(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 110473311 B
(45)授权公告日 2021.07.23

(21)申请号 201810437289.1

(22)申请日 2018.05.09

(65)同一申请的已公布的文献号
申请公布号 CN 110473311 A

(43)申请公布日 2019.11.19

(73)专利权人 杭州海康威视数字技术股份有限公司
地址 310051 浙江省杭州市滨江区阡陌路555号

(72)发明人 魏凡 丁少杰 华丛一 康卫昌 申川

(74)专利代理机构 北京博思佳知识产权代理有限公司 11415
代理人 林祥

(51)Int.Cl.
G07C 9/37(2020.01)
G06K 9/00(2006.01)

(56)对比文件
CN 106778525 A,2017.05.31
CN 106846577 A,2017.06.13
CN 105825562 A,2016.08.03
US 2002191817 A1,2002.12.19
EP 2443532 A1,2012.04.25

审查员 袁蔚涛

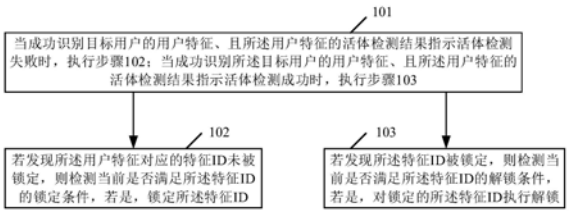
权利要求书3页 说明书8页 附图3页

(54)发明名称

防范非法攻击方法、装置及电子设备

(57)摘要

本申请提供了防范非法攻击方法、装置及电子设备。本申请中，在成功识别目标用户的用户特征的前提下，若用户特征的活体检测失败，则在用户特征对应的特征ID满足锁定条件时锁定所述特征ID，之后，即使后续再对所述用户特征尝试活体检测时发现活体检测成功，也不直接确定用户特征通过身份认证，而是检测所述特征ID是否满足解锁条件，在满足解锁条件时先解锁所述特征ID，之后再对所述用户特征尝试活体检测时发现活体检测成功，才确定所述用户特征通过身份认证，这能够防止误判攻击者提供的用户特征通过身份认证，进一步降低非法攻击的可能，提高安全性。



CN 110473311 B

1.一种防范非法攻击的方法,其特征在于,该方法包括:

当成功识别目标用户的用户特征、且所述用户特征的活体检测结果指示活体检测失败时,若发现所述用户特征对应的特征ID未被锁定,则判断所述特征ID与本地记录的上一次活体检测失败的用户特征的特征ID是否相同,若相同,则将本地存在的与所述特征ID对应的活体检测失败计数器的计数增加第一设定值,检测增加了所述第一设定值的计数是否大于或等于预设阈值N,若是,锁定所述特征ID;

当成功识别所述目标用户的用户特征、且所述用户特征的活体检测结果指示活体检测成功时,若发现所述特征ID被锁定,则判断所述特征ID与本地记录的上一次活体检测成功的用户特征的特征ID是否相同,若相同,将本地存在的与所述特征ID对应的活体检测成功计数器的计数增加第一设定值,检测增加了所述第一设定值的计数是否大于或等于预设阈值M,若是,对锁定的所述特征ID执行解锁。

2.根据权利要求1所述的方法,其特征在于,当成功识别目标用户的用户特征、且所述用户特征的活体检测结果指示活体检测失败时,若发现所述用户特征对应的特征ID未被锁定,则当判断所述特征ID与本地记录的上一次活体检测失败的用户特征的特征ID不同,或者,当判断所述特征ID与本地记录的上一次活体检测失败的用户特征的特征ID相同,但检测增加了所述第一设定值的计数小于预设阈值N,该方法进一步包括:

禁止锁定所述特征ID。

3.根据权利要求2所述的方法,其特征在于,当判断出所述特征ID与本地记录的上一次活体检测失败的用户特征的特征ID不同时,该方法进一步包括:

检测本地是否存在与所述特征ID对应的活体检测失败计数器,

若否,在本地新建所述活体检测失败计数器,将所述活体检测失败计数器的计数置为第二设定值;

若是,将所述活体检测失败计数器的计数置为第二设定值。

4.根据权利要求1所述的方法,其特征在于,当成功识别所述目标用户的用户特征、且所述用户特征的活体检测结果指示活体检测成功时,若发现所述特征ID被锁定,则当判断所述特征ID与本地记录的上一次活体检测成功的用户特征的特征ID不同,或者,当判断所述特征ID与本地记录的上一次活体检测成功的用户特征的特征ID相同,但检测增加了所述第一设定值的计数小于预设阈值M,该方法进一步包括:

禁止对对锁定的所述特征ID执行解锁。

5.根据权利要求4所述的方法,其特征在于,当判断出所述特征ID与本地记录的上一次活体检测成功的用户特征的特征ID不同时,该方法进一步包括:

检测本地是否存在与所述特征ID对应的活体检测成功计数器,

若否,在本地新建所述活体检测成功计数器,将所述活体检测成功计数器的计数置为第二设定值;

若是,将所述活体检测成功计数器的计数置为第二设定值。

6.根据权利要求1所述的方法,其特征在于,在锁定所述特征ID后,该方法进一步包括:启动所述特征ID对应的计时器,所述计时器在启动后从最大计时时间T开始递减,在递减到设定时间门限时指示对所述特征ID执行解锁;

