(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 102567665 B
(45)授权公告日 2015.04.22

(21)申请号 201110386787.6
(22)申请日 2010.06.09
(30)优先权数据
61/187,520 2009.06.16 US
(62)分案原申请数据
201080019812.0 2010.06.09
(73)专利权人 英特尔公司
地址 美国加利福尼亚
(72)发明人 B·费伦
(74)专利代理机构 永新专利商标代理有限公司 72002
代理人 刘瑜 王英
(51)Int.Cl.
*G06F 21/32*(2013.01)
*G06K 7/10*(2006.01)
*H04N 13/02*(2006.01)
(56)对比文件
CN 101256700 A,2008.09.03, 说明书第7-8页, 第9页第1-5行,表1,附图1-2,4-5.
US 6542624 B1,2003.04.01, 权利要求3,权利要求5-6,说明书附图1.
CN 1393823 A,2003.01.29, 说明书摘要.
审查员 刘义乐

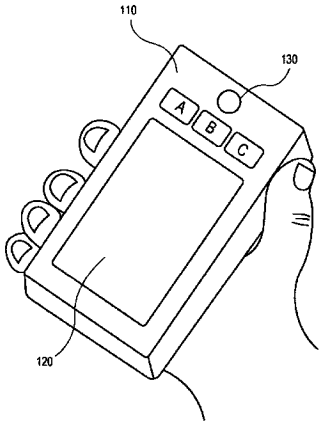
权利要求书3页 说明书9页 附图5页

(54)发明名称

对无线设备的功能的受控访问

(57)摘要

本发明的各实施例可以用来验证通过生物测定技术被授权使用设备的人是真实人而不是意图欺骗系统的某种形式的记录。一些实施例可以设法引起所测量的生物测定特征的改变,并且将在改变之前和之后获取的图像进行比较,以验证发生了改变。在一些实施例中,可以使用多阶段的验证,以增加欺骗安全系统的难度,或者针对对设备功能的不同等级的访问提供不同等级的安全性。




CN 102567665 B

1. 一种电子设备，其包括处理器、存储器和照相机，所述设备用于确定试图使用所述设备的人是否被授权使用所述设备，其中，所述设备：

接收第一类型的第一输入；

执行对于所述第一输入的第一分析，以基于所述第一分析来确定试图使用所述设备的所述人是否被授权使用所述设备中的第一等级的功能；

接收不同于所述第一类型的第二类型的第二输入，其中，所述第二输入是经由以下中的至少一个进行触发的：(1) 所述人手动触发；(2) 在已经获得了所述第一输入之后在经历了预定的时间量时，由所述设备自动触发；以及 (3) 由所述设备通过所述照相机检测所述人，解释运动图片或一系列静止图片，并且选择指示所述人正在试图提供所期望的响应的图片；以及

如果基于所述第一分析所述人被授权使用所述第一等级的功能，则执行对于所述第二输入的第二分析，以基于所述第二分析来确定所述人是否被授权使用第二等级的功能，

其中，所述授权与验证过程相关联，所述验证过程用于确定所接收的输入是来自于真实人还是来自于一种类型的记录，

其中，所述设备还将所述第一分析的结果与所述第二分析的结果进行比较，以确定所测量的生物特征是否以期望的方式改变，并且其中，如果所测量的生物特征以所述期望的方式改变，那么所述人通过所述验证过程，并且其中，如果所测量的生物特征没有以所述期望的方式改变，那么所述人没有通过所述验证过程。

2. 根据权利要求 1 所述的设备，其中，只有所述第一分析指示所述人被授权使用所述第一等级的功能并且所述第二分析指示所述人被授权使用所述第二等级的功能，所述人才被授权使用所述第一等级和所述第二等级的功能。

3. 根据权利要求 1 所述的设备，其中：

如果所述第一分析指示所述人被准许访问，则所述人被准许访问所述设备中的第一等级的功能；以及

如果所述第二分析指示所述人被准许访问，则所述人被准许访问所述设备中的第二等级的功能；

其中，所述第二等级的特性包括所述第一等级的特性。

4. 根据权利要求 1 所述的设备，其中，所述第一输入是键盘输入，并且所述第二输入是生物测量结果的输入。

5. 根据权利要求 1 所述的设备，其中：

所述第一输入和所述第二输入均是生物测量结果的输入；以及

所述第二分析包括比所述第一分析更详细的分析。

6. 一种用于准许对电子设备的多个等级的受限访问的方法，所述方法包括：

在所述电子设备中执行操作，所述操作包括：

接收第一类型的第一输入；

执行对于所述第一输入的第一分析，以基于所述第一分析来确定试图使用所述设备的人是否被授权使用所述设备；

接收不同于所述第一类型的第二类型的第二输入，其中，所述第二输入是经由以下中的至少一个进行触发的：(1) 所述人手动触发；(2) 在已经获得了所述第一输入之后在经历

了预定的时间量时，由所述设备自动触发；以及 (3) 由所述设备通过照相机检测所述人，解释运动图片或一系列静止图片，并且选择指示所述人正在试图提供所期望的响应的图片；以及

如果基于所述第一分析所述人被授权使用所述设备，则执行对于所述第二输入的第二分析，以基于所述第二分析来验证所述人是否被授权使用所述设备，

其中，所述授权与验证过程相关联，所述验证过程用于确定所接收的输入是来自于真实人还是来自于一种类型的记录，

其中，所述方法还包括：将所述第一分析的结果与所述第二分析的结果进行比较，以确定所测量的生物特征是否以期望的方式改变，并且其中，如果所测量的生物特征以所述期望的方式改变，那么所述人通过所述验证过程，并且其中，如果所测量的生物特征没有以所述期望的方式改变，那么所述人没有通过所述验证过程。

7. 根据权利要求 6 所述的方法，其中，所述操作还包括：只有所述第一分析和所述第二分析均指示所述人被授权访问所述设备，才准许所述人访问所述设备。

8. 根据权利要求 6 所述的方法，其中，所述操作还包括：

如果所述第一分析指示所述人被准许访问，则准许所述人访问所述设备中的第一等级的功能；以及

如果所述第二分析指示所述人被准许访问，则准许所述人访问所述设备中的第二等级的功能；

其中，所述第二等级的功能包括所述第一等级的功能。

9. 根据权利要求 6 所述的方法，其中，所述第一输入是键盘输入，并且所述第二输入是生物测量结果的输入。

10. 根据权利要求 6 所述的方法，其中：

所述第一输入和所述第二输入均是生物测量结果的输入；以及

所述第二分析包括比所述第一分析更详细的分析。

11. 一种用于准许对电子设备的多个等级的受限访问的装置，所述装置包括：

用于接收第一类型的第一输入的模块；

用于执行对于所述第一输入的第一分析，以基于所述第一分析来确定试图使用所述设备的人是否被授权使用所述设备的模块；

用于接收不同于所述第一类型的第二类型的第二输入的模块，其中，所述第二输入是经由以下中的至少一个进行触发的：(1) 所述人手动触发；(2) 在已经获得了所述第一输入之后在经历了预定的时间量时，由所述设备自动触发；以及 (3) 由所述设备通过照相机检测所述人，解释运动图片或一系列静止图片，并且选择指示所述人正在试图提供所期望的响应的图片；以及

