(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 101833619 A
(43)申请公布日 2010.09.15

(21)申请号 201010158930.1

(22)申请日 2010.04.29

(71)申请人 西安交通大学
地址 710049 陕西省西安市咸宁路 28 号

(72)发明人 蔡忠闽 沈超 管晓宏 蔡金培

(74)专利代理机构 西安通大专利代理有限责任公司 61200
代理人 朱海临

(51)Int.Cl.
G06F 21/00(2006.01)

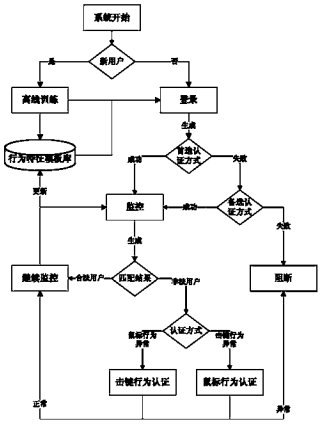
权利要求书 1 页 说明书 8 页 附图 1 页

(54)发明名称

基于键鼠交叉认证的身份判定方法

(57)摘要

本发明公开了一种基于键鼠交叉认证的身份判定方法，将击键行为认证与鼠标行为认证有机结合起来。在用户进行身份登录的过程中，随机选取击键行为认证或鼠标行为认证作为身份认证的首选机制或备选机制，当首选身份认证机制认证成功时，用户认证通过；当首选身份认证机制认证失败时，用备选认证机制进行身份再认证；在用户进行身份监控的过程中，当检测到用户的击键行为发生异常，采用鼠标行为认证的方式进行身份再认证；当检测到用户的鼠标行为发生异常，采用击键行为认证的方式进行身份再认证。本发明利用两种生物行为特征识别的优点及适用的领域，提高容错性，克服单个生物行为特征信息的不完整性，使其具有更广泛的安全性和适用性。



CN 101833619 A

1. 一种基于键鼠交叉认证的身份判定方法，其特征在于，包括下述步骤：

(1) 用户登录前，新用户先注册，启动训练模式，训练模式对用户击键行为或鼠标行为数据进行分析并提取特征，生成参考特征模板，保存入特征模板库；用户登录时，老用户随机选取击键行为或鼠标行为分别作为身份认证的首选认证机制或备选认证机制，当选取击键行为作为身份认证的首选认证机制时，则鼠标行为将作为身份认证的备选机制，记录当前用户的击键行为数据，提取行为特征并生成击键行为的输入特征模板；当选取鼠标行为作为身份认证的首选认证机制时，则击键行为将作为身份认证的备选机制，记录当前用户的鼠标行为数据，提取行为特征并生成鼠标行为的输入特征模板；

(2) 然后将输入特征模板与参考特征模板比较，进行身份认证，当首选身份认证机制认证成功时，用户通过身份认证；当首选身份认证机制认证失败时，用备选认证机制对用户进行身份再认证，若认证通过，则用户登录成功；否则用户登录失败；

(3) 用户登录成功后，启动监控模式，实时采集当前用户的击键和鼠标输入行为数据，提取行为特征并生成击键和鼠标的输入特征模板，随后，将该击键和鼠标的输入特征模板与用户在特征模板库中的参考特征模板匹配，进行验证，如果验证结果为非法用户，则执行步骤 (4)，如果验证结果为合法用户，则继续监控；

(4) 对当前用户进行再认证：再认证方式为，当检测到用户的击键行为发生异常，则采用鼠标行为认证方式进行身份再认证；当检测到用户的鼠标行为发生异常，则采用击键行为认证方式进行身份再认证，如果通过再认证，继续对当前用户身份进行监控；如果未通过再认证，则强制用户登出计算机系统。