当成功识别目标用户的用户特征、且所述用户特征的活体检测结果指示活体检测失败

时，若发现所述用户特征对应的特征ID被锁定，该方法进一步包括：重启所述特征ID对应的计时器；

在解锁所述特征ID之后，该方法进一步包括：关闭或删除所述特征ID对应的计时器。

7.一种防范非法攻击的装置，其特征在于，该装置包括：

特征识别模块，用于识别目标用户的用户特征；

活体检测模块，用于对所述用户特征进行活体检测；

处理模块，用于在所述特征识别模块成功识别所述用户特征、且所述活体检测模块对所述用户特征的活体检测失败时，若发现所述用户特征对应的特征ID未被锁定，则判断所述特征ID与本地记录的上一次活体检测失败的用户特征的特征ID是否相同，若相同，则将本地存在的与所述特征ID对应的活体检测失败计数器的计数增加第一设定值，检测增加了所述第一设定值的计数是否大于或等于预设阈值N，若是，锁定所述特征ID；以及，

在所述特征识别模块成功识别所述用户特征、且所述活体检测模块对所述用户特征的活体检测成功时，若发现所述特征ID被锁定，则判断所述特征ID与本地记录的上一次活体检测成功的用户特征的特征ID是否相同，若相同，将本地存在的与所述特征ID对应的活体检测成功计数器的计数增加第一设定值，检测增加了所述第一设定值的计数是否大于或等于预设阈值M，若是，对锁定的所述特征ID执行解锁。

8.根据权利要求7所述的装置，其特征在于，所述处理模块在当成功识别目标用户的用户特征、且所述用户特征的活体检测结果指示活体检测失败时，若所述用户特征对应的特征ID未被锁定，则当判断所述特征ID与本地记录的上一次活体检测失败的用户特征的特征ID不同，或者，当判断所述特征ID与本地记录的上一次活体检测失败的用户特征的特征ID相同，但检测增加了所述第一设定值的计数小于预设阈值N，进一步禁止锁定所述特征ID。

9.根据权利要求8所述的装置，其特征在于，所述处理模块在判断出所述特征ID与本地记录的上一次活体检测失败的用户特征的特征ID不同时，进一步检测本地是否存在与所述特征ID对应的活体检测失败计数器，

若否，在本地新建所述活体检测失败计数器，将所述活体检测失败计数器的计数置为第二设定值；

若是，将所述活体检测失败计数器的计数置为第二设定值。

10.根据权利要求7所述的装置，其特征在于，所述处理模块在成功识别所述目标用户的用户特征、且所述用户特征的活体检测结果指示活体检测成功时，若发现所述特征ID被锁定，则当判断所述特征ID与本地记录的上一次活体检测成功的用户特征的特征ID不同，或者，当判断所述特征ID与本地记录的上一次活体检测成功的用户特征的特征ID相同，但检测增加了所述第一设定值的计数小于预设阈值M时，进一步禁止对对锁定的所述特征ID执行解锁。

11.根据权利要求10所述的装置，其特征在于，所述处理模块在判断出所述特征ID与本地记录的上一次活体检测成功的用户特征的特征ID不同时，进一步检测本地是否存在与所述特征ID对应的活体检测成功计数器，

若否，在本地新建所述活体检测成功计数器，将所述活体检测成功计数器的计数置为第二设定值；

若是，将所述活体检测成功计数器的计数置为第二设定值。

12.根据权利要求7所述的装置,其特征在于,所述处理模块在锁定所述特征ID后,进一步启动所述特征ID对应的计时器,所述计时器在启动后从最大计时时间T开始递减,在递减到设定计时时间门限时指示对所述特征ID执行解锁;

所述处理模块在所述特征识别模块成功识别目标用户的用户特征、且所述活体检测模块的活体检测失败时,若发现所述用户特征对应的特征ID被锁定,进一步重启所述特征ID对应的计时器;

所述处理模块在解锁所述特征ID之后,进一步关闭或删除所述特征ID对应的计时器。

13.一种电子设备,其特征在于,包括:内部总线、存储器、处理器和通信接口;其中,所述处理器、所述通信接口、所述存储器通过所述内部总线完成相互间的通信;其中,

所述存储器,用于存储防范非法攻击的方法对应的机器可读指令;

所述处理器,用于读取所述存储器上的所述机器可读指令,并执行所述指令以实现权利要求1-6任一项所述的防范非法攻击方法。

防范非法攻击方法、装置及电子设备

技术领域

[0001] 本申请涉及生物识别技术，特别涉及防范非法攻击方法、装置及电子设备。

背景技术

[0002] 在生物识别系统中，为防止攻击者伪造和窃取他人的用户特征(也可称为生物特征信息)通过身份认证，常进一步对用户特征执行活体检测。

[0003] 所谓活体检测，其主要是用于检测获取的用户特征是否从具有生物活体的合法用户身上得到。

[0004] 目前的活体检测并非最优，普遍存在误判问题。比如，当攻击者提供的用户特征执行活体检测失败后，攻击者后续反复尝试多次进行活体检测就有可能有一次误判活体检测成功。

[0005] 一旦误判活体检测成功，则意味着攻击者提供的用户特征通过身份认证。而当攻击者提供的用户特征通过身份认证，则意味着攻击者可以访问只有合法身份才能访问的资源，比如，应用于门禁领域，当门禁设备确定攻击者通过身份认证，则门禁设备会解除本门禁设备控制的门禁让攻击者通过，这为攻击者发起非法攻击提供了可乘之机，大大降低安全性。

发明内容

[0006] 本申请提供了防范非法攻击的方法、装置及电子设备，以防止误判攻击者提供的用户特征通过身份认证，提高安全性。

[0007] 本申请提供的技术方案包括：

[0008] 一种防范非法攻击的方法，包括：

[0009] 当成功识别目标用户的用户特征、且所述用户特征的活体检测结果指示活体检测失败时，若发现所述用户特征对应的特征ID未被锁定，则检测当前是否满足所述特征ID的锁定条件，若是，锁定所述特征ID；

[0010] 当成功识别所述目标用户的用户特征、且所述用户特征的活体检测结果指示活体检测成功时，若发现所述特征ID被锁定，则检测当前是否满足所述特征ID的解锁条件，若是，对锁定的所述特征ID执行解锁。