用于如果基于所述第一分析所述人被授权使用所述设备，则执行对于所述第二输入的第二分析，以基于所述第二分析来验证所述人是否被授权使用所述设备的模块，

其中，所述授权与验证过程相关联，所述验证过程用于确定所接收的输入是来自于真实人还是来自于一种类型的记录，

其中，所述装置还包括：用于将所述第一分析的结果与所述第二分析的结果进行比较，以确定所测量的生物特征是否以期望的方式改变的模块，并且其中，如果所测量的生物特

征以所述期望的方式改变，那么所述人通过所述验证过程，并且其中，如果所测量的生物特征没有以所述期望的方式改变，那么所述人没有通过所述验证过程。

12. 根据权利要求 11 所述的装置，还包括：用于只有所述第一分析和所述第二分析均指示所述人被授权访问所述设备，才准许所述人访问所述设备的模块。

13. 根据权利要求 11 所述的装置，还包括：

用于如果所述第一分析指示所述人被准许访问，则准许所述人访问所述设备中的第一等级的功能的模块；以及

用于如果所述第二分析指示所述人被准许访问，则准许所述人访问所述设备中的第二等级的功能的模块；

其中，所述第二等级的功能包括所述第一等级的功能。

14. 根据权利要求 11 所述的装置，其中，所述第一输入是键盘输入，并且所述第二输入是生物测量结果的输入。

15. 根据权利要求 11 所述的装置，其中：

所述第一输入和所述第二输入均是生物测量结果的输入；以及

所述第二分析包括比所述第一分析更详细的分析。

# 对无线设备的功能的受控访问

[0001] 本申请是申请日为 2010 年 6 月 9 日、申请号为 201080019812.0、发明名称为“对无线设备的功能的受控访问”的中国发明专利申请的分案申请。

## 背景技术

[0002] 小型手持电子设备已经在社会中变得无处不在，并且人们变得越来越依赖于这些设备来获得信息、彼此进行通信、提供娱乐、以及执行财务事务等等。这些设备的小尺寸使得它们易于丢失并成为盗贼的目标，同时其日益增加的能力提供了对敏感的个人数据和财务资源的访问。已经开发了多种安全技术来确定试图使用这种设备的人是否之前已经被授权使用该设备。曾经提出了生物测定 (biometric) 认证，作为避免可能被偷盗的密码或人工制品（例如，密钥、标记等）的方式。但是，通过记录真实的特征（面部的照片、语音的音频记录、指纹的复本等）并且使用所记录的数据来欺骗生物测定传感器，也可能欺骗生物测定识别。

## 附图说明

[0003] 通过参照以下描述和用来示出本发明实施例的附图，可以理解本发明的一些实施例。在附图中：

[0004] 图 1 示出了根据本发明的实施例用于无线通信的多功能手持设备；

[0005] 图 2 示出了根据本发明的实施例验证生物测定输入来自于真实人的方法的流程图；

[0006] 图 3 示出了根据本发明的实施例验证生物测定输入来自于真实人的眼睛的方法的流程图；

[0007] 图 4 示出了根据本发明的实施例验证生物测定输入来自于真实人的方法的流程图；

[0008] 图 5 示出了根据本发明的实施例准许对设备的多个等级的受限访问的方法的流程图。

## 具体实施方式

[0009] 在下面的描述中，给出了许多具体的细节。然而，应当理解，可以在不具有这些具体细节的情况下实施本发明的实施例。在其它情况中，为了不使对本描述的理解模糊，没有详细地示出公知的电路、结构和技术。

[0010] 提及“一个实施例”、“实施例”、“示例性实施例”、“各实施例”等表示这样描述的本发明实施例可以包括特定的特征、结构或者特性，但是并不是每个实施例都必须包括该特定的特征、结构或者特性。此外，一些实施例可以具有一些、全部或者不具有针对其它实施例描述的特征。

[0011] 在下面的描述和权利要求中，可以使用术语“耦合的”和“连接的”及其派生词。应当理解，这些术语并不是要作为彼此的同义词。而是，在特定的实施例中，“连接的”用来表

示两个或更多元件彼此直接物理或者电接触。“耦合的”用来表示两个或更多元件彼此合作或者交互，而它们可以或者可以不直接物理或者电接触。

[0012] 如在权利要求中使用的，除非另外规定，否则使用序数形容词“第一”、“第二”、“第三”等来描述公共元件仅表示正在提及相似元件的不同实例，而并非要暗示这样描述的元件必须在时间上、空间上、顺序上或者以任意其它方式处于给定的次序。

[0013] 本发明的各实施例可以实现在硬件、固件和软件中的一个或者任意组合中。本发明也可以实现为包含在计算机可读介质中或者计算机可读介质上的指令，该指令可以被一个或多个处理器读取并执行，以允许本文描述的操作的执行。计算机可读介质可以包括用于以一个或多个计算机可读的形式存储信息的任何机制。例如，计算机可读介质可以包括有形存储介质，例如但不限于：只读存储器 (ROM)；随机存取存储器 (RAM)；磁盘存储介质；光存储介质；闪存设备等。

[0014] 术语“无线”可以用来描述通过使用穿过非固态介质的已调制电磁辐射来传输数据的电路、设备、系统、方法、技术、通信信道等。该术语并不意味着相关联的设备不包含任何的线缆。无线设备可以包括至少一个天线、至少一个无线电单元以及至少一个处理器，其中该无线电单元通过天线来发送表示数据的信号以及通过天线来接收表示数据的信号，同时处理器可以处理要被发送的数据和已经接收的数据。该处理器还可以处理既没有被发送也没有被接收的其它数据。

[0015] 本发明的各个实施例可以在对旨在确定试图使用设备的人是否已经被批准使用该设备的生物测定技术的使用上进行改进。这种改进的技术可以设法将取自真实人 (living person) 的生物测量结果 (biometric measurement) 与取自人的记录的生物测量结果区分开。在本文档中，术语“授权 (authorize)”及其派生词将用来表示确定试图使用系统的人是否之前已经被批准使用该系统的过程，而术语“验证 (verify)”及其派生词将用来表示确定所接收的生物测定输入是来自于真实人而不是来自某种类型的记录的过程。在大多数应用中，在所请求的访问将被准许之前，必须通过授权过程和验证过程两者。在一些实施例中，可以使用多阶段的授权和 / 或验证，以增加欺骗安全系统的难度，或者针对对设备功能的不同等级的访问来提供不同等级的安全性。

[0016] 本文描述的一些技术涉及使用照相机来拍摄人的一部分的图片，并且分析该图片中人的某种特征。在本文档中使用的术语“图片”可以是静止图片或者是运动图片。在一些情况中，来自运动图片的单个帧可以用作静止图片。在一些实施例中，图片是存储的电子数据的形式，并且分析该图片包括分析该数据。本文档中所使用的术语“照片”表示已经被记录在介质上的图片，其可以在纸上、利用电子显示器或者通过一些其它方式以可以被人眼在视觉上察觉的方式呈现。这种照片可能被用来试图欺骗安全系统，而本文描述的技术可以用来阻止该尝试。

