



(12)发明专利申请

(10)申请公布号 CN 107317682 A

(43)申请公布日 2017. 11. 03

(21)申请号 201710325270.3

(22)申请日 2017.05.10

(71)申请人 史展

地址 063000 河北省唐山市路北区建设路
170号冀东新闻中心1909

(72)发明人 史展

(74)专利代理机构 广州三环专利商标代理有限公司 44202

代理人 郝传鑫 贾允

(51) Int. Cl.

H04L 9/32(2006.01)

H04L 29/06(2006.01)

G06F 21/36(2013.01)

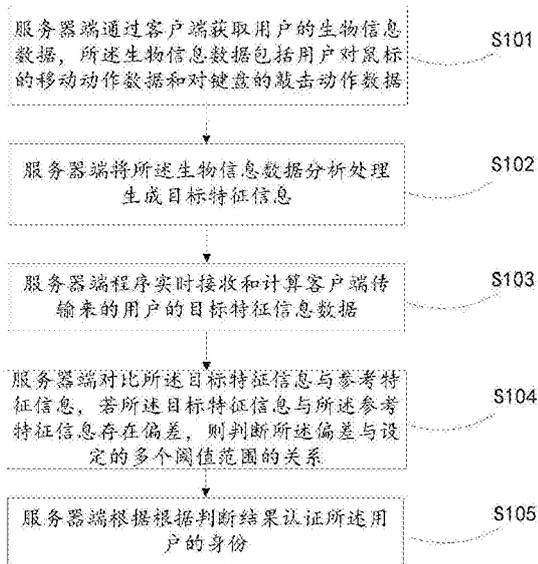
权利要求书2页 说明书10页 附图5页

(54)发明名称

一种身份认证方法及系统

(57)摘要

本发明公开了一种身份认证方法及系统,所述方法包括获取用户的生物信息数据,所述生物信息数据包括用户对鼠标的移动动作数据和对键盘的敲击动作数据;将所述生物信息数据分析处理生成目标特征信息;对比所述目标特征信息与参考特征信息,若所述目标特征信息与所述参考特征信息存在偏差,则判断所述偏差与设定的多个阈值范围的关系;所述参考特征信息包括用户对鼠标移动和对键盘敲击的行为特点对应的特征信息;根据判断结果认证所述用户的身份。本发明能够控制用户对计算机的访问;并且,进一步高准确度地监测恶意入侵行为,时时保护和监测用户帐号/密码被黑客或者组织内部的泄密者窃取的情形。总之,本发明能够全面的且实时地进行网络保护。



1. 一种身份认证方法,其特征在于,所述方法包括:

获取用户的生物信息数据,所述生物信息数据包括用户对鼠标的移动动作数据和对键盘的敲击动作数据;

将所述生物信息数据分析处理生成目标特征信息;

对比所述目标特征信息与参考特征信息,若所述目标特征信息与所述参考特征信息存在偏差,则判断所述偏差与设定的多个阈值范围的关系;所述参考特征信息包括用户对鼠标移动和对键盘敲击的行为特点对应的特征信息;

根据判断结果认证所述用户的身份。

2. 根据权利要求1所述的方法,其特征在于,所述判断所述偏差与设定的多个阈值范围的关系包括:

设定第一阈值范围,若所述偏差位于所述第一阈值范围,则认证当前用户为真实用户;

设定第二阈值范围,若所述偏差位于所述第二阈值范围,则发出告警信号,认证当前用户为待鉴定用户,继续进行目标特征信息与参考特征信息的比对;

设定第三阈值范围,若所述偏差位于所述第三阈值范围,则认证当前用户为错误用户,发出锁定信号,将用户当前操作的客户端界面锁定。

3. 根据权利要求1所述的方法,其特征在于,所述对比所述目标特征信息与参考特征信息,之前包括:

获取客户端采集到的用户对鼠标进行移动的大量动作和对键盘进行敲击的大量动作;

通过分析用户对鼠标进行移动的大量动作信息和对键盘进行敲击的大量动作信息,生成所述参考特征信息;

或者包括:

获取用户在客户端上的训练场景进行训练得出的训练数据;

根据所述训练数据的信息生成所述参考特征信息。

4. 根据权利要求1所述的方法,其特征在于,获取用户的生物信息数据,之前包括:

还包括:判断用户是否输入了生物信息数据,若是,则通过客户端采集所述生物信息数据。

5. 根据权利要求1所述的方法,其特征在于,还包括:

将用户每一次的身份判断结果和每一次采集的目标特征信息以列表的形式进行存储;

检视所述用户的过往登录信息和身份验证信息。

6. 一种身份认证系统,其特征在于,包括:

生物信息获取模块,用于获取用户的生物信息数据;所述生物信息数据包括用户对鼠标的移动动作数据和对键盘的敲击动作数据;

生物信息转换模块,用于将所述生物信息数据分析处理生成目标特征信息;

特征比对模块,用于对比所述目标特征信息与参考特征信息,若所述目标特征信息与所述参考特征信息存在偏差,则判断所述偏差与设定的多个阈值范围的关系;所述参考特征信息包括用户对鼠标移动和对键盘敲击的行为特点对应的特征信息;

身份判断模块,用于根据判断结果认证所述用户的身份。

7. 根据权利要求6所述的系统,其特征在于,所述身份判断模块包括:

第一阈值判断单元,用于设定第一阈值范围,若所述偏差位于所述第一阈值范围,则认

证当前用户为真实用户；

第二阈值判断单元,用于设定第二阈值范围,若所述偏差位于所述第二阈值范围,则发出告警信号,认证当前用户为待鉴定用户,继续进行目标特征信息与参考特征信息的比对;

第三阈值判断单元,用于设定第三阈值范围,若所述偏差位于所述第三阈值范围,则认证当前用户为错误用户,发出锁定信号,将用户当前操作的客户端界面锁定。

8. 根据权利要求6所述的系统,其特征在于,所述特征比对模块包括:

采集动作获取单元,用于获取客户端采集得到的用户对鼠标进行移动的大量动作和对键盘进行敲击的大量动作;

第一参考特征生成单元,用于通过分析用户对鼠标进行移动的大量动作信息和对键盘进行敲击的大量动作信息,生成所述参考特征信息。

或者包括:

训练数据获取模块,获取用户在客户端上的训练场景进行训练得出的训练数据;

第二参考特征生成单元,根据所述训练数据的信息生成所述参考特征信息。

9. 根据权利要求6所述的系统,其特征在于,生物信息获取模块包括:生物信息输入判断单元,用于判断用户是否输入了生物信息数据,若是,则通过客户端采集所述生物信息数据。

10. 根据权利要求6所述的系统,其特征在于,还包括:

第一存储模块,用于将用户每一次的身份判断结果以列表的形式进行存储;

第二存储模块,用于将每一次采集的目标特征信息以列表的形式进行存储;