[0011] 一种防范非法攻击的装置，包括：

[0012] 特征识别模块，用于识别目标用户的用户特征；

[0013] 活体检测模块，用于对所述用户特征进行活体检测；

[0014] 处理模块，用于在所述特征识别模块成功识别所述用户特征、且所述活体检测模块对所述用户特征的活体检测失败时，若发现所述用户特征对应的特征ID未被锁定，则检测当前是否满足所述特征ID的锁定条件，若是，锁定所述特征ID;以及，

[0015] 在所述特征识别模块成功识别所述用户特征、且所述活体检测模块对所述用户特征的活体检测成功时，若发现所述特征ID被锁定，则检测当前是否满足所述特征ID的解锁

条件，若是，对锁定的所述特征ID执行解锁。

[0016] 一种电子设备，其特征在于，包括：内部总线、存储器、处理器和通信接口；其中，所述处理器、所述通信接口、所述存储器通过所述内部总线完成相互间的通信；其中，

[0017] 所述存储器，用于存储防范非法攻击的方法对应的机器可读指令；

[0018] 所述处理器，用于读取所述存储器上的所述机器可读指令，并执行所述指令以实现上述的防范非法攻击方法。

[0019] 由以上技术方案可以看出，本申请中，在成功识别目标用户的用户特征的前提下，若用户特征的活体检测失败，则在用户特征对应的特征ID满足锁定条件时锁定所述特征ID，之后，即使后续再对所述用户特征尝试活体检测时发现活体检测成功，也不直接确定用户特征通过身份认证，而是检测所述特征ID是否满足解锁条件，在满足解锁条件时先解锁所述特征ID，之后再对所述用户特征尝试活体检测时发现活体检测成功，才确定所述用户特征通过身份认证，这能够防止误判攻击者提供的用户特征通过身份认证，进一步降低非法攻击的可能，提高安全性。

附图说明

[0020] 此处的附图被并入说明书中并构成本说明书的一部分，示出了符合本公开的实施例，并与说明书一起用于解释本公开的原理。

[0021] 图1为本申请提供的方法流程图；

[0022] 图2为本申请提供的步骤102中检测当前是否满足所述特征ID的锁定条件的流程图；

[0023] 图3为本申请提供的步骤103中检测当前是否满足所述特征ID的解锁条件的流程图；

[0024] 图4为本申请提供的针对计时器的实现流程图；

[0025] 图5为本申请提供的装置结构示意图；

[0026] 图6为本申请提供的电子设备结构示意图。

具体实施方式

[0027] 本申请中，在用户特征的活体检测失败时，若当前满足与用户特征对应的特征ID的锁定条件，则锁定特征ID，这防止在锁定特征ID后即使后续有一次误判与被锁定的特征ID对应的用户特征的活体检测成功，也不会立即确定身份认证通过，而是判断当前是否满足特征ID的解锁条件，甚至在满足特征ID的解锁条件时也非立即确定身份认证通过，而是仅解锁特征ID，这显然能够防范误判而导致攻击者发起非法攻击，大大提高安全性。

[0028] 为了使本申请更加清楚，下面结合具体实施例对本申请进行描述：

[0029] 参见图1，图1为本申请提供的方法流程图。需要说明的是，本申请提供的方法可以应用于各种领域比如应用于门禁领域等，本申请并不具体限定。以本申请提供的方法应用于门禁领域，则作为一个实施例，本申请提供的方法可应用于门禁设备。其他领域类似，不再一一举例。

[0030] 如图1所示，该流程可包括以下步骤：

[0031] 步骤101，当成功识别目标用户的用户特征、且所述用户特征的活体检测结果指示

活体检测失败时，执行步骤102；当成功识别所述目标用户的用户特征、且所述用户特征的活体检测结果指示活体检测成功时，执行步骤103。

[0032] 在本申请中，作为一个实施例，用户特征可为用户具有的生物特征，比如为脸、虹膜、指纹、或者掌纹等，本申请并不具体限定。

[0033] 需要说明的时，在本申请中，用户特征的识别技术类似现有识别技术。以用户特征为目标用户的脸为例，则本申请中，识别目标用户的脸类似现有人脸识别。再以用户特征为目标用户的虹膜为例，则本申请中，识别目标用户的虹膜类似现有虹膜识别。

[0034] 在具体实现时，当对目标用户的用户特征进行识别时会出现两种结果，一种是：识别成功，另一种是识别失败。本申请图1所示流程是在用户特征识别成功的前提下执行。而一旦识别失败，则可以直接确定用户特征未通过身份认证，无需再执行本申请图1所示流程。

[0035] 步骤102，若发现所述用户特征对应的特征ID未被锁定，则检测当前是否满足所述特征ID的锁定条件，若是，锁定所述特征ID。

[0036] 本步骤102是在成功识别目标用户的用户特征、且所述用户特征的活体检测结果指示活体检测失败的前提下执行的。基于该前提，在本申请中，本步骤102中检测当前是否满足所述特征ID的锁定条件有很多实现方式，下文图2举例示出其中一种实现方式，这里暂不赘述。

[0037] 在本申请中，每一个用户特征都具有对应的特征ID，特征ID是用来表示其对应的用户特征的。具体实现时，特征ID可以是一串序列号或者账号。比如，以人脸为例，人脸对应的特征ID为00001，则应用于本申请中，00001即可表示人脸。

[0038] 需要说明的是，本步骤102中，若检测当前未满足所述特征ID的锁定条件，则不对所述用户特征对应的特征ID执行锁定操作，按照现有处理方式执行，这里暂不赘述。

