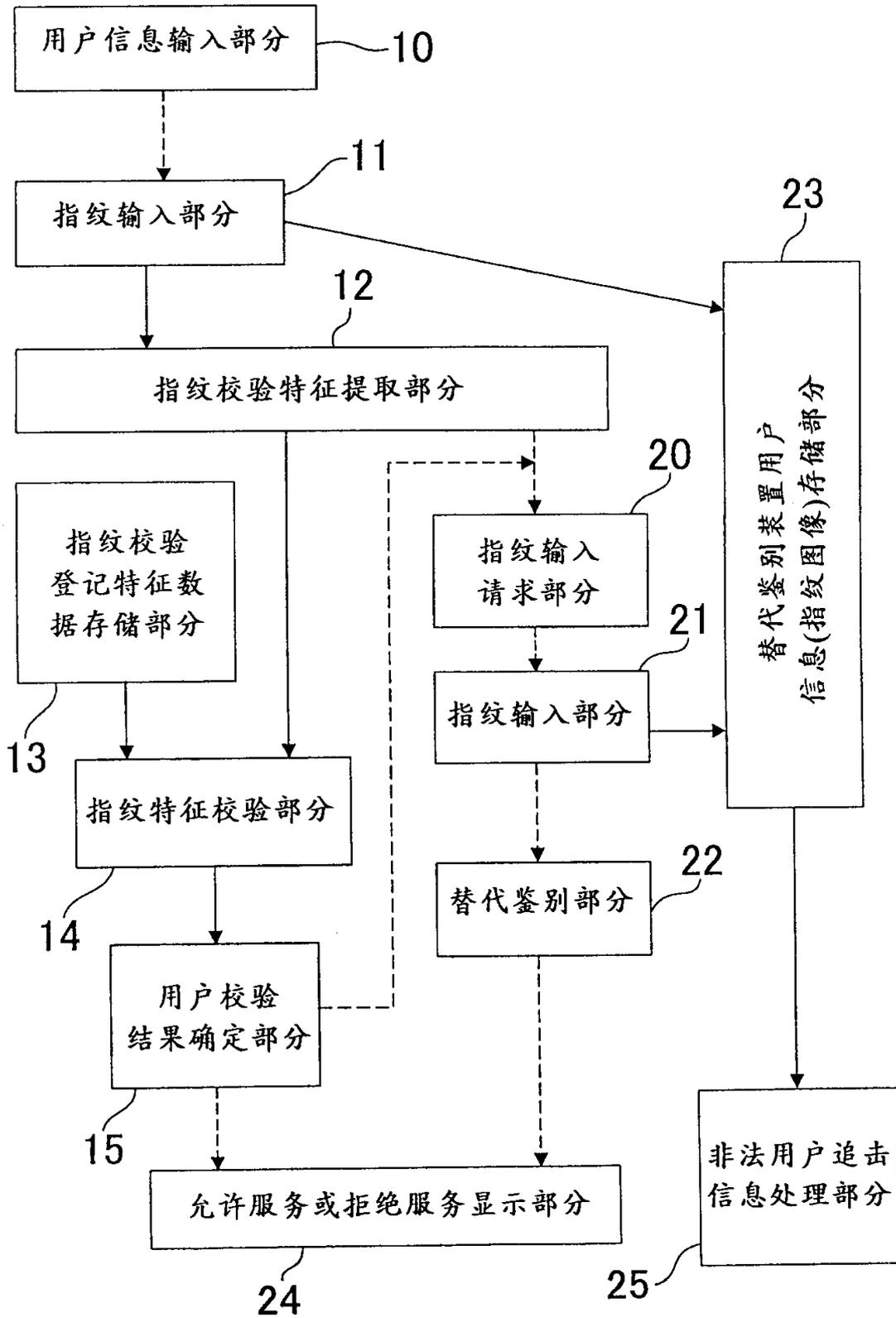


图 2

