(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2017 年 4 月 27 日 (27.04.2017)

WIPO | PCT

(10) 国际公布号
WO 2017/067103 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2016/070988

(22) 国际申请日: 2016 年 1 月 15 日 (15.01.2016)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201510694805.5 2015 年 10 月 22 日 (22.10.2015) CN

(71) 申请人: 同济大学 (TONGJI UNIVERSITY) [CN/CN]; 中国上海市杨浦区四平路 1239 号, Shanghai 200092 (CN)。

(72) 发明人: 蒋昌俊 (JIANG, Changjun); 中国上海市杨浦区四平路 1239 号, Shanghai 200092 (CN)。 闫春钢 (YAN, Chungang); 中国上海市杨浦区四平路 1239 号, Shanghai 200092 (CN)。 陈闵中 (CHEN, Hongzhong); 中国上海市杨浦区四平路 1239 号, Shanghai 200092 (CN)。 丁志军 (DING, Zhijun); 中国上海市杨浦区四平路 1239 号, Shanghai 200092 (CN)。 宋小双 (SONG, Xiaoshuang); 中国上海市杨浦区四平路 1239 号, Shanghai 200092 (CN)。

(74) 代理人: 上海光华专利事务所 (J.Z.M.C. PATENT AND TRADEMARK LAW OFFICE); 中国上海市杨浦区国定路 335 号 5022 室余明伟, Shanghai 200433 (CN)。

(81) 指定国 (除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明，要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

[见续页]

(54) Title: KEYSTROKE BEHAVIOUR-BASED IDENTITY AUTHENTICATION METHOD AND SYSTEM

(54) 发明名称 : 基于击键行为的身份认证方法和系统

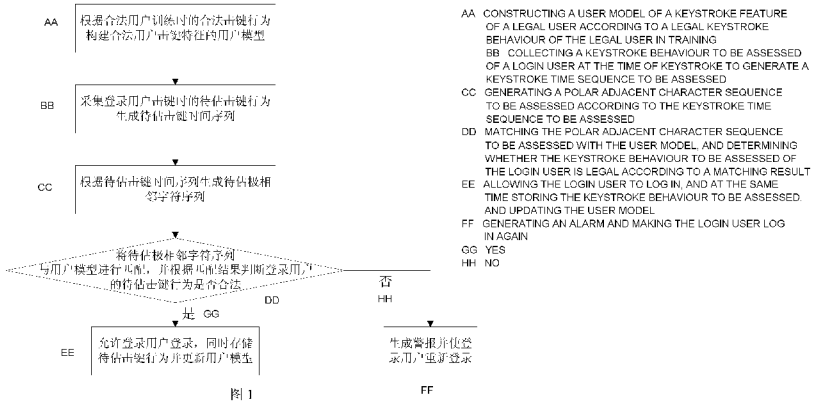

图 1

(57) Abstract: A keystroke behaviour-based identity authentication method, comprising the following steps: S1. constructing a user model of a keystroke feature of a legal user according to a legal keystroke behaviour of the legal user in training; S2. collecting a keystroke behaviour to be assessed of a login user at the time of keystroke to generate a keystroke time sequence to be assessed; S3. generating a polar adjacent character sequence to be assessed according to the keystroke time sequence to be assessed; and S4. matching the polar adjacent character sequence to be assessed with the user model, and determining whether the keystroke behaviour to be assessed of the login user is legal according to a matching result, if not, generating an alarm and making the login user log in again, and if yes, allowing the login user to log in, and at the same time storing the keystroke behaviour to be assessed and updating the user model. Extraction of only few representative keystroke features of a user guarantees an authentication accuracy rate and improves the response capability for continuous authentication at the same time; and monitoring a keystroke behaviour of the user in real time offers continuous account security assurance for the user.

(57) 摘要:

[见续页]

WO 2017/067103 A1

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

一种基于击键行为的身份认证方法，包括以下步骤：S1、根据合法用户训练时的合法击键行为构建合法用户击键特征的用户模型；S2、采集登录用户击键时的待估击键行为生成待估击键时间序列；S3、根据所述待估击键时间序列生成待估极相邻字符序列；S4、将所述待估极相邻字符序列与所述用户模型进行匹配，并根据匹配结果判断登录用户的所述待估击键行为是否合法；若不合法，则生成警报并使登录用户重新登录，若合法，则允许登录用户登录，同时存储所述待估击键行为并更新所述用户模型。仅提取了用户少量的有代表性的击键特征，在保证认证准确率的同时，提高了持续认证的响应能力；实时监控用户的击键行为，为用户提供持续性的账户安全保障。

基于击键行为的身份认证方法和系统

技术领域

本发明涉及互联网领域，特别是涉及一种基于击键行为的身份认证方法和系统。

背景技术

随着互联网的迅速发展，用户对互联网中帐号的安全性的要求也随之提高。目前最常见的方法是基于用户名和密码相结合的文本匹配身份认证。这种方法虽简单易行，然而一旦密码泄露，这种身份认证方法就会失效。由于每个人的行为都有其生物特征，而用户的击键行为与用户的年龄、性别、和对计算机键盘的熟悉程度等都有联系，不同用户的击键行为模式是难以被他人模仿和盗用的。而且基于击键行为的认证方法并不需要额外的硬件支持，成本较低，且系统能够在后台记录用户的击键行为，因此基于用户击键行为的认证方法具有良好的可行性。但基于传统的击键行为的认证方法，无法实时地对用户身份进行合法性的确认。

发明内容

鉴于以上所述现有技术的缺点，本发明的目的在于提供一种基于击键行为的身份认证方法和系统，用于解决现有技术中采集过多、成本较高，且无法实时地对用户身份进行合法性的确认的问题。

