(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 106295295 B
(45)授权公告日 2019.12.10

(21)申请号 201610621151.8

(22)申请日 2016.08.01

(65)同一申请的已公布的文献号
申请公布号 CN 106295295 A

(43)申请公布日 2017.01.04

(73)专利权人 上海交通大学
地址 200240 上海市闵行区东川路800号

(72)发明人 易平 黄程 顾双驰 王科迪

(74)专利代理机构 上海交达专利事务所 31201
代理人 王毓理 王锡麟

(51)Int.Cl.
G06F 21/32(2013.01)

(56)对比文件
CN 105068743 A,2015.11.18,
张英峰等.基于超球面支持向量机的综合传动状态判别.《吉林大学学报》.2012,第42卷(第1期),

审查员 彭明明

权利要求书1页 说明书3页 附图1页

(54)发明名称

基于行为指纹的移动终端用户认证方法

(57)摘要

一种基于行为指纹的移动终端用户认证方法,包括:1)采集行为指纹;2)建立用于保存行为指纹的行为数据库;3)根据行为数据库中的行为指纹建立识别模型;4)用户输入当前行为指纹;5)进行身份识别,用户正确则系统做出响应,本发明能够准确地检测并识别用户身份,安全成本降低,减少了用户对于密钥的保管成本和密钥丢失的风险,由于认证完全是基于用户的行为指纹,无需额外支持设备,只需要通过移动终端传递的用户行为信息即可进行认证。

CN 106295295 B

1.一种基于行为指纹的移动终端用户认证方法,其特征在于,包括:

1)采集行为指纹;

2)建立用于保存行为指纹的行为数据库;

3)根据行为数据库中的行为指纹建立识别模型,具体包括:

3.1)从行为数据库中提取数据;

3.2)提取特征向量F;

3.3)使用SVM建模,获得核函数的参数,得到识别模型;

4)用户输入当前行为指纹;

5)进行身份识别,用户正确则系统做出响应;完成后,进行身份识别的准确率检测,若准确率低于设定值则重新建立识别模型;

所述的行为指纹包括:触点的横坐标x、触点的纵坐标y、按压时长t、按压面积s、角加速度、线加速度g;

所述的角加速度包括:X轴角加速度α、Y轴角加速度β以及Z轴角加速度γ;

所述的特征向量F=(x,y,t,s,g,α,β,γ);

所述的SVM建模,采用超球面而非超平面的方法,从而使得最小化离群点带来的影响;所述的超球面是通过超球面的中心a和半径R,R是中心a到边界(支持向量)的距离,约束条件是R^2需要最小化,中心a是支持向量的线性组合,使用惩罚因子C的松弛变量ξ_i,从而得到核函数;

所述的核函数为$\|\zeta - \boldsymbol{x}\|^2 = \sum_{i=1}^{n} \alpha_i \exp\left(\frac{-\|\zeta - x_i\|^2}{\sigma^2}\right) \geq -\frac{R^2}{2} + C_R$,其中:ζ为松弛变量。

所述的身份识别,其程序化过程包括:

定义若干变量:Role,取值有0,1和-1,其中:0代表未知身份,1代表主人,-1代表非主人,初始状态下Role为0,即不知道操作者身份;Total,当前用户操作计数,一旦Role从0变为1或者-1,则Total置零,否则在身份识别出来之前一直递增;TC,TC_{svm}为一个使用动作经SVM模型预测是主人则TC_{svm}加1,初始为0;CTSS,为用户的TSS计数,CFSS为用户的FSS计数,初始状态下这两个变量均为0,一次TSS则CTSS加1,一旦出现FSS则CFSS加1,CTSS置零;CS,为当前状态,用户动作匹配到的状态机节点,用数据库中的节点id标志,初始为0;

初始状态时所有变量值均为0,用户每操作一次Total加1,同时会进行SVM模型预测和状态机状态判断,当SVM预测为主人,则TCSVM加1;

当CS=0,当前动作匹配到状态机中的节点i,则CS=i,CTSS加1,否则CFSS加1,当CS!=0时,当前动作匹配到CS的下一个节点中的某一个,则CTSS加1,否则CFSS加1且CTSS置0,CS置0,

当出现一下条件时做出身份判断,即Role从0变为1或者-1,其它变量置零,$C_{FSS} \geq 4, \frac{TC_{svm}}{Total} < 25\%$,则Role=-1,$C_{Tss} \geq 4, \frac{TC_{svm}}{Total} \geq 50\%$,则Role=1。

