

# 基于中文自由文本击键特征的自动欺骗检测模型

徐鸿雁<sup>1,2</sup>, 靳亮<sup>1</sup>, 林涛<sup>1</sup>, 彭舰<sup>1</sup>

(1. 四川大学计算机学院, 成都 610065; 2. 西南财经大学天府学院, 绵阳 621000)

**摘要:** 研究表明欺骗行为在一定程度上会影响用户击键模式的变化. 在互联网社交应用领域, 通过击键特征对欺骗行为的检测对网络信息安全建设具有重要意义. 然而, 现有的欺骗行为检测模型侵入性强, 实时性差等问题, 限制了其在互联网社交应用领域的应用. 针对以上问题, 本研究设计了一个实验从短文本中收集了广泛的用户击键特征(单键特征、内容特征、双键特征), 分别采用遗传算法(GA)和支撑向量机(SVM)完成特征选择和模型建立, 开发出一个用以预测用户欺骗行为的模型(GA-SVM). 研究表明: 该模型能够有效地检测出用户的欺骗行为, 获得 82.86% 的分类准确率; 三类击键特征对欺骗行为的检测都有贡献. 此外, 欺骗者认知负荷和心理压力对击键模式影响也被探讨.

**关键词:** 欺骗检测; 个性差异; 击键动力学; 中文自由文本

**中图分类号:** TP31      **文献标识码:** A      **文章编号:** 0490-6756(2017)03-0487-06

## Automatic deception detection model based on keystroke features of Chinese free text

XU Hong-Yan<sup>1,2</sup>, JIN Liang<sup>1</sup>, LIN Tao<sup>1</sup>, PENG Jian<sup>1</sup>

(1. College of Computer Science, Sichuan University, Chengdu 610065, China;  
2. Southwestern University of Finance and Economics, Mianyang 621000, China)

**Abstract:** Research has found that human's deceptive behaviors would affect their keystroke patterns. Detecting deceptive behaviors through keystroke patterns is a critical step toward building a cyber information security system in the field of social networking. However, the existing models detecting deceptive behaviors still suffered from the problems of high invasion and low real-time performance. To solve the problems, the authors first designed an experiment to collect a wide range of stroke features (i. e., single-key features, content features and double-key features) from users' typing process of short text and then developed a predictive model to detect the deceptive behaviors by using Genetic Algorithms (GAs) and Support Vector Machines (SVMs) as feature selection and model building methods, respectively. The results showed that the developed model could effectively detect the deceptive behaviors with accuracy of 82.86%; all the three categories of keystroke features had contributions to detecting deceptive behaviors. In addition, the effects of cognitive workload and pressure on keystroke pattern of deceivers had also been explored.

**Keywords:** Deception detection; Individual differences; Keystroke dynamics; Chinese free text

## 1 引言

研究者发现,在人际交往的行为中,大约有百分之三十的行为涉及欺骗或潜在的欺骗<sup>[1,2]</sup>.互联网环境下分享和交互信息的过程中,也存在着大量的欺骗行为,准确且高效地欺骗行为检测成为一个迫切需要解决的研究问题<sup>[3]</sup>.

近年来学者主要基于生物特征<sup>[4]</sup>、语言内容特征<sup>[5]</sup>、非语言特征<sup>[6]</sup>进行欺骗检测研究.击键动力学特征属于一类非语言特征,在欺骗检测中既不需要额外硬件,也不影响用户交互行为,用户体验较好.

已经有研究表明,欺骗行为在一定程度上会影响用户击键模式的变化.其中,基于击键特征建立的模型对欺骗行为的检测由于其具有自动化程度高,对设备要求低,特征易于获得等特点,被认为是欺骗行为检测的有效手段<sup>[7]</sup>.现有的研究已经表明了基于击键特征的欺骗行为进行预测具有巨大的应用潜力<sup>[8-10]</sup>.然而,现有的欺骗检测方法存在泛化能力弱的问题,严重的限制了现有模型在互联网社交领域的应用,可能的原因包括:1) 数据收集复杂;2) 未考虑击键模式的个体差异;3) 实时性差.此外,现有的机器学习预测模型大都针对长文本及其语义的欺骗行为进行探测,这对模型的广泛应用带来了挑战.

