维普资讯 http://www.cqvip.com

一个基于神经网络的动态手写签名验证模型

李 媛 袁余良 沈 峰 潘金贵

(南京大学软件新技术国家重点实验室 南京大学计算机科学与技术系 南京210093)

摘 要 手写签名验证作为一种有效的生物身份认证技术,具有广泛的应用前景,但由于签名易变化的特点,其性能还不够理想。最近神经网络越来越多地在模式识别领域使用并取得了很好的效果,但在签名验证中尚不多见。本文提出并实现了一个基于BP神经网络的动态手写签名验证原型,并通过实验对网络结构进行了分析。通过对从10人收集的190个本人签名和371个伪造签名评价EER=2.16%,还是比较满意的。

关键词 生物认证,手写签名验证,神经网络

A Model for Dynamic Handwritten Signature Verification Based on Neural Network

LI Yuan YUAN Yu-Liang SHEN Feng PAN Jin-Gui

(State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing 210093)

(Department of Computer Science and Technology, Nanjing University, Nanjing 210093)

Abstract Owing to traditional signatures being widely and maturely used in finance or government department handwritten signature verification(HSV), as an effective and efficient kind of biometric based authentication schemes, has a good perspective. But its performace is not good enough because of signatures' easy change. Recently, neural network is coming to used in Pattern Recognition more and more and has archieve good effects. But there are a few of researches on application of neural network in HSV. This aticale has apposed and implemented a prototype of dynamic HSV based on Back-propagation neural network and has analyzed network structure from experiments. Through 190 own signatures and 371 forged signatures from 10 persons, equal error rate 2.16% are archived.

Keywords Biometrics, Handwritten signature verfication, Neural network

1 引言

最近,神经网络越来越多地在模式识别领域使用,其强大的计算能力,在实际的应用中取得了出乎意料的效果,如字符识别、脸形识别等。但目前还很少将神经网络用于签名验证,已有的研究[1~7]绝大多数也仅仅是基于全局特征的,由于全局特征的局限性,效果不甚理想。最主要的原因在于:签名局部特征数量巨大而签名的训练样本数很少,两者有一定的矛盾性,特征量大要求输入结点多,而输入结点多则要求训练样本也足够多,否则网络将不能被充分训练。因此,对特征的抽取成为利用神经网络方法进行签名验证的关键。

与其它方法相比神经网络不需要了解网络的内部细节和过程,实现相对简单,同时,还有易于自我改进和学习的优点,很容易为签名验证系统增加学习特性,以适应签名书写风格随时间发生的细微变化。从其它模式识别的应用来看,神经网络往往能获得比其它方法更好的分类性能。

为此,针对上述难点和优势,本文提出并实现了一个基于BP神经网络的动态手写签名验证原型系统,设计了自己的特征抽取算法和伪造签名自动生成算法;并通过分析不同的网络结构对验证的影响,最终得到一个优化的模型。

一个动态手写签名验证系统的处理流程包括注册和验证两个阶段。在注册阶段,用户注册若干个样本签名,系统利用样本签名训练出一个参考模型;在验证阶段,用户在线输入一个测试签名,系统将该测试签名同参考模型进行匹配验证,判断是本人签名还是伪造签名,执行相应的操作。一般来说,一个完整的动态手写签名验证系统包括数据收集模块、预处理模块、特征抽取模块、模型的构造和训练模块、模型的验证模块和性能评价模块等6个功能模块。本文将重点描述特征抽取、模型的构造训练和验证部分,其他请参考文[8]。

2 数据准备

2.1 签名收集

采用Wacom公司的手写板进行收集得到等时间间隔的采样点序列,每一个采样点包括其坐标(x,y)和压力p。为此一个具有T个采样点的签名可以表示为:$S_T=\{(x_t,y_t,p_t,h_t)\}^T, t\in[1,T]$,其中$h$表示从第一个采样点开始的相对时间,单位为毫秒。

2.2 预处理

由于在数据收集的过程中,受环境噪声、设备的差异、个人书写姿势等多种因素的干扰,得到的原始签名往往大小不一、倾斜程度不一、采样点个数相差悬殊,给验证带来了很大的影响,因此必须进行预处理,尽可能地消除这些因素的影响。