基于行为指纹的移动终端用户认证方法

技术领域

[0001] 本发明涉及的是一种移动设备安全领域的技术，具体是一种基于行为指纹的移动终端用户认证方法。

背景技术

[0002] 移动终端作为在移动中使用的计算机设备，包括手机以及其它便携设备。随着技术发展，移动终端从简单通话工变成了综合信息处理平台。移动终端的安全保障日益重要，通常采用的被动防御措施，如密码、锁屏图案等，不能有效阻止入侵者。行为指纹是指用户在电子设备操作中，由个人习惯和生物差异导致的与他人不相同的特征。

发明内容

[0003] 本发明针对现有技术大多只采用陀螺仪传感器，单维度的数据不能有效描绘用户的行为特征，并且具有精确度低，模型可靠性差，对于不同的终端适配性不好等缺陷，提出一种基于行为指纹的移动终端用户认证方法，能够准确地检测并识别用户身份，安全成本降低，减少了用户对于密钥的保管成本和密钥丢失的风险。由于认证完全是基于用户的行为指纹，无需额外支持设备，只需要通过移动终端传递的用户行为信息即可进行认证。

[0004] 本发明是通过以下技术方案实现的：

[0005] 本发明包括以下步骤：

[0006] 1)采集行为指纹；

[0007] 2)建立用于保存行为指纹的行为数据库；

[0008] 3)根据行为数据库中的行为指纹建立识别模型；

[0009] 4)用户输入当前行为指纹；

[0010] 5)进行身份识别，用户正确则系统做出响应。

[0011] 所述的行为指纹包括：触点的横坐标x、触点的纵坐标y、按压时长t、按压面积s、角加速度、线加速度g。

[0012] 所述的角加速度包括：X轴角加速度α、Y轴角加速度β以及Z轴角加速度γ。

[0013] 所述的步骤3具体包括以下步骤：

[0014] 3.1)从行为数据库中提取数据；

[0015] 3.2)提取特征向量F；

[0016] 3.3)使用SVM建模，获得核函数的参数，得到识别模型。

[0017] 所述的特征向量F＝(x,y,t,s,g,α,β,γ)。

[0018] 所述的核函数为$\|\zeta - \boldsymbol{x}\|^2 = \sum_{i=1}^{n} \alpha_i \exp\left(\frac{-\|\zeta - x_i\|^2}{\sigma^2}\right) \geq -\frac{R^2}{2} + C_R$，其中：ζ为松弛变量。

[0019] 所述的步骤5)完成后，进行身份识别的准确率检测，若准确率低于设定值则重新建立识别模型。

附图说明

[0020] 图1为本发明流程示意图。

具体实施方式

[0021] 下面对本发明的实施例作详细说明，本实施例在以本发明技术方案为前提下进行实施，给出了详细的实施方式和具体的操作过程，但本发明的保护范围不限于下述的实施例。

[0022] 实施例1

[0023] 如图1所示，本实施例包括以下步骤：

[0024] 1)采集行为指纹。所述的行为指纹包括：触点的横坐标x、触点的纵坐标y、按压时长t、按压面积s、角度速、线加速度g。

[0025] 所述的角加速度包括：X轴角加速度α、Y轴角加速度β以及Z轴角加速度γ。用户通过触摸屏进行输入操作时，采集用户的行为指纹。

[0026] 所述的角加速度通过设置于设备中的陀螺仪传感器采集，而线加速度g则通过加速度传感器采集。触点的横坐标x、触点的纵坐标y、按压时长t和按压面积s则为通过屏幕直接采集的数据。

[0027] 2)建立用于保存行为指纹的行为数据库。将采集到的行为指纹数据保存到行为数据库中。

[0028] 3)根据行为数据库中的行为指纹建立识别模型。

[0029] 3.1)从行为数据库中提取数据；

[0030] 3.2)提取特征向量F；

[0031] 3.3)使用SVM建模，获得核函数的参数，得到识别模型。

[0032] 所述的特征向量F＝(x,y,t,s,g,α,β,γ)。

[0033] 所述的SVM建模，采用超球面而非超平面的方法，从而使得最小化离群点带来的影响。超球面是通过超球面的中心a和半径R，R是中心a到边界(支持向量)的距离，约束条件是R^2需要最小化。中心a是支持向量的线性组合。虽然可以要求所有的数据点与中心的距离都小于R，但是考虑到离群点和噪声点，需要创建一个有稍许弹性的边界，所以使用惩罚因子C的松弛变量ξ_i，从而得到核函数。