[0039] 步骤103，若发现所述特征ID被锁定，则检测当前是否满足所述特征ID的解锁条件，若是，对锁定的所述特征ID执行解锁。

[0040] 本步骤103是在成功识别所述目标用户的用户特征、且所述用户特征的活体检测结果指示活体检测成功的前提下执行的。基于该前提，则作为一个实施例，本步骤103中，若发现所述特征ID未被锁定，则可直接确定用户特征通过身份认证。

[0041] 在本申请中，本步骤103中检测当前是否满足所述特征ID的解锁条件有很多实现方式，下文图3举例示出其中一种实现方式，这里暂不赘述。

[0042] 至此，完成图1所示流程。

[0043] 通过图1所示流程可以看出，本申请中，在成功识别目标用户的用户特征的前提下，若用户特征的活体检测失败，则在当前满足锁定所述用户特征对应的特征ID的锁定条件时锁定所述特征ID，之后，后续再对所述用户特征尝试活体检测时即使活体检测成功，也不直接确定用户特征通过身份认证，而是检测当前是否满足所述特征ID的解锁条件，在满足解锁条件时先对锁定的所述特征ID执行解锁，之后，再对所述用户特征尝试活体检测时若活体检测成功，才确定所述用户特征通过身份认证，这能够防止误判攻击者提供的用户特征通过身份认证，进一步降低非法攻击的可能，提高安全性。

[0044] 下面对步骤102中检测当前是否满足所述特征ID的锁定条件进行描述：

[0045] 参见图2，图2为本申请提供的步骤102中检测当前是否满足所述特征ID的锁定条

件的流程图。

[0046] 如图2所示，该流程可包括以下步骤：

[0047] 步骤201，判断所述特征ID与本地记录的上一次活体检测失败的用户特征的特征ID是否相同，若是，执行步骤202，若否，执行步骤203。

[0048] 在本申请中，每一次对用户特征执行的活体检测都会在本地记录。基于此，本步骤201很容易依据本地记录判断所述特征ID与本地记录的上一次活体检测失败的用户特征的特征ID是否相同。

[0049] 本步骤201之所以判断所述特征ID与本地记录的上一次活体检测失败的用户特征的特征ID是否相同，目的是确定出对所述用户特征执行的活体检测是否连续失败，具体见下文步骤202描述。

[0050] 步骤202，将本地存在的与所述特征ID对应的活体检测失败计数器的计数增加第一设定值，检测增加了所述第一设定值的计数是否大于或等于预设阈值N，若是，确定当前满足所述特征ID的锁定条件，若否，确定当前未满足所述特征ID的锁定条件。

[0051] 本步骤202是在判断出所述特征ID与本地记录的上一次活体检测失败的用户特征的特征ID相同的前提下执行的。其中，所述特征ID与本地记录的上一次活体检测失败的用户特征的特征ID相同，则意味着上一次也是对所述特征ID对应的用户特征执行活体检测且执行的活体检测失败(相当于对所述特征ID对应的用户特征连续执行的活体检测失败)，此时可以直接将所述活体检测失败计数器的计数增加第一设定值，这里的第一设定值可举例为1。作为一个实施例，这里的第一设定值远小于预设阈值N。

[0052] 通过步骤202可以看出，在本申请中，所述特征ID对应的用户特征在连续至少N次活体检测失败时确定满足锁定所述特征ID的锁定条件，而其他情况下，确定未满足锁定所述特征ID的锁定条件。

[0053] 步骤203，确定当前未满足所述特征ID的锁定条件。

[0054] 本步骤203是在判断出所述特征ID与本地记录的上一次活体检测失败的用户特征的特征ID不同的前提下执行的。其中，所述特征ID与本地记录的上一次活体检测失败的用户特征的特征ID不同，则意味着上一次并非对所述特征ID对应的用户特征执行活体检测(相当于对所述特征ID对应的用户特征执行的活体检测当前并非是连续执行)，基于此，本次对所述特征ID对应的用户特征执行的活体检测有可能是首次，也有可能不是。

[0055] 作为一个实施例，本申请中，本次对所述特征ID对应的用户特征执行的活体检测是否是首次，可通过检测本地是否存在与所述特征ID对应的活体检测失败计数器实现。

[0056] 其中，当检测出本地不存在与所述特征ID对应的活体检测失败计数器，则确定本次对所述特征ID对应的用户特征执行的活体检测是首次，此时，可在本地新建所述活体检测失败计数器，将所述活体检测失败计数器的计数置为第二设定值；这里，第二设定值举例可为1。

[0057] 当检测出本地存在与所述特征ID对应的活体检测失败计数器，则确定本次对所述特征ID对应的用户特征执行的活体检测并非是首次，此时，可将所述活体检测失败计数器的计数置为第二设定值。第二设定值如上描述，举例可为1。这里之所以将所述活体检测失败计数器的计数置为第二设定值，其目的是便于记录所述特征ID对应的用户特征连续执行活体检测失败的次数。

[0058] 至此，完成图2所示流程。

[0059] 通过图2所示流程实现了步骤102中如何检测当前是否满足所述特征ID的锁定条件。

[0060] 下面对步骤103中如何检测当前是否满足所述特征ID的解锁条件进行描述：

[0061] 参见图3，图3为本申请提供的步骤103中检测当前是否满足所述特征ID的解锁条件的流程图。

[0062] 如图3所示，该流程可包括以下步骤：

[0063] 步骤301，判断所述特征ID与本地记录的上一次活体检测成功的用户特征的特征ID是否相同，若是，执行步骤302，若否，执行步骤303。

[0064] 在本申请中，每一次对用户特征执行活体检测时都会在本地记录。基于此，本步骤301很容易依据本地记录判断所述特征ID与本地记录的上一次活体检测成功的用户特征的特征ID是否相同。