为了应对以上挑战,本研究针对短文本信息输入,首先设计了一个实验从用户击键行为中提取了广泛的击键特征,包括单键特征、内容特征、双键特征;接下来对数据进行归一化,消除个体差异;然后采用遗传算法(GA)<sup>[11]</sup>和支撑向量机(SVM)完成特征选择和模型建立,建立基于遗传算法的支持向量机(GA-SVM)模型对欺骗行为进行检测;最后对模型的性能,击键特征对欺骗检测的相对重要性以及欺骗者认知负荷和心理压力对击键模式影响进行了分析.研究结果表明:该模型获得 82.86% 的分类准确率,能够有效地检测出用户的欺骗行为;单键特征、内容特征、双键特征三类击键特征对欺骗行为的检测都有较大的贡献.

## 2 研究现状

心理学研究表明,在网络上进行欺骗行为会导致情绪的唤醒和认知负荷的增加,从而导致精细运动控制的减少,这种控制的减少在击键行为上就表现为偏离基准的击键动力学特征的增加. Mark

Grimes 等人设计了一个击键动力学模型用于欺骗检测<sup>[7]</sup>,证实了欺骗性行为会引起情绪唤醒和认知负荷的可测性变化,进而影响一个人的击键行为.这些击键动力学和心理学的研究为欺骗能够影响击键特征提供了理论依据.

击键动力学研究的是用户在使用键盘或虚拟键盘进行输入时的打字节奏或模式的独特性,通常涉及到人们打字时他们的击键数据的时序特征.这些特征包括一个按键的持续时间和连续按键之间的延迟.一些研究中基于距离的分类方法,通过不同的距离函数来衡量击键特征的相似性,如曼哈顿距离<sup>[12]</sup>和序列相对距离<sup>[13]</sup>,这些基于距离的应用可以实现基于自由文本击键特征进行身份识别, Tappert<sup>[14]</sup>等人研究中发现输入大约 300 个字符的自由文本时,能够比较准确的进行身份识别.有些研究把机器学习方法和统计学方法也被用于研究击键动力学领域<sup>[11]</sup>.

击键特征的选择对研究结果有着非常大的作用. Joyce 等最早提出了利用击键特征进行用户的身份识别<sup>[15]</sup>.击键模型只选用了击键平均时间这单一特征,计算量小使得这个模型能够快速识别用户身份.但击键特征过于单一和特征值的处理过于简单的问题影响了用户识别的结果; Kacholia<sup>[16]</sup>等人根据 Joyce 模型提取击键特征过于单一的缺点,采用按下和释放两阶段来构建在持续发生的键盘事件情形下的模型.该模型提升了身份识别率,但对用户的击键过程的细分导致了计算量的增大. Banerjee<sup>[9]</sup>采用停顿时间、插入、删除、方向键等特征对在线文本编辑的作者进行欺骗检测,在原来语义检测方法的基础上,提升了近 10% 的检测率; Yin 和 Chen<sup>[17]</sup>使用统计工具证实了用户认知负荷越高,说话停顿率越高. Ruiz 等人<sup>[18]</sup>的实验得出说话时停顿的次数随着认知负荷程度的增长而增加.这些统计指标常用于语音特征的分析,但在击键输入中存在的停顿也与认知负荷的高低强相关,认知负荷会随着说谎而增加,因此,认知负荷在击键欺骗检测中也同样适用.