[0017] 图 1 示出了根据本发明的实施例用于无线通信的多功能手持用户设备。所示的设备 110 被示出为具有各种组件，例如触摸屏 ( 触敏显示屏 )120 以及按钮 A、B 和 C。还示出了镜头 130，其可以是该设备的照相机的外部可视部分。还可以包括其它的按钮、传感器、输出设备等，但是为了避免附图中过于混乱，没有示出这些组件。在各实施例中，照相机可以根据需求拍摄静止图片或者运动图片。

[0018] 虽然所示的设备 110 被描绘为具有特定的形状、比例和外观，且各种元件位于特

定位置处，但是这仅仅是举例，并且本发明的实施例可以不限于该特定的物理配置。例如，在一些实施例中，按钮可以具有与所示出的不同的尺寸和 / 或不同的形状，位于设备的相同侧上的其它位置处或者位于不同侧上，等等。在一些实施例中，设备 110 的总体形状可以与所示出的不同。设备 110 还可以包括用于无线通信的功能、用于各种视觉、音频和物理输入的功能以及用于各种视觉、音频和物理输出的功能。设备 110 可以包括处理器、存储器、照相机、用于与其它设备进行无线通信的无线电单元以及可以用来完成本文档所描述的功能的各种其它组件。

[0019] 关于生物测定读数来自于真实人的证据

[0020] 已经开发了多种生物测量技术来验证试图使用系统的人实际上被批准使用该系统。不管被用来对人进行认证的具体生物测定参数如何，传统的安全系统所使用的感测方法一般是静态的，这会使得利用已记录的参数来欺骗系统成为可能。注意 :在该文档中，生物测量结果是取自人的身体的一部分的测量结果。这可以包括对物理形状、运动、从该部分反射的光和 / 或由该身体产生的声音的检测。

[0021] 为了使这种欺骗更加困难，本发明的各实施例可以发起身体特征的改变，并且捕获该特征在改变前和改变后的图像，从而防止使用简单的静态记录来欺骗系统。该改变可以是主动的（例如，使用户故意改变面部表情）或者可以是非主动的（例如，使用光来改变人眼的瞳孔的大小）。

[0022] 在一些情况中，为了试图攻克系统，有可能会进行两个记录，一个针对最初的读数而另一个针对随后的读数。各实施例可以以多种方式来阻止这种尝试，所述方式包括但不限于 :1) 使改变不可预测，从而随后的读数是无法预见的，2) 使最初的读数不可预测，从而这两个读数均是无法预见的，3) 获取在时间上彼此接近的读数，使得在读数之间切换记录是困难的或者不实际的。

[0023] 图 2 示出了根据本发明的实施例验证生物测定输入是来自于真实人的方法的流程图。本文描述的过程旨在验证所述输入是来自于真实人而不是来自于已记录的人工制品，并且没有被具体地设计为验证该人被授权使用该系统。但是，在一些实施例中，相同的输入可以用来确定该人被授权以及验证该输入来自于真实人。在其它的实施例中，授权以及验证的操作可以不使用相同的输入或者仅使用一些相同的输入。

[0024] 在 210 处，电子设备可以接收访问设备功能、或者至少访问特定等级的设备功能（不同等级的功能可以要求不同等级的授权，并因此具有用于提供该授权的不同过程）的请求。该请求可以是由请求访问的人（例如，通过按动按钮、触摸触摸屏等）直接发起的，或者可以是响应于触发事件（例如，检测到设备的运动、通过设备的照相机观察到外部的移动、听到特定的口述短语等）而自动发起的。作为用于确定是否准许这种访问的授权过程的部分，在 220 处，设备可以准备接收来自该人的生物测定输入。这可以包括例如但不限于 :激活用于面部识别、用于瞳孔检测、用于检测手移动的软件，激活照相机的照明源等。在 230 处，设备可以接收第一生物测定输入。该输入可以采取诸如语音输入、指纹或者人身体某部分的图片等的多种形式中的任一种。将在下文中描述人身体各部分的具体实例。

[0025] 在获得第一生物测定输入之后，在 240 处，该设备可以设法发起该人的改变，其中该改变可以从第二生物测定输入中检测到。在一些实施例中，这可以采取提示该人来进行该改变（例如，使用音频或者视频提示来指导该用户执行某种动作）的形式。在其它实施

例中，该用户可以从之前的训练中知道要进行哪种改变。在其它实施例中，该设备可以引起该用户的生物测定响应的非主动改变。

[0026] 在经过了发生改变所需的足够的时间之后，在 250 处，该设备可以接收第二生物测定输入。该输入可以以各种方式触发，诸如但不限于 :1) 该用户可以通过按下按钮、说出语音命令等来手动地触发该输入，2) 在第一输入之后的预定时间量，该设备可以自动地触发该输入，3) 该设备可以通过照相机来监测该人，解释运动图片或者一系列静止图片，并且选择指示出该用户正试图提供所期望的响应的图片。

[0027] 在分析两个输入之后，在 260 处，可以比较该结果，以在 270 处确定所测量的特征是否以期望的方式改变。如果没有，则如 290 处所指示的，该人没有通过该验证过程。在一些实施例中，可以允许预定数量的重试，并且直到该人没有通过所有的重试，或者未能在没有通过的情况下在特定时段内尝试进行所允许次数的重试，该安全过程才被视为是没有通过的。然而，在第一次尝试或者允许的重试时，如果生物测定特征以期望的方式改变，则如 280 处所指示的，该人通过了该验证过程。应当注意，通过了验证过程并不意味着通过了授权过程，因此，如果没有通过授权过程，则访问仍然可能被拒绝。

[0028] 在一些实施例中，用来验证该人是否被授权的测试以及用来确定生物测定输入是否来自于真实人的测试可以使用相同的输入。例如，可以通过面部识别来处理人面部的图片，以确定该人是否被授权，并且相同的图片可以用来分析该人面部上的表情。相似地，眼睛的图片可以用来验证该眼睛具有被授权人的眼睛的特征，并且相同的图片可以用来确定瞳孔的大小。将在下文中描述这些以及其它可能的实施例。

[0029] 防止安全欺骗的眼睛行为分析

[0030] 近几年，已经开发了生物测定认证技术，其通过捕获目标用户的眼睛的某个特征（例如，虹膜的图案）的图像，并将其与所存储的被授权用户的眼睛的图像进行比较，来验证该用户的身份。然而，可以通过获得被授权用户眼睛的照片并将其呈现给照相机来欺骗这种方法。本文描述的技术可以通过感测照片不能提供的事物来避免以上述方式被欺骗。本文描述的技术仅仅旨在防止欺骗，并且可以与验证用户身份的另一方法结合使用。

[0031] 在一个实施例中，设备上的照相机可以拍摄用户眼睛的带闪光图片 (flash picture)，其中该闪光位于足够接近于照相机镜头的光轴的位置上，以产生被称为“红眼”的现象，在该现象中，眼睛的视网膜反射红光和 / 或红外范围内的光，从而使瞳孔在图像中看起来是红色的。在标准的基于照相机的闪光单元的变型中，可以沿着围绕镜头的同心环设置照明器。可替换地，可以将照明器放置于照相机内，所放置的位置使得光照通过镜头向外投射而同时被捕获的图像通过镜头进入（例如，可以将照明器安装在成像芯片上，或者可以使用分束器来使来自分离的内部光源的光沿着镜头光轴被引向外部）。然而，不管光源的结构如何，当拍摄一张照片的带闪光图片时，并不会发生红眼，这是由于并不存在真实的视网膜来产生红眼效果。有可能的是，照片是带闪光拍摄的，并因此在瞳孔的位置处示出红点，但是该红点的亮度不如来自真实眼睛的反射的红光强烈。