[0065] 本步骤301之所以判断所述特征ID与本地记录的上一次活体检测成功的用户特征的特征ID是否相同，目的是验证对所述用户特征执行的活体检测是否连续成功。

[0066] 步骤302，将本地存在的与所述特征ID对应的活体检测成功计数器的计数增加第一设定值，检测增加了所述第一设定值的计数是否大于或等于预设阈值M，若是，确定当前满足所述特征ID的解锁条件，若否，确定当前未满足所述特征ID的解锁条件。

[0067] 本步骤302是在判断出所述特征ID与本地记录的上一次活体检测成功的用户特征的特征ID相同的前提下执行的。其中，所述特征ID与本地记录的上一次活体检测成功的用户特征的特征ID相同，则意味着上一次也是对所述特征ID对应的用户特征执行活体检测且执行的活体检测成功(相当于对所述特征ID对应的用户特征连续执行活体检测成功)，此时可以直接将所述特征ID对应的活体检测成功计数器的计数增加第一设定值，这里的第一设定值可举例为1。作为一个实施例，这里的第一设定值远小于预设阈值M。

[0068] 通过步骤302可以看出，在本申请中，所述特征ID对应的用户特征在连续至少M次活体检测成功时确定满足解锁已锁定的所述特征ID的解锁条件，而其他情况下，确定未满足解锁已锁定的所述特征ID的解锁条件。

[0069] 步骤303，确定当前未满足所述特征ID的解锁条件。

[0070] 本步骤303是在判断出所述特征ID与本地记录的上一次活体检测成功的用户特征的特征ID不同的前提下执行的。其中，所述特征ID与本地记录的上一次活体检测成功的用户特征的特征ID不同，则意味着上一次并非对所述特征ID对应的用户特征执行活体检测(相当于对所述特征ID对应的用户特征执行的活体检测当前并非是连续执行)，基于此，本次对所述特征ID对应的用户特征执行的活体检测有可能是在所述特征ID被锁定后首次执行的活体检测，也有可能不是。

[0071] 作为一个实施例，本申请中，本次对所述特征ID对应的用户特征执行的活体检测是否为在所述特征ID被锁定后首次执行的活体检测，可通过检测本地是否存在与所述特征ID对应的活体检测成功计数器实现。

[0072] 其中，当检测出本地不存在与所述特征ID对应的活体检测成功计数器，则确定本次对所述特征ID对应的用户特征执行的活体检测是在所述特征ID被锁定后执行的首次活体检测，此时，可在本地新建所述活体检测成功计数器，将所述活体检测成功计数器的计数

置为第二设定值;这里,第二设定值举例可为1。

[0073] 当检测出本地存在与所述特征ID对应的活体检测成功计数器,则确定本次对所述特征ID对应的用户特征执行的活体检测并非是在所述特征ID被锁定后执行的首次活体检测,此时,可将所述活体检测成功计数器的计数置为第二设定值。第二设定值如上描述,举例可为1。这里之所以将所述活体检测成功计数器的计数置为第二设定值,其目的是便于记录在所述特征ID被锁定后对所述特征ID对应的用户特征连续执行活体检测成功的次数。

[0074] 至此,完成图3所示流程。

[0075] 通过图3所示流程实现了步骤103中如何检测当前是否满足所述特征ID的解锁条件。

[0076] 需要说明的是,本申请中,上述步骤102在锁定所述特征ID后,可进一步包括:启动所述特征ID对应的计时器。

[0077] 还需要说明的是,本申请中,上述步骤102中,若发现所述用户特征对应的特征ID被锁定,则可进一步包括:重启所述特征ID对应的计时器。

[0078] 在本申请中,所述计时器在启动后从最大计时时间T开始递减,在递减到设定时间门限时指示对所述特征ID执行解锁。因此,本申请中,当所述特征ID对应的计时器递减到设定时间门限时,不管当前是否有对所述特征ID对应的用户特征进行识别和活体检测,也不管当前对所述特征ID对应的用户特征进行识别的识别结果(成功识别或失败识别)、以及对所述特征ID对应的用户特征进行活体检测的检测结果(活体检测成功或失败),对需要对所述特征ID执行解锁。

[0079] 基于此,本申请中,还需实时图4所示的以下步骤:

[0080] 步骤401,检测所述特征ID对应的计时器当前的计时时间是否等于设定时间门限,若是,执行步骤402,若否,执行步骤403。

[0081] 这里,作为一个实施例,设定时间门限可为0。

[0082] 步骤402,解锁已被锁定的所述特征ID。

[0083] 步骤403,继续保持所述特征ID被锁定。

[0084] 至此,完成图4所示流程。

[0085] 需要说明的是,在本申请中,上述步骤103中在解锁所述特征ID之后,可进一步包括:关闭或删除所述特征ID对应的计时器,以防止所述特征ID对应的计时器在所述特征ID被解锁后还处于工作状态,节省资源。

[0086] 以上对本申请提供的方法进行了描述。下面对本申请提供的装置进行描述:

[0087] 参见图5,图5为本申请提供的装置结构图图。如图5所示,该装置可包括:

[0088] 特征识别模块,用于识别目标用户的用户特征;

[0089] 活体检测模块,用于对所述用户特征进行活体检测;

[0090] 处理模块,用于在所述特征识别模块成功识别所述用户特征、且所述活体检测模块对所述用户特征的活体检测失败时,若发现所述用户特征对应的特征ID未被锁定,则检测当前是否满足所述特征ID的锁定条件,若是,锁定所述特征ID;以及,

[0091] 在所述特征识别模块成功识别所述用户特征、且所述活体检测模块对所述用户特征的活体检测成功时,若发现所述特征ID被锁定,则检测当前是否满足所述特征ID的解锁条件,若是,对锁定的所述特征ID执行解锁。