信息检视模块,用于检视所述用户的过往登录信息和身份验证信息。

一种身份认证方法及系统

技术领域

[0001] 本发明涉及数据处理技术领域,尤其涉及一种身份认证方法及系统。

背景技术

[0002] 联网技术的迅猛发展改变了人们使用计算机的方式,并使人们更加方便的在全球范围内随时随地的获取信息和资源,同时这也增大了恶意攻击和入侵发生的机会。因此,保证互联网中用户身份的可靠性成为一个重要的课题。

[0003] 因计算机和网络技术的发展,传统的身份认证方案已经不能满足当前网络环境中对于身份认证的安全性需求;现有的身份认证技术主要包括三类,分别利用了不同的信息:1) 记忆信息,如密码、PIN等;2) 辅助设备、如ID卡、令牌等;3) 生物特征,如指纹,虹膜等。这些传统的识别技术自身均存有缺陷,对于用户名密码方案来说,密码难于记忆并容易搞混和泄露,ID卡需要随身携带且易失窃或遭到破解导致失效,同时这种方案并不能确保用户身份的唯一性,而令牌持有物方案中,持有物容易丢失,并且存在仿造的可能性;即任何可以获得用户名密码的人都可以在网络上以该用户的身份进行登录,并访问其得到的资源;对于基于物理特征的生物认证技术,这些方案实施起来过程相对较复杂,而且大多数都需要一些复杂、昂贵的硬件设备,比如指纹识别仪等,其硬件成本比较高。同时这些认证技术大部分都不能应用于在互联网环境下。

[0004] 鉴于此,研究人员仍然在不断寻找新的身份认证手段和方法。其中基于计算机输入行为特征的认证方法,因为不需要添加额外的设备,在当前大多数计算机系统中可以直接部署,实施无干扰的监控,逐渐成为身份认证研究中的新热点。

发明内容

[0005] 为了解决上述技术问题,本发明提出了一种身份认证方法及系统。

[0006] 本发明是以如下技术方案实现的:

[0007] 第一方面提供了一种身份认证方法,所述方法包括:

[0008] 获取用户的生物信息数据,所述生物信息数据包括用户对鼠标的移动动作数据和对键盘的敲击动作数据;

[0009] 将所述生物信息数据分析处理生成目标特征信息;

[0010] 对比所述目标特征信息与参考特征信息,若所述目标特征信息与所述参考特征信息存在偏差,则判断所述偏差与设定的多个阈值范围的关系;所述参考特征信息包括用户对鼠标移动和对键盘敲击的行为特点对应的特征信息;

[0011] 根据判断结果认证所述用户的身份。

[0012] 进一步地,所述判断所述偏差与设定的多个阈值范围的关系包括:

[0013] 设定第一阈值范围,若所述偏差位于所述第一阈值范围,则认证当前用户为真实用户;

[0014] 设定第二阈值范围,若所述偏差位于所述第二阈值范围,则发出告警信号,认证当

前用户为待鉴定用户,继续进行目标特征信息与参考特征信息的比对;

[0015] 设定第三阈值范围,若所述偏差位于所述第三阈值范围,则认证当前用户为错误用户,发出锁定信号,将用户当前操作的客户端界面锁定

[0016] 进一步地,所述对比所述目标特征信息与参考特征信息,之前包括:

[0017] 获取客户端采集到的用户对鼠标进行移动的大量动作和对键盘进行敲击的大量动作;

[0018] 通过分析用户对鼠标进行移动的大量动作信息和对键盘进行敲击的大量动作信息,生成所述参考特征信息。

[0019] 或者包括:

[0020] 获取用户在客户端上的训练场景进行训练得出的训练数据;

[0021] 根据所述训练数据的信息生成所述参考特征信息。

[0022] 进一步地,所述获取用户的生物信息数据,之前包括:

[0023] 判断用户是否输入了生物信息数据,若是,则通过客户端采集所述生物信息数据。

[0024] 进一步地,还包括:将用户每一次的身份判断结果和每一次采集的目标特征信息以列表的形式进行存储。

[0025] 检视所述用户的过往登录信息和身份验证信息。

[0026] 第二方面提供了一种身份认证系统,包括:生物信息获取模块,用于获取用户的生物信息数据;所述生物信息数据包括用户对鼠标的移动动作数据和对键盘的敲击动作数据;

[0027] 生物信息转换模块,将所述生物信息数据分析处理生成目标特征信息;

[0028] 特征比对模块,用于对比所述目标特征信息与参考特征信息,若所述目标特征信息与所述参考特征信息存在偏差,则判断所述偏差与设定的多个阈值范围的关系;所述参考特征信息包括用户对鼠标移动和对键盘敲击的行为特点对应的特征信息;

[0029] 身份判断模块,用于根据判断结果认证所述用户的身份。

[0030] 进一步地,所述身份判断模块包括:

[0031] 第一阈值判断单元,用于设定第一阈值范围,若所述偏差位于所述第一阈值范围,则认证当前用户为真实用户;

[0032] 第二阈值判断单元,用于设定第二阈值范围,若所述偏差位于所述第二阈值范围,则发出告警信号,认证当前用户为待鉴定用户,继续进行目标特征信息与参考特征信息的比对;

[0033] 第三阈值判断单元,用于设定第三阈值范围,若所述偏差位于所述第三阈值范围,则认证当前用户为错误用户,发出锁定信号,将用户当前操作的客户端界面锁定。

[0034] 进一步地,所述特征比对模块包括:

[0035] 采集动作获取单元,用于获取客户端采集到的用户对鼠标进行移动的大量动作和对键盘进行敲击的大量动作;

[0036] 第一参考特征生成单元,用于通过分析用户对鼠标进行移动的大量动作信息和对键盘进行敲击的大量动作信息,生成所述参考特征信息。

[0037] 或者包括:

[0038] 训练数据获取模块,获取用户在客户端上的训练场景进行训练得出的训练数据;

- [0039] 第二参考特征生成单元,根据所述训练数据的信息生成所述参考特征信息。
- [0040] 进一步地,所述生物信息获取模块,包括生物信息输入判断单元,用于判断用户是否输入了生物信息数据,若是,则通过客户端采集所述生物信息数据。
- [0041] 进一步地,还包括:
- [0042] 第一存储模块,用于将用户每一次的身份判断结果以列表的形式进行存储;
- [0043] 第二存储模块,用于将每一次采集的目标特征信息以列表的形式进行存储。
- [0044] 信息检视模块,用于检视所述用户的过往登录信息和身份验证信息。
- [0045] 本发明具有如下的有益效果:
- [0046] (1) 通过本发明的技术方案,公司和组织可以用它来监控内部网络中用户的行踪,且能够控制用户对计算机的访问,组织错误用户对计算机的操作。
- [0047] (2) 通过本发明的技术方案,能够持续地对用户身份进行认证,时时保护和监测用户帐号/密码被黑客或者组织内部的泄密者窃取的情形。
- [0048] (3) 本发明的技术方案,系统管理员可以通过管理界面监控当前内部网络中用户帐号的登录情况,及时了解可能的帐号信息失密个案,进而采取行动阻止窃密者的侵害行为。