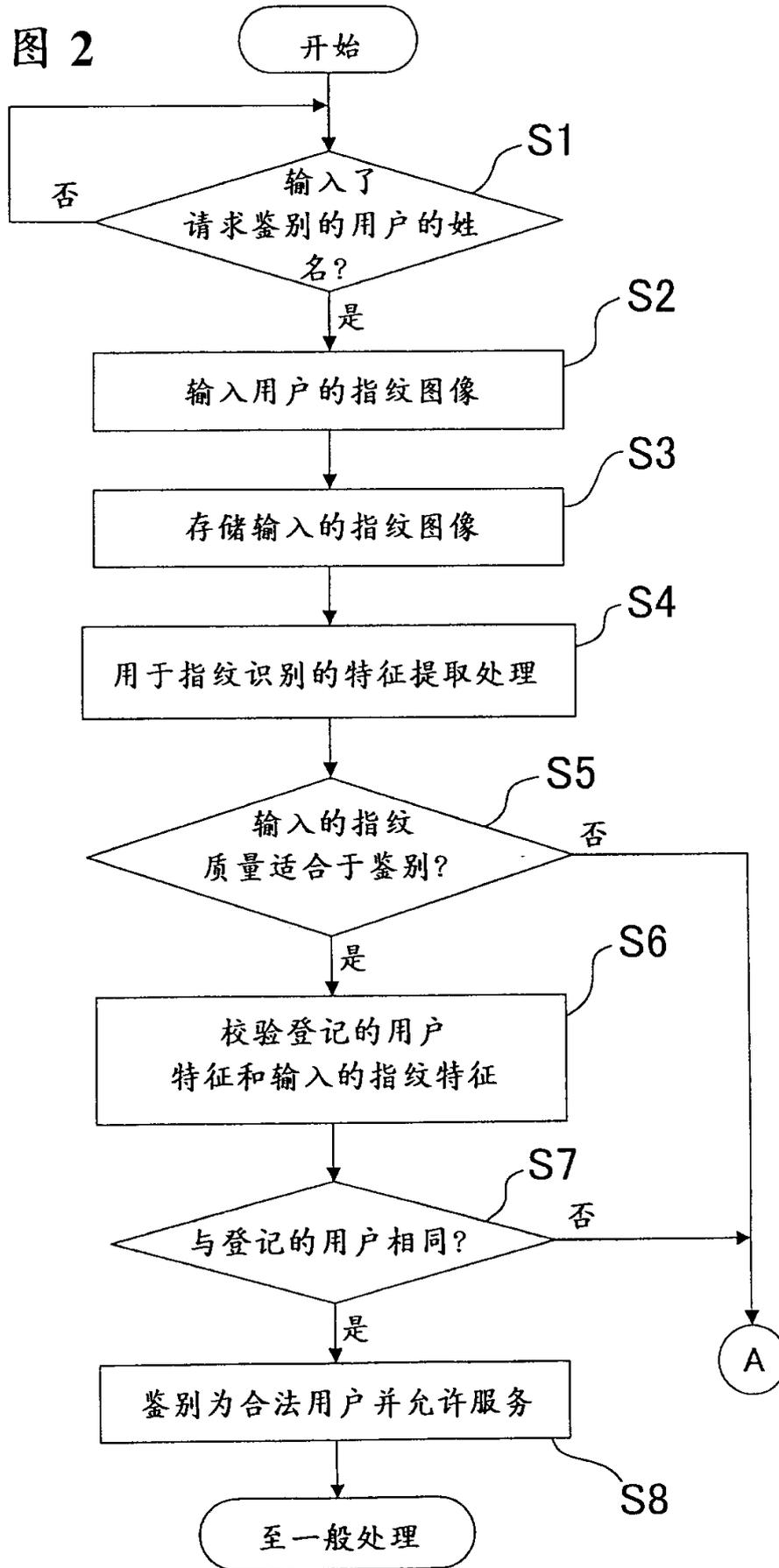


图 3