[0092] 在一个例子中,所述处理模块检测当前是否满足所述特征ID的锁定条件包括:

[0093] 判断所述特征ID与本地记录的上一次活体检测失败的用户特征的特征ID是否相同,

[0094] 若不同,则确定当前未满足所述特征ID的锁定条件,

[0095] 若相同,将本地存在的与所述特征ID对应的活体检测失败计数器的计数增加第一设定值,检测增加了所述第一设定值的计数是否大于或等于预设阈值N,若是,确定当前满足所述特征ID的锁定条件,若否,确定当前未满足所述特征ID的锁定条件。

[0096] 在一个例子中,所述处理模块在判断出所述特征ID与本地记录的上一次活体检测失败的用户特征的特征ID不同时,进一步检测本地是否存在与所述特征ID对应的活体检测失败计数器,

[0097] 若否,在本地新建所述活体检测失败计数器,将所述活体检测失败计数器的计数置为第二设定值;

[0098] 若是,将所述活体检测失败计数器的计数置为第二设定值。

[0099] 在一个例子中,所述处理模块检测当前是否满足所述特征ID的解锁条件包括:

[0100] 判断所述特征ID与本地记录的上一次活体检测成功的用户特征的特征ID是否相同,

[0101] 若不同,确定当前未满足所述特征ID的解锁条件;

[0102] 若相同,将本地存在的与所述特征ID对应的活体检测成功计数器的计数增加第一设定值,检测增加了所述第一设定值的计数是否大于或等于预设阈值M,若是,确定当前满足所述特征ID的解锁条件,若否,确定当前未满足所述特征ID的解锁条件。

[0103] 在一个例子中,所述处理模块在判断出所述特征ID与本地记录的上一次活体检测成功的用户特征的特征ID不同时,进一步检测本地是否存在与所述特征ID对应的活体检测成功计数器,

[0104] 若否,在本地新建所述活体检测成功计数器,将所述活体检测成功计数器的计数置为第二设定值;

[0105] 若是,将所述活体检测成功计数器的计数置为第二设定值。

[0106] 在一个例子中,所述处理模块在锁定所述特征ID后,进一步启动所述特征ID对应的计时器,所述计时器在启动后从最大计时时间T开始递减,在递减到设定计时时间门限时指示对所述特征ID执行解锁;

[0107] 所述处理模块在所述特征识别模块成功识别目标用户的用户特征、且所述活体检测模块的活体检测失败时,若发现所述用户特征对应的特征ID被锁定,进一步重启所述特征ID对应的计时器;

[0108] 所述处理模块在解锁所述特征ID之后,进一步关闭或删除所述特征ID对应的计时器。

[0109] 至此,完成图5所示装置的结构描述。

[0110] 相应于上述方法实施例,本申请实施例还提供了一种电子设备;在具体应用中,该电子设备可以为门禁设备等等,本申请并不具体限定。

[0111] 如图6所示,所述电子设备包括:内部总线、存储器(memory)、处理器(processor)和通信接口(Communications Interface);其中,所述处理器、所述通信接口、所述存储器

通过所述内部总线完成相互间的通信；

[0112] 所述存储器，用于存储防范非法攻击的方法对应的机器可读指令；

[0113] 所述处理器，用于读取所述存储器上的所述机器可读指令，并执行所述指令以实现防范非法攻击方法。

[0114] 本实施例中，防范非法攻击方法的相关描述可以参见本申请所提供方法实施例中的描述内容，在此不做赘述。

[0115] 至此，完成本申请提供的电子设备的结构描述。

[0116] 对于装置实施例而言，由于其基本对应于方法实施例，所以相关之处参见方法实施例的部分说明即可。以上所描述的装置实施例仅仅是示意性的，其中所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本申请方案的目的。本领域普通技术人员在不付出创造性劳动的情况下，即可以理解并实施。

[0117] 以上所述仅为本申请的较佳实施例而已，并不用以限制本申请，凡在本申请的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本申请保护的范围之内。

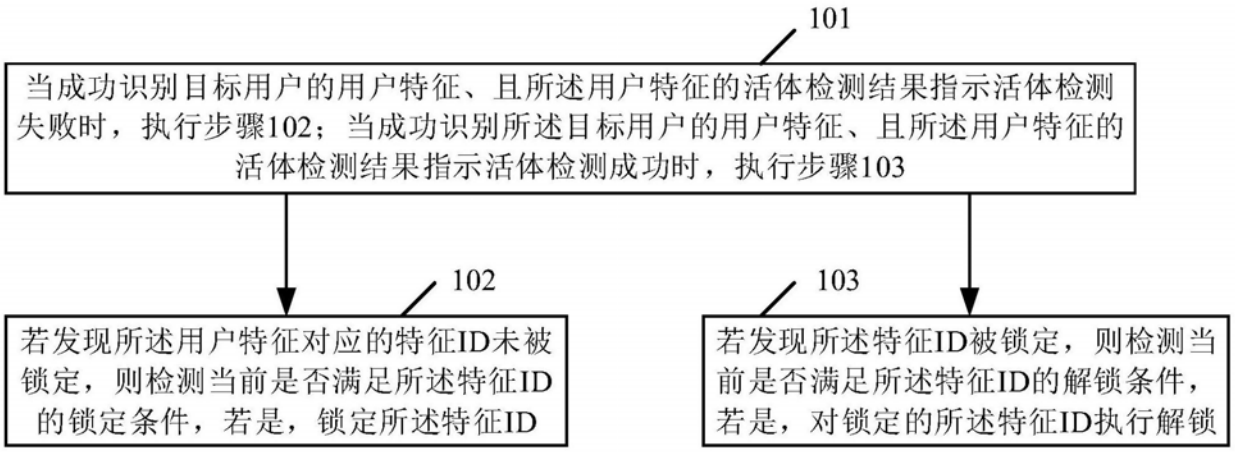

101
当成功识别目标用户的用户特征、且所述用户特征的活体检测结果指示活体检测失败时，执行步骤102；当成功识别所述目标用户的用户特征、且所述用户特征的活体检测结果指示活体检测成功时，执行步骤103
102
若发现所述用户特征对应的特征ID未被锁定，则检测当前是否满足所述特征ID的锁定条件，若是，锁定所述特征ID
103
若发现所述特征ID被锁定，则检测当前是否满足所述特征ID的解锁条件，若是，对锁定的所述特征ID执行解锁