预处理包括三个步骤:平滑化、重采样和规范化。平滑化一般采用高斯等滤波器对原始签名滤波,去除收集过程中引入的噪声;重采样的目的是为了减少需要处理的数据量,加快系统的响应速度,采用均等时间间隔采样的方法选择部分采样点用于后续的处理;规范化主要是进行几何变换,包括平移、旋转和缩放,消除由签名的倾斜角度和大小不一带来的影响,最终得到规范一致的数据。

2.3 特征抽取

特征抽取我们分两步进行,第一步为导出属性的计算,第二步为关键点的提取。

2.3.1 导出属性的计算 一般来说,人在签名时的速度

李 媛 硕士研究生,研究方向为模式识别、多媒体技术和网络应用。袁余良 硕士研究生,研究方向为模式识别、多媒体技术和网络应用。沈峰 硕士,研究方向为模式识别。潘金贵 教授,博士生导师,从事知识处理程序系统、中间件、Agent技术及多媒体信息处理技术等的研究。

维普资讯 http://www.cqvip.com

不会随着签名的大小而发生改变，因此计算采样点的速度必须在预处理的等比例缩放之前而在平移和旋转之后。

第 t 个采样点的速度(v_{xt}, v_{yt})为：

$$v_{xt}=\frac{x_{t+1}-x_t}{h_{t+1}-h_t}, v_{yt}=\frac{y_{t+1}-y_t}{h_{t+1}-h_t}$$

则速度的大小 v_{rt}和方向 θ_t 分别为：

$$v_{rt}=\sqrt{v_{xt}^2+v_{yt}^2},\ \theta_t=\arctan\frac{y_{t+1}-y_t}{x_{t+1}-x_t}$$

角度变化 $\Delta\theta_t$ 为 $\Delta\theta_t=\theta_t-\theta_{t-1}$

由此，得到点的坐标、压力、速度和角度组成的向量：$(x_t, y_t, p_t, v_{xt}, v_{yt}, v_{rt}, \theta_t, \Delta\theta_t)$

2.3.2 关键点的提取 关键点提取的目的有两个：一是为了将签名中能反映签名本质特征的点标记出来，在后续的处理中给予特别的关注，而将其余的点放到次要的位置，或者干脆去除。二是将各个签名不同的采样点数转化为统一的关键点数。为此我们设计了自己的关键点抽取算法，算法分两步进行：

第一步，对采样点的重要度进行量化。规定自然笔划端点的重要度总是比非端点大。当某个采样点被选为关键点时，整个签名中重要度比其大的点都已经设为关键点。

针对笔划的端点：设签名的笔划数为 N_S，则端点数为 N_S+1，记端点的集合为 $SE=\{P_1, P_2, \cdots, P_{N_S+1}\}$。各端点的重要度为 $I_t, t=1, \cdots, N_S+1$

(1)计算各笔划的长度 $SL=\{L_1, L_2, \cdots, L_{N_s}\}$；

(2)设签名的开始点和结束点的重要度为 $\sum_1^{N_S} L_t$，并将开始点和结束点标记为已处理；

(3)分别计算各端点同开始点和结束点的笔迹距离，取其较小值作为该点的重要度，即 $I_t=\min(\sum_1^t L_j, \sum_t^{N_s} L_j)$；

(4)将上述未处理点中重要度最大的点，标记为已处理，将此点作为前一段的结束点和后一段的开始点，调用(3)更新重要度；

(5)递归执行(3)和(4)，直到所有的点都为已处理。

针对非笔划端点的采样点，进行下述处理：

(1)对签名中的每个实笔划和虚笔划执行(2)～(6)各步；

(2)标记笔划的端点为已处理；

(3)当两个已处理点相邻时，直接进入下一笔划的计算；

(4)如图1所示，针对上述两点组成的笔划段，计算两点之间任意采样点 P_t 同它们所组成线段的垂直距离 $P_t\rightarrow\overline{P_sP_e}$，以及同两点的直线距离 $P_t\rightarrow P_s, P_t\rightarrow P_e$，则点 P_t 的重要度可定义为：

$$I_t=(P_t\rightarrow\overline{P_sP_e})+\frac{1}{2}\min(P_t\rightarrow P_s, P_t\rightarrow P_e)$$