以上研究从理论和应用的相关研究为该领域的发展奠定了基础,但网络环境下欺骗检测过程中的一些问题仍未解决,也不能确定使用中文输入法时的击键特征是否适用于欺骗检测.本文模拟更接近真实的实验环境,在单键特征和双键特征的基础上,增加与认知负载和情绪唤醒较为相关的内容特征,进一步提升了欺骗检测的分类准确率.

### 3 基于 GA-SVM 的欺骗检测模型

在进行 SVM 建模时,特征选择和参数优化两个任务将显著影响最终模型的分类能力,也有很多研究单独使用 SVM 解决特定的问题<sup>[19]</sup>,但独立执行这两个任务可能导致模型的分类能力损失.因此,近来流行将这两个任务整合为一个多目标优化问题,应用遗传算法(GA)、粒子群算法(PSO)等全局优化算法同时执行两个任务. GA 模拟生物遗传进化的方式迭代地搜索最优解.从包含一定数量个体的初代种群开始,按优胜劣汰的原则逐代地应用遗传学算子对种群中的个体进行交叉、变异,繁殖产生新个体,形成子代种群.在每一代都会评估每个个体的适应度.此过程将使后代个体的适应度较前代个体越来越优.末代种群中适应度最优的个体解码后即是问题的近似最优解. GA 具有内在的隐性并行性,具有较好的全局寻优能力.

为特征选择结果和 SVM 参数;(4) 向 SVM 输入特征子集和参数,建立模型并使用预定义的适应值函数(Fitness function)评估染色体;(5) 根据每个染色体的适应值,进行选择、交叉、变异操作,产生新的个体;(6) 重复步骤(3)~(5),直至满足终止条件;(7) GA 停止,使用最优染色体对应的特征子集和参数建立 SVM 模型.

### 4 实验设计

参与人员共 35 人,为 20~30 岁的在校大学生,能熟练使用 QQ 或微信等互联网通讯软件.

实验模仿了研究中经常使用的“二真一假”游戏进行欺骗检测.实验把被试随机分成若干个二人组,每个组内的被试通过键盘输入对另外一个人发送 QQ 消息.被试从预设的十五个主题中选择一个进行描述(如:描述你喜欢的动物等).描述内容要求 40 个字符以上.被试可以从预设题目中选择自己更容易描述的主题,目的是希望减少额外的认知负荷.实验者参与者挑选 3~6 个主题,其中 3 个主题的描述是实验者真实的意图,另外 3 个主题的描述是欺骗性的,这里允许实验者挑选同一主题分别描述欺骗性和真实的情况.当实验者在发送消息之前,他们需要在数据收集界面上标注实验编号和真实性.

通过基于互联网通讯软件的欺骗检测实验,收集了各个用户 QQ 聊天的击键数据.我们使用 C# 程序编写的 Windows 后台程序,收集用户在互联网通讯软件中通过键盘输入的按键信息.共收集到 210 条样本数据,包含 105 条欺骗性样本和 105 条非欺骗性样本.

实验使用的击键特征包括了研究常用的 Joyce 特征模型和 PR-RP 模型的特征,同时增加针对中文输入欺骗行为有关联内容特征<sup>[20]</sup>.特征共包含 102 个,其中 52 个单键特征,10 个内容特征,40 个双键特征.

实验过程中采集了 26 个字母的持续时间(从按下到释放的时间间隔)的平均值和方差组成了单键特征(见表 1).

表 1 单键特征描述

Tab. 1 Description of single-key feature

特征	含义
$M(T[KEY])$	键 KEY 从按下到释放的平均时间
$SD(T[KEY])$	键 KEY 从按下到释放的时间的方差

其中:KEY={A,B,C,...,Z}.