2. 根据权利要求 1 所述的基于键鼠交叉认证的身份判定方法，其特征在于，步骤 (3) 中，如果验证结果为合法用户，则继续监控后同时对行为特征模板库进行更新。

3. 根据权利要求 1 所述的基于键鼠交叉认证的身份判定方法，其特征在于，步骤 (2)、(4) 中，所述身份认证、身份再认证的具体实施方式为：

a、基于击键行为身份认证、身份再认证包括如下步骤：

1) 对记录的击键操作行为数据进行预处理操作；

2) 对记录的击键行为信号进行特征提取获得击键行为的基本特征；

3) 根据提取的击键行为特征生成相应的行为特征模板；

4) 利用击键行为模板匹配的方法对计算机用户的击键行为进行认证；

b、基于鼠标行为的身份认证、身份再认证包括如下步骤：

1) 对记录的鼠标操作行为数据进行预处理操作；

2) 对鼠标行为操作进行定义与分割并提取相应的鼠标操作特征；

3) 根据提取的鼠标行为特征生成相应的行为特征模板；

4) 利用鼠标行为模板匹配的方法对计算机用户的鼠标行为进行认证。

4. 根据权利要求 1 所述的基于键鼠交叉认证的身份判定方法，其特征在于，步骤 (3) 中，所述匹配的具体实施方式为：击键行为模板匹配的算法采用加权贝叶斯算法；鼠标行为模板匹配的算法采用类间距离分类或贝叶斯决策算法。

基于键鼠交叉认证的身份判定方法

技术领域

[0001] 本发明涉及一种生物特征识别和信息系统安全领域的身份判定方法，具体涉及一种基于键鼠交叉认证的身份判定方法。

背景技术

[0002] 在生物特征识别和信息系统安全领域，基于生物行为的身份认证已经变成了一个非常重要和前沿的研究课题。信息系统通过身份认证或身份监控等技术手段为系统使用者与系统账号之间建立起合法的对应关系，这是后续进行权限控制、行为审计等其它安全管理措施的先决条件。当前判定用户身份的依据主要有三类：1. 你所知道的，如口令、PIN等；2. 你所拥有的，如ID卡（身份卡）、令牌等；3. 你自身，如指纹、虹膜等生物生理特征(PhysicalBiometrics)。口令是应用最广泛的身份判定手段，但口令难于记忆、容易混淆和泄露，安全性不高；ID卡需要随身携带、易失窃或失效；基于指纹、虹膜甚至是DNA等生理特征的身份判定方法是目前国内外研究的热点，也是当前最为准确的身份判定手段，但这类方法需要额外的硬件设备，短期内也无法在互联网环境中大范围使用。

[0003] 击键、鼠标等指点设备是计算机图形环境下进行人机互动的基本操作工具，不同用户间由于生理、习惯、工作性质等各种因素的差异会产生不同的行为特征，基于此可对用户的身份进行认证。同口令、ID卡，指纹或虹膜等现有方法相比，基于击键、鼠标等操作行为特征判定身份的方法具有以下优点：

[0004] 1) 不需要额外的硬件，适用于现有的互联网环境；

[0005] 2) 无需记忆或携带，也无法被窃取，其它用户很难进行模仿和伪造；

[0006] 3) 还可对登录后用户操作的全过程进行无干扰的实时身份跟踪与监控。

[0007] 但是由于行为特征存在一定的波动性，基于击键或鼠标行为的身份判定方法会产生误判，特别是较容易将合法用户错判为非法用户。因此要成为一种实用的身份判定方法，必须解决合法用户身份错判的问题。本发明提出一种可以较为有效地解决这一问题的新方法。

发明内容

[0008] 本发明的目的是提供一种基于键鼠交叉认证的身份判定方法，用于对计算机用户进行身份监控和身份认证。该方法基于计算机操作行为（击键和鼠标行为）对用户进行身份监控和身份认证，利用交叉认证的方法将击键行为认证与鼠标行为认证有机的结合起来，从而解决基于单独使用击键或鼠标行为特征判定身份时的合法用户身份误判的问题。

[0009] 为达到以上目的，本发明是采取如下技术方案予以实现的：

[0010] 一种基于键鼠交叉认证的身份判定方法，其特征在于，包括下述步骤：

[0011] (1) 用户登录前，新用户先注册，启动训练模式，训练模式对用户击键行为或鼠标行为数据进行分析并提取特征，生成参考特征模板，保存入特征模板库；用户登录时，老用户随机选取击键行为或鼠标行为分别作为身份认证的首选认证机制或备选认证机制，当选