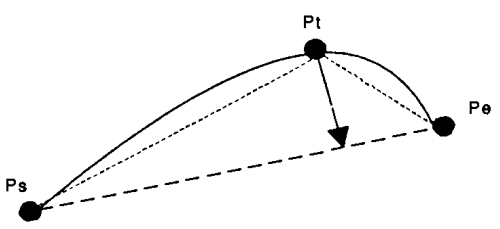

图1 关键点提取算法

(5)将上述未处理点中重要度最大的点标记为已处理，将此点作为前一段的结束点和后一段的开始点，调用(3)更新重要度；

(6)递归执行(3)和(4)，直到所有的点都为已处理。

第二步，根据指定的关键点数 N_{key}，将采样点按照重要度由高到低的顺序逐一标记为关键点。其在原始签名中的先后关系仍保持不变，由此可以得到同关键点数相等的点特征向量序列：

$SP=\{(x_t, y_t, p_t, v_{xt}, v_{yt}, v_{rt}, \theta_t, \Delta\theta_t)\}^{N_{key}}$，其中 $t\in[1, N_{key}]$。

3 模型

3.1 模型构造

图2表示 BP 网络模型的结构图[9]，记输入结点数为 S_0，输入向量为$\{p_1, p_2, \cdots, p_{s0}\}$，隐层1和隐层2的结点数分别为 S_1和 S_2，除了可以由 BP 学习算法在训练阶段根据训练样本调整的网络权值 w 和阈值 b 外，需要事先确定的模型参数为输入结点数 S_0、隐层结点数 S_1、S_2和输出结点数 S_3。

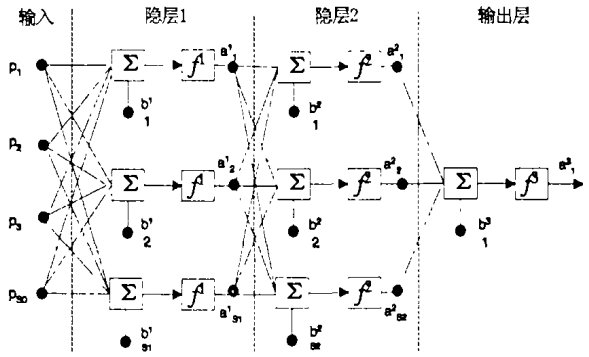

图2 BP 网络结构图

由于验证只需要分为本人和伪造签名两类，因此只需要一个输出结点即可，即 $S_3=1$。在训练时，设定本人签名的目标值为1，伪造签名的目标值为0；在验证时，输出值为[0,1]之间的实数，将输出值同阈值比较，如果大于阈值则为本人签名，否则为伪造签名。

输入层结点个数 S_0同所选择的特征有关，点特征模型的输入结点数为关键点的个数，分别取100、150和200进行实验，为不同的特征分量建立不同的神经网络模型。当系统在实际使用时，将选择若干最优的特征组合成一个综合的输入向量，用于训练和验证。

对于两个隐层、隐层结点数和传递函数类型的确定目前还缺乏有效的方法，只能根据问题本身通过实验手工确定。

隐层结点数 为了确定隐层结点数 S_1和 S_2的值，我们先假设隐层数为1，即 $S_2=0$。在本模型中由于输入结点数很大而输出结点数仅为1，隐层结点数应该介于输入结点数和输出结点数之间。为此，我们设定点特征的隐层结点数为1、10、20和50进行分析。从实验可知，只要保证模型能正常收敛，隐层结点数对性能的影响不大，为了简单起见，设只有一个隐层，即采用两层的 BP 网络。

传递函数类型 BP 模型使用的传递函数只能是对数或者正切 Sigmoid 函数。确定了传递函数也就确定了该层结点的输入和输出值的范围。由于我们要求神经网络的输出在(0, 1)范围内，因此输出层的传递函数必须采用对数 Sigmoid 函数，而隐层的传递函数可以是上述两者中的任何一个，对此将通过实验进行比较，究竟采用哪个函数更好。从后面的实验可知，传递函数对系统性能的影响不大。相比之下，采用对数 Sigmoid 函数略好一些。

3.2 模型训练

同一般的模式识别问题相比，签名验证的最大不同之处

维普资讯 http://www.cqvip.com

在于在注册阶段其两类中的伪造签名类的训练样本是未知的。理论上讲，非本人签名的任何签名都可以成为其训练样本，而不管其内容是否相同。在两类特征空间都必须有足够的训练样本，将整个空间覆盖，否则神经网络将不能正确判别。对于本人训练样本和伪造训练样本分别采用下面的方法来增加训练样本数。

