基于非参数回归和卷积神经网络的在线手写签名身份认证模型研究

报告人：郑滨彬

中国人民大学统计学院

December 1, 2017

- 王星，Phd，中国人民大学统计学院概率论与数理统计教研室主任、副教授。主要研究方向：大数据分析、网络挖掘、文献内容分析、图模型、数据挖掘应用。主要作品《非参数统计》、《大数据分析：方法与应用》、《统计学习导论-基于R的应用》、《人文社会科学文献网络知识模型》
- 郑滨彬，中国人民大学统计学院硕士二年级学生，目前主要研究方向包括卷积神经网络、函数型数据、变量选择
- 朱枫怡，中国人民大学经济学院硕士研究生
- 罗超，Phd，主要研究方向包括机器学习、签名识别

目录

CAPITAL OF STATISTICS
PROFESSION, HUMANITY & INTEGRITY
IT大咖说 知识共享平台

- 在线手写签名认证作为身份识别技术中的常用方法正受到越来越多的关注
- 卷积神经网络作为图片识别中常用的方法，用于对在线签名轨迹做静态识别
- 存在的问题:忽略了时间信息，可用信息变少；签名相较于一般图片识别问题，更容易受图片失真的影响
- 本次研究使用两种方法来处理该问题，提出了与时间信息的结合的方法，一是添加时间信息作为其中的输入维度、二是先使用基函数拟合再进行卷积神经网络
- 同时探究了样本自身结构对模型识别效果的影响

CAPITAL OF STATISTICS PROFESSION, HUMANITY & INTEGRITY
IT大咖说 知识共享平台

- 使用手写板进行签名从而完成数据收集
- 收集到数据是四元组$\{t, x, y, p\}$，每个签名轨迹的序列长度不定，由签名所用时长决定
- t代表该落笔点采集的时间，x, y代表该落笔点坐标，p代表手写笔是否离开手写板
- 共16个不同的签名，签名通过使用常用姓氏、常用名字进行随机组合，由实验人员书写
- 共522条数据，其中正签名348条、负签名174条

数据特点

与图像识别问题最大的不同在于，对于在线签名而言，受安全性、以及系统记录的影响，签名轨迹数据一般会有如下的特点：

- 每个签名记录的数据一般不会太多（样本量较少）
- 签名系统中以记录正签名为主、一般不记录负签名（正负签名的比例不平衡）
- 多次签名风格多变的签名会被认为无效

实际应用中关注的指标：

- 高准确率、低误判率（高TPR，低FPR）
- 用于训练的样本量尽量少
- 系统响应时间短

CAPITAL OF STATISTICS
PROFESSION, HUMANITY & INTEGRITY
IT大咖说 知识共享平台

- 对于在线签名真假识别问题，常用方法包括利用特征提取、再进行分类；使用马尔科夫模型等方法
- 本研究考虑尝试使用处理图片识别的卷积神经网络进行处理
- 卷积神经网络是静态图像识别的常用方法

卷积神经网络建模步骤一般分为两阶段：

- 第一阶段，利用所有数据，对网络结构进行训练(亦即提取特征)
- 第二阶段，利用第一阶段训列所得特征(亦即保留分类器之前的网络结构，截取最后的输出神经元作为输入空间)，针对每个签名单独训练模型