附图说明

- [0049] 为了更清楚地说明本发明实施例中的技术方案,下面将对实施例描述中所需要使用的附图作简单地介绍,显而易见地,下面描述中的附图仅仅是本发明的一些实施例,对于本领域普通技术人员来讲,在不付出创造性劳动的前提下,还可以根据这些附图获得其他的附图。
- [0050] 图1是实施例一提供的一种身份认证方法的方法流程图;
- [0051] 图2是实施例一中服务器端根据根据判断结果认证所述用户的身份的方法流程图;
- [0052] 图3是实施例一中服务器端对比所述目标特征信息与参考特征信息之前包括的一种方法的流程图;
- [0053] 图4是实施例一中服务器端对比所述目标特征信息与参考特征信息之前包括的另一种方法的流程图;
- [0054] 图5是实施例二提供的一种身份认证方法的方法流程图;
- [0055] 图6是实施例三提供的一种身份认证系统的系统框图;
- [0056] 图7是实施例三提供的另一种身份认证系统的系统框图。
- [0057] 图中:110-生物信息获取模块,111-生物信息输入判断单元,120-生物信息转换模块,130-特征比对模块,131-采集动作获取单元,132-第一参考特征生成单元,133-训练数据获取模块,134-第二参考特征生成单元,140-身份判断模块,141-第一阈值判断单元,142-第二阈值判断单元,143-第三阈值判断单元,150-第一存储模块,160-第二存储模块,170-信息检视模块。

具体实施方式

- [0058] 为了使本技术领域的人员更好地理解本发明方案,下面将结合本发明实施例中的

附图,对本发明实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例仅仅是本发明一部分的实施例,而不是全部的实施例。基于本发明中的实施例,本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例,都应当属于本发明保护的范围。

[0059] 需要说明的是,术语“包括”和“具有”以及他们的任何变形,意图在于覆盖不排他的包含,例如,包含了一系列步骤或单元的过程、方法、系统、产品或设备不必限于清楚地列出的那些步骤或单元,而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。

[0060] 实施例一:

[0061] 身份认证是计算机安全、网络安全的第一道防线,长久以来,人们一直在研究这方面的技术,试图寻找一种安全的、可靠的、可行的身份认证方式来满足安全需求。生物认证是近年来流行的用户身份鉴别技术,并且逐渐得到关注。从最初的指纹识别,到后来的声音、手势、掌纹、虹膜及人脸等的识别,这些生物认证在硬件安装和使用上需要花费财力和培训,很难进入一般的商业和个人用户领域,不利于系统的实施和推广。

[0062] 目前,基于计算机输入行为特征的认证方法,具有鲜明的特点,如:行为方式难以模仿,行为方式无需记忆,行为数据量多,行为密码不具有明显的特征;无需额外设备,并且在当前的大多数计算机系统中可以直接部署;又结合键盘和鼠标普及率高,所以,通过监听用户键盘击键特征或鼠标行为特征,对用户进行身份识别已成为生物认证领域的一个新的研究热点。

[0063] 如图1所示,本实施例提供了一种身份认证方法,所述方法包括:

[0064] S101.服务器端通过客户端获取用户的生物信息数据,所述生物信息数据包括用户对鼠标的移动动作数据和对键盘的敲击动作数据;

[0065] 具体的是,客户端程序部署在内网中需要保护的计算机上。当用户登录后,客户端程序将自动启动并开始收集用户的生物信息数据并传送给服务器端程序做分析。其中,数据收集和传输的整个过程对用户完全透明,并且不会对用户使用的其他程序或者性能产生显著的影响。

[0066] S102.服务器端将所述生物信息数据分析处理生成目标特征信息;

[0067] 首先通过客户端对鼠标和键盘进行采集用户训练行为数据,然后用优化过的支持向量机SVM结合鼠标键盘双指标对所述系统的用户进行身份认证。

[0068] S103.服务器端程序实时接收和计算客户端传输来的用户的目标特征信息数据,

[0069] S104.服务器端对比所述目标特征信息与参考特征信息,若所述目标特征信息与所述参考特征信息存在偏差,则判断所述偏差与设定的多个阈值范围的关系;

[0070] 所述参考特征信息包括用户对鼠标移动和对键盘敲击的行为特点对应的特征信息;

[0071] 其中,考虑到真实用户随时间等因素,其使用计算机熟练度变化可能造成特征数据超过设定的偏差,为保证真实用户主体的合法性,用户必须重新申请训练,以更新服务器端的用户的参考特征信息数据。

[0072] S105.服务器端根据根据判断结果认证所述用户的身份。

[0073] 进一步地,服务器端根据根据判断结果认证所述用户的身份,如图2所示,包括:

[0074] S1051. 设定第一阈值范围, 若所述偏差位于所述第一阈值范围, 则认证当前用户为真实用户;

[0075] S1052. 设定第二阈值范围, 若所述偏差位于所述第二阈值范围, 则发出告警信号, 认证当前用户为待鉴定用户, 继续进行目标特征信息与参考特征信息的比对;

[0076] S1053. 设定第三阈值范围, 若所述偏差位于所述第三阈值范围, 则认证当前用户为错误用户, 发出锁定信号, 将用户当前操作的客户端界面锁定。

[0077] 具体地, 所述目标特征信息与所述参考特征信息之间的偏差具有不同的程度, 对应着不同的认定结果; 其中, 若所述偏差位于所述第一阈值范围, 则服务器端认证当前用户为真实用户, 满足用户对当前客户端的操作; 若所述偏差位于所述第二阈值范围, 则发出告警信号, 服务器端认证当前用户为待鉴定用户, 继续进行目标特征信息与参考特征信息的比对, 直至给与最终判断结果, 判断出所述用户为真实用户还是错误用户; 需要说明的是, 若多次出现所述偏差位于所述第二阈值范围的情况, 则通过在客户端上弹出问题对话框, 让当前用户回答问题的形式进一步鉴定用户的身份; 若所述偏差位于所述第三阈值范围, 则服务器端认证当前用户为错误用户, 此时服务器端会直接发送锁定信号, 将用户当前操作的客户端界面锁定

[0078] 进一步地, 所述服务器端对比所述目标特征信息与参考特征信息, 之前包括, 如图3所示:

[0079] S1041a. 服务器端获取客户端采集到的, 用户对鼠标进行移动的大量动作和对键盘进行敲击的大量动作; 并将其发送给服务器端;

[0080] S1042a. 服务器端通过分析用户对鼠标进行移动的大量动作信息和对键盘进行敲击的大量动作信息, 生成所述参考特征信息。

[0081] 具体地, 鼠标键盘的行为特征是指用户操作鼠标键盘的习惯。对每个用户而言, 其鼠标键盘操作都存在与其他用户显著不同的模式; 每个用户由于个人原因可能造成在使用鼠标键盘时有不同的习惯; 比如用户对鼠标的使用来说, 包括鼠标左键单击行为、鼠标右键单击行为、鼠标左键双击行为、鼠标移动行为、鼠标左键拖拽行为、鼠标右键拖拽行为、鼠标移动加左键单击行为、鼠标移动加右键单击行为、鼠标移动加左键拖拽行为、鼠标移动加右键拖拽行为和鼠标移动加左键双击行为。

