(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 102713887 A
(43)申请公布日 2012.10.03

(21)申请号 200980161704.4

(22)申请日 2009.09.30

(85)PCT申请进入国家阶段日
2012.03.30

(86)PCT申请的申请数据
PCT/CN2009/001114 2009.09.30

(87)PCT申请的公布数据
WO2011/038533 EN 2011.04.07

(71)申请人 英特尔公司
地址 美国加利福尼亚州

(72)发明人 Z·黄 Q·张 K·桂
M·K·托比亚斯

(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 姜冰 朱海煜

(51)Int.Cl.
G06F 17/00(2006.01)

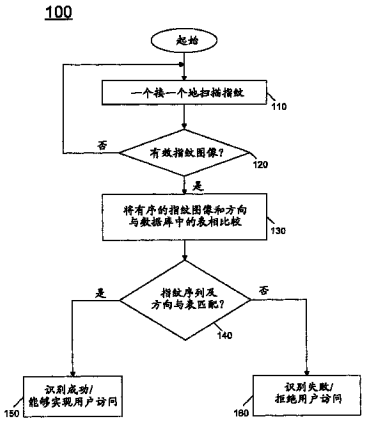
权利要求书 2 页 说明书 6 页 附图 7 页

(54)发明名称

增强系统的生物测定安全性

(57)摘要

在一个实施例中，一种方法包括经由生物测定传感器接收来自用户的生物测定输入的有序序列、确定有序序列中的每个输入是否与存储在表中的对应条目相匹配，所述表包括与用户的密码模式对应的生物测定输入的存储的有序序列，并且如果匹配，则使得用户能够访问处理系统，否则阻止用户访问处理系统。其他的实施例被描述并且被要求权利。



CN 102713887 A

1. 一种方法，包括：

经由与处理系统相关联的生物测定传感器接收来自用户的生物测定输入的有序序列；

确定生物测定输入的所述有序序列中的每个输入是否与所述处理系统的非易失性存储装置的表中存储的对应条目相匹配，所述表包括与所述用户的密码模式对应的生物测定输入的存储的有序序列；并且

如果匹配，则使得所述用户能够访问所述处理系统，并且否则阻止所述用户访问所述处理系统。

2. 如权利要求 1 所述的方法，其中生物测定输入的所述有序序列中的每个输入对应于所述用户的不同指头。

3. 如权利要求 1 所述的方法，其中生物测定输入的所述有序序列中的每个输入对应于所述用户的不同指头和所述生物测定传感器上的指头的移动的方向。

4. 如权利要求 1 所述的方法，其中每个条目还包括将生物测定输入的所述存储的有序序列中的一个输入与字母数字字符相对应的映射，并且其中所述用户的第一指头被映射到第一字母数字字符和所述用户的第二指头被映射到第二字母数字字符。

5. 如权利要求 4 所述的方法，其中如果生物测定输入的所述有序序列中的每个输入与对应的条目相匹配，则还包括确定每个条目的字母数字字符的汇集是否与密码数据库中存储的密码相匹配。

6. 如权利要求 1 所述的方法，还包括当生物测定输入的所述有序序列的数量少于生物测定输入的所述存储的有序序列的数量时，使得所述用户能够访问所述处理系统的有限部分。

7. 如权利要求 1 所述的方法，其中生物测定输入的所述有序序列具有第一长度 N，并且生物测定输入的所述存储的有序序列具有第二长度 M，其中 N 小于 M。

8. 如权利要求 1 所述的方法，还包括使得所述用户能够访问所述处理系统的第一功能以响应与生物测定输入的所述存储的有序序列的第一输入相匹配的单个生物测定输入。

9. 如权利要求 8 所述的方法，其中所述第一功能是所述处理系统的电话功能。

10. 如权利要求 9 所述的方法，还包括使得所述用户能够访问所述处理系统的第二功能以响应与生物测定输入的所述存储的有序序列的对应多个输入相匹配的多个生物测定输入。

11. 如权利要求 10 所述的方法，其中所述第二功能使得所述用户能够执行包括所述用户的账户信息的安全金融交易。

12. 一种包括机器可访问的存储媒体的物品，所述媒体包括指令，所述指令当被运行时使得系统能够：

请求用户经由与所述系统相关联的生物测定传感器录入生物测定输入的有序序列，生物测定输入的所述有序序列中的每个输入提供相对于所述生物测定传感器的指头的移动的方向；

经由所述生物测定传感器在所述系统中接收来自所述用户的生物测定输入的所述有序序列；以及

在与所述用户相关联的表的条目中存储生物测定输入的所述有序序列的每个输入的

扫描、与移动的方向有关的元数据、以及字母数字字符，所述表被存储在非易失性存储器中。

13. 如权利要求 12 所述的物品，还包括在被运行时使得所述系统能使所述用户能够选择密码的指令。

14. 如权利要求 13 所述的物品，还包括在被运行时使得所述系统能够存储所述密码到所述表中的条目的映射的指令，其中对于所述密码的元素的映射包括到包括所述元素的字母数字字符的所述表的条目的索引。

15. 如权利要求 12 所述的物品，还包括在被运行时使得所述系统能够执行以下操作的指令：

经由所述生物测定传感器在所述系统中接收来自所述用户的生物测定输入的第二有序序列；并且

确定生物测定输入的所述第二有序序列的每个输入是否与所述表中存储的对应条目相匹配，并且如果匹配，则使得所述用户能够访问所述系统，否则阻止所述用户访问所述系统。

16. 如权利要求 15 所述的物品，还包括在被运行时使得所述系统能够确定生物测定输入的所述第二有序序列是否对应于胁迫密码、并且如果是则向第三方传送胁迫警示的指令。

17. 如权利要求 15 所述的物品，还包括在被运行时使得所述系统能够确定生物测定输入的所述第二有序序列的每个输入是否与所述表的条目相匹配的指令，其中生物测定输入的所述第二有序序列的数量少于生物测定输入的所述有序序列的数量。

18. 一种系统，包括：

处理器，运行指令以接收来自用户的生物测定输入的有序序列，确定生物测定输入的所述有序序列的每个输入是否与表中存储的对应条目相匹配，所述表包括与用于所述用户的密码模式对应的生物测定输入的存储的有序序列，并且如果匹配，则使得所述用户能够访问所述系统，以及否则阻止所述用户访问所述系统；