图1

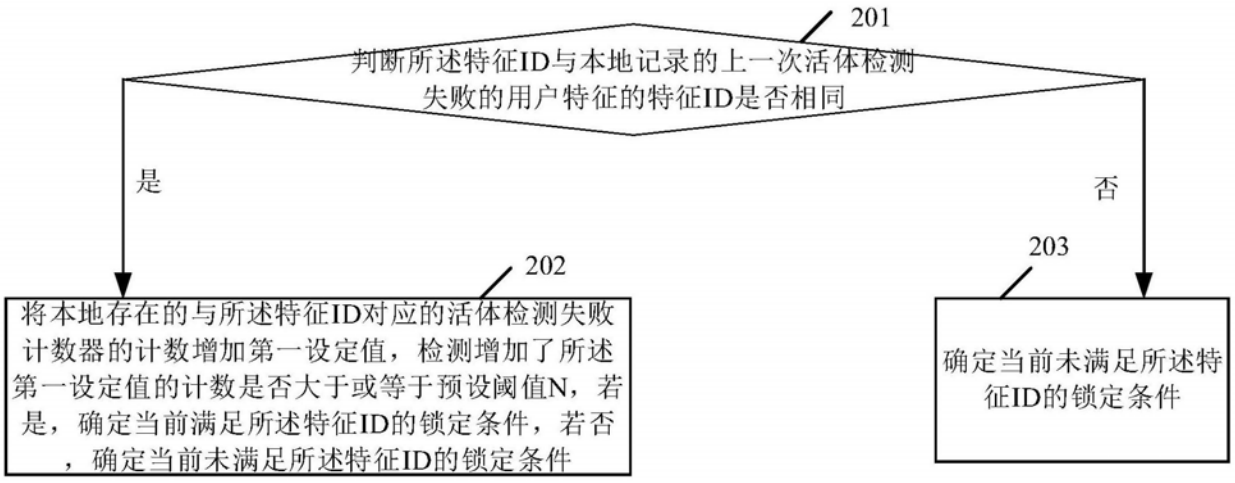

201
判断所述特征ID与本地记录的上一次活体检测失败的用户特征的特征ID是否相同
是
否
202
将本地存在的与所述特征ID对应的活体检测失败计数器的计数增加第一设定值，检测增加了所述第一设定值的计数是否大于或等于预设阈值N，若是，确定当前满足所述特征ID的锁定条件，若否，确定当前未满足所述特征ID的锁定条件
203
确定当前未满足所述特征ID的锁定条件

图2

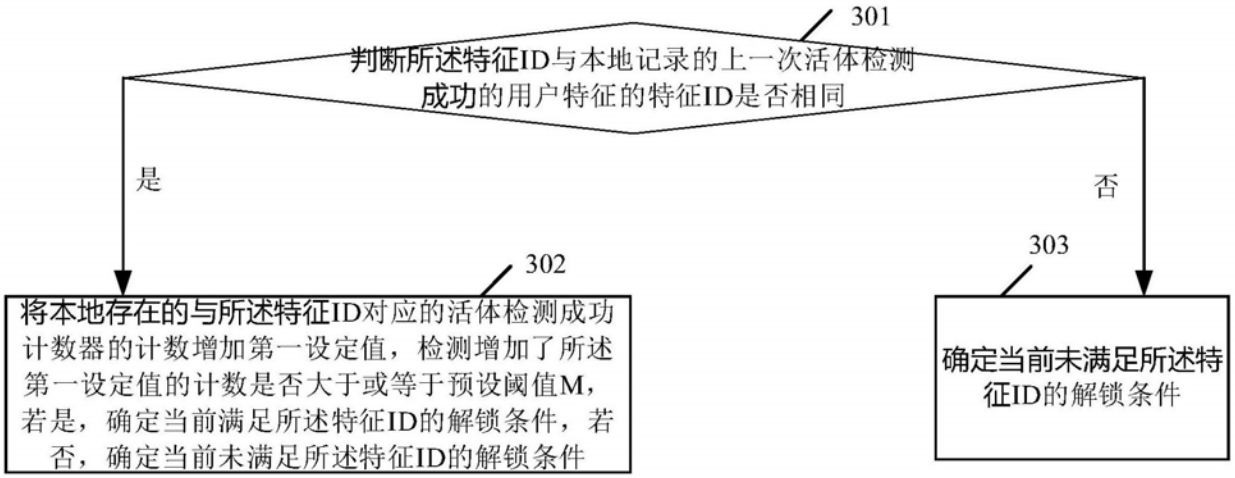

301
判断所述特征ID与本地记录的上一次活体检测成功的用户特征的特征ID是否相同
是
否
302
将本地存在的与所述特征ID对应的活体检测成功计数器的计数增加第一设定值，检测增加了所述第一设定值的计数是否大于或等于预设阈值M，若是，确定当前满足所述特征ID的解锁条件，若否，确定当前未满足所述特征ID的解锁条件
303
确定当前未满足所述特征ID的解锁条件