对于本人训练样本，采用 Hold-out 方法的思想，首先给注册的样本签名进行编号，记样本签名集合为$\{SR_1, SR_2, \cdots, SR_R\}$，其中 R 表示样本签名的个数；然后产生 N_R^* 个[1,R]之间的随机自然数$\{q_1, q_2, \cdots, q_{N_R^*}\}$，将与随机数值对应下标的签名取出来，组成一个新的集合$\{SR_{q_1}, SR_{q_2}, \cdots, SR_{qN_R^*}\}$，这样就将训练样本数从 R 转化成了 N_R^*，在本系统中取 $N_R^*=100$。

从文[10]在运用神经网络解决脸形检测问题中提到的自动生成训练用伪造脸形的思想受到启发，在手写签名验证中，应能根据注册的本人签名样本自动生成训练用伪造签名。理论上讲，只要是非本人的任意签名都可以成为伪造签名，而不一定要签名的内容和本人签名的内容相同。本系统中，根据不同特征的维度生成[0,1]之间的随机数，作为同注册的本人签名相对应的伪造签名用于模型的训练。对于每个用户，我们取自动生成的伪造签名数为400。

根据训练时模型参数调整的先后，可以将训练过程分为两种方式：一种是增量式训练方式；另一种是批量式训练方式。在增量式训练方式中，模型参数在每一个训练样本计算得到误差后都及时更新，因此训练的结果跟样本输入的顺序有关；在批量式训练方式中，模型参数并不及时更新，而是等全部样本输入后统一更新，因此训练的结果跟样本输入的顺序无关。在本系统中，我们采用批处理 BP 学习算法进行训练，设定学习目标为0.01，性能评价函数为标准方差函数，最大训练步数为5000，以保证模型能充分训练和收敛。

3.3 模型验证

由于签名验证要求签名的内容相同，不同签名者的签名间差异很大，因此为每一个签名者采用不同的神经网络模型，模型的输出在[0,1]范围内，为实数，而最终结果要求为0或者1。为此，可以定义阈值函数为：

$$f(x)=\begin{cases}1 & x\geqslant Threshold\\ 0 & x<Threshold\end{cases}$$

即如果输出值比指定的阈值大，那么就认为该签名是本人真实签名，否则认为是伪造签名。阈值 $Threshold$ 的取值范围在(0,1)之间，可以根据系统对系统安全性的要求自行设定，一般情况下可以取 $Threshold=0.5$。

伪造签名可以分为三类：偶然伪造签名(Casual Forgeries)、熟练伪造签名(Skilled Forgeries)和描摹伪造签名(Traced Forgeries)。显然采用偶然伪造签名时，系统的性能比采用另两种伪造签名时要差。在实际的签名验证系统中，伪造者是不知道本人真实签名的，因此属于偶然伪造签名。在我们的签名收集中，伪造者可以看到真实签名，并且要求其尽力模仿该签名。采用这样的伪造签名，在评价时如果结果相同那么其安全性应该要比偶然伪造签名略高。

4 性能评价

4.1 性能评价指标

常用的指标为 FRR(False Reject Rate)、FAR(False Accept Rate)和 EER(Equal Error Rate)，FRR 是指本人签名被错误拒绝的比例，FAR 是指伪造签名被错误接受的比例。其中 FRR 和 FAR 曲线的交点称为 EER(等价错误率)，是一个综合评价指标。

4.2 签名收集情况

为了对分类器进行性能评价，必须收集一定数量的签名。收集的签名可以分为训练分类器的样本签名和测试分类器的测试签名。对于测试签名，又可以分为签名者本人的真实签名和其他签名者的伪造签名。

签名的收集分两个阶段进行，第一阶段是样本签名的收集，第二阶段是测试签名的收集。每个签名者用于注册的样本签名为10个，测试签名分三次收集完成，分本人测试签名和伪造测试签名。在伪造签名时，伪造者从签名者中随机抽取，要求尽力模仿相应的真实签名。共收集本人测试签名190个，伪造测试签名371个。