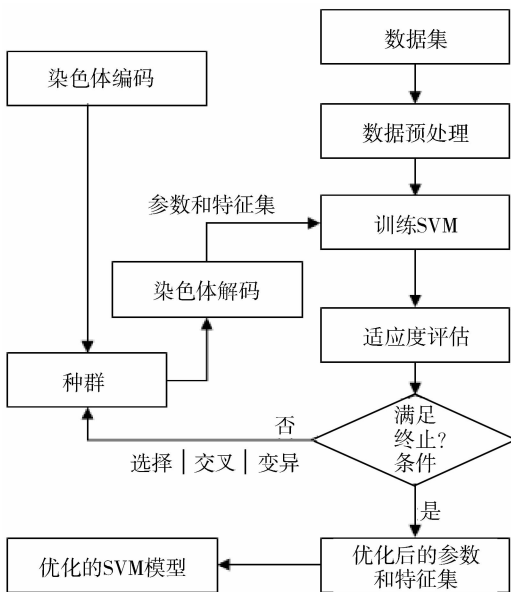


图 1 GA-SVM 模型  
Fig. 1 SVM-GA Model

本文采用 GA 与 SVM 相结合的方法进行自动欺骗模型的建模(如图 1 所示).利用 GA 选择最优特征子集和优化 SVM 的参数,得到分类准确率最优的 SVM 模型. GA-SVM 的工作流程步骤如下:(1) 使用最大最小法将所有特征值线性缩放到 [0, 1] 区间,避免不同量级的特征值对分类准确率产生影响;(2) 将特征子集和 SVM 参数随机编码为初始染色体并初始化 GA 的种群大小、进化代数、交叉变异概率等运行参数;(3) 将染色体解码

同时,实验过程中一些相关控制键的统计量(详见表 2)的采集,组成了实验中的内容特征。

表 2 击键内容特征描述

Tab. 2 Description of keystroke content feature

特征	含义
$M(T[\text{space}])$	空格键的按键平均持续时间
$SD(T[\text{space}])$	空格键的按键持续时间的方差
Velo	击键速度, 击键数/时间
$C_{\text{error}}$	错误次数, 使用删除\退格键的数量
$C_{\text{sp}}$	输入标点符号的数量
$M(T[\text{pause}])$	停顿平均时间, 停顿总时间/总次数
$SD(T[\text{pause}])$	停顿时间的方差
$R_{\text{pause}}$	停顿率, 总停顿次数/总击键数
$M(T_1)$	平均击键时间, 总时间/总击键数
$M(T_2)$	修正后的平均击键时间, 总时间-总停顿时间/总击键数

我们对双键特征集进行频次分析,由于键盘中任意两个按键的组合超过了 1200 个<sup>[21]</sup>, 所以需要进行筛选以避免维度过高。

考虑到汉语拼音中“WO”, “OU”, “AO”等连续按键序列经常出现,而有些按键序列(如“UV”等)基本不会出现或只有无效输入时才会出现,所以本文重点分析原始数据中出现频度最高的那些连续双键序列. 实验前收集 5 名实验者一周之内的所有按键信息,并对这些按键信息中的双键序列数量进行了排序,确定用户使用频率最高双键组合(GRAPH)集为 { AN, NG, LA, SH, AO, IN, JI, EN, OU, XI }, 实验最终采用双键特征对应统计量如表 3 所示。

表 3 双键特征描述

Tab. 3 Description of double-key feature

特征	含义
$M(\text{PR}[\text{GRAPH}])$	第一个键按下到第二个键释放的平均时间
$SD(\text{PR}[\text{GRAPH}])$	第一个键按下到第二个键释放时间的方差
$M(\text{RP}[\text{GRAPH}])$	第一个键释放到第二个键按下的平均时间
$SD(\text{RP}[\text{GRAPH}])$	第一个键释放到第二个键按下时间的方差

其中:  $\text{GRAPH} = \{\text{AN}, \text{NG}, \text{LA}, \text{SH}, \text{AO}, \text{IN}, \text{JI}, \text{EN}, \text{OU}, \text{XI}\}$

每个个体在输入中文自由文本时的击键模式有很大的差异,为了消除这种差异,我们对每个实验者的每个击键特征数据进行去除差异化处理<sup>[14]</sup>,具体计算方法见式(1)。

$$F_{\text{new}} = F_{\text{orig}} - \sum_{i=1}^N F_{\text{orig},i}/N \quad (1)$$