为实现上述目的及其他相关目的，本发明提供 1、一种基于击键行为的身份认证方法，包括以下步骤：

S1、根据合法用户训练时的合法击键行为构建合法用户击键特征的用户模型；

S2、采集登录用户击键时的待估击键行为生成待估击键时间序列；

S3、根据所述待估击键时间序列生成待估极相邻字符序列；

S4、将所述待估极相邻字符序列与所述用户模型进行匹配，并根据匹配结果判断登录用户的所述待估击键行为是否合法；若不合法，则生成警报并使登录用户重新登录，若合法，则允许登录用户登录，同时存储所述待估击键行为并更新所述用户模型。

优选的，所述步骤 S1 还包括步骤：

S11、采集合法击键行为，并生成合法时间间隔向量；

S12、遍历所述合法时间间隔向量，并判断所述合法时间间隔向量的两个相邻字符序列的时间间隔是否小于预设临界时间间隔；

若是，则所述两个相邻字符置于同一个极相邻字符；

若否，则以所述两个相邻字符中后一个字符为首字符，生成一个新的所述极相邻字符；

S13、计算字符数量为 2 和 3 的所述极相邻字符所占的比重，并设置比重最大时的所述预设临界时间间隔为合法临界时间间隔；

S14、通过所述合法临界时间间隔重新生成合法极相邻字符序列，并记录所述合法极相邻字符序列的持续时间。

优选的，所述步骤 S1 还包括步骤：

提取所述合法极相邻字符序列的时间特征集，并构建所述合法极相邻字符序列服从的分布模型。

优选的，所述步骤 S3 还包括步骤：

S31、采集所述待估击键行为；

S32、生成所述待估击键行为的待估时间间隔向量；

S33、结合所述合法临界间隔时间与所述待估时间间隔向量生成所述待估极相邻字符序列。

优选的，所述步骤 S2 还包括步骤：

获取所述待估击键时间序列，并将所述待估击键时间序列存入预设大小的缓冲区，当所述缓冲区满时，发送所述缓冲区中的所有所述估击键时间序列。

优选的，所述步骤 S4 中所述待估极相邻字符序列与所述用户模型通过高斯模型进行匹配，所述匹配根据的评分公式为：

$$S_{GPD} = e^{-\frac{(t_{S'}-\mu_S)^2}{2\delta_S^2}}$$

其中，tS’表示待估极相邻字符序列，而 μ S 和 σ S 分别为所述高斯模型中高斯分布的期望和标准差；

所述判断登录用户的所述待估击键行为是否合法的步骤还包括：

计算单个待估极相邻字符序列的评分，再去除低于预设值的所述评分后将所述评分汇总，比较汇总后的所述评分是否大于阈值；若是，则允许登录，同时存储所述待估击键行为并更新所述用户模型；若否，则发出警告并重新登录。

本发明还提供了一种基于击键行为的身份认证系统，包括数据采集模块、特征提取模块、模型训练模块、持续认证模块和模型库；

所述数据采集模块用于采集合法用户合法击键行为时的合法击键时间序列和登录用户击键时的待估击键行为生成的的待估击键时间序列，并将所述合法击键时间序列和待估击键时

间序列发送至所述特征提取模块；

所述特征提取模块用于根据所述合法击键时间序列和待估击键时间序列分别对应生成合法极相邻字符序列和待估极相邻字符；

所述模型训练模块用于根据所述合法击键行为和合法击键时间序列构建合法用户击键特征的用户模型；

所述持续认证模块用于将所述待估相邻字符序列与所述用户模型进行匹配，并根据匹配结果判断登录用户的所述待估击键行为是否合法，在待估击键行为不合法时生成警报并使登录用户重新登录；在待估击键行为合法时允许登录用户登录，同时存储所述待估击键行为，并反馈给所述模型训练模块更新所述用户模型；

所述模型库用于存储合法用户击键特征的用户模型。

优选的，所述数据采集模块还用于在采集合法击键行为，并生成合法时间间隔向量；

所述特征提取模块还用于遍历所述合法时间间隔向量，并根据所述合法时间间隔向量的两个相邻字符序列的时间间隔与预设临界时间间隔的大小生成极相邻字符；计算字符数量为2和3的所述极相邻字符所占的比重，并设置比重最大时的所述预设临界时间间隔为合法临界时间间隔；通过所述合法临界时间间隔重新生成合法极相邻字符序列，并记录所述合法极相邻字符序列的持续时间；

所述特征提取模块还用于提取所述合法极相邻字符序列的时间特征集，并构建所述合法极相邻字符序列服从的分布模型。

优选的，所述特征提取模块还用于生成所述待估击键行为的待估时间间隔向量；并结合所述合法临界间隔时间与所述待估时间间隔向量生成所述待估极相邻字符序列。

优选的，所述特征提取模块还用于获取所述待估击键时间序列，并将所述待估击键时间序列存入预设大小的缓冲区，当所述缓冲区满时，发送所述缓冲区中的所有所述估击键时间序列。

如上所述，本发明的自适应调制方法，具有以下有益效果：

本发明仅提取了用户少量的有代表性的击键特征，去除了大量冗余的击键特征序列，在保证认证准确率的同时，提高了持续认证的响应能力；在用户登陆网络账户时，实时监控用户的击键行为，为合法用户提供持续性的账户安全保障。

附图说明

图1显示为本发明基于击键行为的身份认证方法的流程方框图；

图 2 显示为图 1 中构建合法用户击键特征的用户模型的流程方框图；

图 3 显示为图 1 中生成待估极相邻字符序列的流程方框图；

图 4 显示为图 1 中认证过程的流程方框图；

图 5 显示为本发明基于击键行为的身份认证系统的逻辑方框图；

图 6 显示为本发明的认证结果的曲线图。

具体实施方式

以下通过特定的具体实例说明本发明的实施方式，本领域技术人员可由本说明书所揭露的内容轻易地了解本发明的其他优点与功效。本发明还可以通过另外不同的具体实施方式加以实施或应用，本说明书中的各项细节也可以基于不同观点与应用，在没有背离本发明的精神下进行各种修饰或改变。