[0082] 进一步具体说明的是, 鼠标左键单击行为信息包括: 点击时间和点击的移动距离, 所述的点击时间是指鼠标按下和鼠标弹起之间的时间间隔, 所述的点击的移动距离是指鼠标按下和鼠标弹起之间的移动距离;

[0083] 鼠标右键单击行为信息包括: 点击时间和点击的移动距离;

[0084] 鼠标左键双击行为信息包括: 第一次点击时间、第一次点击的移动距离、双击间隔时间、双击间隔距离、第二次点击时间和第二次点击的移动距离。

[0085] 通过将大量数据的分析和处理得出用户的参考特征信息, 进行保存便于后续的调用。

[0086] 或者, 作为一种优选地实施方式, 所述服务器端对比所述目标特征信息与参考特征信息, 之前包括, 如图4所示,

[0087] S1041b. 获取用户在客户端上的训练场景进行训练得出的训练数据;

[0088] S1042b. 根据所述训练数据的信息生成所述参考特征信息。

[0089] 其中,训练必须在设定的场景内进行,每一个场景都对应于一个特定的鼠标或键盘的行为指标。若系统共提供9个场景用于训练,用户需根据当前场景给出的提示完成指定的操作;每一个场景的设计都是建立在一定的背景之上的,避免了使用过程中的枯燥和复杂。它们分别是:妈妈的大餐(双击图片)、按点划线(鼠标轨迹相关)、妹妹的数数测试(单击图片)、力量训练(鼠标滚轮操作)、姐姐的购物(右击图片)、口算训练(键盘按键相关指标)、宠物市场大抢购(鼠标轨迹相关)、我的密码手势(轨迹相关)、传统密码字符(击键特征)。每一个场景都对应一个或多个特定的行为指标,在场景过程中,用户必须按照场景给出的提示完成相应的操作,对于非指定操作,场景将给出操作失误的提示,该操作所对应的行为数据也将被丢弃。场景指标都是经过测试后选出来的;用这些指标进行身份认证时,需要的样本数据量小,自然数据收集时间也相应的减少,这样在训练和认证的过程中就省了不少的时间;所选出的这些指标,在进行身份判别测试中,它们的效果也是不一样的。因此,用安全级别对认证时这些指标的使用进行划分归类:对于效果比较好的指标,将归入高的安全级别;对于效果一般的指标,将归入一般或较低的安全级别。这样在进行认证时,用户只需通过预先设定好的安全级别所对应的场景,而不需要通过全部的场景,相比训练时间又减少了不少。

[0090] 通过使用特定的场景环境,再结合全局的键盘钩子(WH_KEYBOARD_LL)和全局鼠标钩子(WH_MOUSE_LL),可以精确地收集到想要的行为数据。在场景环境中,用户需要根据场景所给出的提示完成一系列的操作,如单击鼠标左键、单击鼠标右键、双击鼠标左键、滚动鼠标滚轮、移动鼠标光标、输入预定的密码字符串等。在场景中,单场景中的每一步操作、场景间的切换都具有可控性,所以可以很精确地获取用户当前时间段所产生的行为数据是什么,进而可以对这些行为数据进行分类整理;本实施例采用优化的SVM算法对采集的数据进行整理。

[0091] 其中,SVM算法在解决小样本、非线性极高危模式识别中表现出许多特有的优势,主要解决的是两类问题。先来看下面的目标函数:

$$[0092] \quad W \cdot X + b = 0 \quad (1)$$

[0093] 这是一条直线,在确定的W值和b值下,只有唯一的X值可以满足(1)式,其他的X值带入后,要么大于零,要么小于零,这样其他的X值便被分成两类,不可分的是满足(1)式的X。

[0094] 以上W和X值是一维的情况,SVM在此基础上给这参数赋予全新定义,将原先的W值和X值扩展到多维,得到如下目标函数:

$$[0095] \quad X = (x_1, x_2, x_3, \dots, x_n) \quad n=1, 2, 3 \dots n \quad (2)$$

$$[0096] \quad Y = (y_1, y_2, y_3, \dots, y_n) \quad n=1, 2, 3 \dots n \quad (3)$$

$$[0097] \quad A = (a_1, a_2, a_3, \dots, a_n) \quad n=1, 2, 3 \dots n \quad (4)$$

$$[0098] \quad W = y_1 \cdot a_1 \cdot X_1 + y_2 \cdot a_2 \cdot X_2 + \dots + y_n \cdot a_n \cdot X_n \quad n=1, 2, 3 \dots n \quad (5)$$

$$[0099] \quad \langle W, X \rangle + b = 1 - C \cdot E \quad C \text{和} E \text{为实数} \quad (6)$$

[0100] 这里定义了两个新值Y和A,同时也不难看出X和W都变成了多维,(6)式相当于原来的(1)式,将不满足(6)式的多维X分成两类。

[0101] 用户定义为一个n维的向量X,取值为用户鼠标或键盘操作特征,如用户=(左键单击时间t1)。假设有两个用户甲和乙。甲有三组鼠标键盘特征样本X1, X2, X3,一组样本就对

应一个式(2),如 $X1 = (x1, x2, x3)$, $X2 = (x1, x2, x3)$, $X3 = (x1, x2, x3)$ 。应该注意不同样本中 xn 值不一定相等,但都是同一类型的值(如鼠标或键盘特征),而且括号中的数据个数必须相等。至于数据个数为自定义,比如增加一个双击数据记为 $x4$,则 $X1 = (x1, x2, x3, x4)$, $X1 = (x1, x2, x3, x4)$, $X1 = (x1, x2, x3, x4)$ 。同理,乙有三组鼠标键盘特征样本 $X4, X5, X6$ 。甲乙样本数可以不等,但样本中的鼠标或键盘特征必须一一对应,现在总样本数为6。

[0102] 再来看(3)(4)式,由于总样本为6,因此,(3)(4)式子括号中的 n 为6,即由样本总数确定,(3)(4)括号中的值要与6个样本一一对应,如 $X1$ 对应 Y 中的 $y1$ 以及 A 中的 $a1$,其他样本以此类推,现将以上对应关系整理如下:

[0103] 甲: $X1 = (x1, x2, x3) y1 a1$

[0104] $X2 = (x1, x2, x3) y2 a2$

[0105] $X3 = (x1, x2, x3) y3 a3$

[0106] 乙: $X4 = (x1, x2, x3) y4 a4$

[0107] $X5 = (x1, x2, x3) y5 a5$

[0108] $X6 = (x1, x2, x3) y6 a6$

[0109] 至于 Y 中的值,做这样的处理:对应甲的所有 y 都赋1,对应乙的为-1,也可以反过来,即 $y1 = y2 = y3 = 1, y4 = y5 = y6 = -1$;或者, $y1 = y2 = y3 = -1, y4 = y5 = y6 = 1$ 。 A 中的值是在用户训练时程序对用户各样本组计算后自动产生的。本例以用户甲的 y 为1作为标准。

[0110] 再来看(5)式,发现将以上整理的甲乙关系数据代入(5)式右边,便可得出左边的 W 值了。(5)式便是认证的式子,(6)式中的 W 便是(5)式的 W , b 为用户训练时程序自动产生, C 和 E 为本算法自定义值, X 代表待认证用户的一组新样本。注意:这里的待认证用户只能是决定 W 的两个用户,这是因为(6)式和(1)式一样,解决的是两类问题,如本例中 W 由甲乙的样本而得来,则只能认证甲乙,之后数据都带入(6)式,大于式子左边,认证通过。

[0111] 那么,要对获取的行为数据进行整理,并把它们转化为符合算法要求的格式。由于SVM算法是解决两类样本的分类问题的,因而只用一条分类线可以区分两个样本。对于多用户的区分,采取这种方式判定当前用户的身份。如对用户1进行判定,且当前训练过的用户样本有6个时,那么用户1的训练样本与其余5个用户的训练样本分别进行分类线计算,然后用这5条分类线进行样本判定。这里需要注意的是:训练样本必须保持奇数个,若当前用户训练量不足奇数个,系统会自动调用存根样本去补足。若分类线判定时投给用户1的票数超过一半(一条分类线相当于一次投票),那么就判定为1用户。算法的优化情况:现在再将以上(2)~(6)式的参数值确定情况整理如表1所示。由表1看出,可以在这些参数中作改变的为 X (上面已讲过 X 可自定义,即鼠标指标数自定义且鼠标指标自定义)、 C (程序自定义具体值),而剩下的参数要么固定,要么由其他参数算出。

[0112] 由于SVM算法的特性,系统可以根据用户当前的训练数据给出一个评估,即根据当前训练的数据,对在进行特征对比时通过的可能性进行估计。并且,用户可以根据此评估结果决定是否再次进行训练。训练状态下,用户除了完成全部场景的训练任务,还需要根据当前用户的权限设置安全级别。

[0113] 进一步地,所述获取用户的生物信息数据,之前包括:

[0114] 通过客户端判断用户是否输入了生物信息数据,若是,则通过客户端采集所述生物信息数据。

[0115] 需要说明的是,系统采用了优化后的SVM算法,具有灵活的结构布局,能够允许用户在应用系统原有的基础上进行二次开发,有很好的移植性。

[0116] 实施例二:

[0117] 本实施例提供了一种身份认证方法,如图5所示,所述方法除了包括实施例一中所述的方法之外,进一步地还包括:

[0118] S106.服务器端将用户每一次的身份判断结果和每一次采集的目标特征信息以列表的形式进行存储;

[0119] S107.通过服务器端的控制界面检视所述用户的过往登录信息和身份验证信息。

[0120] 需要说明的是,提供对应的Web界面的管理平台,管理员可以用通过服务器的图形控制界面检视用户过往登录和身份验证的记录;公司管理人员可以查看当前内网中用户登录的实时摘要信息,通过查看列表的形式清晰地获取每个用户的登录情况和身份判断的结果信息。

[0121] 实施例三:

[0122] 本实施例提供了一种身份认证系统,所述系统通过客户端和服务器端共同完成。如图6和图7所示,具体包括:

[0123] 生物信息获取模块110,用于获取用户的生物信息数据;所述生物信息数据包括用户对鼠标的移动动作数据和对键盘的敲击动作数据;

[0124] 具体地,对鼠标的移动数据和对键盘的敲击数据的采集是在用户的行为动作中完成的,每个参与数据采集的用户都在各自的计算机匹配一个可以监控记录用户鼠标行为和键盘的敲击的模块,并将采集的数据自动送到采集服务器。

[0125] 需要说明的是,采集到的鼠标数据中或多或少都会存在一些干扰或噪音,对含有这种干扰的数据进行分析,必定会降低识别的准确性。例如,不同的计算机用户有不同的鼠标单击速度,一般人的鼠标单击时间间隔大约在40~500ms之间,有时差异可能会更大。如果对所有用户设立统一的过滤阈值,阈值定低了,会将一些点击速度慢的人的正常数据滤除掉;阈值定高了,又会带来很大的误差,因此分别为不同用户确定不同阈值 L_i 是更客观的选择。

[0126] $L_i = kM_i$ (7)

[0127] 其中, M_i 是第*i*个用户的左键单击时间间隔,系数*k*可以通过一些优化工具来确定。

[0128] 生物信息转换模块120,将所述生物信息数据分析处理生成目标特征信息;

[0129] 特征比对模块130,用于对比所述目标特征信息与参考特征信息,若所述目标特征信息与所述参考特征信息存在偏差,则判断所述偏差与设定的多个阈值范围的关系;所述参考特征信息包括用户对鼠标移动和对键盘敲击的行为特点对应的特征信息;

[0130] 身份判断模块140,用于根据判断结果认证所述用户的身份。

[0131] 进一步地,所述身份判断模块140包括:

[0132] 第一阈值判断单元141,用于设定第一阈值范围,若所述偏差位于所述第一阈值范围,则认证当前用户为真实用户;

[0133] 第二阈值判断单元142,用于设定第二阈值范围,若所述偏差位于所述第二阈值范围,则发出告警信号,认证当前用户为待鉴定用户,继续进行目标特征信息与参考特征信息的比对;

[0134] 第三阈值判断单元143,用于设定第三阈值范围,若所述偏差位于所述第三阈值范围,则认证当前用户为错误用户,发出锁定信号,将用户当前操作的客户端界面锁定。

[0135] 进一步地,所述特征比对模块130包括:

[0136] 采集动作获取单元131,用于获取从客户端采集得到的,用户对鼠标进行移动的大量动作和对键盘进行敲击的大量动作;

[0137] 第一参考特征生成单元132,用于通过分析用户对鼠标进行移动的大量动作信息和对键盘进行敲击的大量动作信息,生成所述参考特征信息。

[0138] 或者包括:

[0139] 训练数据获取模块133,获取用户在客户端上的训练场景进行训练得出的训练数据;

[0140] 第二参考特征生成单元134,根据所述训练数据的信息生成所述参考特征信息。

[0141] 需要说明的是,用户在使用该系统之前,需要先被授权,成为授权用户,之后,所述系统针对每一个授权用户的键盘和鼠标使用特点建立一个独一无二的参考特征集,也就是本实施例的第一参考特征生成单元。

[0142] 进一步地,所述生物信息获取模块110,包括生物信息输入判断单元111,用于判断用户是否输入了生物信息数据,若是,则通过客户端采集所述生物信息数据。

[0143] 进一步地,还包括:

[0144] 第一存储模块150,用于将用户每一次的身份判断结果以列表的形式进行存储;

[0145] 第二存储模块160,用于将每一次采集的目标特征信息以列表的形式进行存储。

[0146] 信息检视模块170,用于检视所述用户的过往登录信息和身份验证信息。

[0147] 具体地,所述系统提供Web界面的管理平台,管理员可以通过服务器端的控制界面检视用户过往登录和身份验证的记录,可查看当前内网中用户登录的实时摘要信息,当前时间每个用户的登录以及身份认证的情况。

[0148] 需要说明的是,本发明通过收集和分析用户的鼠标运动和键盘敲击所产生的生物信息来持续地对计算机用户进行识别。

[0149] 进一步说明的是,持续身份认证系统还可以结合对异常网络流量的分析,用先进的启发式算法来检测网络中的入侵行为;并且,综合用户帐号的身份识别和网络入侵分析,进一步高准确度地监测恶意入侵行为。

[0150] 进一步说明的是,若本发明应用在个人计算机上,且当前使用者是经过计算机主人的同意下进行操作的,此时主人也就是真实用户可以访问权限的设置,将该权限限制进行取消,或是在屏幕锁定之后主人将该锁定解除。

[0151] 本发明具有如下的有益效果:

[0152] (1) 通过本发明的技术方案,公司和组织可以用它来监控内部网络中用户的行踪,且能够控制用户对计算机的访问。

[0153] (2) 通过本发明的技术方案,能够持续地对用户身份进行认证,时时保护和监测用户帐号/密码被黑客或者组织内部的泄密者窃取的情形。

[0154] (3) 本发明的技术方案,系统管理员可以通过管理界面监控当前内部网络中用户帐号的登录情况,及时了解可能的帐号信息失密个案,进而采取行动阻止窃密者的侵害行为。

[0155] 总之,本发明从人机交互和用户生理行为层面出发,能够全面的且实时地进行网络保护,具有较高的准确率。

[0156] 在本发明的上述实施例中,对各个实施例的描述都各有侧重,某个实施例中沒有详述的部分,可以参见其他实施例的相关描述。

[0157] 本发明中的技术方案中的各个模块均可通过计算机终端或其它设备实现。所述计算机终端包括处理器和存储器。所述存储器用于存储本发明中的程序指令/模块,所述处理器通过运行存储在存储器内的程序指令/模块,实现本发明相应功能。

[0158] 本发明中的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或部分可以以软件产品的形式体现出来,该计算机软件产品存储在存储介质中,包括若干指令用以使得一台或多台计算机设备(可为个人计算机、服务器或者网络设备等)执行本发明各个实施例所述方法的全部或部分步骤。

[0159] 本发明中所述模块/单元的划分,仅仅为一种逻辑功能划分,实际实现时可以有另外的划分方式,例如多个单元或组件可以结合或者可以集成到另一个系统,或一些特征可以忽略,或不执行。可以根据实际的需要选择其中的部分或者全部模块/单元来达到实现本发明方案的目的。

[0160] 另外,在本发明各个实施例中的各模块/单元可以集成在一个处理单元中,也可以是各个单元单独物理存在,也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现,也可以采用软件功能单元的形式实现。

[0161] 以上所述仅是本发明的优选实施方式,应当指出,对于本技术领域的普通技术人员来说,在不脱离本发明原理的前提下,还可以做出若干改进和润饰,这些改进和润饰也应视为本发明的保护范围。