其中,  $F_{\text{new}}$  表示归一化之后的特征值;  $F_{\text{orig}}$  表示原始的特征值;  $N$  为某个参与者在数据库中的样本

总数. 使用这种个体归一化方法能够消除每个用户每个特征的均数差异,且保留了个体特征差异的变化. 最后,使用标准化方法对每种特征进行标准化以便于用于机器学习过程。

## 5 实验结果

实验通过对 210 个样本数据进行分析,得到不同的特征子集和分类准确率。

### 5.1 特征选择

本文通过 GA 的搜索策略生成子集,并使用 SVM 的准确率去评估特征子集. 在实际操作中,初始种群取时,随机生成 50 个个体,每一代保留适应度最高的 10 个个体,交叉概率为 0.6,变异率为 0.033,进化代数为 100,若在 10 代之内最优的特征子集和适应度都不发生变化,遗传算法终止。

基于遗传算法特征选择方法产生的特征子集中的单键特征包含了 G 键、J 键、R 键、U 键的平均按键持续时间. 这符合 3 个声母和 1 个韵母在日常用语汉语拼音中使用频次较高这一现象;包含了 LA, EN, OU, XI 双键特征的 PR 或 RP 持续时间;在内容特征上包括了输入错误次数、停顿时间的方差和平均击键时间. 特征子集分布结果在一定程度上证明了我们在本文中使用的三类击键特征能够进行欺骗检测. 尤其在内容特征中,空格键/回车键的按键时间,击键速度,输入错误数量,击键停顿时间,平均击键时间和修正后的平均击键时间这些特征的选取,也代表了几乎所有的内容特征都与欺骗检测相关。

### 5.2 模型分类准确率

为了探究击键特征的个体差异对特征选择的影响,以及对表现最好的机器学习算法性能的影响,我们分别将去除个体差异前后的实验数据进行对比. 信息增益(IG)是使用过滤方法进行特征选择的一种方式,GA 属于包裹法,实验采用两种特征选择方法作为 SVM 算法的特征子集,来说明不同的特征子集选择方法对算法性能的影响. 为了验证去除个体差异是否会对分类准确率带来显著差异,我们去除个性差异前后的分类准确率采用了 t 检验进行分析。

表 4 展示了模型 10 折交叉验证的平均准确率. t 检验的结果表明,对于两类建模方法(IG-SVM 和 GA-SVM),归一化后模型准确率都显著的大于归一化之前的准确率(all p-values < 0.05). 这说明:去除个体差异能够显著提升模型分类准确率。

表4 模型的分类准确率

Tab. 4 Classification accuracy of models

模型	准确率(归一化前)	准确率(归一化后)	P值( $df=18$ )
IG-SVM	69.52%	77.98%	0.014
GA-SVM	74.28%	82.86%	0.001

此外, $t$ 检验的结果表明,在基于归一化后的特征建立的模型中,GA-SVM模型的准确率显著的大于IG-SVM模型( $p=0.018$ ;  $df=18$ ).这表明,对于归一化后的数据,GA-SVM的都获得了最好的分类准确率.

### 5.3 基于信息增益的特征分析

实验进一步挖掘每个特征对欺骗检测模型的实际贡献,计算了去除个性差异后的特征集的信息增益.表5列出了信息增益值从高到低的10个特征,包含1个单键特征、2个双键特征和7个内容特征共.实验预设的三类击键特征都有被选入.从特征分布情况看,内容特征被选入的整体数量和权值要大于单键特征和组合键特征,可以体现欺骗行为对这些内容特征的影响更加明显,也说明本文提出的这些内容特征更适合用于进行欺骗检测.