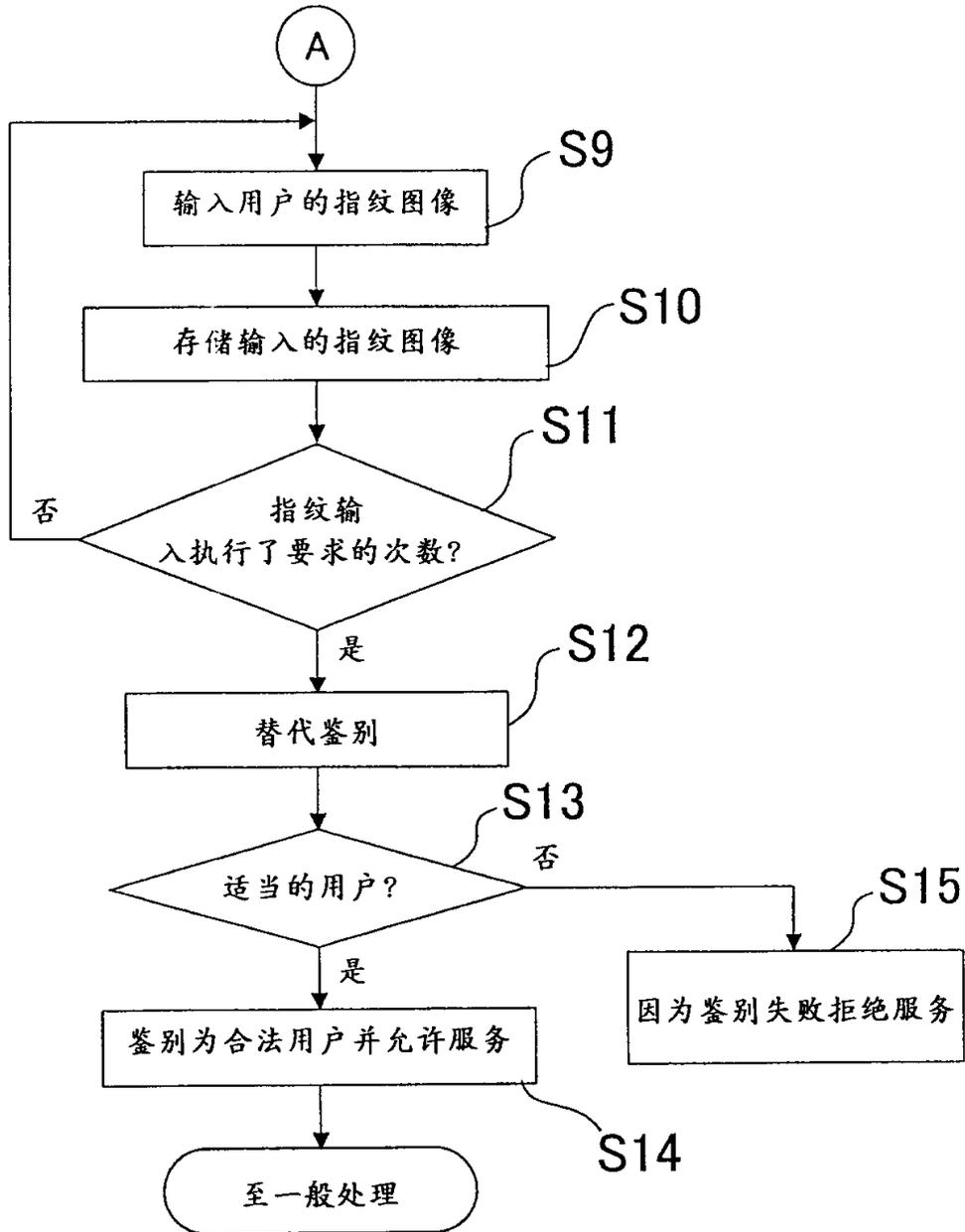


图 4