取击键行为作为身份认证的首选认证机制时，则鼠标行为将作为身份认证的备选机制，记录当前用户的击键行为数据，提取行为特征并生成击键行为的输入特征模板；当选取鼠标行为作为身份认证的首选认证机制时，则击键行为将作为身份认证的备选机制，记录当前用户的鼠标行为数据，提取行为特征并生成鼠标行为的输入特征模板；

[0012] (2) 然后将输入特征模板与参考特征模板比较，进行身份认证，当首选身份认证机制认证成功时，用户通过身份认证；当首选身份认证机制认证失败时，用备选认证机制对用户进行身份再认证，若认证通过，则用户登录成功；否则用户登录失败；

[0013] (3) 用户登录成功后，启动监控模式，实时采集当前用户的击键和鼠标输入行为数据，提取行为特征并生成击键和鼠标的输入特征模板，随后，将该击键和鼠标的输入特征模板与用户在特征模板库中的参考特征模板匹配，进行验证，如果验证结果为非法用户，则执行步骤 (4)，如果验证结果为合法用户，则继续监控；

[0014] (4) 对当前用户进行再认证：再认证方式为，当检测到用户的击键行为发生异常，则采用鼠标行为认证方式进行身份再认证；当检测到用户的鼠标行为发生异常，则采用击键行为认证方式进行身份再认证，如果通过再认证，继续对当前用户身份进行监控；如果未通过再认证，则强制用户登出计算机系统。

[0015] 根据上述方法，步骤 (3) 中，如果验证结果为合法用户，则暂停监控后同时对行为特征模板库进行更新。所述匹配的具体实施方式为：击键行为模板匹配的算法采用加权贝叶斯算法；鼠标行为模板匹配的算法采用类间距离分类或贝叶斯决策算法。

[0016] 根据上述方法，步骤 (2)、(4) 中，所述身份认证、身份再认证的具体实施方式为：基于击键行为身份认证、身份再认证包括如下步骤：1) 对记录的击键操作行为数据进行预处理操作；2) 对记录的击键行为信号进行特征提取获得击键行为的基本特征；3) 根据提取的击键行为特征生成相应的行为特征模板；4) 利用击键行为模板匹配的方法对计算机用户的击键行为进行认证。基于鼠标行为的身份认证、身份再认证包括如下步骤：1) 对记录的鼠标操作行为数据进行预处理操作；2) 对鼠标行为操作进行定义与分割并提取相应的鼠标操作特征；3) 根据提取的鼠标行为特征生成相应的行为特征模板；4) 利用鼠标行为模板匹配的方法对计算机用户的鼠标行为进行认证。步骤 (3) 中，所述匹配的具体实施方式为：击键行为模板匹配的算法采用加权贝叶斯算法；鼠标行为模板匹配的算法采用类间距离分类或贝叶斯决策算法。

[0017] 本发明的基于击键行为和鼠标行为的交叉认证方法有以下优点：

[0018] 1. 利用多种生物行为特征（击键、鼠标）进行交叉身份认证，把两种身份认证方法有机的结合起来。

[0019] 2. 该方法实现简单，利用两种生物行为特征识别的优点及适用的领域，提高容错性，降低不确定性，克服单个生物行为特征信息的不完整性，使其具有更广泛的安全性和适用性。

附图说明

[0020] 图 1 是本发明的基于键鼠交叉认证的身份判定结构示意图；

[0021] 图 2 是本发明的基于键鼠交叉认证的身份登录和身份监控流程示意图；

具体实施方式

[0022] 下面结合附图和实施样例对本发明做进一步的详细描述。

[0023] 系统结构

[0024] 参见图 1，本发明基于计算机操作行为（击键和鼠标行为）对用户身份进行监控，利用交叉认证的方法将击键行为认证与鼠标行为认证结合起来。在对计算机用户进行身份登录的过程中，随机选取击键行为认证或鼠标行为认证作为身份认证的首选机制或备选机制，当首选身份认证机制认证成功时，用户通过身份认证；当首选身份认证机制认证失败时，用备选认证机制对用户进行身份再认证，若认证成功，则用户通过身份认证；否则用户身份认证失败。在对计算机用户进行身份监控的过程中，当检测到用户的击键行为发生异常，采用鼠标行为认证的方式进行身份再认证；当检测到用户的鼠标行为发生异常，采用击键行为认证的方式进行身份再认证。如果通过再认证，继续对当前用户身份进行监控；如果未通过再认证，则对用户行为进行阻断。