请参阅图 1 至图 4。需要说明的是，本实施例中所提供的图示仅以示意方式说明本发明的基本构想，遂图式中仅显示与本发明中有关的组件而非按照实际实施时的组件数目、形状及尺寸绘制，其实际实施时各组件的型态、数量及比例可为一种随意的改变，且其组件布局型态也可能更为复杂。

如图 1 所示，本发明提供了一种基于击键行为的身份认证方法，包括以下步骤：S1、根据合法用户训练时的合法击键行为构建合法用户击键特征的用户模型；S2、采集登录用户击键时的待估击键行为生成待估击键时间序列；S3、根据待估击键时间序列生成待估极相邻字符序列；S4、将待估极相邻字符序列与用户模型进行匹配，并根据匹配结果判断登录用户的待估击键行为是否合法；若不合法，则生成警报并使登录用户重新登录，若合法，则允许登录用户登录，同时存储待估击键行为并更新用户模型。

在用户登陆网络账号后，监控器会实时地跟踪用户的击键行为，并记录下用户的击键行为时间序列。在用户模型的训练阶段，采集用户账号使用阶段的所有击键行为，并在用户账号登出后将数据发送。

用户的击键行为时间序列如表 1 所示，表 1 为用户击键行为日志表。其中 down 表示键被按下，up 表示键弹起，Time 表示键按下或弹起时的时间戳。

down	up	Time(ms)
h		0
e		138
	h	240
	e	335

1		524

表 1

在特征提取时，首先会处理上传的击键行为日志，提取出用户击键的时间间隔向量。在用户模型的训练阶段，需要迭代时间间隔向量的特征值 $Interval =< I_1, I_2, ...I_{p-1} >$，以挖掘出反映用户击键特征的临界间隔时间α，并根据这一特征进一步挖掘出用户的极相邻字符序列。

所以，如图 2 所示，步骤 S1 还包括步骤：

S11、采集合法击键行为，并生成合法时间间隔向量；

S12、遍历合法时间间隔向量，并判断合法时间间隔向量的两个相邻字符序列的时间间隔是否小于预设临界时间间隔；遍历时间间隔特征向量 $Interval =< I_1, I_2, ...I_{p-1} >$ 中的值，

若是，则两个相邻字符置于同一个极相邻字符；

若否，则以两个相邻字符中后一个字符为首字符，生成一个新的极相邻字符；

S13、计算字符数量为 2 和 3 的极相邻字符所占的比重，并设置比重最大时的预设临界时间间隔为合法临界时间间隔；

S14、通过合法临界时间间隔重新生成合法极相邻字符序列，并记录合法极相邻字符序列的持续时间。

提取出的极相邻字符序列入表 2 所示，表 2 为极相邻字符序列时间特征集表。

极相邻字符序列	持续时间/ms
app	<749,758,693,725>
cm	<270,280,260,250,240>

表 2

优选地，构建合法用户击键特征的用户模型时，还包括了步骤：提取合法极相邻字符序列的时间特征集，并构建合法极相邻字符序列服从的分布模型。

优选地，如图 3 所示，步骤 S3 还包括步骤：

S31、采集待估击键行为；

S32、生成待估击键行为的待估时间间隔向量；

S33、结合合法临界间隔时间与待估时间间隔向量生成待估极相邻字符序列。

对于一个用户，假定其输入极相邻字符序列的持续时间服从于一个正态分布的过程。提取模块挖掘出的极相邻字符序列时间特征集，构建每个极相邻字符序列服从的正态分布模型。对于极相邻字符序列 S 的时间特征集合<S1,S2,S3,…,Sk-1,Sk>，利用最大似然估计的方法计算

期望和方差。其中，$\hat{\mu}=\frac{\sum_{i=1}^{k}S_i}{k}$，$\hat{\sigma}^2=\frac{\sum_{i=1}^{k}[S_i-\hat{\mu}]^2}{k-1}$。由合法用户的训练数据挖掘得到的极相邻字符序列及其服从的正态分布模型构成了用户模型的主要部分，临界时间间隔这一用户击键特征也是用户模型的一部分。

通过将待估击键行为数据与用户模型进行匹配，给出待估击键行为数据的评分，根据决策算法给出认证结果。当认证结果显示该击键行为数据属于合法用户时，该模块将此次待估数据挖掘出的极相邻字符序列的时间特征集存入缓冲区，待特征数量达到设定值时，便对模型库中对应的极相邻字符序列的模型进行更新。

进一步地，步骤 S2 还包括步骤：

获取待估击键时间序列，并将待估击键时间序列存入预设大小的缓冲区，当缓冲区满时，发送缓冲区中的所有估击键时间序列。在用户身份的持续认证阶段，数据采集模块会设定一个固定大小的字符序列缓冲区，当缓冲区满时，采集模块便将缓冲区中的数据提交给特征提取模块，以便进行身份认证，案例中缓冲区的窗口值大小为 30 个字符。

优选地，高斯概率密度函数是一种相似度评价的函数，在用户认证中，用于评价待估的极相邻字符序列与用户模型中的极相邻字符序列的相似度。步骤 S4 中待估极相邻字符序列与用户模型通过高斯模型进行匹配，匹配根据的评分公式为：

$$S_{GPD}=e^{-\frac{(t_{S'}-\mu_S)^2}{2\delta_S^2}}$$

其中，$t_{S'}$表示待估极相邻字符序列，而 μ_s 和 σ_s 分别为高斯模型中高斯分布的期望和标准差；

入图 4 所示，判断登录用户的待估击键行为是否合法的步骤还包括：

计算单个待估极相邻字符序列的评分，再去除低于预设值的评分后将评分汇总，比较汇总后的评分是否大于阈值；若是，则允许登录，同时存储待估击键行为并更新用户模型；若否，则发出警告并重新登录。