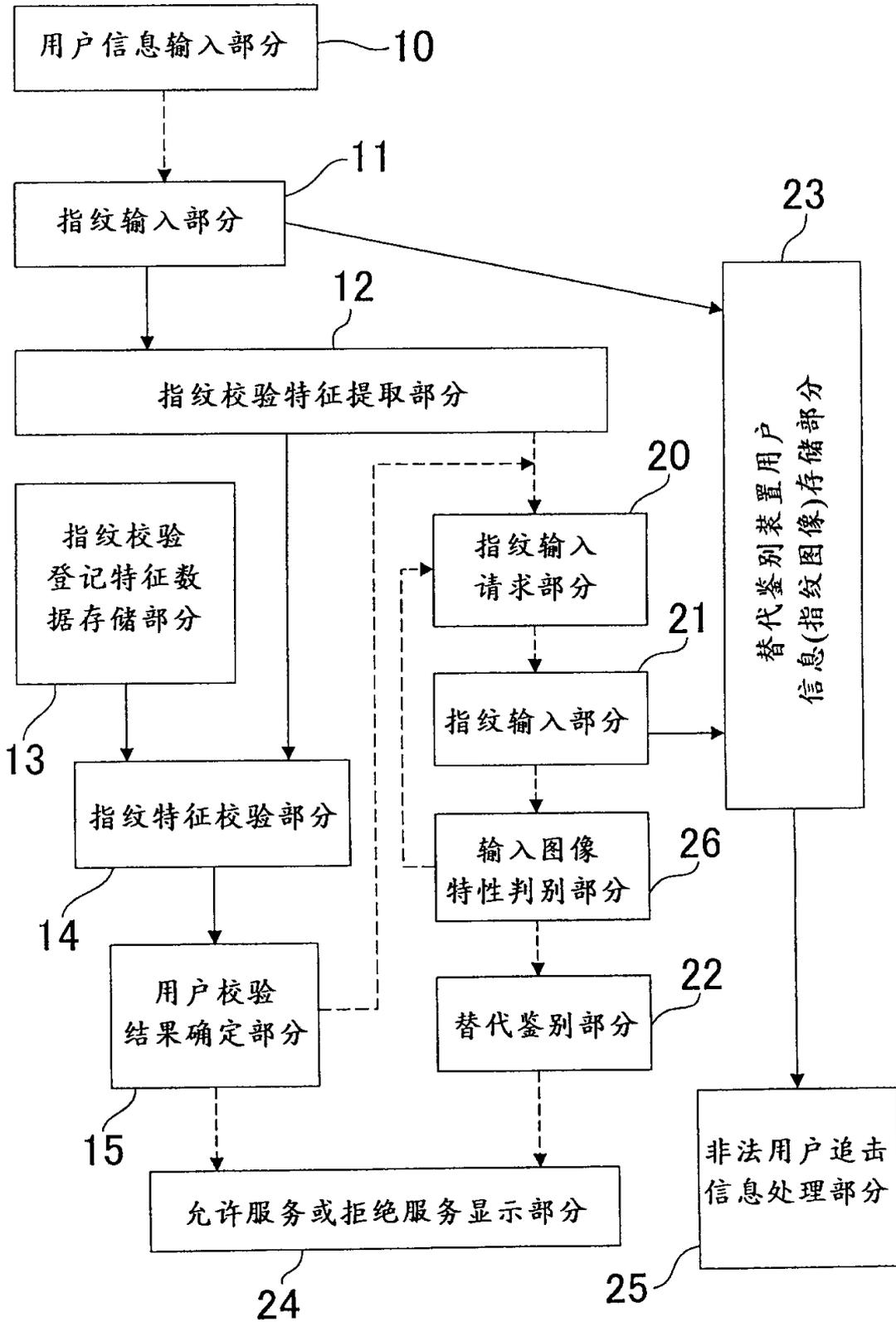


图 5