[0025] 基于键鼠交叉认证的身份判定

[0026] 参见图 2，用户登录前，新用户先注册，启动训练模式，训练模式对用户击键行为或鼠标行为数据进行分析并提取特征，生成参考特征模板，保存入特征模板库。用户登录时，老用户随机选取击键行为认证或鼠标行为认证作为身份认证的首选机制或备选机制，记录当前用户的行为数据（击键行为数据或鼠标行为数据），提取行为特征并生成击键或鼠标的输入特征模板。然后将输入特征模板与参考特征模板比较，进行身份认证，当首选身份认证机制认证成功时，用户通过身份认证；当首选身份认证机制认证失败时，用备选认证机制对用户进行身份再认证，若认证通过，则用户登录成功；否则用户登录失败。用户登录成功后，启动监控模式，实时地采集当前用户的击键和鼠标输入行为数据，提取行为特征并生成当前用户的特征模板。随后，将当前监控用户生成的击键和鼠标输入特征模板与用户在特征模板库中的参考特征模板匹配。如果验证结果为非法用户，则对当前用户进行再认证：再认证方式为，当检测到用户的击键行为发生异常，则采用鼠标行为认证的方式进行身份再认证；当检测到用户的鼠标行为发生异常，则采用击键行为认证的方式进行身份再认证。如果验证结果为合法用户，则继续监控，并将当前用户的特征模板加入到特征模板库中对注册用户的模板进行更新。

[0027] 用户登录时的基于击键行为的身份认证、身份再认证过程

[0028] 假设已经记录下计算机用户产生的击键操作行为数据，如表 1 所示，本发明将按以下步骤进行击键认证。

[0029] 表 1 击键行为记录信息

[0030]

按键值（虚拟键码）	按键状态	系统时间 (ms)	进程信息 (PID)
30	0	639256	6076
30	1	639384	6076

按键值（虚拟键码）	按键状态	系统时间 (ms)	进程信息 (PID)
43	0	639576	6076
43	1	639880	6076

[0031] 注：按键状态中，0 表示按键处于键下状态，1 表示按键处于弹起状态

[0032] 第一步，对记录的击键操作行为数据进行预处理操作，避免数据信息出现重复记录或漏记现象，且避免出现数据信息顺序混乱的现象。具体来说，分为以下几种情况：

[0033] (1) 过滤出现某按键持续按下时的击键信息，这种信息往往与系统性能有关，但不能反映用户的行为特征。

[0034] (2) 对原始输入序列进行重排。在人们日常击键输入过程中，往往不是按照每个按键的键下、弹起序列出现，而是多个按键的键下、弹起混乱出现。为了准确提取用户击键行为特征，需要对这种乱序序列进行校正。

[0035] 第二步，对记录的击键行为信号进行特征提取获得击键行为的基本特征，主要包括击键间隔时间 (inter-key time) 和击键延迟时间 (hold time)，如表 2 所示。

[0036] 表 2 击键操作行为特征

[0037]

击键特征	说明
击键间隔时间	指一次按键到下一次按键之间的时间
击键延迟时间	指一个键的按下和弹起之间的时间

[0038] 第三步，根据提取的击键行为特征生成相应的行为特征模板，定义键盘上的每个键值为 $B_k(1 < k < 36)$，采集 A ～ Z(26 个字母）及 0 ～ 9（十个数字）的击键相关信息，并定义击键间隔时间矩阵为：

[0039]

	A	…	Z	0	…	9
A	$T(1,1)$	…	$T(1,26)$	$T(1,27)$	…	$T(1,36)$
…	…		…	…		…
Z	$T(26,1)$	…	$T(26,26)$	$T(26,27)$	…	$T(26,36)$
0	$T(27,1)$	…	$T(27,26)$	$T(27,27)$	…	$T(27,36)$
…	…		…	…	⋱	…
9	$T(36,1)$	…	$T(36,26)$	$T(36,27)$	…	$T(36,36)$

[0040] 其中 T(i，j)(i ≠ j) 指两个不同键之间（如 e 与 r 等）的击键间隔时间 (inter-key time)，T(i，j)(i ＝ j) 指该键（如 l，s 等）与自身的击键间隔时间。