4.3 实验结果

4.3.1 *隐层结点数* 表1表示 y 方向速度(此时关键点数为100)在不同隐层结点数时两类错误率值，从表中可见，当隐层结点数约为输入结点数的1/5时最佳。

表1 不同隐层结点数时 Vy 两类错误率值

隐层结点数	阈值	0.4	0.6	0.8	EER
10	FRR	8.42%	11.05%	18.42%	4.74%
	FAR	1.08%	0.27%	0.27%	
20	FRR	6.84%	7.89%	15.26%	4.68%
	FAR	1.89%	0.54%	0.27%	
50	FRR	12.63%	13.68%	16.32%	12.13%
	FAR	11.32%	4.58%	1.08%	

4.3.2 *传递函数类型* 表2表示 y 方向速度在不同传递函数时两类错误率值，从表中可见，传递函数对结果的影响不大，相比之下对数 Sigmoid 函数略好。

表2 不同传递函数时 Vy 两类错误率值

函数类型	阈值	0.4	0.6	0.8	EER
对数 Sigmoid	FRR	8.42%	11.05%	18.42%	4.74%
	FAR	1.08%	0.27%	0.27%	
正切 Sigmoid	FRR	21.05%	23.68%	32.11%	5.79%
	FAR	0.27%	0.27%	0.27%	

4.3.3 *关键点数* 表3表示不同关键点数时两类错误率值，从表中可见当关键点数为100时最佳。

表3 不同关键点数时两类错误率值

关键点数	阈值	0.4	0.6	0.8	EER
100	FRR	1.05%	2.11%	5.26%	2.16%
	FAR	3.50%	1.89%	1.35%	
150	FRR	3.68%	4.21%	6.84%	4.21%
	FAR	6.74%	4.04%	2.96%	
200	FRR	9.47%	13.68%	18.42%	4.21%
	FAR	1.62%	1.08%	0.81%	

4.4 最终模型

由此当上述参数都取得最佳值时，可得到一个最终的模型，其两类错误率值如表4所示，对应的曲线如图3。其 EER 约为2.16%，从性能来看，还是比较满意的。

维普资讯 http://www.cqvip.com

表4 部分阈值时两类错误率值

阈值	0.2	0.4	0.5	0.6	0.8	0.9
FRR	1.05%	1.05%	1.58%	2.11%	5.26%	10.00%
FAR	5.12%	3.50%	2.43%	1.89%	1.35%	0.81%

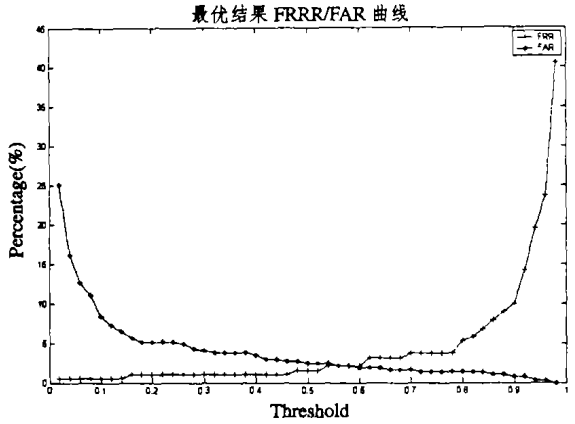

图3 两类错误率随阈值变化曲线

结论和进一步研究方向 综上所述，基于神经网络的动态手写签名验证模型能获得比较满意的结果，在最优的情况下 EER=2.16%，还是比较满意的。

只要保证神经模型能正常收敛，隐层结点数和传递函数类型对性能的影响不大。但相比之下，当隐层结点数约为输入结点数的1/5，传递函数为对数 Sigmoid 函数时，性能最佳。

本文的研究还存在不少不足之处，进一步的工作可以从以下方面展开：(1)研究如何能更有效地生成伪造签名。因各个特征之间有很大的相关性，本文采用的简单随机数生成法生成的签名，同实际书写而成的签名差别很大，不甚合理。(2)本文采用的神经网络结构比较简单，可以考虑采用更复杂和更先进的神经网络模型，以进一步提高系统的性能。(3)考虑为系统加入学习特性。