[0032] 在一些实施例中，倘若设备能够测量红外光的强度，则可以分析从视网膜反射的光的红外分量。在一些实施例中，可以将红外照明器投射至面部，以有助于该过程，并且该过程可以分析从瞳孔反射的红外光与从面部的至少一个其它部分反射的红外光之间的强度差。如果在低光条件下执行验证、和 / 或不希望使用明亮的广谱闪光或其不可行，则这种

红外照明器也会是有用的。

[0033] 可替换地，设备的照相机可以拍摄两张图片，一张不带闪光从而获得没有红眼的图片，而另一张带闪光从而获得有红眼的图片。呈现给照相机的单张照片不能产生这两种结果，因此不能被用来以这种方式欺骗系统。如果图像是快速连续地拍摄的，则用户应当不可能呈现两张连续的照片，其中一张有红眼而另一张没有红眼。

[0034] 在涉及捕获多个图像的另一技术中，设备可以拍摄两张图片，这两张图片之间被与人瞳孔的迟缓反应时间 (dilatory response time) 相当的一个时段分开。在拍摄人眼睛的第一图片之后，该设备可以通过将适量的光引向该眼睛来使该眼睛的瞳孔缩小。这可以以多种方式来实现，诸如但不限于 :1) 在图片之间增加稳态照明，2) 在图片之间开启一个或多个闪光，3) 如果第一图片是利用闪光单元来拍摄的，则在拍摄第二图片之前，该闪光可能足以使瞳孔缩小，因此附加的光可能并不是必需的。在一些实施例中，可以拍摄多于两张的图片，以示出瞳孔在迟缓响应时间上的渐进缩小。在一些实施例中，例如，如在选项 1 中，如果环境光的等级足够低，使得设备的显示器的亮度足以影响瞳孔的大小，则可以使用设备的显示器的亮度来增加照明。

[0035] 在等待使瞳孔缩小的足够长的时间之后，可以捕获第二图片。然后，该设备可以将两张图片进行比较，以观察第二图片中的瞳孔是否小于第一图片中的瞳孔。该比较可以以两种方式进行。在第一种方式中，可以直接测量瞳孔的大小，并且大小上的充分减小表明所述图片是真实的眼睛的图片，而不是照片的图片。在第二种方式中，如果使用闪光单元来拍摄这两张图片，则可以针对这两张照片来比较通过瞳孔从眼睛视网膜反射的红光和 / 或红外光的量。如果第二图片显示了反射光的充分减小的量，则其可以表明该瞳孔更加小，并且所述图片是真实的眼睛的图片，而不是眼睛照片的图片。

[0036] 在另一实施例中，可以使用视频照相机来检测眼睑的眨动，其意味着真实人的存在。这可以以多种方式中的任意一种来处理，诸如但不限于 :1) 使用视频来确认该人在预定的时段期间眨动了至少一次，2) 测量眨动速率以确认其与真实人的眨动速率一致，3) 使用高速光检测器来测量在一次眨动期间眼睑的上升和 / 或下降时间以确认其与真实人的眼睑的上升和 / 或下降时间一致，4) 使用高速光检测器来测量左眼睑和右眼睑的定时或上升 / 下降时间之间的不匹配 ( 在两只眼睛之间，眨动很少是完全同步的 )，5) 等等。在另一技术中，可以使用检测器来检测扫视，即，当眼睛在视场中的点到点之间移动时眼睛的快速移动。

[0037] 虽然作为分别的技术进行了描述，但是，这些技术中的任意技术可以彼此结合使用，或者与本文没有描述的其它技术结合使用。可以将这些技术中的大多数用在一只眼睛上，或者用在两只眼睛上以用于附加的验证。在一些实施例中，可以使用设备的通用照相机来捕获图像，而在其它实施例中，可以单独地或与该照相机结合地使用附加的器材。在一些实施例中，滤光器可以与照相机一起使用以突出特定波长的光 ( 例如，红光和 / 或红外光 )。

[0038] 图 3 示出了根据本发明的实施例验证生物测定输入是来自于真实人的眼睛的方法的流程图。在 310 处，电子设备可以接收访问设备功能、或者至少访问特定等级的设备功能的请求。如之前针对图 2 描述的，该请求可以以各种方式发起。

[0039] 由于该过程涉及眼睛的视觉分析，因此在可以获得有意义的输入之前，该眼睛需要在照相机的视场内。在 315 处，可以将眼睛定位在照相机的视场内。在一些实施例中，人

简单地使照相机对准其自己的面部，而在其它的实施例中，可以分析来自设备的照相机的一个或多个图像，以确保眼睛在图像中。在 320 处，该设备可以拍摄眼睛的第一图片，并且在 325 处，可以分析瞳孔。取决于所使用的特定过程，该分析可以采取多种不同形式中的一种。在一种形式中，可以注意红眼效果的不存在或存在，而在另一种形式中，可以计算瞳孔的大小。在简单的仅寻找红眼存在的一张图像过程中，该过程可以跳至 350，以确定是否存在红眼效果。然而，大多数这种过程将拍摄至少两张图片。

[0040] 在 330 处，该设备可以发起瞳孔大小的改变，诸如但不限于使用光来使瞳孔缩小。然后在 335 处，可以拍摄第二图片，并且在 340 处，再次分析瞳孔。在一些实施例中，在拍摄第二图片之前，可以再次确定图像中眼睛的位置。虽然该流程图示出了在拍摄第二图片之前执行对第一图片的分析，但是在一些实施例中，可以拍摄这两张图片，然后再分析其中任意一张图片。在 345 处，可以比较这两张图片，以确定瞳孔是否以预期的方式发生改变。如果没有，则立即或者在预定数量的重试之后，如在 360 处所指示的，该验证过程会没有通过。如果瞳孔确实如所预期的那样发生改变，则如 355 处所指示的，该验证过程会通过。

[0041] 防止安全欺骗的身体行为 (physical body behavior)

[0042] 已经开发了面部识别技术，其中可以将所捕获的面部图像与面部数据库进行比较，以识别该人是谁。但是在以前，有时可能通过将被授权人的图片放置在照相机前来欺骗这些系统。然而，可以通过提示用户改变面部表情，并且验证该面部的图片以所要求的方式发生改变，来克服这种缺点。这种提示可以以任何可行的形式来呈现，例如但不限于口头命令、触摸屏上的文本指示、所期望的表情的图形图像等。

[0043] 在一些实施例中，在拍摄面部的第一图片之后，可以提示用户改变表情，并且可以拍摄第二图片，并将其与第一图片进行比较。在该技术的简单版本中，该比较可以仅验证表情发生了改变。在更复杂的版本中，可以提示用户呈现特定的第二表情（例如，微笑、皱眉、张嘴、闭眼、眨眼、看特定的方向等），并且分析可以确认该第二表情是所要求的表情。在另一版本中，可以提示第一和第二表情，并且可以分析这两个表情，以验证它们为正确的表情。在再一版本中，可以提示其它的身体移动，例如特定的手势、将头转向左或右等。