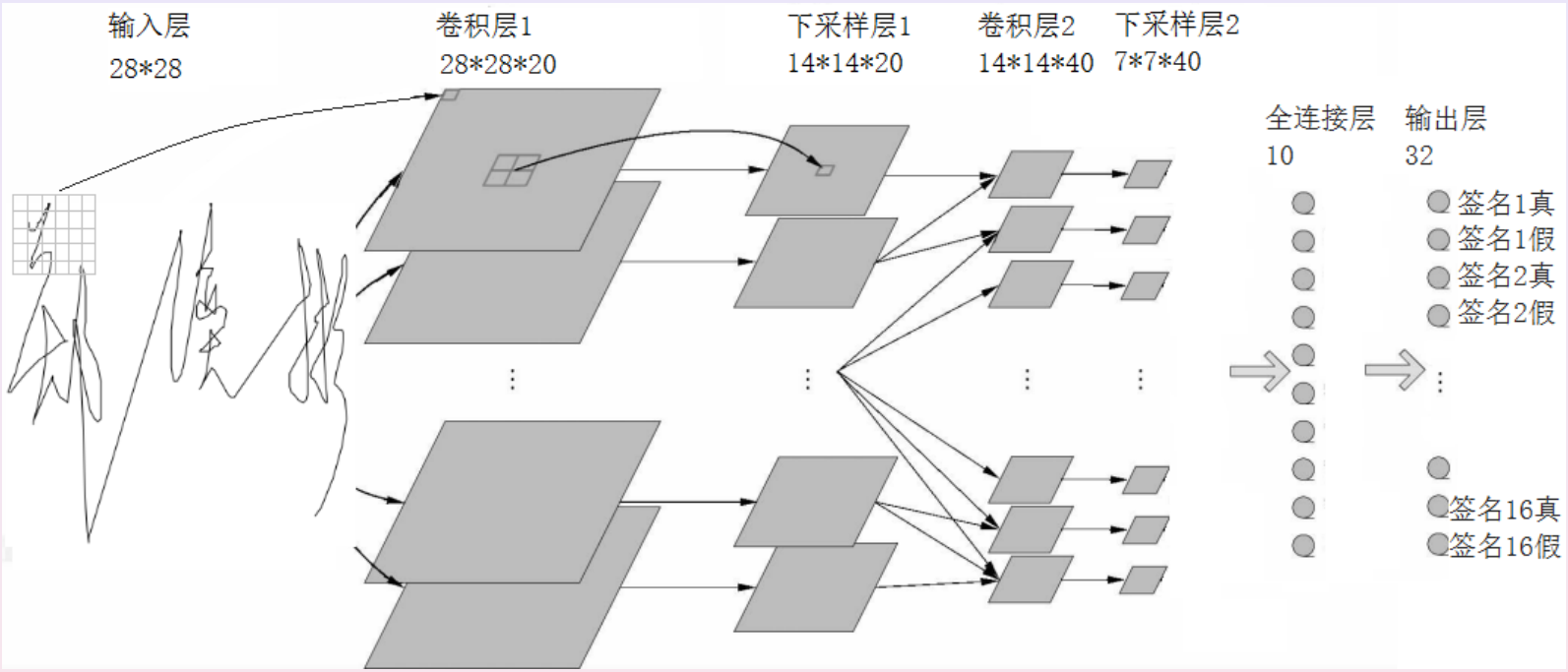


Figure 1：网络结构

使用卷积神经网络，从图片识别的角度来出来该问题，主要的问题在于忽略了时间信息。对于专业伪造的签名而言，签名是很相似的，但由于模仿时书写速度较慢，从时间上考虑则更容易发现