[0034] 所述的核函数为$\|\zeta - \boldsymbol{x}\|^2 = \sum_{i=1}^{n} \alpha_i \exp\left(\frac{-\|\zeta - x_i\|^2}{\sigma^2}\right) \geq -\frac{R^2}{2} + C_R$，其中：ζ为松弛变量。

[0035] 4)用户输入当前行为指纹。

[0036] 5)进行身份识别，用户正确则系统做出响应。根据当前使用者即用户进行操作时，系统采集行为指纹与识别模型中设定的阀值进行比较，以识别用户的身份。用户正确则系统做出应有的响应，如果不正确则采取防护措施。其程序化的过程为：

[0037] 定义若干变量：Role，取值有0,1和-1，其中：0代表未知身份，1代表主人，-1代表非主人。初始状态下Role为0，即不知道操作者身份。

[0038] Total，当前用户操作计数。一旦Role从0变为1或者-1，则Total置零，否则在身份识别出来之前一直递增。

[0039] TC(True Count)，TC_{svm}为一个使用动作经SVM模型预测是主人则TC_{svm}加1，初始为

0。

[0040] CTSS,为用户的TSS计数。CFSS为用户的FSS计数。初始状态下这两个变量均为0。一次TSS则CTSS加1,一旦出现FSS则CFSS加1,CTSS置零。

[0041] CS(current state),为当前状态,用户动作匹配到的状态机节点,用数据库中的节点id标志,初始为0。

[0042] 初始状态时所有变量值均为0。用户每操作一次Total加1,同时会进行SVM模型预测和状态机状态判断。若SVM预测为主人,则TCSVM加1。

[0043] 若CS＝0,当前动作匹配到状态机中的节点i,则CS＝i,CTSS加1,否则CFSS加1。当CS!＝0时,当前动作匹配到CS的下一个节点中的某一个,则CTSS加1,否则CFSS加1且CTSS置0,CS置0。

[0044] 当出现一下条件时做出身份判断,即Role从0变为1或者-1,其它变量置零。$C_{FSS}\geq 4$,$\frac{TC_{svm}}{Total}<25\%$,则Role＝-1,$C_{TSS}\geq 4$,$\frac{TC_{svm}}{Total}\geq 50\%$,则Role＝1。

[0045] 所述的步骤5)完成后,进行身份识别的准确率检测,若准确率低于设定值则重新建立识别模型。

[0046] 本实施例中采用基于行为指纹的安全防护系统来实现本方法,该系统包括:采集模块、训练模块以及对比模块,其中:采集模块采集用户的行为指纹信息并传送到训练模块,训练模块利用SVM建模得到行为指纹信息的判断阀值,对比模块从采集模块接收新的指纹信息并与判断阀值相比较以识别用户身份。

[0047] 所述的训练模块将采用基于行为指纹的移动终端用户认证方法,获得各项行为指纹信息,并且将相应的判断依据传递到对比模块。

[0048] 所述的训练模块完成训练后,用户使用该移动设备时,采集模块采集该用户的行为指纹信息,并传输到对比模块。

[0049] 所述的对比模块接收到的新的行为指纹信息代入到相应的用户行为指纹的认证方法中,进行用户合法性的判定。

[0050] 所述的训练模块在进行一次用户识别后,记录用户识别的准确率。当准确率低于设定值时,建议用户重新进行训练。

[0051] 与现有技术相比,本发明能够准确地检测并识别用户身份,安全成本降低,减少了用户对于密钥的保管成本和密钥丢失的风险。由于认证完全是基于用户的行为指纹,无需额外支持设备,只需要通过移动终端传递的用户行为信息即可进行认证。

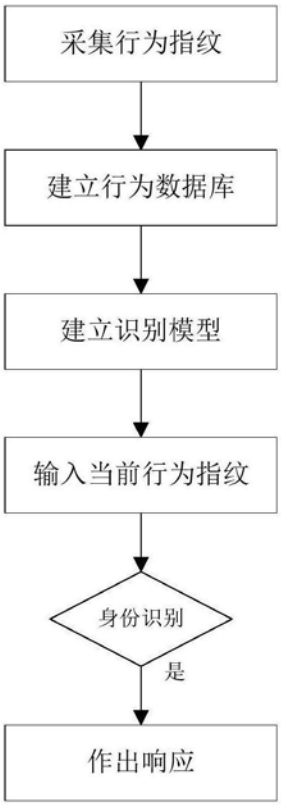

图1