[0041] 同理，我们可以得到击键延迟时间矩阵：

[0042]

	A	…	Z	0	…	9
T	T(1)	…	T(26)	T(27)	…	T(36)

[0043] 其中 T(i) 指单击一个键的击键延迟时间。

[0044] 第四步，利用击键行为模板匹配的方法对计算机用户的击键行为进行认证。训练模式下生成的模板作为合法用户的行为特征模板保存入特征模板库，认证模式下生成的特征模板将会等待与正常行为特征模板进行匹配，可采用加权贝叶斯算法。

[0045] 对击键特征分析建模，我们可以得到在贝叶斯算法中击键模式 X 的概率密度为

[0046] $$p_i(X) = (2\pi)^{-n/2}|c_i|^{-1/2}\exp[(-1/2)(X-m_i)^T c_i^{-1}(X-m_i)]$$

[0047] 其中，m_i 和 c_i 分别是第 i 个用户击键档案中总体时间统计量的均值和协方差，n 是 X 的维数。

[0048] $$m_i = (\frac{1}{N_i})\sum_{j=1}^{N_i} x_{ij}$$

[0049] $$c_i = (\frac{1}{N_i})\sum_{j=1}^{N_i} x_{ij}x_{ij}^T - m_i m_i^T$$

[0050] N_i 是一个用户的训练集中样本的数量。贝叶斯算法以概率密度的最大值为标准，当 $p_i(X)$ 的最大值大于一个给定的阈值 P，即可判定该用户为正常用户。

[0051] $p_i(X) > P$

[0052] 对上式进行代入化简后，得到贝叶斯判断规则：

[0053] $$d_i(X) = (X-m_i)^T c_i^{-1}(X-m_i) < D$$

[0054] 给定一个阈值 D，当 $d_i(X) < D$ 时，认为当前用户为合法用户，当 $d_i(X) > D$ 时，则认为异常行为发生，判断当前用户为非法用户。

[0055] 传统的贝叶斯算法仅依据用户击键时间的总体均值和方差进行分析，不考虑具体键的统计概率分布，因此，我们在考虑具体健的基础上，将加权贝叶斯算法应用于击键序列的识别上。

[0056] 依据我们建立的用户训练数据中具体键的间隔时间和延迟时间的统计概率分布建立用户击键档案，得到用户的击键模式矩阵

[0057]

	B_1	B_2	…	B_N
B_1	(m_{11},c_{11})	(m_{12},c_{12})	…	(m_{1N},c_{1N})
B_2	(m_{21},c_{21})	(m_{22},c_{22})	…	(m_{2N},c_{2N})
…	…	…	…	…
B_N	(m_{N1},c_{N1})	(m_{N2},c_{N2})	…	(m_{NN},c_{NN})

[0058] 当 i = j 时，即对角线上的 (m_{ii}, c_{ii}) 指用户 B_i 键延迟时间的均值和方差，当 i 延迟时，即其余的 (m_{ij}, c_{ij}) 指用户 B_i 键和 B_j 键间隔时间的均值和方差。

[0059] 在实际检测中，X 的每个分量 X_{ij} 都遵从高斯概率分布，满足贝叶斯判断规则，因此可得到相应矩阵 D

[0060] $$D=\begin{bmatrix} d_{11} & d_{12} & \cdots & d_{1N} \\ d_{21} & d_{22} & \cdots & d_{2N} \\ \cdots & \cdots & \cdots & \cdots \\ d_{N1} & d_{N2} & \cdots & d_{NN} \end{bmatrix}$$

[0061] $$d_{ij}(X_{ij})=(X_{ij}-m_{ij})^T c_{ij}^{-1}(X_{ij}-m_{ij})$$

[0062] 然后我们根据每个分量出现的频率 O_{ij} 和均值 m_{ij} 来评估该分量的重要程度，计算出对应的权值 w_{ij}，对 d_{ij} 进行加权和计算，以此来比较当前用户的整个击键序列与正常用户击键模板的差异，从而得出异常度 S。