如图 5 所示，本发明还提供了一种基于击键行为的身份认证系统，包括数据采集模块、特征提取模块、模型训练模块、持续认证模块和模型库；

数据采集模块用于采集合法用户合法击键行为时的合法击键时间序列和登录用户击键时的待估击键行为生成的的待估击键时间序列，并将合法击键时间序列和待估击键时间序列发送至特征提取模块；

特征提取模块用于根据合法击键时间序列和待估击键时间序列分别对应生成合法极相邻

字符序列和待估极相邻字符；

模型训练模块用于根据合法击键行为和合法击键时间序列构建合法用户击键特征的用户模型；

持续认证模块用于将待估相邻字符序列与用户模型进行匹配，并根据匹配结果判断登录用户的待估击键行为是否合法，在待估击键行为不合法时生成警报并使登录用户重新登录；在待估击键行为合法时允许登录用户登录，同时存储待估击键行为，并反馈给模型训练模块更新用户模型。

模型库用于存储合法用户击键特征的用户模型。

优选地，数据采集模块还用于在采集合法击键行为，并生成合法时间间隔向量；

特征提取模块还用于遍历合法时间间隔向量，并根据合法时间间隔向量的两个相邻字符序列的时间间隔与预设临界时间间隔的大小生成极相邻字符；计算字符数量为 2 和 3 的极相邻字符所占的比重，并设置比重最大时的预设临界时间间隔为合法临界时间间隔；通过合法临界时间间隔重新生成合法极相邻字符序列，并记录合法极相邻字符序列的持续时间；

特征提取模块还用于提取合法极相邻字符序列的时间特征集，并构建合法极相邻字符序列服从的分布模型。

优选地，特征提取模块还用于生成待估击键行为的待估时间间隔向量；并结合合法临界间隔时间与待估时间间隔向量生成待估极相邻字符序列。

优选地，特征提取模块还用于获取待估击键时间序列，并将待估击键时间序列存入预设大小的缓冲区，当缓冲区满时，发送缓冲区中的所有估击键时间序列。

用户击键行为认证方法主要由数据采集模块、特征提取模块、模型训练模块和持续认证模块构成。数据采集模块负责采集用户击键时的击键时间序列；特征提取模块负责挖掘用户的极相邻字符序列；模型训练模块根据合法用户训练数据的时间特征构建用户击键特征的高斯模型；持续认证模块根据用户键入的一段字符序列进行决策评分，以判断用户身份的合法性，同时它存储合法用户的最近一段时间的击键行为特征，当特征数量满足一定条件时，便用新的特征来构建模型，并对模型库中对应的序列模型进行更新。

数据采集模块：在用户登陆网络账号后，监控器会实时地跟踪用户的击键行为，并记录下用户的击键行为时间序列。在用户模型的训练阶段，数据采集模块会采集用户账号使用阶段的所有击键行为，并在用户账号登出后将数据发送给特征提取模块。而在用户身份的持续认证阶段，数据采集模块会设定一个固定大小的字符序列缓冲区，当缓冲区满时，采集模块便将缓冲区中的数据提交给特征提取模块，以便进行身份认证，案例中缓冲区的窗口值大小

为 30 个字符。

特征提取模块：该模块首先会处理采集模块上传的击键行为日志，提取出用户击键的时间间隔向量。在用户模型的训练阶段，特征提取模块需要迭代时间间隔向量的特征值 $Interval = < I_1, I_2, ... I_{p-1} >$，以挖掘出反映用户击键特征的临界间隔时间α，并根据这一特征进一步挖掘出用户的极相邻字符序列。

模型训练模块：对于一个用户，假定其输入极相邻字符序列的持续时间服从于一个正态分布的过程。该模块利用特征提取模块挖掘出的极相邻字符序列时间特征集，构建每个极相邻字符序列服从的正态分布模型。对于极相邻字符序列 S 的时间特征集合 <S1,S2,S3,…,Sk-1,Sk>，利用最大似然估计的方法计算期望和方差。

其中，$\hat{\mu} = \frac{\sum_{i=1}^{k} S_i}{k}$，$\hat{\sigma}^2 = \frac{\sum_{i=1}^{k} [S_i - \hat{\mu}]^2}{k-1}$。

由合法用户的训练数据挖掘得到的极相邻字符序列及其服从的正态分布模型构成了用户模型的主要部分，临界时间间隔这一用户击键特征也是用户模型的一部分。

持续认证模块：该模块通过将待估击键行为数据与用户模型进行匹配，给出待估击键行为数据的评分，根据决策算法给出认证结果。当认证结果显示该击键行为数据属于合法用户时，该模块将此次待估数据挖掘出的极相邻字符序列的时间特征集存入缓冲区，待特征数量达到设定值时，便对模型库中对应的极相邻字符序列的模型进行更新。

高斯概率密度函数是一种相似度评价的函数，在用户认证中，用于评价待估的极相邻字符序列与用户模型中的极相邻字符序列的相似度。根据高斯概率密度函数给出评分公式:

$$S_{GPD} = e^{-\frac{(t_{S'} - \mu_S)^2}{2\delta_S^2}}$$

其中 tS'表示待估击键行为数据中根据用户的临界时间间隔α，挖掘出的极相邻字符序列，而 μS，σS 分别为用户模型中对应的序列的高斯分布的期望和标准差。

如图 6 所示，在本发明的一实施例中，使用本发明基于击键行为的身份认证方法和系统的认证结果的 ROC 曲线表明了本发明的认证方法和系统在误报率达 5.3%的情况下，检测率高达 90%以上，能够有效的对用户身份的合法性进行判别，保障用户账号的安全。