生物测定传感器，耦合到所述处理器以向所述处理器提供生物测定输入的所述有序序列；并且

非易失性存储器，耦合到所述处理器，所述非易失性存储器存储所述表。

19. 如权利要求 18 所述的系统，其中所述表中的每个条目还包括将生物测定输入的所述存储的有序序列中的一个输入与字母数字字符相对应的映射，并且其中，所述用户的第一指头被映射到第一字母数字字符，和所述用户的第二指头被映射到第二字母数字字符。

20. 如权利要求 19 所述的系统，其中所述表中的每个条目还包括将生物测定输入的所述存储的有序序列的一个输入与对应的生物测定输入的移动方向相对应的映射。

21. 如权利要求 19 所述的系统，其中所述非易失性存储器还包括密码数据库以存储各自对应于用于所述用户的密码的多个条目。

22. 如权利要求 21 所述的系统，其中所述密码数据库的每个条目包括所述密码到所述表的条目的映射，其中，对于所述密码的元素的映射包括到包括所述密码元素的字母数字字符的所述表的条目的索引。

增强系统的生物测定安全性

背景技术

[0001] 随着基于处理器的系统的用户对他们的系统以及在此类系统中存储的数据越来越多的依赖，安全性顾虑增加。为了对此类系统提供安全性，时常密码被建立并且通常用于保护对系统的访问。附加的密码能用于保护对特定的应用、文件的访问以及与远程资源（诸如系统可访问的网站）的交互。更进一步的是，通过数据和文件的加密能提供安全性。

[0002] 然而，随着系统的各种使用，用户能面对越来越多数量的密码，这能导致丢失或混乱。因此，一些用户为许多不同类型的应用选择共同的密码，这能极大地危害安全性。

[0003] 一些系统通过某一类型的生物测定传感器 (biometric sensor) 来提供附加的安全性。例如，许多基于处理器的装置装配有充当识别设备的指纹传感器。然而，用户在该传感器上简单地一次放置 / 滑动（在任何移动的方向中）单个手指，而装置执行识别处理。然而，对于许多目的，这类安全性机制并不够强。

附图说明

[0004] 图 1 是表示按照本发明的一个实施例的指头的说明性映射的图。

[0005] 图 2 是按照本发明的一个实施例示出将指头和移动方向都映射到密码元素的图；

[0006] 图 3 是按照本发明的一个实施例的用于生成密码的方法的流程图；

[0007] 图 4 是按照本发明的一个实施例的用于密码认证的方法的流程图；

[0008] 图 5 是按照本发明的一实施例的用于生成密码的方法的流程图；

[0009] 图 6 是按照本发明的另一实施例的用于密码认证的方法的流程图；

[0010] 图 7 是用于与本发明的一个实施例一起使用的系统的框图。

具体实施方式

[0011] 实施例提供增强的安全识别过程，例如，以用于具有诸如指纹传感器的生物测定传感器的系统。为了按照本发明的一实施例执行识别，用户可在传感器上以预定的序列或顺序放置不同的指头（例如，手指或脚趾）。在一些实现中，用户可在不同的方向中滑动指头以使得扫描序列不同，甚至在使用相同的手指时。以此方式，识别比单个输入样式更健壮，因为即使心怀恶意的人看见用户将哪个手指放在传感器上，他可能不会意识到具体手指的顺序和滑动方向，并且因此不会学习到密码。

[0012] 在不同的实现中，不同指头的有序的序列（具有或不具有移动方向）能形成密码，在本文中也称为密码模式。注意到在一些实现中，密码模式可不包括任何字母数字字符，并且转而只对应于移动 / 指头的序列。在其他的实现中，将生物测定信息和 / 或用户移动映射到密码的元素（例如，字母数字值）的不同方式能被实现。虽然本发明的范畴在这方面中不受限制，但在一些实现中，用户的指头各自可映射到数字码，使得十个手指映射到数 0-9。

[0013] 在一个实施例中，不同指头的指纹的有序序列可用于表示纯数字的密码。以此方式，现有的数字（和 / 或字母数字）的密码能被转换为对于具体用户独特的指纹序列。以此方式，以前生成的密码能被转换为基于生物测定的密码以改善安全性健壮性。然而，如上

所述，在其他实现中，移动和手指的序列本身可形成序列密码，而无需到键盘字符的分开映射。

[0014] 图 1 是表示按照本发明的一个实施例的说明性映射的图。在图 1 的实施例中，左和右手两个的每个指头的指纹表示从 0-9 的数。虽然这是映射的一个示例，但用户可为每个指纹使用仅仅对他 / 她独特的任何表示。以此方式，实施例为密码提供了更强的物理加密，因为相同的密码（例如，01234）对于不同的用户（例如，对应于不同用户的指纹）将有不同的有序序列。例如，在一个实现中，使用对于不同的指头的密码的各个元素的映射，密码 0123 可映射到左手上的拇指、食指、中指和无名指的指纹的单个序列的识别简档 (profile)，正如图 1 中见到的。

[0015] 在其他实现中，用户移动和指头的组合可映射到对应的元素。例如，拇指印和给定方向中的移动（例如，左到右或上到下）可映射到给定的数或其他字符。在一些实现中，用户可选择期望的映射，而在其他实施例中，映射可由系统来预设。使用移动方向和指头的组合（例如，每个指头两个方向），能获得 20 个字符。

[0016] 在其中移动和指头的组合映射到值的实现中，一个示例的映射可如下：上到下和下到上的拇指滑动可映射到 0 和 1（分别）；上到下和下到上的食指滑动可映射到 2 和 3（分别）；并且上到下和下到上的中指滑动表示 4 和 5（分别）。当然，用户能使用不同的手指来表示不同的元素。