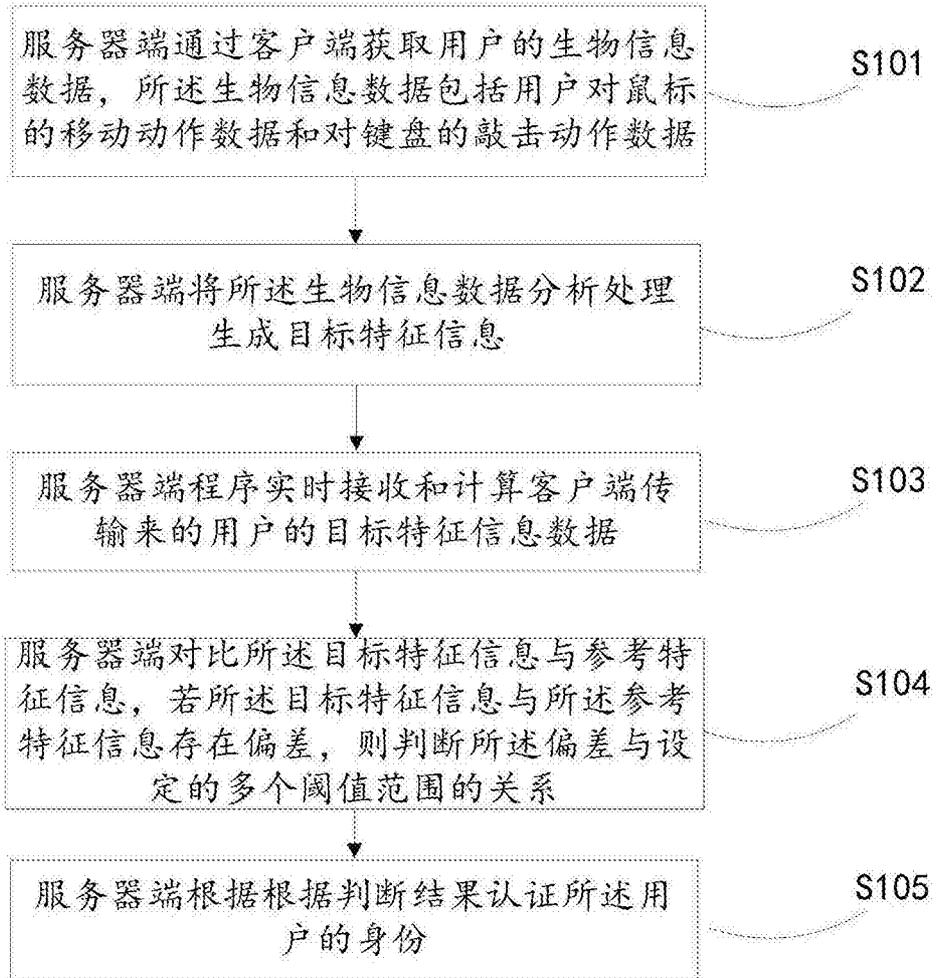


图1

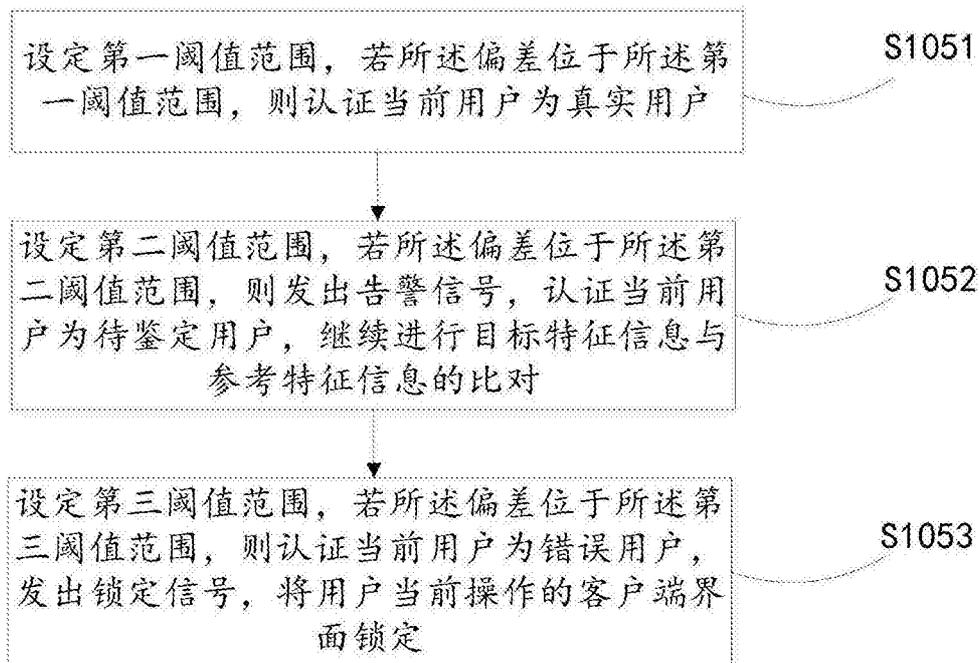


图2

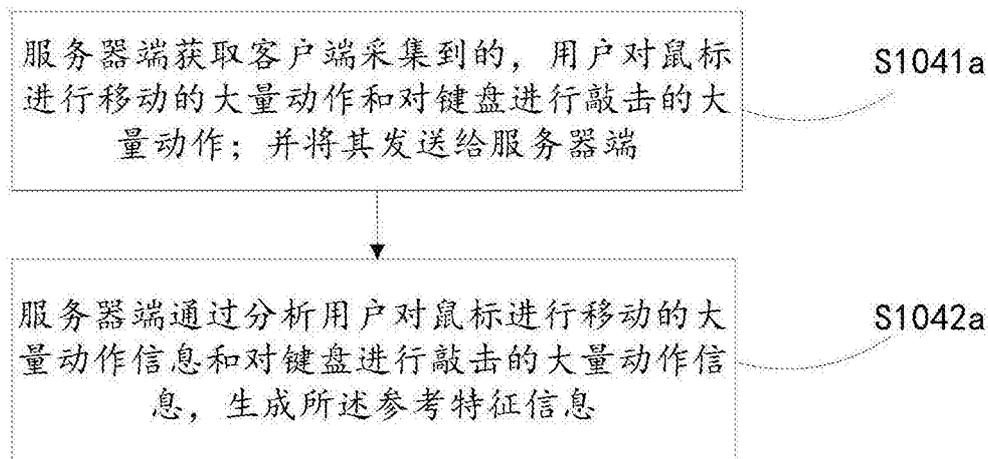


图3

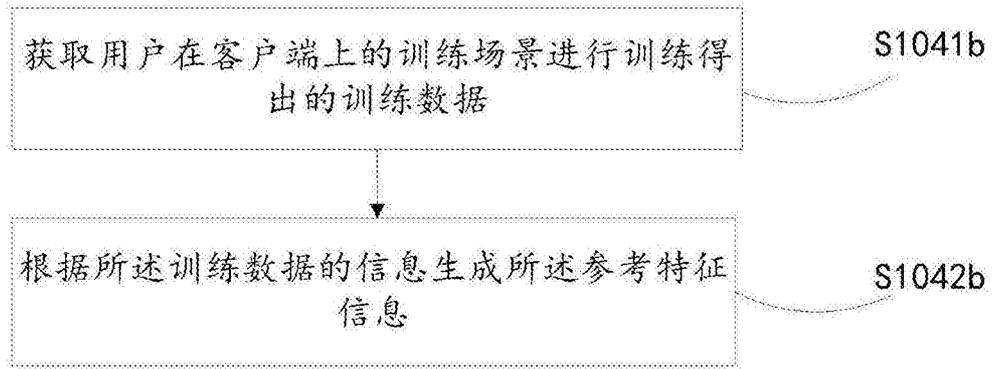