综上，本发明，仅提取了用户少量的有代表性的击键特征，去除了大量冗余的击键特征序列，在保证认证准确率的同时，提高了持续认证的响应能力；在用户登陆网络账户时，实时监控用户的击键行为，为合法用户提供持续性的账户安全保障。

上述实施例仅例示性说明本发明的原理及其功效，而非用于限制本发明。任何熟悉此技术的人士皆可在不违背本发明的精神及范畴下，对上述实施例进行修饰或改变。因此，举凡所属技术领域中具有通常知识者在未脱离本发明所揭示的精神与技术思想下所完成的一切等效修饰或改变，仍应由本发明的权利要求所涵盖。

权利要求书

1、一种基于击键行为的身份认证方法，其特征在于，包括以下步骤：

S1、根据合法用户训练时的合法击键行为构建合法用户击键特征的用户模型；

S2、采集登录用户击键时的待估击键行为生成待估击键时间序列；

S3、根据所述待估击键时间序列生成待估极相邻字符序列；

S4、将所述待估极相邻字符序列与所述用户模型进行匹配，并根据匹配结果判断登录用户的所述待估击键行为是否合法；若不合法，则生成警报并使登录用户重新登录，若合法，则允许登录用户登录，同时存储所述待估击键行为并更新所述用户模型。

2、根据权利要求 1 所述的基于击键行为的身份认证方法，其特征在于，所述步骤 S1 还包括步骤：

S11、采集合法击键行为，并生成合法时间间隔向量；

S12、遍历所述合法时间间隔向量，并判断所述合法时间间隔向量的两个相邻字符序列的时间间隔是否小于预设临界时间间隔；

若是，则所述两个相邻字符置于同一个极相邻字符；

若否，则以所述两个相邻字符中后一个字符为首字符，生成一个新的所述极相邻字符；

S13、计算字符数量为 2 和 3 的所述极相邻字符所占的比重，并设置比重最大时的所述预设临界时间间隔为合法临界时间间隔；

S14、通过所述合法临界时间间隔重新生成合法极相邻字符序列，并记录所述合法极相邻字符序列的持续时间。

3、根据权利要求 2 所述的基于击键行为的身份认证方法，其特征在于，所述步骤 S1 还包括步骤：

提取所述合法极相邻字符序列的时间特征集，并构建所述合法极相邻字符序列服从的分布模型。

4、根据权利要求 3 所述的基于击键行为的身份认证方法，其特征在于，所述步骤 S3 还包括步骤：

S31、采集所述待估击键行为；

S32、生成所述待估击键行为的待估时间间隔向量；

S33、结合所述合法临界间隔时间与所述待估时间间隔向量生成所述待估极相邻字符序列。

5、根据权利要求 1 所述的基于击键行为的身份认证方法，其特征在于，所述步骤 S2 还包括步骤：

获取所述待估击键时间序列，并将所述待估击键时间序列存入预设大小的缓冲区，当所述缓冲区满时，发送所述缓冲区中的所有所述估击键时间序列。

6、根据权利要求 1 至 5 任一项所述的基于击键行为的身份认证方法，其特征在于，所述步骤 S4 中所述待估极相邻字符序列与所述用户模型通过高斯模型进行匹配，所述匹配根据的评分公式为：

$$S_{GPD} = e^{-\frac{(t_{S'}-\mu_S)^2}{2\delta_S^2}}$$

其中，$t_{S'}$表示待估极相邻字符序列，而 μ_S和 σ_S分别为所述高斯模型中高斯分布的期望和标准差；

所述判断登录用户的所述待估击键行为是否合法的步骤还包括：

计算单个待估极相邻字符序列的评分，再去除低于预设值的所述评分后将所述评分汇总，比较汇总后的所述评分是否大于阈值；若是，则允许登录，同时存储所述待估击键行为并更新所述用户模型；若否，则发出警告并重新登录。

7、一种基于击键行为的身份认证系统，其特征在于，包括数据采集模块、特征提取模块、模型训练模块、持续认证模块和模型库；

所述数据采集模块用于采集合法用户合法击键行为时的合法击键时间序列和登录用户击键时的待估击键行为生成的的待估击键时间序列，并将所述合法击键时间序列和待估击键时间序列发送至所述特征提取模块；

所述特征提取模块用于根据所述合法击键时间序列和待估击键时间序列分别对应生成合法极相邻字符序列和待估极相邻字符；

所述模型训练模块用于根据所述合法击键行为和合法击键时间序列构建合法用户击键特征的用户模型；

所述持续认证模块用于将所述待估相邻字符序列与所述用户模型进行匹配，并根据匹配结果判断登录用户的所述待估击键行为是否合法，在待估击键行为不合法时生成警报并使登

录用户重新登录；在待估击键行为合法时允许登录用户登录，同时存储所述待估击键行为，并反馈给所述模型训练模块更新所述用户模型；

所述模型库用于存储合法用户击键特征的用户模型。

8、根据权利要求 7 所述的基于击键行为的身份认证系统，其特征在于，

所述数据采集模块还用于在采集合法击键行为，并生成合法时间间隔向量；

所述特征提取模块还用于遍历所述合法时间间隔向量，并根据所述合法时间间隔向量的两个相邻字符序列的时间间隔与预设临界时间间隔的大小生成极相邻字符；计算字符数量为 2 和 3 的所述极相邻字符所占的比重，并设置比重最大时的所述预设临界时间间隔为合法临界时间间隔；通过所述合法临界时间间隔重新生成合法极相邻字符序列，并记录所述合法极相邻字符序列的持续时间；