[0044] 这些具体的动作仅仅是被称为身体行为的一大组动作的示例，其中提示人利用身体的特定一部分、利用身体的多个部分、或者利用整个身体来执行动作。该动作可以将身体部分置于可以在静止图片中捕获的特定形态（例如，面部上的特定表情、或者伸出一只手上的特定数目的手指），或者该动作可以是以可以在运动图片中捕获的特定方式来移动身体（例如，向上和下移动左手、或者将头从左转向右等）。一些实施例还可以提示用户以某种方式与该用户的周围事物进行交互，使得感测到周围事物的方式上的改变也可以是比较的一部分。

[0045] 图 4 示出了根据本发明实施例验证生物测定输入来自于真实人的方法的流程图。在 410 处，电子设备可以接收访问设备功能、或者至少访问特定等级的设备功能的请求。如之前针对图 2 描述的，该请求可以以各种方式发起。

[0046] 由于该过程涉及对特定身体部分（面部、手等）的视觉分析，因此在可以获得有意义的输入之前，该身体部分需要在照相机的视场内。在 415 处，可以将该身体部分定位在照相机的视场内。在一些实施例中，人简单地使照相机对准所指示的身体部分，而在其它的实施例中，可以分析来自设备的照相机的一个或多个图像，以确保该身体部分在图像中。在

420 处，该设备可以拍摄该身体部分的第一图片，并且在 425 处，可以分析该图片。取决于所使用的特定过程，该分析可以采取多种不同形式中的一种。如果静止图像是足够的，则可以分析单个帧的内容。但是，如果系统希望观察并分析运动，则在该过程中“图片”可以由组成运动图片的一系列帧构成，并且可以执行逐帧分析以观察是否存在所预期的运动。

[0047] 如果所预期的身体行为的一次实例 (one-time instance) 就是所寻求的全部，则该过程可以跳至 450，以确定在第一图片中是否存在所预期的行为。但是，如果要比较之前的和之后的结果，则在 430 处，该设备可以提示该人以某种方式改变该身体部分的可见位置，并且在 435 处，拍摄第二图片。在 440 处，可以分析该第二图片。虽然该流程图示出了在拍摄第二图片之前执行对第一图片的分析，但是在一些实施例中，可以拍摄这两张图片，然后再分析其中任意一张图片。在 445 处，可以比较这两张图片，以确定该身体部分是否显示出了所预期的改变。如果没有，则立即或者在预定数量的重试之后，如在 460 处所指示的，该验证过程没有通过。但是如果该身体部分显示出了所预期的改变，则如 455 处所指示的，该验证过程通过。

[0048] 多阶段认证

[0049] 在一些应用中，对用户进行授权所需的安全等级可以取决于要访问的数据和 / 或要执行的操作。通常，更鲁棒的安全措施要求更高的计算功率和 / 或更多的时间来验证用户是被授权的。但是，大多数传统的安全访问过程是固定的，而不管该特定访问所要求的安全等级如何。与所需要的安全等级所要求的相比，这可能要求设备花费更多的功率，并且要求用户花费更长的时间。

[0050] 在一些实施例中，可以使用多等级的安全访问过程。一个相当简单且快速的过程可以准许用户访问一个等级的功能，其中功能包括对特定数据和 / 或操作的访问。在计算上要求更强分析的第二过程可以准许用户访问更高等级的功能。这可以扩展为包括针对更多等级的访问的更多过程，其中每个过程适合于所需等级的功能。在一些实施例中，可以通过经由设备的无线电单元将输入发送至另一设备（例如，服务器、“云”等）进行处理，来在该设备的外部执行更高要求的安全分析。

[0051] 在一些实施例中，可以要求用户通过一个等级的安全性，之后再给用户通过更高一等级的安全性的机会。由于可能会涉及到多种技术，因此这种多阶段过程可以提供极好的总体安全性。其也是灵活的，这是由于可以使用不同的分析组合来适应不同的情况和 / 或用户。

[0052] 但是在另一实施例中，用户可以请求特定等级的访问，并且将向用户仅呈现适合于该等级的安全访问过程。一旦准许，可以允许该用户访问直到并且包括该等级在内的所有等级的功能，但是不允许该用户访问更高等级的功能。

[0053] 实际上，这可以以多种方式来工作。作为实例，在设备的键盘上输入简单的 PIN 可以允许用户进行第一等级的访问。如果用户没有通过该过程，则可以不允许任何等级的访问。但是，如果用户通过，则诸如稍微详细的生物测定分析这样的更鲁棒的访问方法可以准许该用户进行更高等级的访问。如果用户没有通过该第二过程，则可以拒绝对该第二等级的访问。如果用户通过了第二等级过程，则可以准许他访问第二等级的功能，并且，利用更进一步鲁棒的访问过程，他可以有机会获得更进一步高等级的访问。当然，每个访问过程可以允许一定数量的重试，以适应简单的用户失误和 / 或测量系统的容限。

[0054] 在一些实施例中，没有通过访问过程将拒绝用户进入下一个等级，但是将允许该用户留在当前等级。在其它实施例中，没有通过访问过程将拒绝对下一个等级的访问，而且还将终止对当前等级的访问，并且可以终止对更低等级的访问。

[0055] 可以使用多个访问等级来控制对多个不同功能的访问。仅作为实例并且不应当被视为限制的一个实例可以是这五个渐进的访问等级：1）保持电话不锁定，2）对电话解锁，3）访问电子邮件，4）进行小于特定数额的财务事务，5）进行大于该特定数额的财务事务。

[0056] 虽然有时被描述为是访问的“更高”等级，但是在一些实施例中，各访问等级仅仅是不同的，而不意味着一个等级比另一个等级更重要或者更全面。例如，两部分数据可以具有同样的重要性和限制性，但是对每一部分的访问可以要求不同的访问过程，该过程示出了该用户之前已经获得了访问该数据的许可。

[0057] 图 5 示出了根据本发明的实施例准许对设备进行多个等级的受限访问的方法的流程图。在 510 处，设备可以接收对该设备功能的特定等级的访问的请求。该请求可以以各种方式被触发，诸如但不限于：1）人按下该设备上的一个或多个按钮，2）该设备感测到移动，3）开启该设备的电源，4）等等。在一些实施例中，第一等级的访问可以仅允许非常基础的功能，而不允许访问任何受限的、秘密的或者私人的信息。在一些实施例中，该等级的访问可以允许用于请求更高等级的访问的刚好够的功能。