[0017] 在图 2 的实现中，映射被执行，其将指头和移动方向映射到密码元素。如在图 2 中见到的，用户将拇指按在传感器上并由左向右滑动为 0 值密码元素，而由右向左的移动代表 1 值密码元素。在这个示例中，密码 01010 能通过在传感器上将拇指移动为（起始自）左、右、左、右、左和右来表示。其他的手指和 / 或其他的移动能映射到不同的数，或甚至更具体的意义，其对不同的用户是独特的。例如，如果用户运用美国手语，他或她能选取使用“拼写”对于用户而言有意义的东西的方向和手指的集合。通常，用户能选取来自于任何语言的任何手指手势并用其创建具体的、容易记忆的模式，这些模式对用户而言是独特的。软件或固件考虑到传感器表面的形状和尺寸，并且能给用户不同的指导来设定密码。在一个实现中，系统可为用户呈现乐器布局，其能够实现序列或弦和指纹的组合的输入。或者映射能通过显示来自组合锁的转盘并追踪转盘被转到的数、并且哪个手指（且多少个手指）用于转动转盘来实现。在仍有的另一个实现（其中，生物测定传感器具有三维 (3D) 特征）中，滑过 3D 表面的动作能被映射到显示，例如，Rubik’s™ 的立方体或其他的设计的显示。

[0018] 现在参考图 3，所示的是按照本发明的一个实施例的方法的流程图。如图 3 中所示，方法 10 可用于映射用户的指纹和移动或笔划的方向以能够实现密码模式的生成。如图 3 中所示，该方法通过启动一个接一个指纹的捕获来开始（框 20）。例如，系统可启动指纹获取模块以引起生物测定传感器接收手指输入。在一个实施例中，可提供屏幕显示以通过不同的手指和移动方向的条目来指导用户。具体而言，如图 3 中见到的，在框 30，系统可要求用户录入 (enter) 对应于密码模式的移动 / 指纹的有序序列。系统然后可扫描给定指头的指纹并确定其移动的方向（框 40）。例如，密码模式的第一元素可对应于当其由上到下移过生物测定传感器的左食指。响应于这个输入，系统可在数据库的表的条目中存储指纹图像以及笔划方向（框 50）。在一个实施例中，该方向可作为注释扫描在其中发生的方向的元数据被存储。例如，指纹图像和笔划方向的这个组合可被录入到表的第一条目中，该表将

为这个特定用户存储密码模式，并且其本身可以是存储在系统中的用户密码的数据库的部分。

[0019] 仍然参考图 3，在菱形 60，可确定密码模式是否已被完成（菱形 60）。如果没有，则控制传递回框 40 等等以便对指纹 / 方向扫描的进一步获取和存储。注意到表可因此包括多个条目，这些条目各自存储对应的指纹图像和笔划方向。否则，控制传递到框 70，在该框，可完结 (conclude) 数据库中的表。因此，图 3 示出了获取对应于密码模式的有序序列的用户的指纹图像和移动方向的方法。注意到，在这个实施例中，不需将这些图像 / 移动映射到经由键盘可用的字符，因为密码模式转而可以是完全物理码，其组合所录入的具体用户指纹和移动方向。

[0020] 为了使得用户能够访问其中他 / 她具有一个或更多已存储的密码模式的系统，诸如有关图 4 描述的方法可被使用。现在参考图 4，所示出的是按照本发明的一个实施例的密码认证方法的流程图。如图 4 中所示，方法 100 可通过一个接一个地扫描指纹来开始（框 110）。此类扫描可通过用户录入具体顺序的指纹 / 方向来执行，如上面有关图 3 讨论的为密码模式生成所做的一样。对于每个输入，可确定有效指纹是否被获取（菱形 120）。如果是，则控制传递到框 130。否则控制传递回框 110 以寻求对应指纹的再录入。在一些实现中，系统可为用户提供关于是否每个输入被正确传感的信息并能按照需要来请求再输入。注意，在一些实施例中，在进行到框 130 之前，所有的指纹 / 方向可被扫描。在一些实施例中，用户输入可指示何时用户已经完成输入、以及哪个也是用户选择的。

[0021] 依据指纹 / 方向的接收，扫描 / 移动可与数据库中的表相比较（框 130），其中每个表对应于为用户存储的密码模式。更具体而言，在一个实现中，第一扫描 / 移动方向输入可与每个表中的第一条目相比较以确定是否存在匹配。框 130 和菱形 140 的比较 / 确定可逐一地进行直到检测到完全匹配表中存储的扫描 / 移动的完整密码模式。接下来，控制传递到菱形 140，其中可确定指纹序列和方向是否与数据库中的表相匹配。如果识别到完全的匹配，则识别过程已经成功地完成，并且能够实现用户访问（菱形 150）。否则，控制传递到框 160，在此访问能被拒绝。注意到访问通常可针对系统，或者针对具体应用、文件或等等。虽然在图 4 的实施例中以此特定的实现来示出，但本发明的范畴在这方面中不受限制。

[0022] 如上面讨论的，在其他实现中，指纹扫描（具有或不具有方向）的用户的条目可被映射到字符，例如，键盘的字母数字字符。因此，上面有关图 3 和 4 所讨论的密码创建和认证的实施例可被改变为接纳此类映射。现在参考图 5，所示的是按照本发明的一实施例的生成密码的方法的另一实施例。如图 5 中所示，方法 200 可用于生成密码。通常方法如上面有关图 3 讨论的进行。具体而言，指纹捕获的启动可被执行（框 210）。然后指纹的扫描可发生，具有或不具有方向元数据的捕获（框 220）。然后这个指纹扫描可被映射到密码元素（框 230）。在一个实施例中，在密码元素（例如，字母数字字符）和指纹扫描 / 方向之间的这个映射形成将被存储在数据库表中的条目，即，表的每个条目可包括对应的扫描、字符以及（可能的）扫描方向。用户可选择密码元素或者计算机可如此做。然后控制传递到菱形 240，其中可确定是否所有的指头已经被扫描。如果没有，则控制传递回上面所讨论的框 220。

[0023] 仍然参考图 5，当已经扫描进完全数量的指头时，这些映射可为用户被存储到非易失性存储装置中（框 250）。例如，包括各自对应于给定扫描（具有或不具有方向）和到字