所述特征提取模块还用于提取所述合法极相邻字符序列的时间特征集，并构建所述合法极相邻字符序列服从的分布模型。

9、根据权利要求 8 所述的基于击键行为的身份认证系统，其特征在于，

所述特征提取模块还用于生成所述待估击键行为的待估时间间隔向量；并结合所述合法临界间隔时间与所述待估时间间隔向量生成所述待估极相邻字符序列。

10、根据权利要求 7 所述的基于击键行为的身份认证系统，其特征在于，

所述特征提取模块还用于获取所述待估击键时间序列，并将所述待估击键时间序列存入预设大小的缓冲区，当所述缓冲区满时，发送所述缓冲区中的所有所述估击键时间序列。

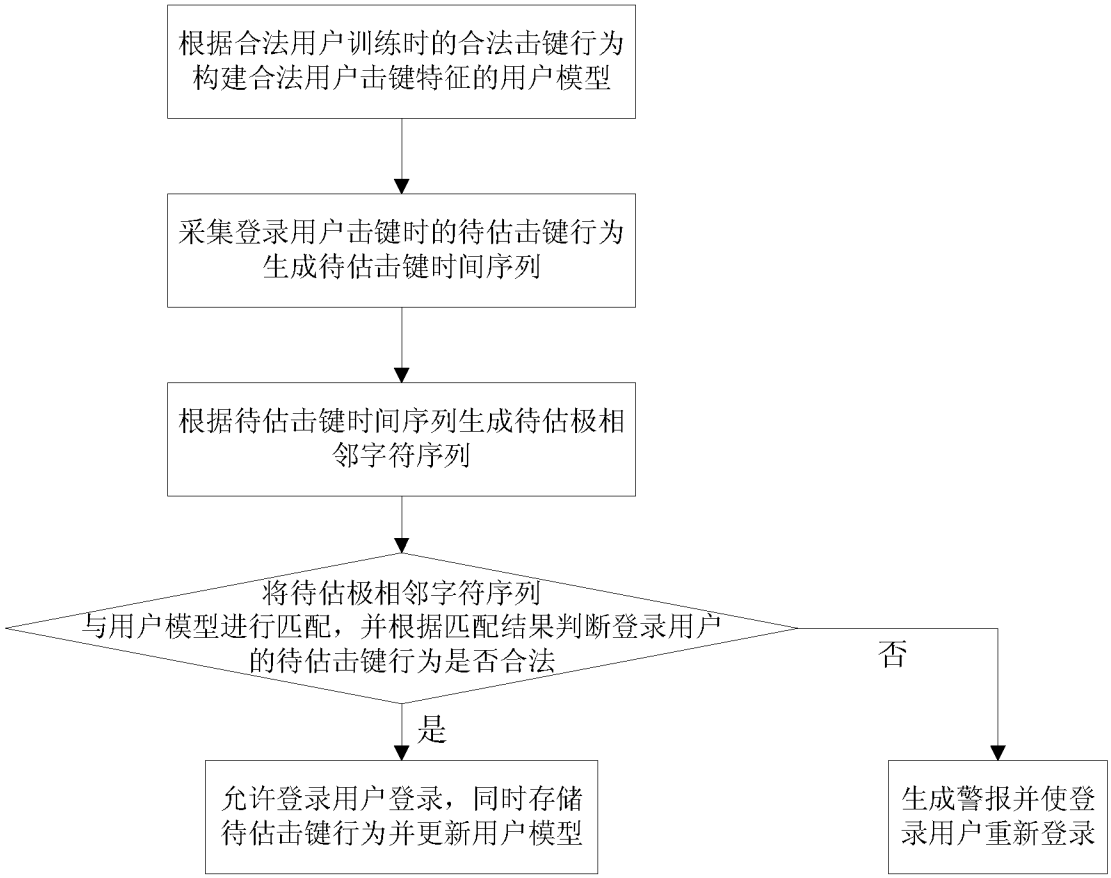
根据合法用户训练时的合法击键行为构建合法用户击键特征的用户模型
采集登录用户击键时的待估击键行为生成待估击键时间序列
根据待估击键时间序列生成待估极相邻字符序列
将待估极相邻字符序列与用户模型进行匹配，并根据匹配结果判断登录用户的待估击键行为是否合法
否
是
允许登录用户登录，同时存储待估击键行为并更新用户模型
生成警报并使登录用户重新登录