表5 去除差异化后的特征信息增益值

Tab. 5 Information gain of feature after removed individual difference

排名	特征	信息增益
1	$M(T_1)$	0.3243
2	$V_{elo}$	0.2887
3	$M(T_2)$	0.2365
4	$R_{pause}$	0.1660
5	$C_{error}$	0.1079
6	$M(T[pause])$	0.1033
7	$M(T[G])$	0.0969
8	$SD(T[pause])$	0.0756
9	$M(PR[AN])$	0.0745
10	$M(PR[LA])$	0.0744

与心理负荷紧密相关的内容特征70%被选入特征子集中,说明本文预设的特征在交互击键行为的欺骗检测表现尤为突出.信息增益最大的 $M(T_1)$ 为平均按键时间,这个结果也丰富了已有研究<sup>[22]</sup>中提到的击键速率反映了思考负荷的增加和情绪的波动.去除个体差异后的击键速度所有 $C_{error}$ 特征综合考虑了试验样本中退格键(Backspace)和删除键>Delete)的使用频次,把退格键和删除键的使用数量作为欺骗检测特征是类似研究中一种新的尝试.已有研究表明,用户(欺骗者)欺

骗时认知负荷和心理压力的增加很可能导致精细运动的改变,从而体现在输入内容的错误.但是,由于输入法具有自动矫正的功能,实验中不能记录中文拼音输入时所有退格键和删除键次数,例如键入“lixinag”时,有些中文输入法能够自动修正为中文词汇“理想”,类似的错误很难全部找出;把停顿时间作为特征也是基于相同的考量,一般情况下,心理压力负荷的增加会导致思路间歇性停顿,在击键过程中表现为停顿; $C_{ip}$ 是统计四种常见标点符号按键的使用数量,标点符号代表了语句的停顿,在一定程度上反映欺骗时键盘输入的停顿过程.在机器学习算法中加入内容特征,有效地印证了已有的理论研究,提升了分类准确率.

从训练的欺骗检测模型中可以发现,中文用户敲击键盘的模式能够进行欺骗检测.实验预设的击键特征包含单键特征,组合键特征和内容特征,最优特征子集中包含了这三种特征,实验数据说明这三种击键特征相结合能够得到较高的欺骗检测准确率.

通过实验数据和分析,我们解决了以下几个问题.首先,建立基于中文自由文本的击键特征来识别欺骗/非欺骗状态的模型,证明了用户使用键盘输入的中文自由文本时,机器学习方法能够区分出欺骗和非欺骗的语句;其次,无论是使用基于信息增益进行特征选择,还是用基于遗传算法进行特征选择,得到的最优特征子集都包含了实验前预设的三类击键特征,也证明了本文提出的三类击键特征能够进行基于中文自由文本的欺骗检测.最后,通过对比每个模型的准确率,得到适合欺骗检测的最有效的特征子集和表现最佳的预测模型.

## 6 结论

心理学研究表明,人的行为是人心理活动的外在表现,如何量化这种关系是研究者面临的挑战.使用机器学习方法学习人进行欺骗活动时外在行为的变化模式,实现自动的欺骗检测,这是计算机科学应用于心理学的新尝试.这种尝试提供了一种简便易行的非侵入式的欺骗检测方法,为互联网环境下欺骗检测的应用提供了新的契机.

本文针对中文自由文本这一背景条件下,使用击键这一特殊的交互行为数据进行自动化欺骗检测的可行性.并设计并实现了一个探索性实验来验证其可行性.在实验过程中,用户的击键行为特征被收集并使用机器学习方法进行分析.实验结果表

明:(1) 网络环境下的欺骗行为能够致使用户击键模式的变化,这种变化可以被机器学习方法所侦测;(2) 在使用机器学习方法进行自动欺骗检测建模时,基于内容的击键特征与用户的欺骗行为联系更为紧密;(3) 特征选择与参数优化会显著影响到所建模型的分类能力,未来研究中应重点考虑。