[0063] $$S=\sum_{i=1}^{N}\sum_{j=1}^{N} w_{ij} d_{ij}(X),$$

$$w_{ij}=\begin{cases} 0 & \text{击键模板或当前用户击键序列中没有该分量时} \\ \dfrac{O_{ij}/m_{ij}}{\sum_{i=1}^{N}\sum_{j=1}^{N} O_{ij}/m_{ij}} & \text{否则} \end{cases}$$

[0064] 当 S 超过一定阈值时将当前用户判定为异常用户。

[0065] 用户登录时的基于鼠标行为的身份认证、身份再认证过程

[0066] 假设已经记录下计算机用户产生的鼠标操作行为数据，如表 3 所示，本发明将按以下步骤进行鼠标行为认证。

[0067] 表 3 鼠标操作行为记录信息

[0068]

记录信息	鼠标动作	屏幕坐标	系统时间	进程信息
数据项	基本事件类型编码	（横向 x 坐标，纵向 y 坐标）	系统时间 t	进程名
示例	512	(312,508)	3418652	Explorer.exe

[0069] 第一步，对记录的鼠标操作行为数据进行预处理操作，避免在操作切分和特征提取时出现的数据冗余混乱情况，主要过滤如下两种情况：

[0070] (1) 过滤在同一时间点重复出现的鼠标移动事件，两次事件的记录时间点相同，会对速度相关特征的提取造成影响。

[0071] (2) 过滤重复记录的操作事件，如鼠标左键单击按下操作后面必定会有一个弹起操作作为结束，若有两个重复的左键单击按下出现在相邻的记录时间点上，会对操作分割程序的运行造成影响。

[0072] 第二步，对鼠标行为操作进行定义与分割并提取相应的鼠标操作特征，鼠标操作事件从大体上可以分为鼠标的移动和鼠标的点击操作，具体包括：

[0073] (1) 单击（左 / 右 / 中键），鼠标左 / 右 / 中键一次按下到弹起的过程。如左键单击可能完成程序执行，文件图标选择等；右键单击可能完成图标选择，快捷菜单弹出等；

[0074] (2) 双击（左 / 右 / 中键），鼠标左 / 右 / 中键连续 2 次完成按下到弹起的过程，其中第一次弹起和第二次按下的时间间隔小于操作系统中设定的阈值。如左键双击操作可能完成文件或程序的执行等。

[0075] (3) 拖拽（左 / 右 / 中键），在按下鼠标左 / 右 / 中键的同时，将光标从坐标 (x_1, y_1) 移动至坐标 (x_2, y_2) 处，然后弹起按键的过程。如左键拖拽可以实现图标的移动，文本内容选择等操作；中键拖拽可以实现屏幕滚动操作。

[0076] (4) 中键滚动，鼠标中键前后进行滚动的操作，如可以进行页面滚动浏览等操作。

[0077] (5) 鼠标的移动点击，光标从坐标 (x_1, y_1) 移动至坐标 (x_2, y_2) 处，随后进行点击等其他操作的过程。可以实现光标定位，完成后续动作，是主要的输入行为操作。

[0078] (6) 鼠标的静止，指鼠标未进行按键动作，同时光标停留在同一位置超过一定时间阈值的操作。

[0079] 基于上面对鼠标基本行为操作的定义和分割，可以在各种不同的操作中，或者利用操作的组合，提取出有意义的鼠标行为特征，具体包括：操作频率分布，静止时间占空比，屏幕坐标范围的分布，其他统计特征（移动方向频率，移动距离频率等），极限点击频率，单击时间间隔，双击内部时间间隔，中键滚动持续时间，平均移动速度与距离的关系，平均移动速度与方向的关系，移动中速度变化的微结构，移动轨迹距离与位移的比值，移动中的其他统计量，组合操作中的反应切换时间。

[0080] 第三步，根据提取的鼠标行为特征生成相应的行为特征模板，利用鼠标行为模板匹配的方法对计算机用户的鼠标行为进行认证。训练模式下生成的模板作为合法用户的行为特征模板保存入特征模板库，认证模式下生成的特征模板将会等待与参考特征模板进行匹配，可对不同的特征分别采用不同的类间距离分类或贝叶斯决策算法。

[0081] 比如对于事件频率分布和静止占空比，可采用类间距离进行分类。

[0082] $$\begin{cases} E(X_1, X_2) \geq TH^i & F_i = 1 \\ E(X_1, X_2) < TH^i & F_i = 0 \end{cases}$$