图 1

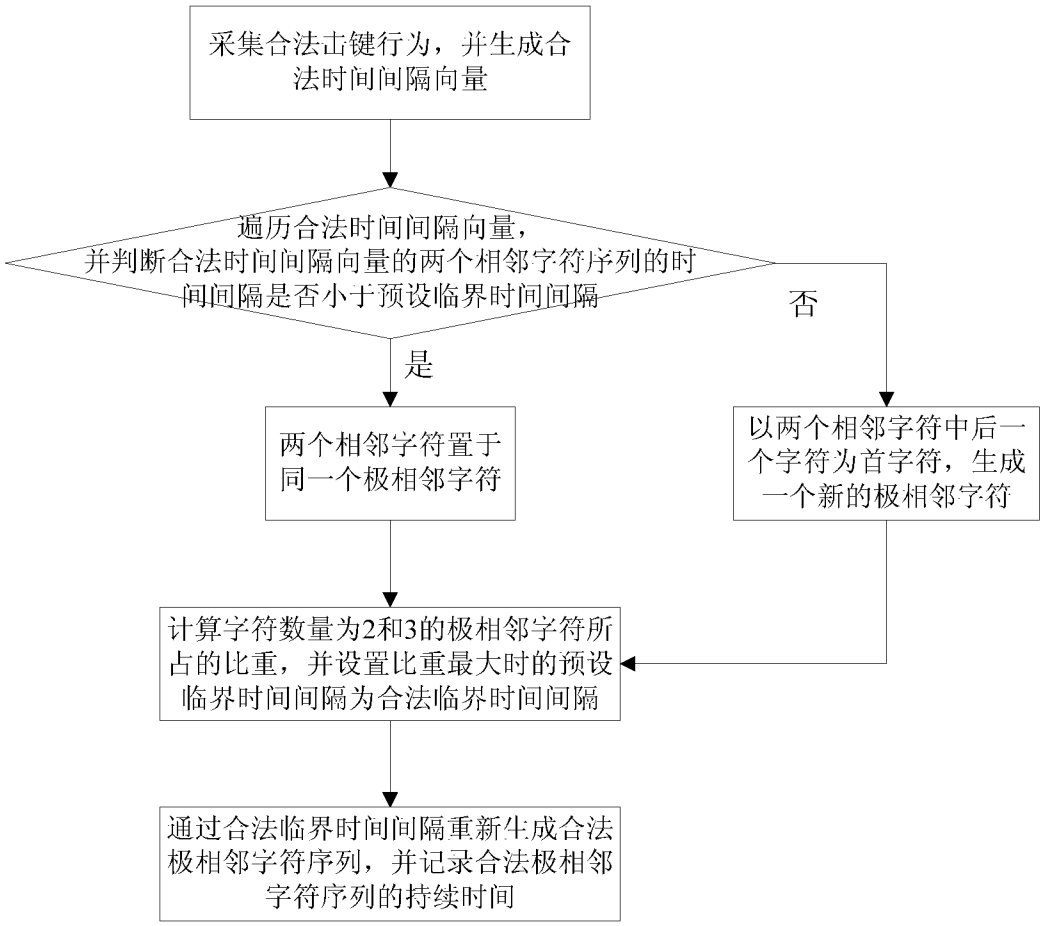
采集合法击键行为，并生成合法时间间隔向量
遍历合法时间间隔向量，并判断合法时间间隔向量的两个相邻字符序列的时间间隔是否小于预设临界时间间隔
否
是
两个相邻字符置于同一个极相邻字符
以两个相邻字符中后一个字符为首字符，生成一个新的极相邻字符
计算字符数量为2和3的极相邻字符所占的比重，并设置比重最大时的预设临界时间间隔为合法临界时间间隔
通过合法临界时间间隔重新生成合法极相邻字符序列，并记录合法极相邻字符序列的持续时间

图 2

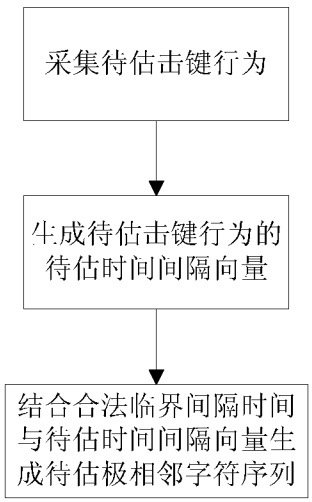
采集待估击键行为
生成待估击键行为的待估时间间隔向量
结合合法临界间隔时间与待估时间间隔向量生成待估极相邻字符序列

图 3

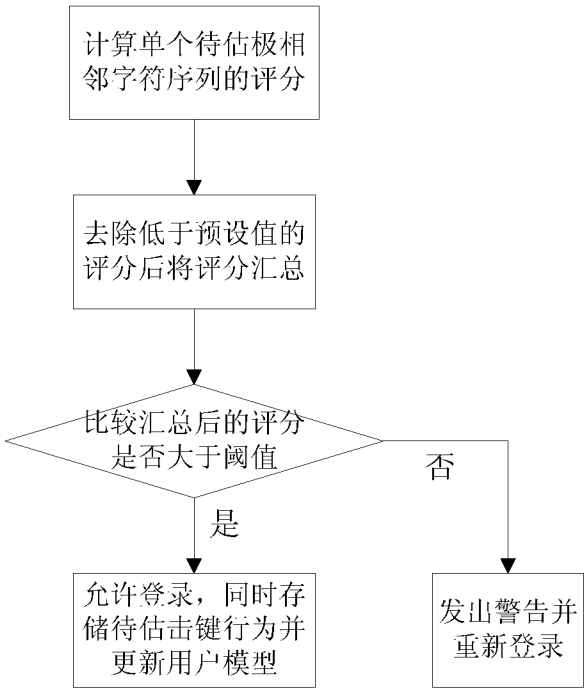
计算单个待估极相邻字符序列的评分
去除低于预设值的评分后将评分汇总
比较汇总后的评分是否大于阈值
否
是
允许登录，同时存储待估击键行为并更新用户模型
发出警告并重新登录

图 4

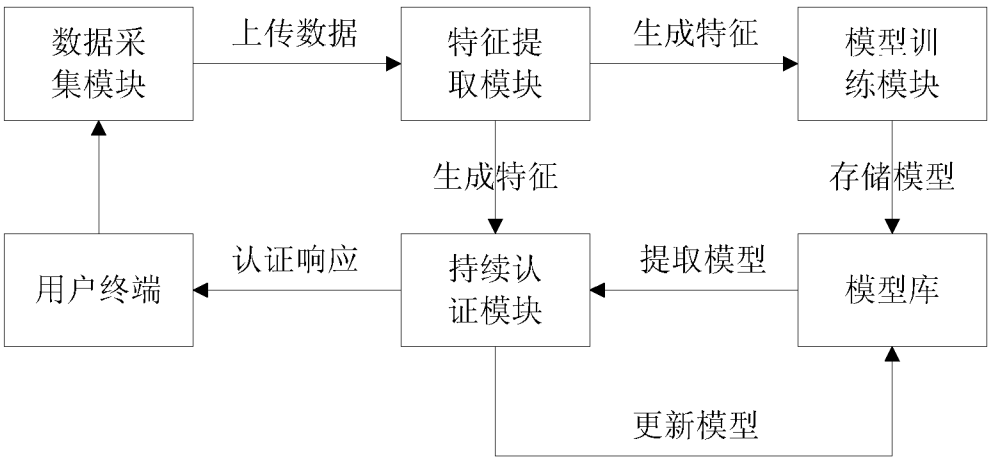
数据采集模块
上传数据
特征提取模块
生成特征
模型训练模块
生成特征
存储模型
用户终端
认证响应
持续认证模块
提取模型
模型库
更新模型