解决方法一：
通过利用记录中包含的时间信息，对签名轨迹数据计算在x轴y轴方向上的速度，将速度作为输入空间的一部分进行模型的训练

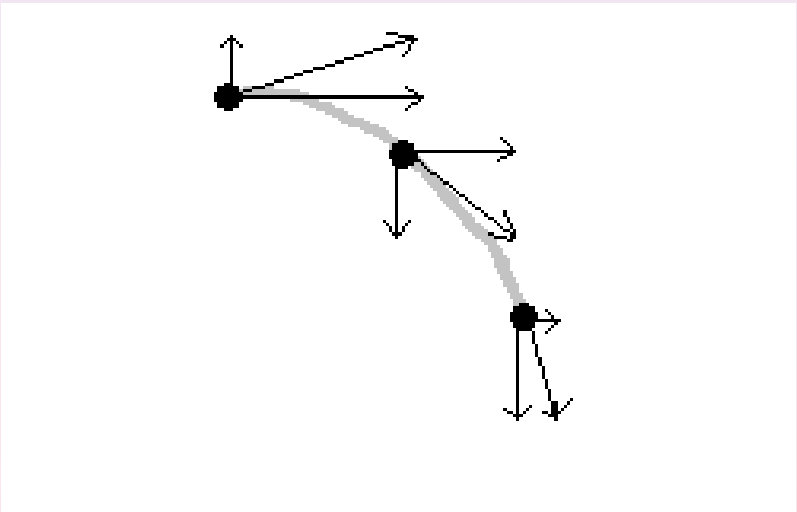


Figure 2 : 速度分解

解决方法二：
先使用基函数对签名进行拟合再进行识别，由于对轨迹序列$x(t), y(t)$进行拟合，亦即从时间上考虑了轨迹的问题

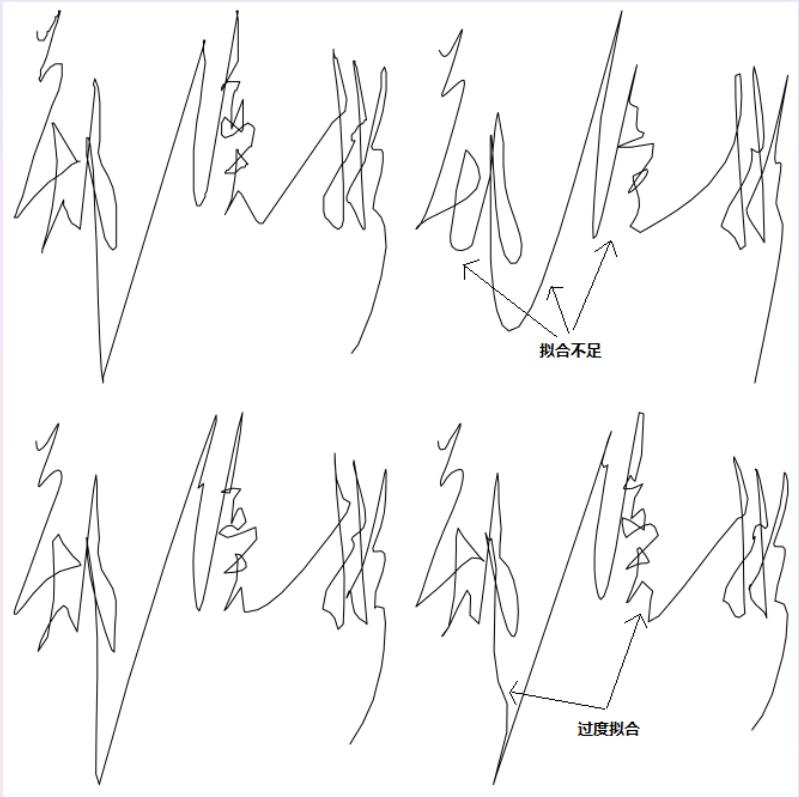


Figure 3：使用基函数拟合

影响模型识别效果的因素包括：

- 样本自身结构特点
  - 样本复杂度（方差）
  - 训练样本量
  - 训练正负样本比例
- 模型选择
  - 不同模型之间的差别
  - 卷积神经网络结构（如层数、卷积核个数、卷积核大小、神经元个数）

CAPITAL OF STATISTICS PROFESSION, HUMANITY & INTEGRITY
IT大咖说 知识共享平台

- 可以人工从笔画多少对签名的复杂度进行区分，下面从统计的角度，利用方差来进行分类
- 对于每个签名轨迹而言，可以看作由$\{x(t), y(t)\}$两个时间函数来决定的轨迹
- 进而,对于某一类签名中的其中一个签名，可以根据方差的计算公式

$$Var_i = \int (x_i(t) - \bar{x}(t))^2 \, dt, \bar{x}(t_0) = \frac{1}{n_i} \sum_{i}^{n_i} x_i(t_0)$$

- 在进行方差计算之前，对不同样本需要利用动态时间规整（DTW）进行时间上的对齐后，再利用上述公式进行计算，对于y进行同样的计算，最后进行相加，即可获得该类签名的方差，亦即其签名复杂度

CAPITAL OF STATISTICS
PROFESSION, HUMANITY & INTEGRITY
IT大咖说 知识共享平台

Table 1：不同正负比例对模型结果的影响

真：伪样本比例		7：1	4：4	1：7
正样本方差小 负样本方差小	TPR	0.992(0.019)	0.956(0.096)	0.913(0.129)
	FPR	0.465(0.284)	0.141(0.254)	0.117(0.192)
正样本方差小 负样本方差大	TPR	1.000(0.000)	0.943(0.122)	0.951(0.112)
	FPR	0.000(0.000)	0.177(0.294)	0.019(0.059)
正样本方差大 负样本方差大	TPR	0.971(0.051)	0.940(0.088)	0.902(0.206)
	FPR	0.441(0.285)	0.223(0.221)	0.127(0.186)