符的对应映射的的多个条目的表可被存储。

[0024] 在一个实施例中，系统然后可准许用户能够实现密码的选择（框 260）以便每个手指（具有或不具有方向）映射到密码的不同的字符元素。在一个实施例中，这个映射可经由到对于对应字符的对于用户的数据库表的条目的位置的索引，即，密码表的每个条目可存储字符以及到对于这个字符的数据库表的位置的索引。因此，这个密码可以是与用户映射相关联的并被存储（例如）在非易失性存储装置的密码表中（框 270）。虽然在图 5 的实施例中以这个特定的实现来示出，本发明的范畴在此方面中不受限制。

[0025] 类似地，一种认证方法可考虑到此类映射。现在参考图 6，所示的是按照本发明的另一实施例的认证方法的流程图。如图 6 中所示，方法 300 可如上面有关图 4 讨论的一样开始。具体而言，多个指纹可一次一个地被扫描（框 310）并且可确定每个此类图像是否有效（菱形 320）。然后，每个有序的指纹图像可针对表的数据库被检查（每个表用于某个用户且包括到字符的扫描 / 方向的映射的条目）并且基于非易失性存储装置中所存储的映射而被转化（框 330）。上面步骤对于每个用户输入扫描可被执行。然后可确定转化的字符是否与密码数据库中存在的用户的存储的密码相匹配（菱形 340）。如果不匹配，则可确定是否访问已经被尝试了阈值次数（菱形 380）。如果没有，则指纹可被再扫描。如果访问已经被尝试了阈值次数，则控制传递到框 390，其中用户访问可被拒绝。

[0026] 在菱形 340，如果转化的字符确实与密码相匹配，接下来可确定其是与标准密码相匹配还是与胁迫密码相匹配（菱形 350）。事实上，一些实施例可能够实现备用密码的检测，即，当用户出于胁迫之下时所录入的胁迫密码，其可能够实现对系统的最小访问和 / 或能够实现到第三方的信号以警告该胁迫。在这些实施例中，用户在胁迫之下以备用模式录入密码，并且系统不同地响应。系统能认出该录入为恐慌 (panic) 密码并且可给予对系统有限的（或无）访问，和 / 或引起胁迫警示 (alert) 被发送。

[0027] 如果在菱形 350 中确定是标准密码匹配，则控制传递到框 370，其中识别是成功的并且能够实现用户访问，即，正常的用户访问。如果转而匹配是对于胁迫密码的，则控制可传递到框 360，其中识别成功可导致可能有限的用户访问（或无访问）以及胁迫警报的启动。

[0028] 注意到，图 6 的方法也可用于对之前以纯字母数字密码存储的密码接收生物测定用户输入，从而能够实现向后兼容性以提高健壮性。虽然在图 5 和 6 的实施例中以此特定的实现来示出，但应当理解本发明的范畴在这方面中不受限制并且如上面的讨论的，具有或不具有移动方向的指纹扫描本身可形成密码而没有到字符的转化或映射。

[0029] 许多变化是可能的。例如，在一些实现中，生物测定认证能用作一种不必使用键盘而执行（例如字母数字）字符的安全输入以直接向计算机录入信息而不是密码的方式。因此，对于公共场合中的用户来说，诸如信用卡信息的信息能无需在键盘上键入就能录入，因此能够实现录入信息的安全方式。

[0030] 随着在密码中包括了更多离散的元素，认证的强度也被增加。在一些实现中，不同数量的密码元素能用于提供对系统或者系统上信息 / 应用的变化级别的访问。例如，对于解锁移动电话以进行电话呼叫，单个手指的单次滑过就能将其解锁，从而给出对电话功能的访问。然而如果，对于期望访问个人信息（例如，信用卡信息）的金融交易，不是仅使用单个指头，而是能要求多个指头 / 方向（例如，三个手指）。以此方式，能够实现认证的等

级。

[0031] 在一个示例中，单个密码模式可以是第一数量的元素（例如，20），密码的不同部分（例如，从第一元素开始）可用于不同的认证级别。例如，仅仅一个元素可用于获得对装置的访问，五个元素用于访问一个类型的应用，并且还有附加的元素用于访问安全应用等等。其他实施例可准许 M 中的 N 密码的使用。在此类实现中，认证要求 M 元素密码的至少 N 个元素，例如，十个中的三个或者五个中的三个或等等。当与一实施例一起使用时，M 中的 N 可通过指定必须使用的手指的数量和模式刷 (swipe) 并且使得使用的实际手指是不相关的来实现。例如，认证策略可接收至少三个不同的手指，其各自具有移动模式。其他的实现可要求双手上的多个手指。

[0032] 在日常生活中有如此多的密码，并且一些人总是忘记密码，引起许多不便。使用本发明的一实施例，人们甚至能够在记事本中写下他们的密码而无需顾及危害，因为没有手指和移动的物理组合，仅有密码的录入将不准许访问。

[0033] 实施例可被结合到许多不同的处理系统中，例如，实施例可连同计算机来使用，其中计算机的范围从笔记本、台式机到服务器计算机以及移动因特网装置、智能电话等等。任何此类处理系统可包括或被关联于生物测定传感器，而生物测定传感器可被配置到系统中或与系统相适应，例如，作为诸如经由通用串行总线 (USB) 端口的外围装置。在一些实现中，不是经由专用的生物测定传感器，而是经由触摸屏（例如电容传感触摸屏）和将触摸屏上的动作转换为生物测定扫描的逻辑和 / 或固件、软件的组合能实现生物测定传感功能。

[0034] 图 7 是用于与本发明的一个实施例一起使用的系统的框图。在一个实施例中，处理系统 400 可以是诸如智能电话的移动因特网装置，虽然实施例能被结合到许多不同的处理系统中。如所见到的，系统 400 包括应用处理器 410，其可以是通用的或专用的处理器，诸如微处理器、微控制器、可编程门阵列 (PGA) 或诸如此类。处理器 410 可包括多个核 412 和高速缓存存储器 414。处理器 410 可还包括集成的存储器控制器 430，其在一个实施例中可被耦合到系统存储器 420（例如，动态随机存取存储器 (DRAM)）。处理器 410 可还包括集成的输入 / 输出 (I/O) 控制器中心 (hub)440。处理器 410 可耦合到视频控制器 435，其又可耦合到可包括电容触摸屏以接收用户输入的显示器 437。