参 考 文 献

1 Plamondon R, Srihari S N. On-Line and Off-Line Handwriting Recognition: A Comprehensive Survey. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2000, 22(1): 63～84
2 Gupta J, McCabe A. A Review of Dynamic Handwritten Signature Verification. Feb. 2003. http://citeseer.nj.nec.com/gupta97review.html
3 Wu Q-Z, et al. On-line Signature Verification Using LPC Cepstrum and Neural Networks. IEEE Transactions on Systems, Man and Cybernetics, Part B, 1997, 27(1): 148～153
4 Julio Martinez-R, Rogelio Alcantara-S. On-line Signature Verification Based on Optimal Feature Representation and Neural-netwoek-driven Fuzzy Reasoning. Feb. 2003. http://citeseer.nj.nec.com/554379.html
5 Lyon R F, Yaeger L S. On-Line Hand-Printing Recognition with Neural Networks. In: Fifth Intl. Conf. on Microelectronics for Neural Networks and Fuzzy Systems, Lausanne, Switzerland, Feb. 1996
6 Higashino J. Signature verification system on neuro-computer. In: Proc. of 11th IAPR Intl. Conf. on Pattern Recognition. Vol. III. Conference C: Image, Speech and Signal Analysis, IEEE, 1992. 517～521
7 Tsend L Y, Huang T H. An online Chinese signature verification scheme. In: IJCNN Intl. Joint Conf. on Neural Networks, Vol. 3, IEEE, 1992. 624～630
8 袁余良，沈峰，杨飞，潘金贵. 一个基于 HMM 的动态手写签名认证系统的设计与实现. 模式识别与人工智能，2004，17(2)
9 haykin S. Neural Networks: A Comprehensive Foundation, Second Edition. Tsinghua University Press & Prentice Hall, 2001, 10: 161～175
10 Rowley H, Baluja S, Kanade. Neural Network-Based Face Detection. IEEE Transactions on Pattern Analysis and Machine Intelligence, 1998, 20(1): 23～38

(上接第169页)

记录，余下10%测试集包含282篇文档共1.16M，生成的事务数据库共有41816条记录。

我们分别比较了首字 hash 方法[6]和本文的 prefix-hash-tree 在上述数据集上的运行时间，实验结果见表1(注：表1所列时间均不包含写数据库的时间)。该结果表明本文所述方法在将中文文本转化为事务数据时所用时间要大大低于首字 hash 方法。在单字词的查找上这两种方法没有本质区别，都可以在 $O(1)$ 的时间内找到，但是对于二字以上的词，首字 hash 方法为了实现二分查找，对每个首字相同的儿子节点都采用数组实现，从而导致频繁的挪动操作，这正是该方法耗时的根源。

表1 实验结果对比表

	训练集上查询和插入时间(ms)	单篇文章处理时间(ms)	测试集上查询时间(ms)	平均单词查询时间(μs)
首字 hash 方法	1758	1.22	86	5.16
prefix-hash-tree	3083	0.69	216	2.06

本实验在 PentiumIV，RAM512M 机器上通过，OS 为 Windows2000，数据库采用 Microsoft SQL Server2000。

附注：本文的相关研究成果收录在第21届全国数据库学术会议论文集中。

参 考 文 献

1 Liu B, Hsu W, Ma Y. Integrating Classification and Association Rule Mining. [C]. In: The Fourth Intl. Conf. on Knowledge Discovery and Data Mining(KDD), New York, USA, 1998
2 Antonie M-L, Zaiane O R. Text Document Categorization by TermAssociation. [C]. In: Proc. of the IEEE Intl. Conf. on Data Mining, ICDM, Maebashi City, Japan, 2002. 19～26
3 王元珍，钱铁云，冯小年. 基于关联规则挖掘的中文文本自动分类[J]. 小型微型计算机系统，已录
4 孙茂松，左正平，黄昌宁. 汉语自动分词词典机制的实验研究[J]. 中文信息学报，2000，14(1)：1～6
5 杨文峰，陈光英，李星. 基于 PATRICIA tree 的汉语自动分词词典机制[J]. 中文信息学报，2001，15 (3)：44～49
6 陈桂林，王永成，韩客松，王刚. 一种高效的中文电子词表数据结构[J]. 计算机研究与发展，2000，37(1)：109～116
7 刘源，谭强，沈旭昆. 信息处理用现代汉语分词规范及自动分词方法. 清华大学出版社，1994