图4

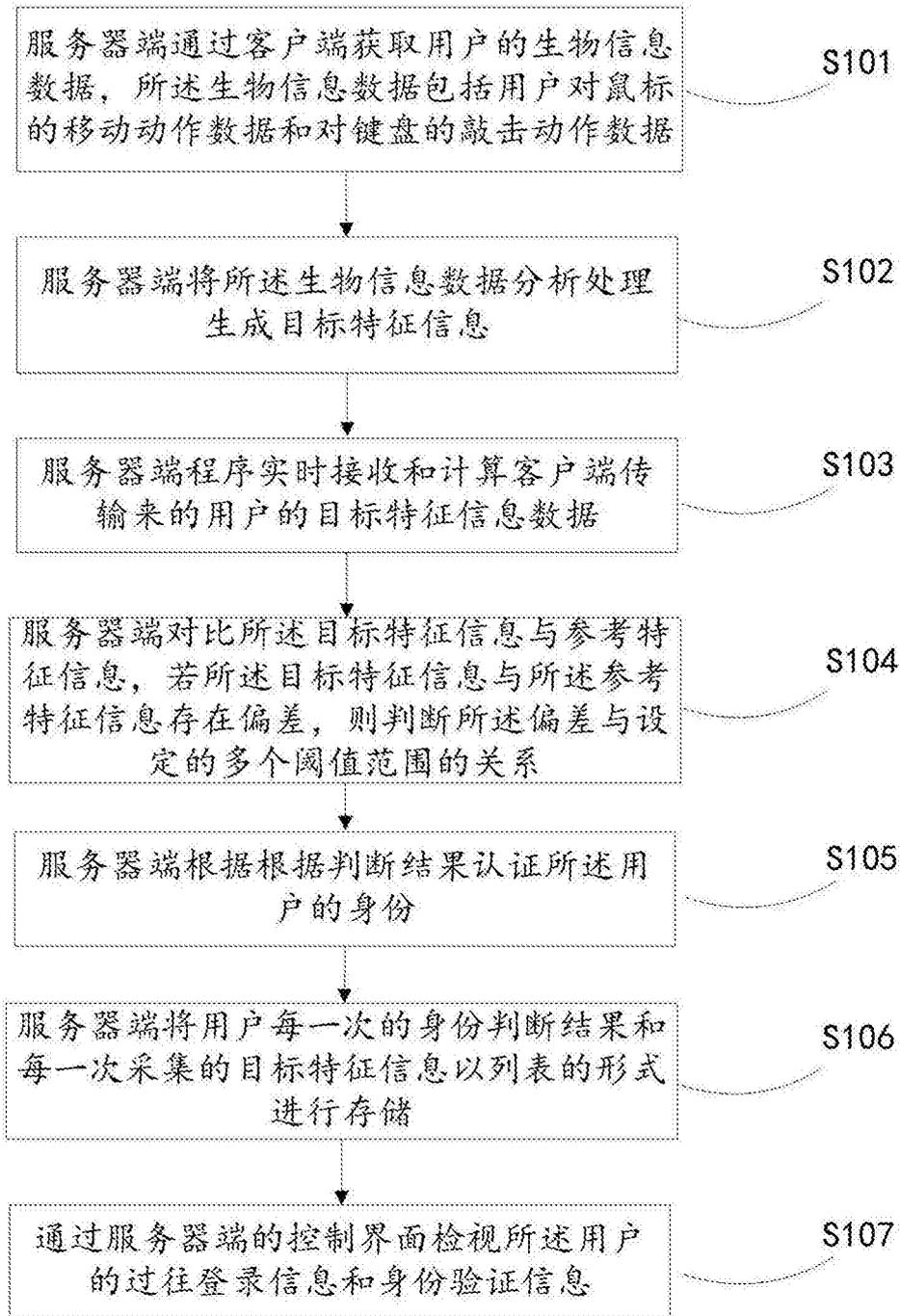


图5

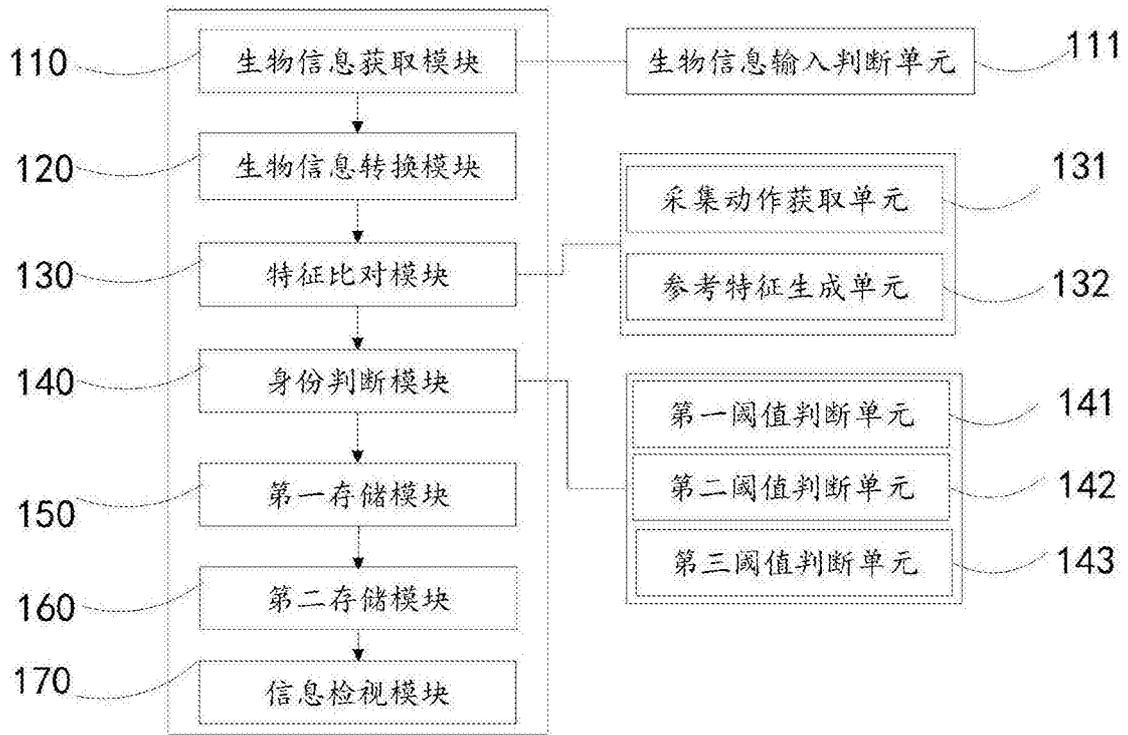


图6

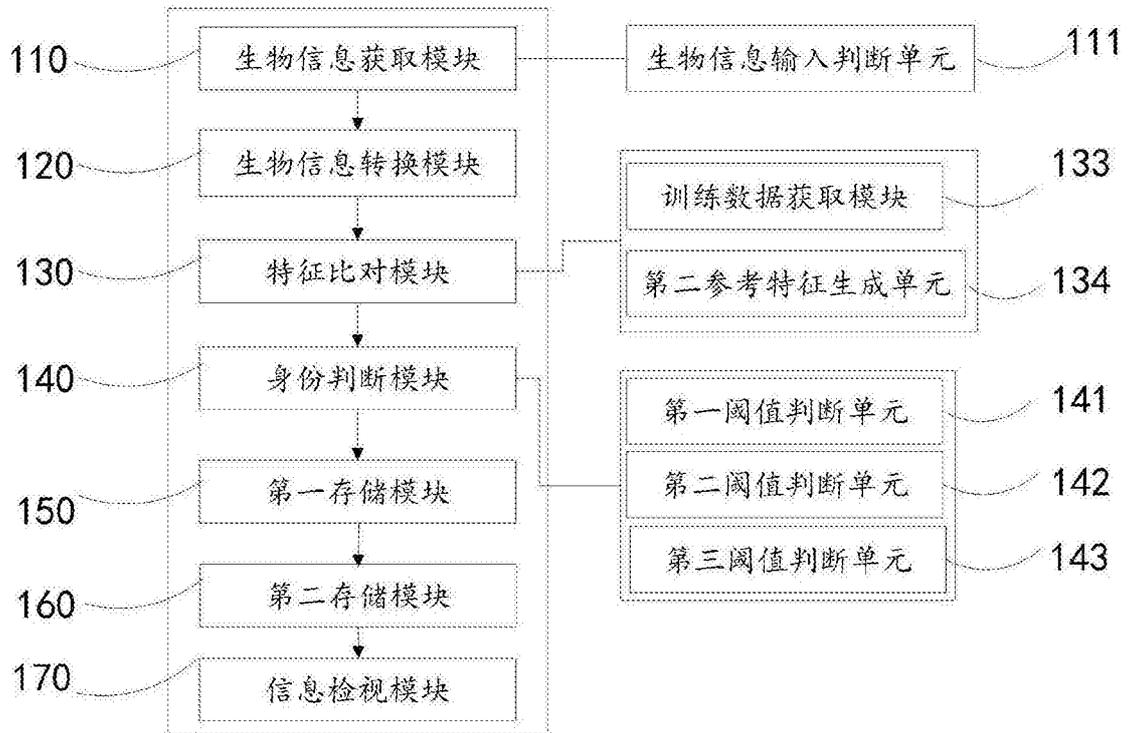


图7