[0035] 闪速存储器 460 可提供非易失性存储，其可包括密码表，所述密码表包括用于系统的一个或更多用户的基于生物测定的条目，并且其能用于与来自寻求访问的用户的生物测定输入的接收进行比较。此外，基带处理器 450 可经由无线接口 462 来控制通信，该接口可用于经由蜂窝或其他无线网络进行通信。

[0036] 此外，按照本发明的一实施例，生物测定传感器 470 可存在于系统中以能够实现指纹或其他扫描，从而为系统提供安全性。虽然在图 7 的实施例中被示为分开的组件，但理解在其他的实现中生物测定传感器 470 可被配置在显示器之内。虽然描述对系统 400 的具体组件进行了参考，但是预期到描述和示出的实施例的众多修改和变化可以是可能的。

[0037] 实施例可以在代码中实现或者可被存储在存储媒体中，其上已经存储了能用于编程系统以执行指令的指令。所述存储媒体可包括但不限于，包括软盘、光盘、光盘、固态驱动 (SSD)、紧致盘只读存储器 (CD-ROM)、可改写紧致盘 (CD-RW) 以及磁光盘的任何类型的盘、诸如只读存储器 (ROM)、诸如动态随机存取存储器 (DRAM) 和静态随机存取存储器 (SRAM) 的随机存取存储器 (RAM)、可擦除可编程只读存储器 (EPROM)、闪速存储器、电可擦除可编程

只读存储器 (EEPROM) 的半导体装置、磁或光卡、或适合于存储电子指令的任何其他类型的媒体。

[0038] 虽然已关于有限数量的实施例描述了本发明，但是本领域的技术人员将从其领会到许多修改和变化。附带的权利要求旨在覆盖如落入本发明的真正精神和范畴内的所有此类修改或变化。