[0058] 在接收到该请求后，在 515 处，该设备可以执行被设计为确定目标用户是否被授权进行这种访问的过程。如 520 处所确定的，如果授权过程没有通过，则在 525 处，可以拒绝该访问。但是，如果该授权过程通过，则在 530 处，可以准许所请求的访问，并且该设备可以执行在该等级处允许的任何功能。如果在 535 处，接收到对更高等级的访问的请求，则在 540 处，该设备可以执行被设计为确定目标用户是否被授权进行这种访问的更高等级访问过程。如果该过程没有通过，则在 550 处，可以拒绝所请求的访问，并且在一些实施例中，可以终止当前等级的访问。但是，如果该过程通过，则在 555 处，可以准许该更高等级的访问。如果针对该设备存在更进一步高等级的访问，则该过程可以针对这种等级继续。虽然所描述的过程是针对授权的，但是，在一些实施例中，一些或者全部的所述授权过程可以伴随有相关联的验证过程。在这种情况中，如果授权或者验证过程没有通过，则可以拒绝所请求的访问。

[0059] 在一些实施例中，授权所需要的具体动作可以是预定的并且被编程到设备中。在其它实施例中，所述动作可以是变化的但是在该设备中是确定的。在另外的实施例中，所述动作可以由该设备外部的源来指定。例如，为了准许用于执行大额的财务事务的用户授权，通信另一端的人或者计算机可以指定用户被授权所需要执行的动作。

[0060] 使用方法

[0061] 上述技术可以用于各种目的。一种这样的目的是允许用户访问手持电子设备。这种设备可以包括用于输入 PIN 或者其它访问代码的键盘，并且还可以包括用于捕获用户的眼睛、面部、手等的图像的照相机。这些技术可以用于初始访问，和 / 或可以用来在访问丢失（例如，如果设备在一段时间的不使用之后进入非操作低功率模式）之后恢复访问。这些技术还可以用于其它目的，诸如获得对更大的计算机、网络、建筑、空间、区域等的访问。在一些实施例中，如果人没有通过特定的技术，或者如果读数是含糊不清的，则可以使用不同的技术。相似地，不同的验证技术可以用来对预定特性的不同集合进行访问，而不管对这些