[0083] X_1, X_2 表示两个模板中的相应特征。不同的特征采用不同的类间距离 $E(X_1, X_2)$，如欧式距离或海明距离等。

[0084] 对于用户的生理特征，如单双击时间间隔，可通过假设检验验证其符合正态分布，不同用户有着不同的分布参数。

[0085] $$P(X \mid C_i) = \frac{1}{\sqrt{2\pi}\sigma_i} e^{\frac{(x-\mu_i)^2}{2\sigma_i^2}}$$

[0086] 其中 C_i 表示第 i 个用户，而

[0087] $$U = \frac{\sqrt{n}(\bar{x} - \mu_0)}{\sigma_0} \cdot N(0,1)$$

[0088] 符合标准正态分布。调节检验的显著水平 α，我们可以得到

[0089] $$\begin{cases} \left|\frac{\sqrt{n}(\bar{x}_2-\mu_1)}{\sigma_1}\right| \geq u_{\frac{\alpha}{2}} & F_i=1 \\ \left|\frac{\sqrt{n}(\bar{x}_2-\mu_1)}{\sigma_1}\right| < u_{\frac{\alpha}{2}} & F_i=0 \end{cases}$$

[0090] F_i 表示第 i 个特征的分类结果，为 1 表示该特征不匹配，为 0 表示该特征匹配。最后，我们对所有特征采取多数投票 (Majority Voting) 的决策融合方法，对用户身份进行验证。

[0091] 令 $S = \sum w_i F_i$

[0092] 则 $\begin{cases} S \geq Z & \text{当前为非法用户} \\ S < Z & \text{当前为合法用户} \end{cases}$

[0093] 当 S 超过一定阈值 Z 时将当前用户判定为异常用户。其中，各个特征的权值 w_i，总的决策阈值 Z 和各个特征的分类阈值 TH^i 可以通过优化的方法进行调节。

[0094] 用户监控时的模板匹配过程

[0095] 用户登录成功后，启动监控模式，实时采集当前用户的击键和鼠标输入行为数据，提取行为特征并生成击键和鼠标的输入特征模板，随后，将该击键和鼠标的输入特征模板与用户在特征模板库中的参考特征模板匹配：击键行为模板匹配的算法采用加权贝叶斯算法；鼠标行为模板匹配的算法采用类间距离分类或贝叶斯决策算法。具体参见“用户登录时的基于鼠标行为的身份认证、身份再认证过程”和“用户登录时的基于鼠标行为的身份认证、身份再认证过程”的模板匹配过程。

[0096] 用户监控时的基于击键行为的身份认证、身份再认证过程

[0097] 在监控过程中，当检测到用户的鼠标行为发生异常，则采用击键行为认证方式进行身份再认证。具体过程请参见“用户登录时的基于鼠标行为的身份认证、身份再认证过程”。

[0098] 用户监控时的基于鼠标行为的身份认证、身份再认证过程

[0099] 在监控过程中，当检测到用户的击键行为发生异常，则采用鼠标行为认证方式进行身份再认证。具体过程请参见“用户登录时的基于鼠标行为的身份认证、身份再认证过程”。

[0100] 最后应说明的是：以上实施例仅用以说明本发明而并非限制本发明所描述的技术方案；因此，尽管本说明书参照上述的各个实施例对本发明已进行了详细的说明，但是，本领域的普通技术人员应当理解，仍然可以对本发明进行修改或等同替换；而一切不脱离发明的精神和范围的技术方案及其改进，其均应涵盖在本发明的权利要求范围当中。