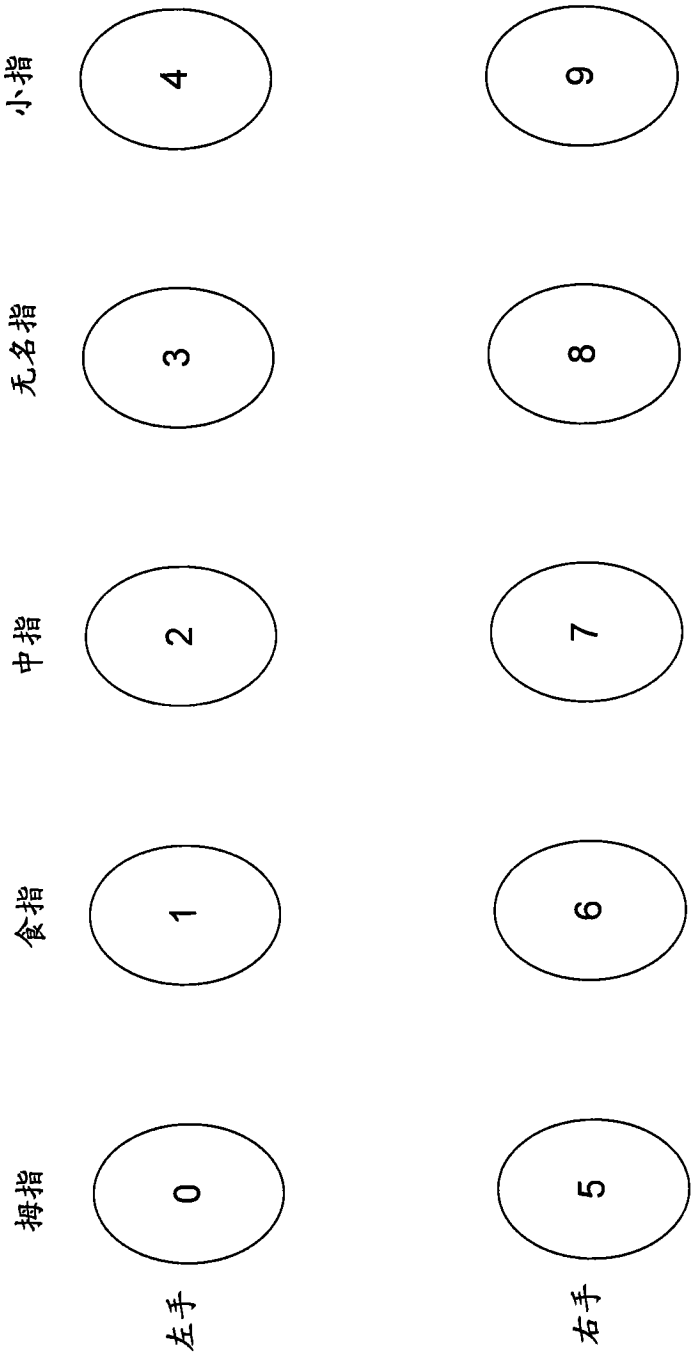


图 1

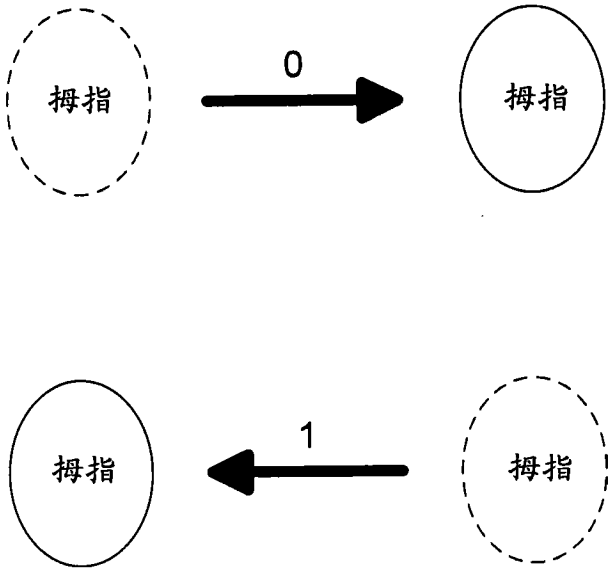


图 2

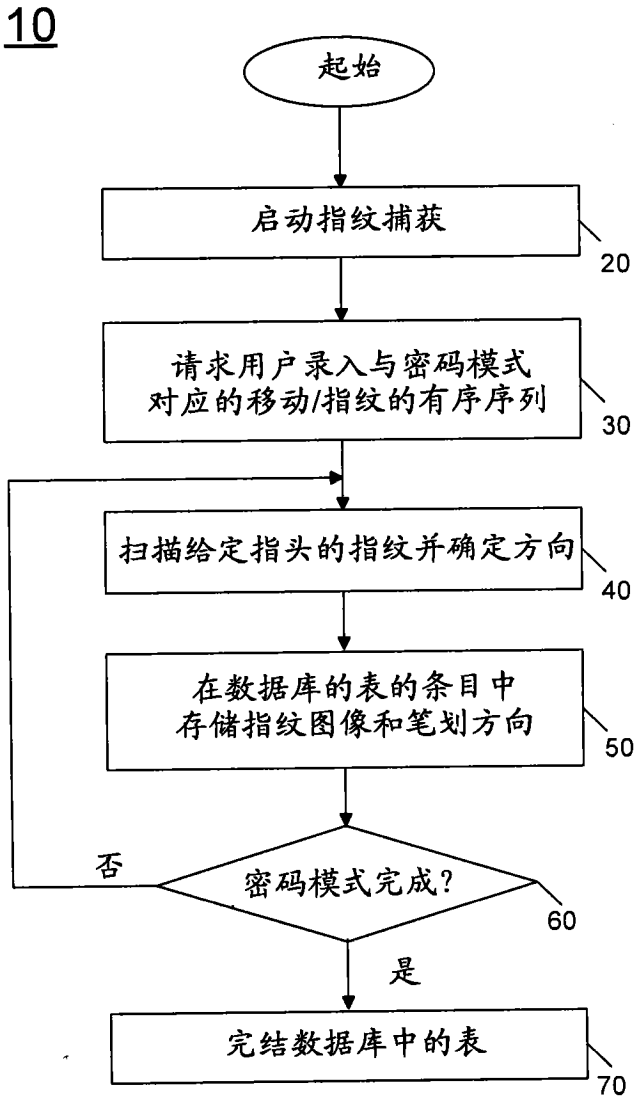

10
起始
启动指纹捕获
20
请求用户录入与密码模式
对应的移动/指纹的有序序列
30
扫描给定指头的指纹并确定方向
40
在数据库的表的条目中
存储指纹图像和笔划方向
50
否
密码模式完成?
60
是
完结数据库中的表
70

图 3

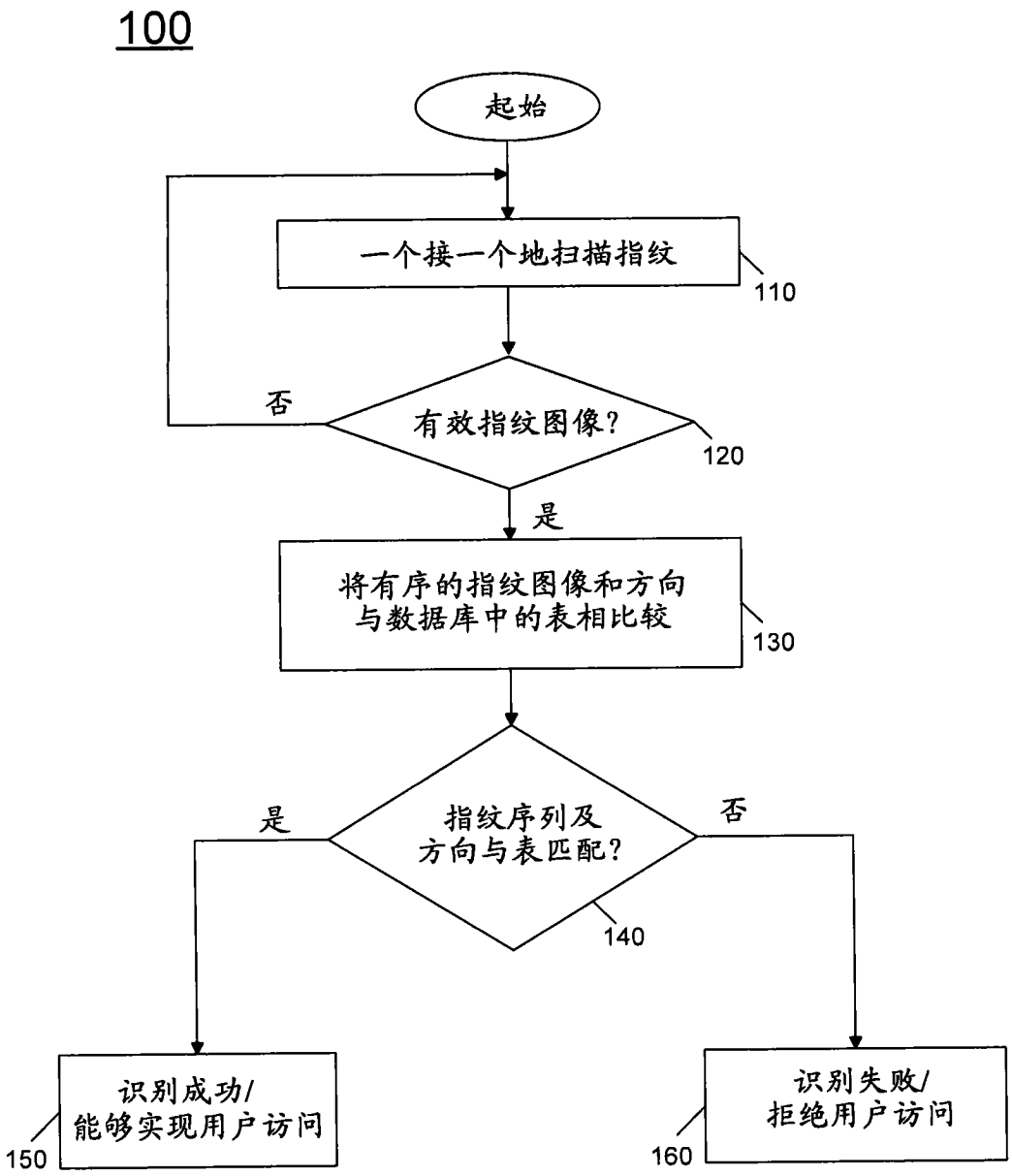

100
起始
一个接一个地扫描指纹
110
否
有效指纹图像?
120
是
将有序的指纹图像和方向
与数据库中的表相比较
130
是
指纹序列及
方向与表匹配?
否
140
识别成功/
能够实现用户访问
150
识别失败/
拒绝用户访问
160