图3

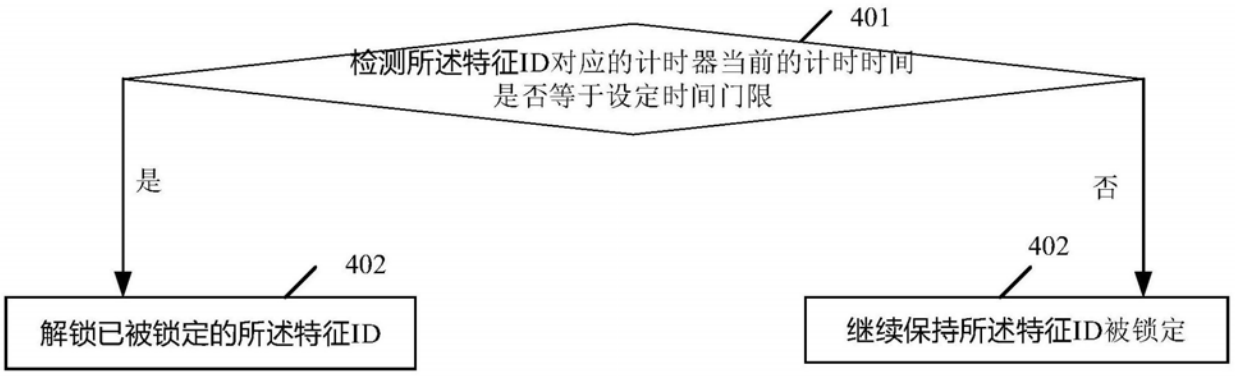

401
检测所述特征ID对应的计时器当前的计时时间
是否等于设定时间门限
是
否
402
解锁已被锁定的所述特征ID
402
继续保持所述特征ID被锁定

图4

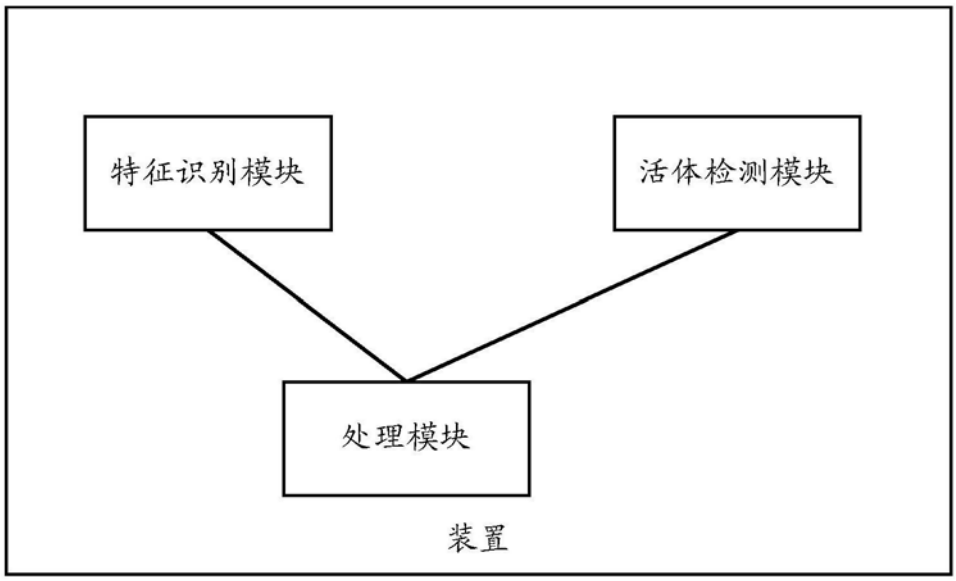

特征识别模块
活体检测模块
处理模块
装置

图5

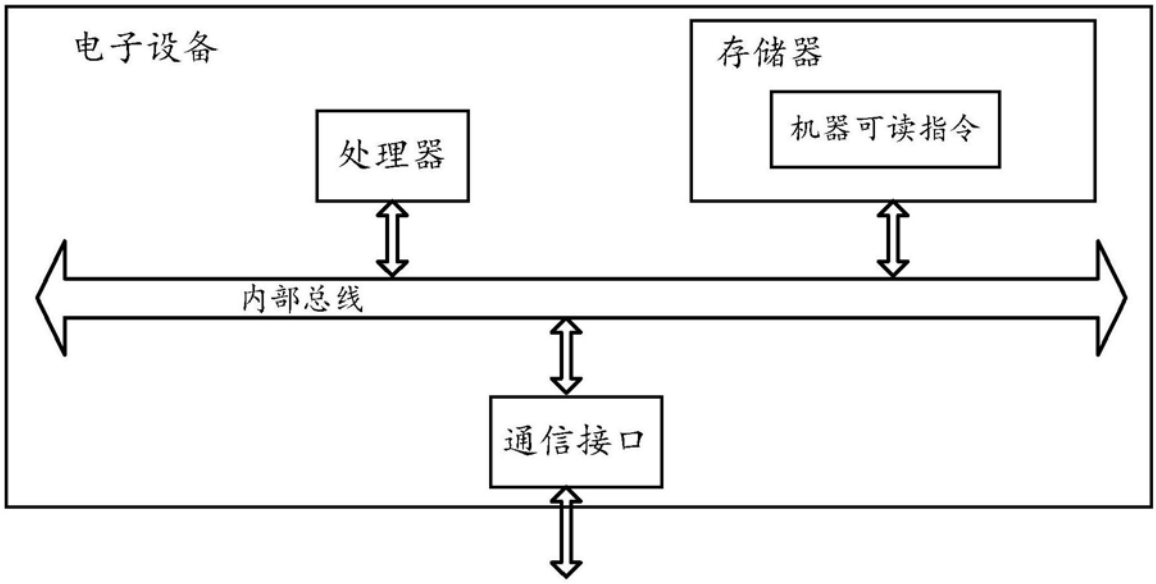


图6