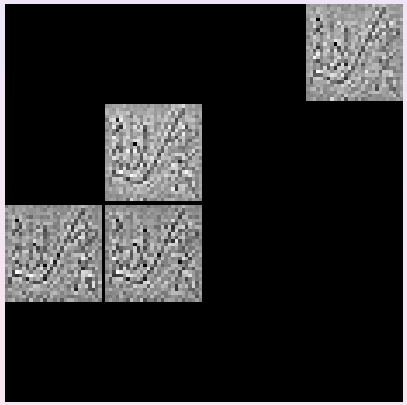
CAPITAL OF STATISTICS PROFESSION, HUMANITY & INTEGRITY
IT大咖说 知识共享平台

Table 2：不同卷积核个数对模型识别的影响

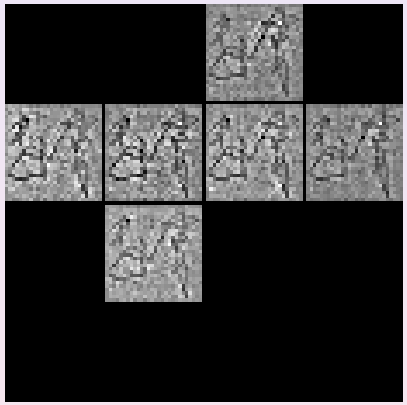
神经原层数、卷积核个数		模型1	模型2	模型3
正样本方差小	TPR	0.962(0.052)	0.816(0.172)	0.971(0.044)
负样本方差小	FPR	0.030(0.074)	0.103(0.122)	0.000(0.000)
正样本方差小	TPR	1.000(0.000)	1.000(0.000)	1.000(0.000)
负样本方差大	FPR	0.000(0.000)	0.000(0.000)	0.000(0.000)
正样本方差大	TPR	0.914(0.144)	0.971(0.044)	0.935(0.106)
负样本方差大	FPR	0.087(0.101)	0.041(0.483)	0.036(0.062)