图 4

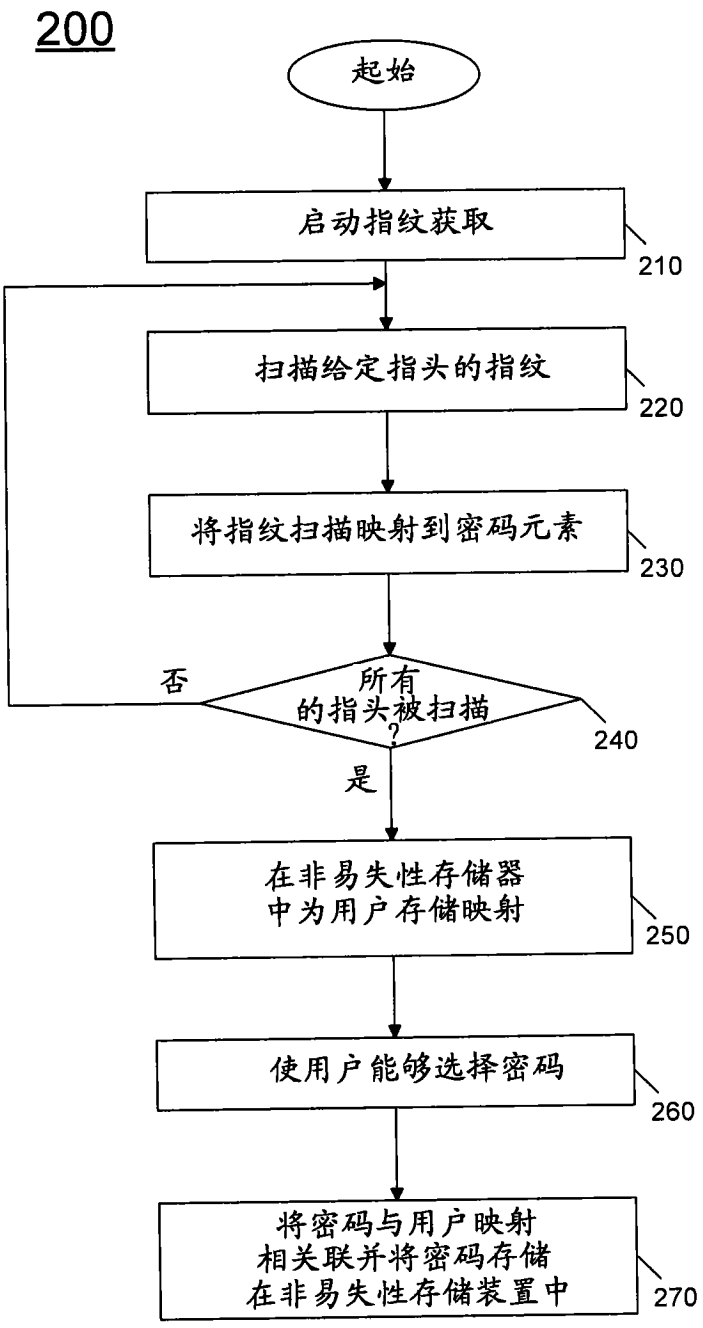

200
起始
启动指纹获取
210
扫描给定指头的指纹
220
将指纹扫描映射到密码元素
230
否
所有的指头被扫描？
240
是
在非易失性存储器中为用户存储映射
250
使用户能够选择密码
260
将密码与用户映射相关联并将密码存储在非易失性存储装置中
270