#### 参考文献:

- [1] 张虎,谭红叶,钱宇华,等. 基于集成学习的中文文本欺骗检测研究[J]. 计算机研究与发展, 2015, 52(5): 1005.
- [2] Serota, K B, Levine, T R, Boster F J. The prevalence of lying in america; three studies of self-reported lies[J]. Hum Commun Res, 2010, 36(2): 1.
- [3] Bond C F, DePaulo B M. Accuracy of deception judgments [J]. Personal Soc Psychol Rev, 2006, 10(3): 214.
- [4] 张亭玉,张雨青. 说谎行为及其识别的心理学研究[J]. 心理科学进展, 2008, 16(4): 651.
- [5] Aldert V. Challenging interviewees during interviews: the potential effects on lie detection[J]. Psychol Crime Law, 2006, 12(12): 193.
- [6] Warren G, Schertler E, Bull P. Detecting deception from emotional and unemotional cues[J]. J Nonverbal Behav, 2009, 33(1): 59.
- [7] Grimes G M, Jenkins J L, Valacich J S. Assessing credibility by monitoring changes in typing behavior: the keystroke dynamics deception detection model [C]//HICSS-46 Symposium on Credibility Assessment and Information Quality in Government and Business. Maui, Hawaii; [s. n.], 2013.
- [8] Vizer L M, Zhou L, Sears A. Automated stress detection using keystroke and linguistic features: An exploratory study[J]. Int J Hum-Comput St, 2009, 67(10): 870.
- [9] Choi Y. Keystroke patterns as prosody in digital writings; a case study with deceptive reviews and essays [J]. Empir Methods Nat Lang Process (EMNLP), 2014, 6: 1
- [10] Zhong Y, Deng Y. A survey on keystroke dynamics biometrics: approaches, advances, and evaluations [C]. [s. l.]: Science Gate Publishing, 2015.
- [11] 余乐正,赵柳青,陈曼,等. 基于 SVM 的革兰氏阴性菌分泌系统蛋白识别方法[J]. 四川大学学报:自然科学版, 2016, 53(2): 443.
- [12] 黄怡然,胡晓勤. 基于击键动力学的中文自由文本持续认证方法[J]. 计算机工程, 2016, 42(1): 138.
- [13] Kang P, Cho S. Keystroke dynamics-based user authentication using long and free text strings from various input devices[J]. Infor Sci, 2015, 308: 72.
- [14] Tappert C C, Cha S H, Villani M, et al. A keystroke biometric system for long-text input[J]. Int J Inf Secur Priv, 2010, 4(1): 32.
- [15] Joyce R, Gupta G. Identity authentication based on keystroke latencies [J]. Commu ACM, 1990, 33(2):168.
- [16] Kacholia V, Pandit S. Biometric authentication using random distributions (bioart) [C]//Canadian IT Security Symposium. Ottawa, Canada: [s. n.], 2003.
- [17] Yin B, Chen F. Towards automatic cognitive load measurement from speech analysis [M]// Human-Computer Interaction. Interaction Design and Usability. Berlin Heidelberg: Springer, 2007.
- [18] Yin B, Chen F, Ruiz N, et al. Speech-based cognitive load monitoring system[C]. IEEE International Conference on Acoustics. [s. l.]: IEEE, 2008.
- [19] 袁培飒,陈锐,林涛,等. 基于遗传算法和神经网络的软件界面美感建模[J]. 四川大学学报:自然科学版, 2015, 52(2): 269.
- [20] Lee P M, Tsui W H, Hsiao T C. The influence of emotion on keyboard typing: an experimental study using visual stimuli, [J]. Plos One, 2015, 10(1): 81.
- [21] Kolakowska A. Recognizing emotions on the basis of keystroke dynamics[C]//Proceedings of 2015 8th International Conference on Human System Interactions (HSI). Warsaw, Poland:[s. n.], 2015.
- [22] 张虎. 面向中文文本的欺骗行为检测研究[D]. 太原: 山西大学, 2014.