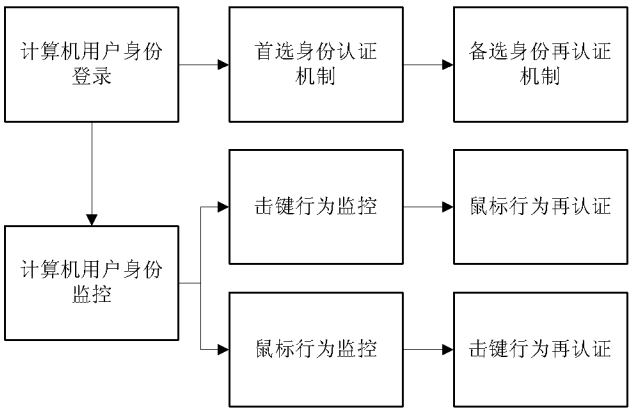

计算机用户身份登录
首选身份认证机制
备选身份再认证机制
计算机用户身份监控
击键行为监控
鼠标行为再认证
鼠标行为监控
击键行为再认证

图 1

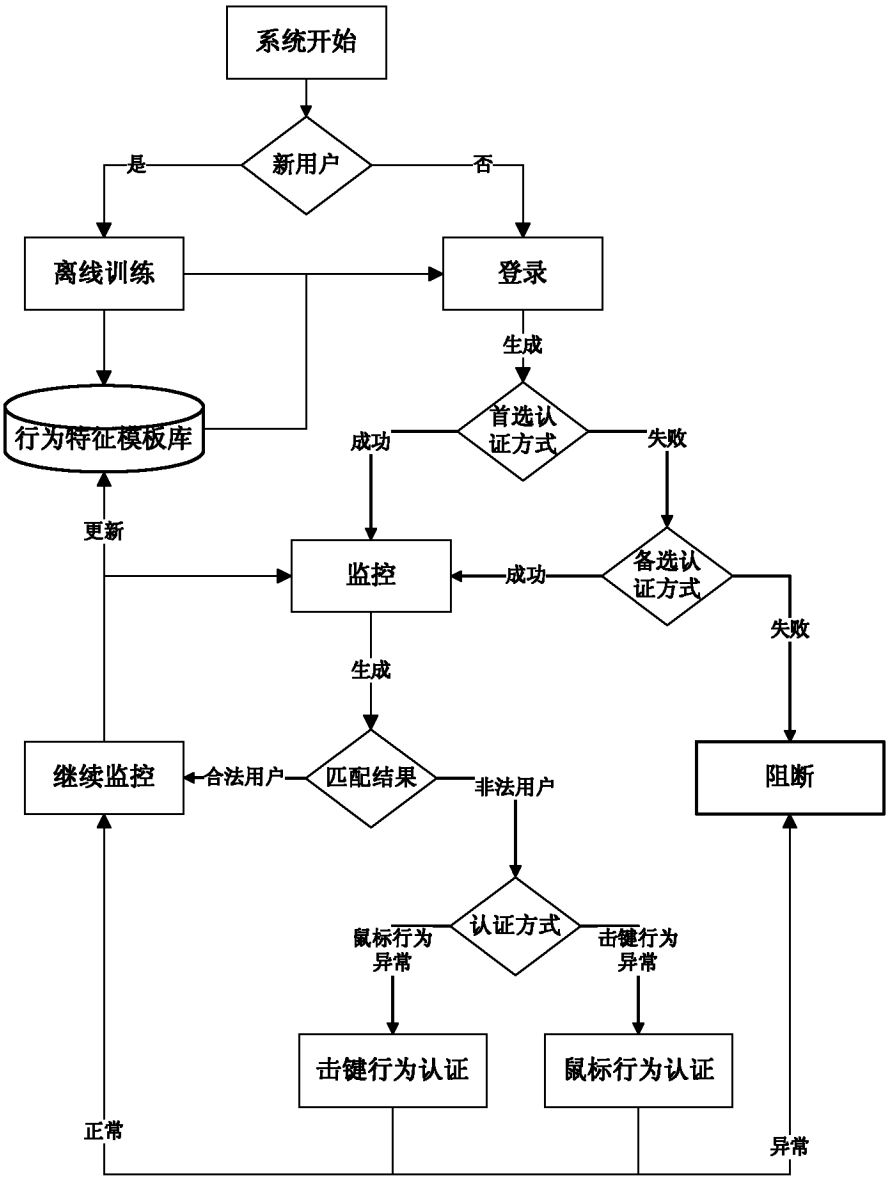

系统开始
新用户
是
否
离线训练
登录
生成
行为特征模板库
首选认证方式
成功
失败
更新
监控
成功
备选认证方式
失败
生成
继续监控
合法用户
匹配结果
非法用户
阻断
认证方式
鼠标行为异常
击键行为异常
击键行为认证
鼠标行为认证
正常
异常

图 2