图 5

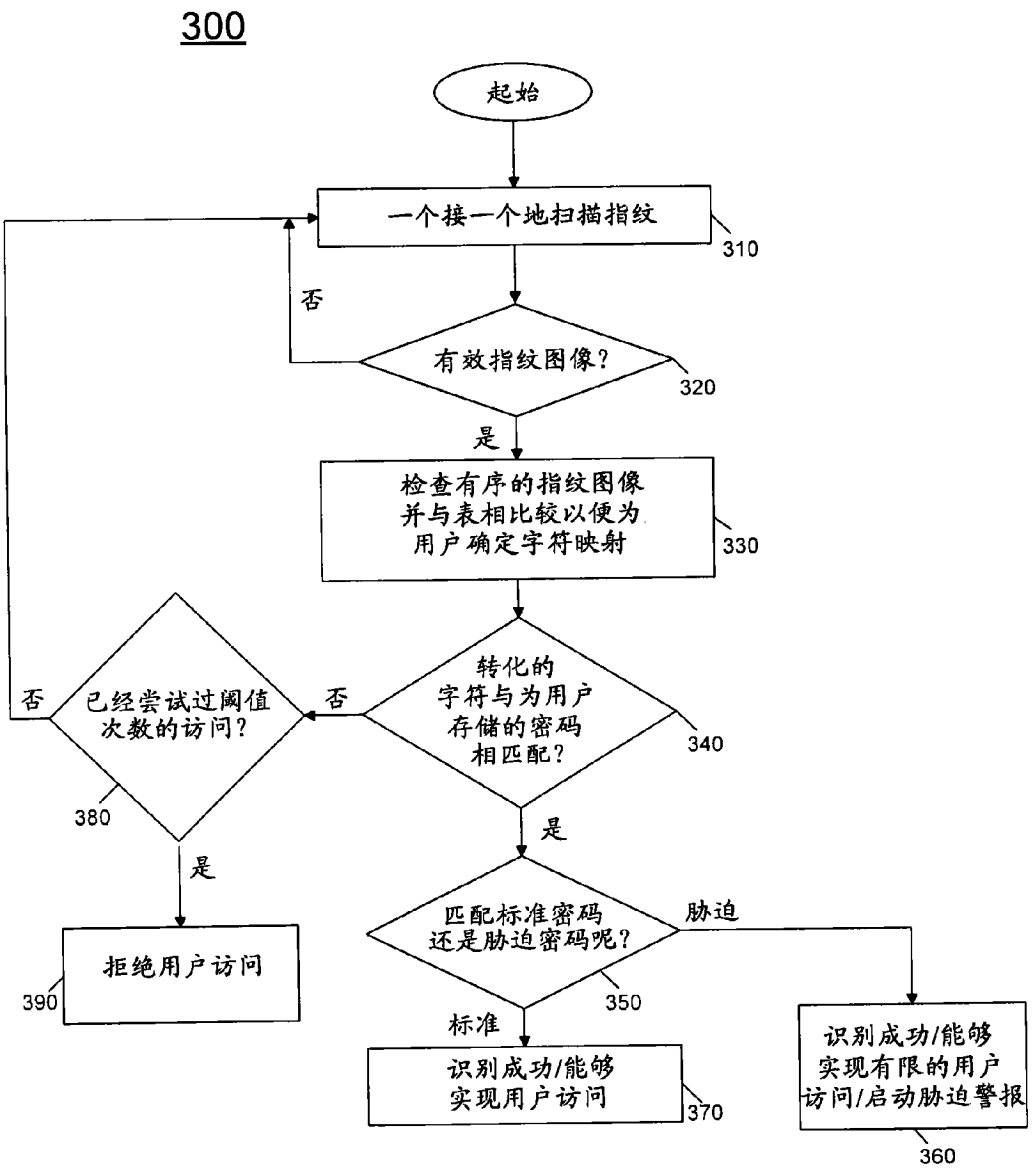

300
起始
一个接一个地扫描指纹
310
否
有效指纹图像?
320
是
检查有序的指纹图像
并与表相比较以便为
用户确定字符映射
330
转化的
字符与为用户
存储的密码
相匹配?
340
否
已经尝试过阈值
次数的访问?
380
否
是
拒绝用户访问
390
是
匹配标准密码
还是胁迫密码呢?
350
胁迫
标准
识别成功/能够
实现用户访问
370
识别成功/能够
实现有限的用户
访问/启动胁迫警报
360

图 6

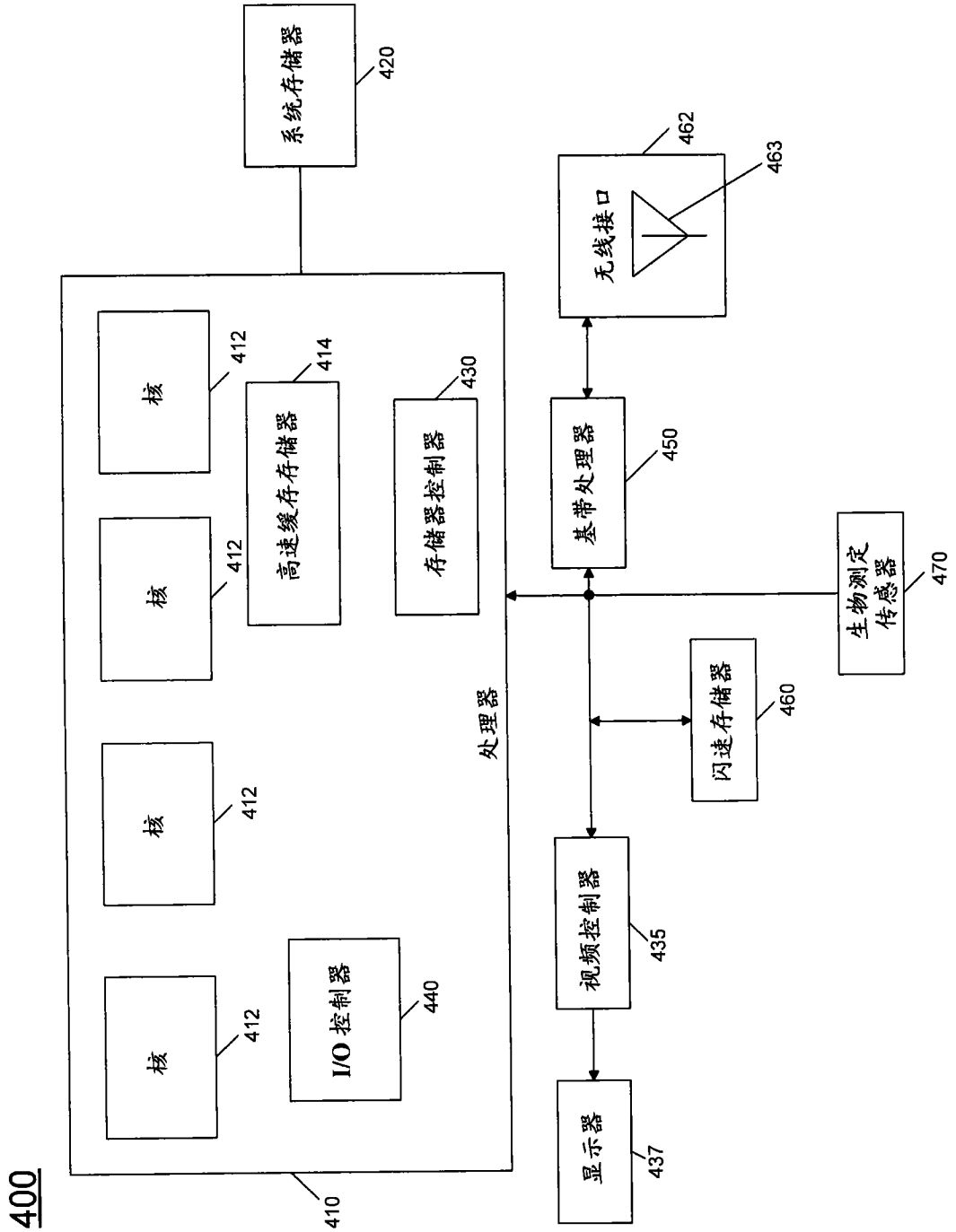

400
处理器
410
核
412
核
412
核
412
核
412
高速缓存存储器
414
存储器控制器
430
I/O 控制器
440
系统存储器
420
基带处理器
450
无线接口
462
463
闪速存储器
460
生物测定传感器
470
视频控制器
435
显示器
437

图 7