特性的访问是否被视为要求不同等级的安全性。

[0062] 上述描述旨在进行举例说明而非进行限制。本领域技术人员将会想到各种变型。这些变型也应被包括在仅由所附权利要求的范围来限制的本发明的各种实施例中。

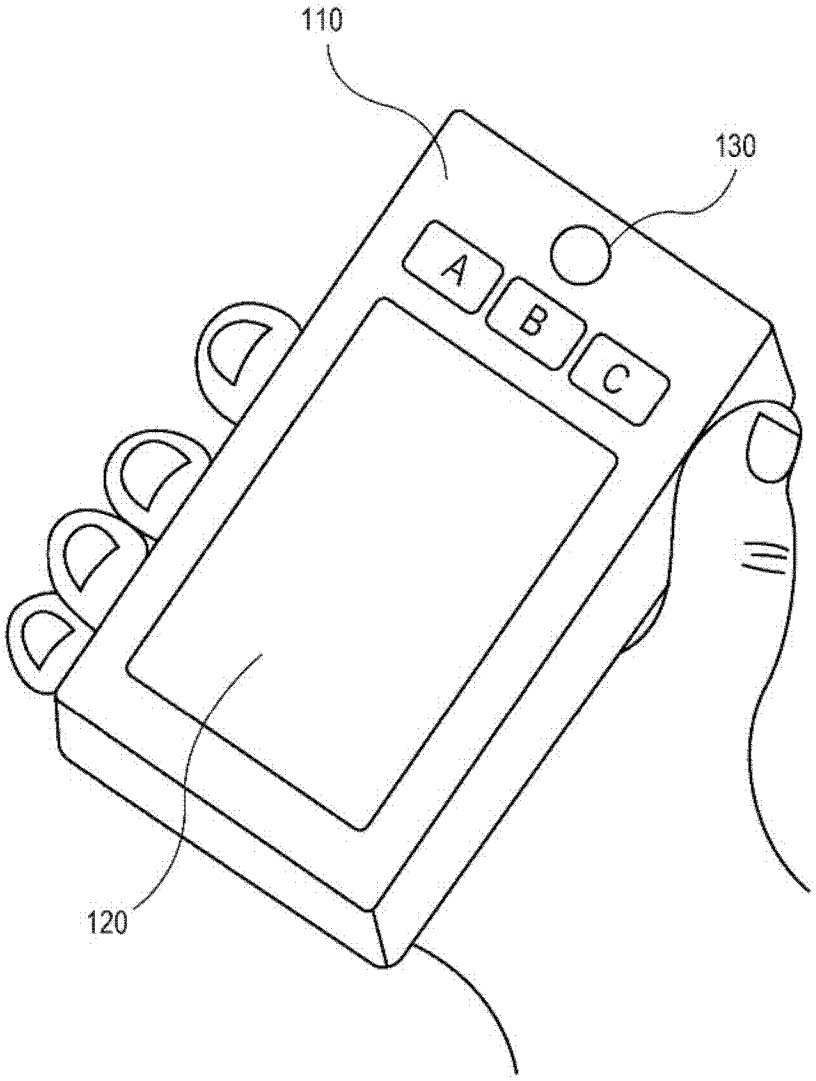



图 1

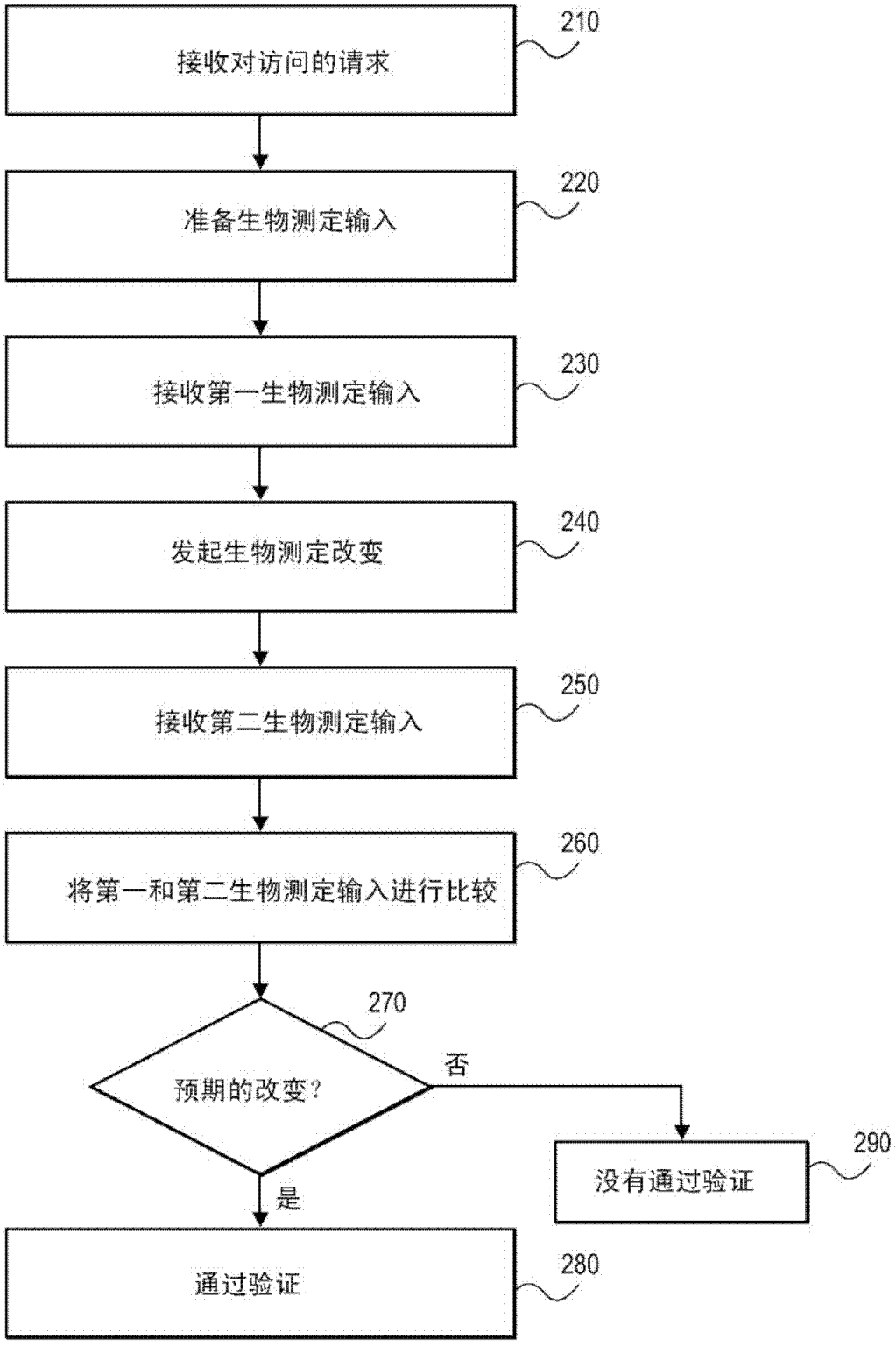

接收对访问的请求
210
准备生物测定输入
220
接收第一生物测定输入
230
发起生物测定改变
240
接收第二生物测定输入
250
将第一和第二生物测定输入进行比较
260
预期的改变？
270
否
没有通过验证
290
是
通过验证
280

图 2

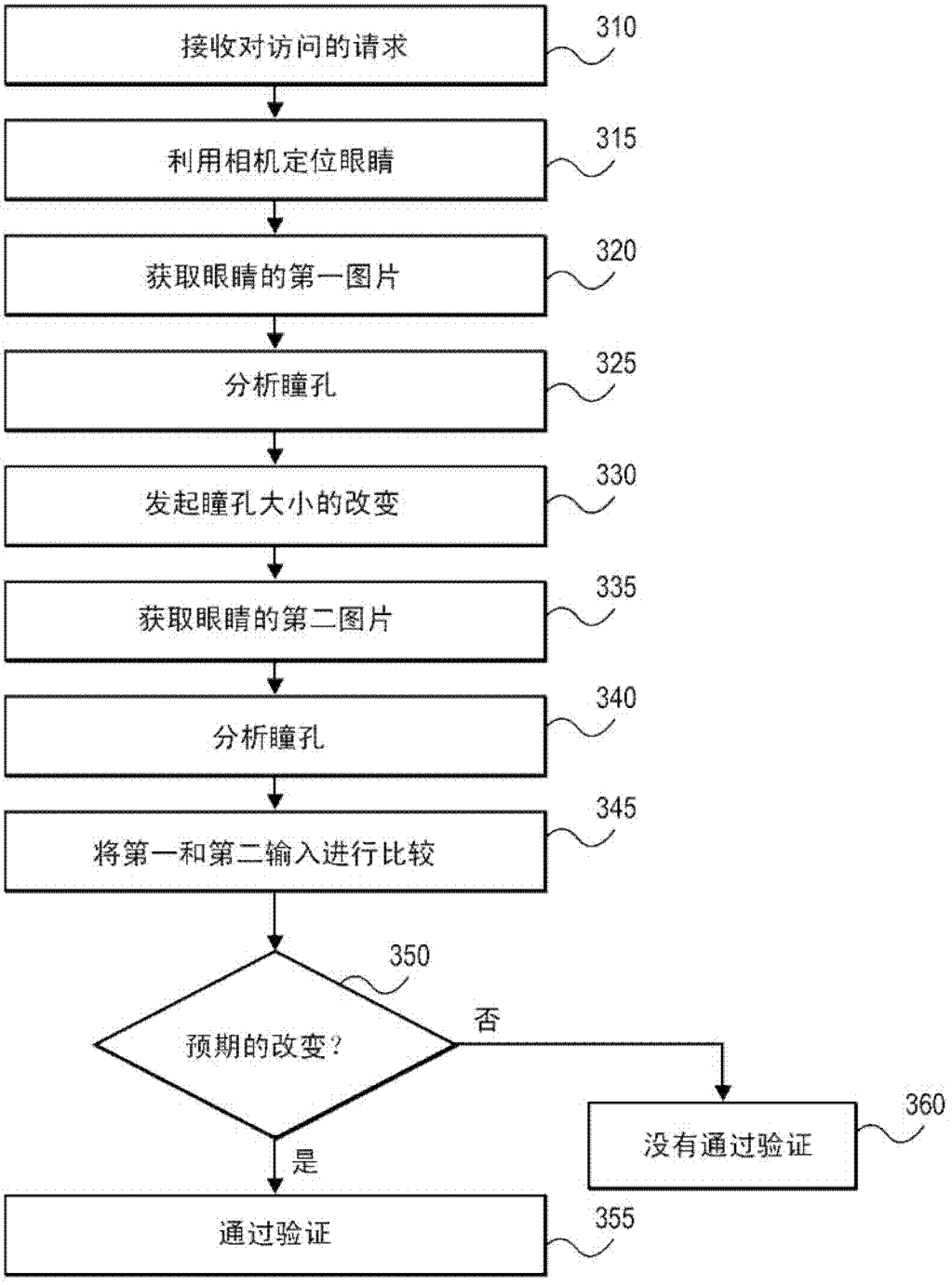

接收对访问的请求
310
利用相机定位眼睛
315
获取眼睛的第一图片
320
分析瞳孔
325
发起瞳孔大小的改变
330
获取眼睛的第二图片
335
分析瞳孔
340
将第一和第二输入进行比较
345
预期的改变？
350
否
是
没有通过验证
360
通过验证
355