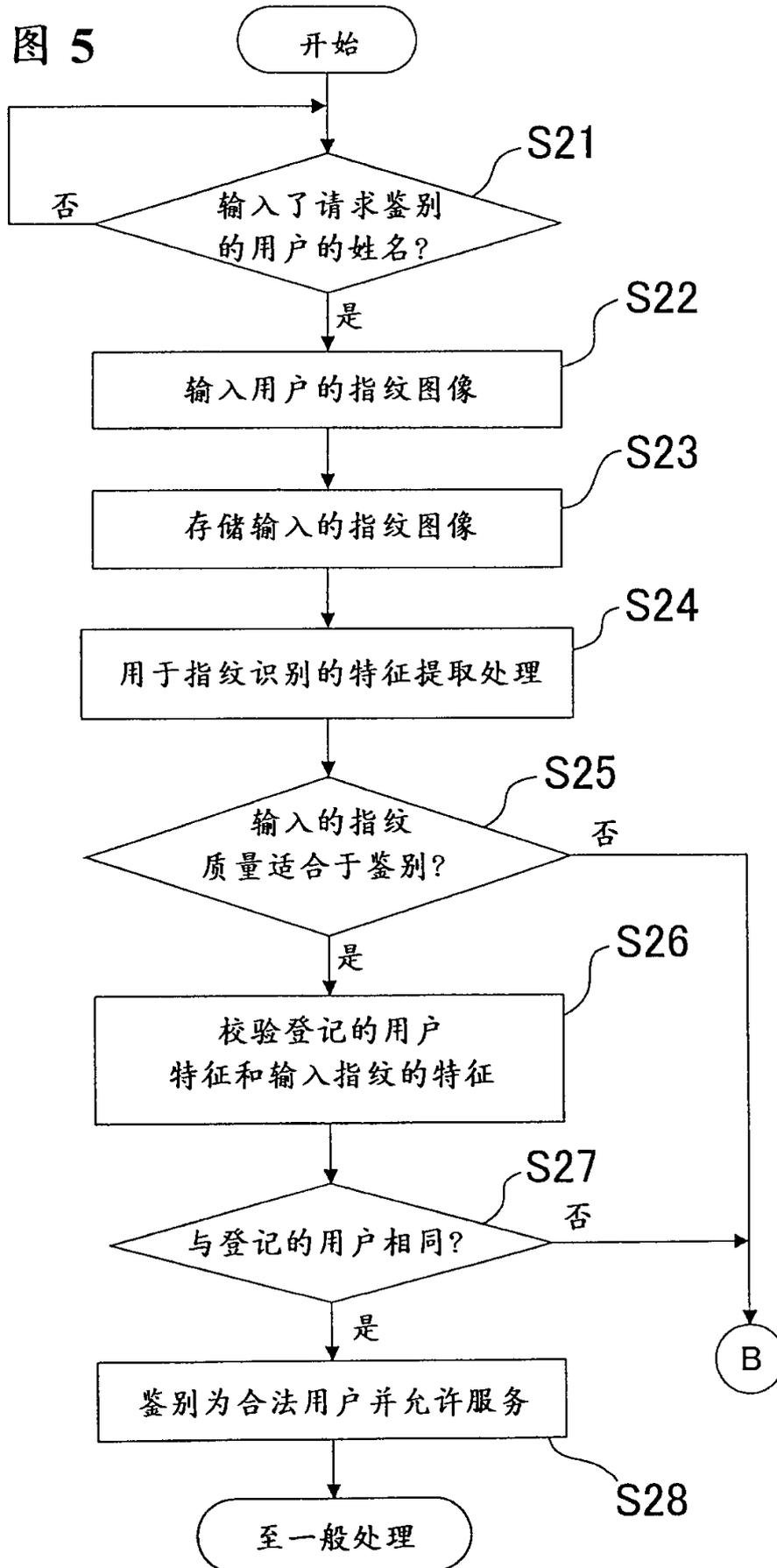


图 6