图 5

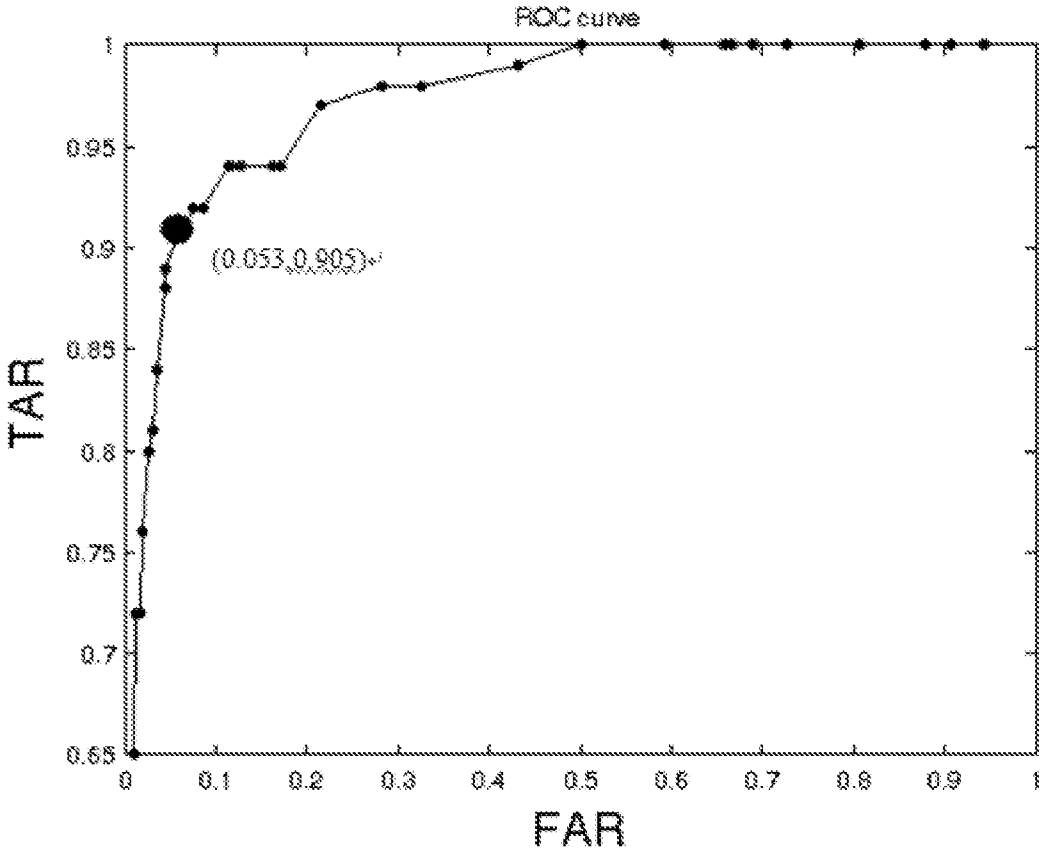
ROC curve
TAR
FAR
(0.053,0.905)
1
0.95
0.9
0.85
0.8
0.75
0.7
0.65
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1

图 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/070988

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNKI, CNPAT, WPI, EPODOC: keystroke, key, behaviour, legal, user, train, model, match, time, sequence

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 104318136 A (TONGJI UNIVERSITY), 28 January 2015 (28.01.2015), description, paragraphs [0006]-[0014]	1-10
A	CN 101478401 A (NORTHEASTERN UNIVERSITY), 08 July 2009 (08.07.2009), the whole document	1-10
A	CN 101833619 A (XI'AN JIAOTONG UNIVERSITY), 15 September 2010 (15.09.2010), the whole document	1-10
A	CN 103646197 A (CHINA UNIVERSITY OF PETROLEUM), 19 March 2014 (19.03.2014), the whole document	1-10

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 June 2016 (28.06.2016)	**20 July 2016 (20.07.2016)**
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer **ZHAO, Xiaomin** Telephone No.: (86-10) **62414041**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/070988

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 104318136 A	28 January 2015	WO 2016049983 A1	07 April 2016
CN 101478401 A	08 July 2009	None	
CN 101833619 A	15 September 2010	None	
CN 103646197 A	19 March 2014	None	

国际检索报告

国际申请号
PCT/CN2016/070988

A. 主题的分类

H04L 29/06(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNKI,CNPAT,WPI,EPODOC：击键、行为、合法、用户、训练、模型、匹配、时间、序列、key、behavior、legal、user、train、model、match、time、sequence

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
A	CN 104318136 A (同济大学) 2015年 1月 28日 (2015-01-28) 说明书第[0006]-[0014]段	1-10
A	CN 101478401 A (东北大学) 2009年 7月 8日 (2009-07-08) 全文	1-10
A	CN 101833619 A (西安交通大学) 2010年 9月 15日 (2010-09-15) 全文	1-10
A	CN 103646197 A (中国石油大学华东) 2014年 3月 19日 (2014-03-19) 全文	1-10

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2016年 6月 28日	2016年 7月 20日

ISA/CN的名称和邮寄地址	受权官员
中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088	赵晓敏
传真号 (86-10)62019451	电话号码 (86-10)62414041

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2016/070988

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	104318136	A	2015年 1月 28日	WO	2016049983	A1	2016年 4月 7日
CN	101478401	A	2009年 7月 8日		无		
CN	101833619	A	2010年 9月 15日		无		
CN	103646197	A	2014年 3月 19日		无		