图 3

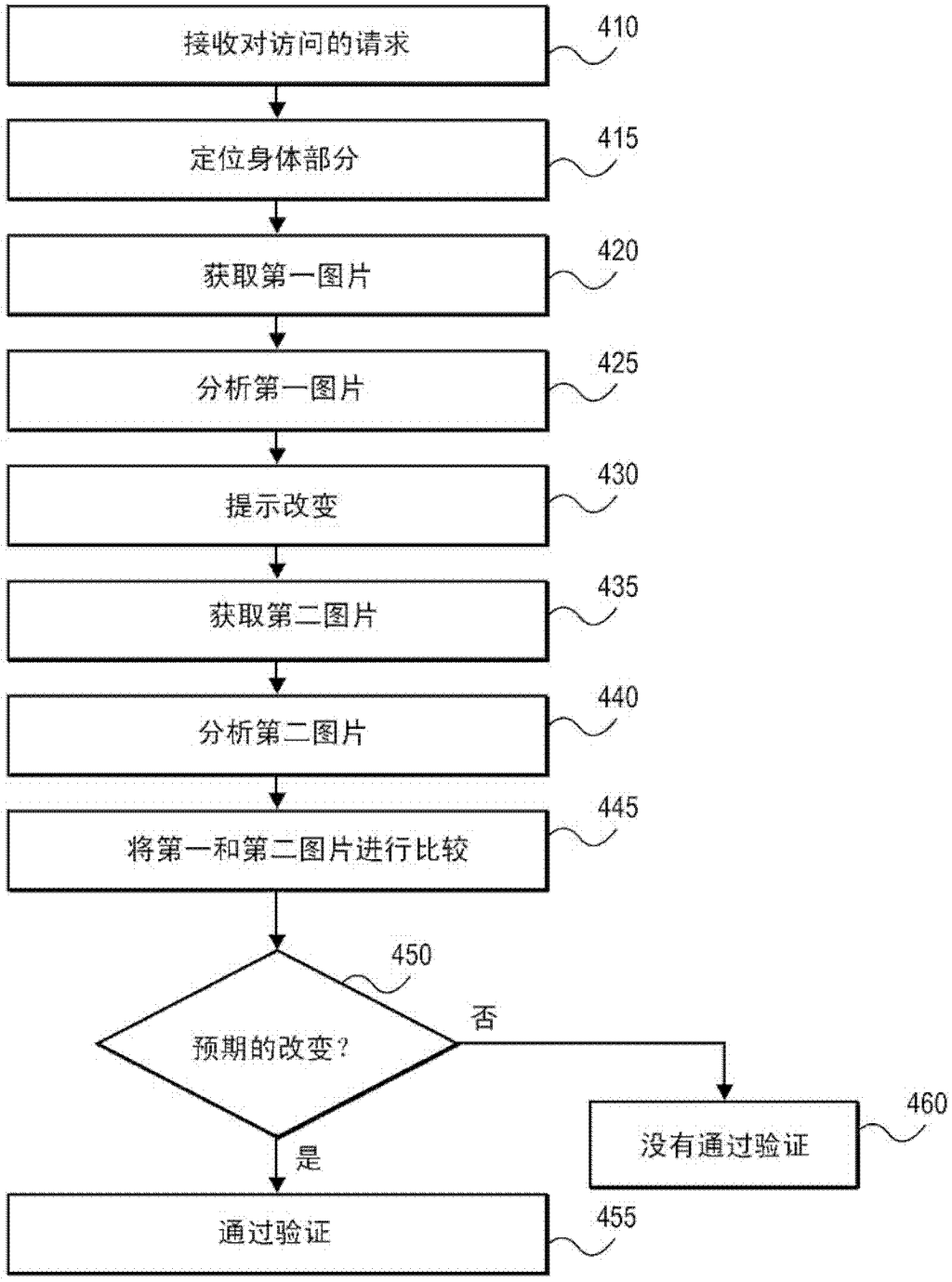

接收对访问的请求
410
定位身体部分
415
获取第一图片
420
分析第一图片
425
提示改变
430
获取第二图片
435
分析第二图片
440
将第一和第二图片进行比较
445
预期的改变？
450
否
是
没有通过验证
460
通过验证
455

图 4

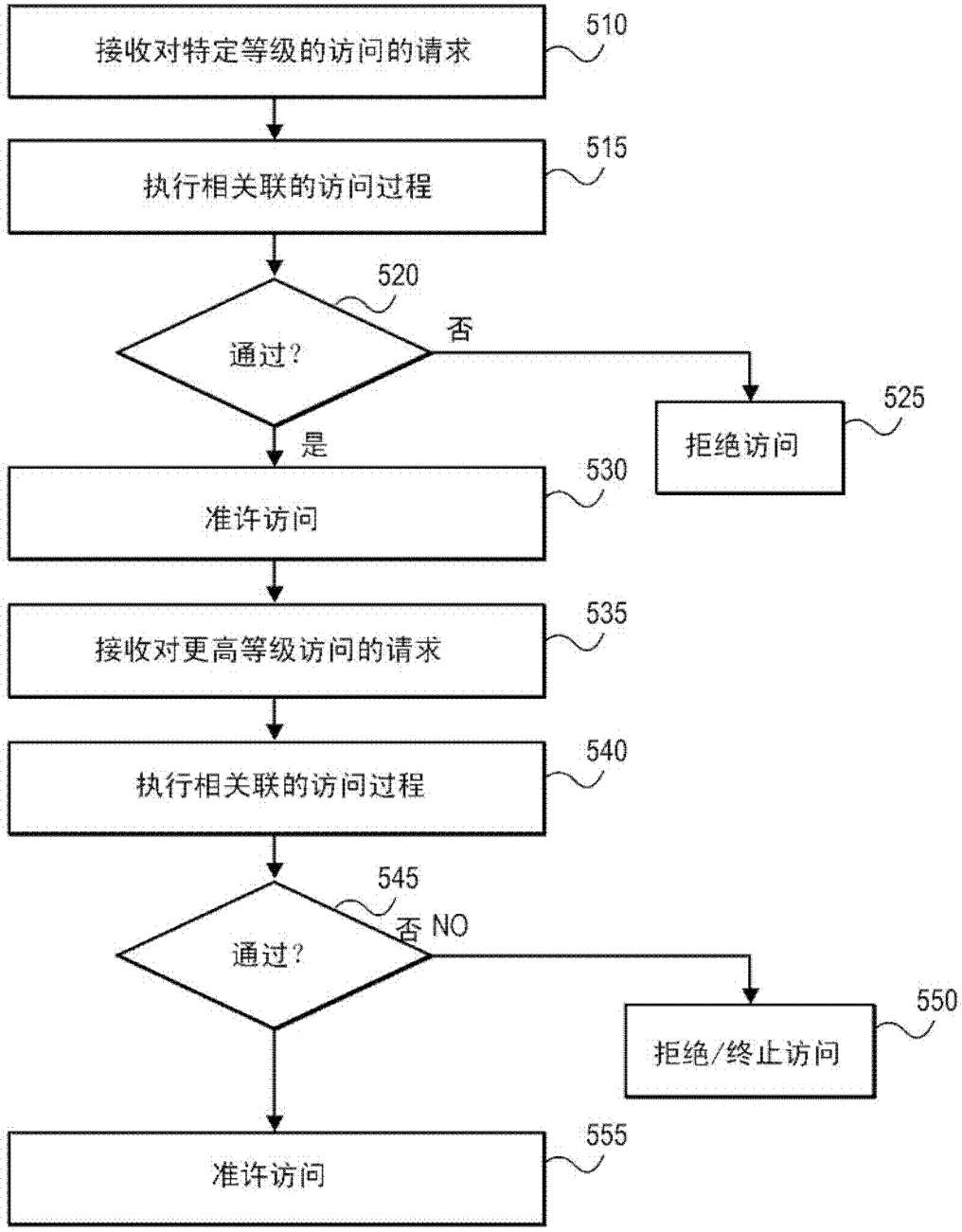

接收对特定等级的访问的请求
510
执行相关联的访问过程
515
520
通过?
否
525
拒绝访问
是
530
准许访问
接收对更高等级访问的请求
535
执行相关联的访问过程
540
545
通过?
否 NO
550
拒绝/终止访问
555
准许访问

图 5