模型1：一层神经元15
模型2：两层神经元15，20
模型3：两层神经元20，40

为更好地对卷积神经网络得到的结果进行深入理解，采用反卷积神经网络（deconvolutional network）的技术，对结果进行可视化

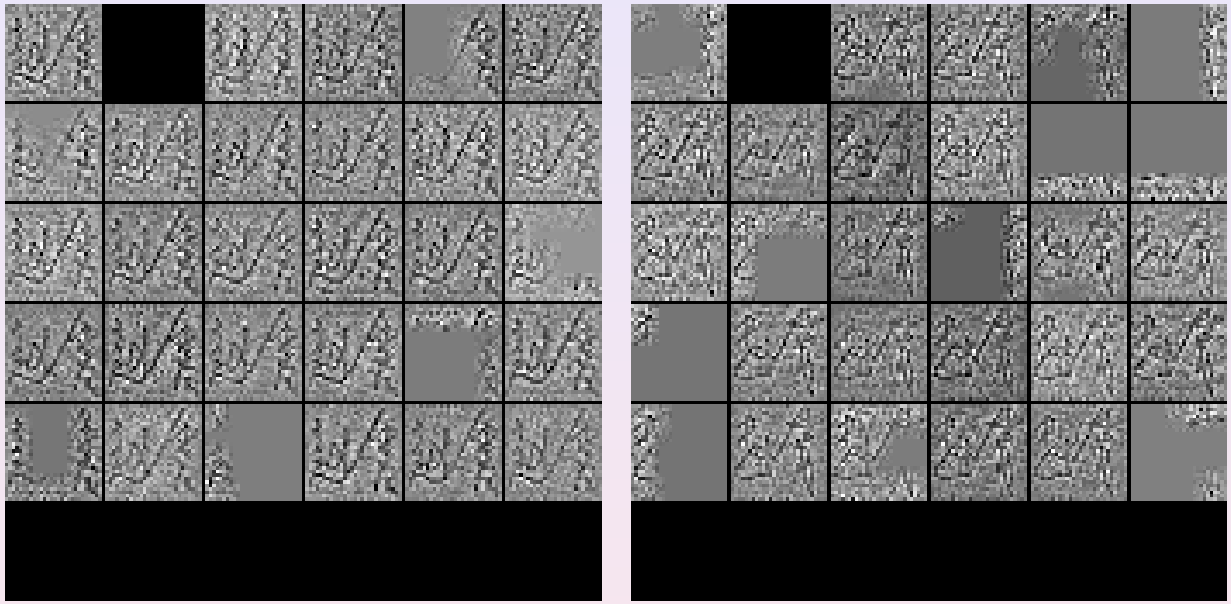


(a) 正签名



(b) 负签名

Figure 4：正负签名激活情况



(a) 正签名　　(b) 负签名

Figure 5：正负签名激活情况

CAPITAL OF STATISTICS
PROFESSION, HUMANITY & INTEGRITY
IT大咖说 知识共享平台

- 如一般对卷积神经网络的认识类似，浅层的卷积核主要处理边沿的信息、更深层次的卷积核才会进一步关注更细节的内容
- 从结果来看，对签名进行正负识别主要在于两部分：
  - 签名的主体轮廓
  - 局部的签名细节

CAPITAL OF STATISTICS
PROFESSION, HUMANITY & INTEGRITY
IT大咖说 知识共享平台

加上速度信息作为输入空间对模型识别效果的提升

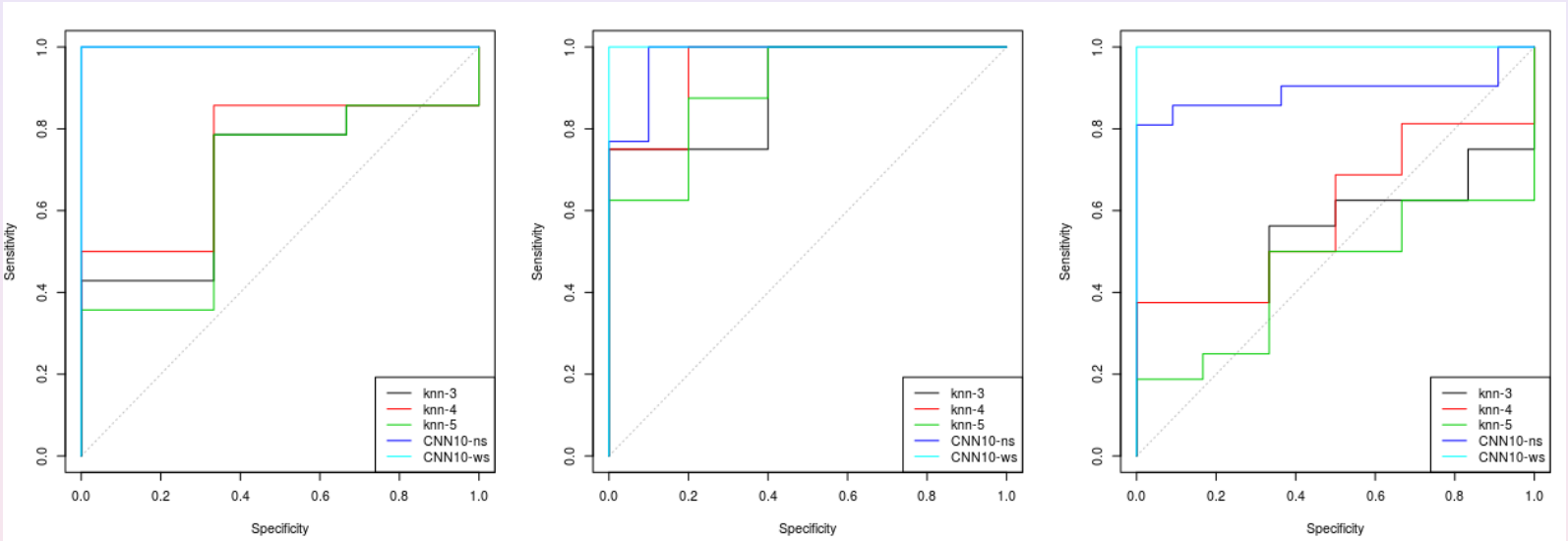
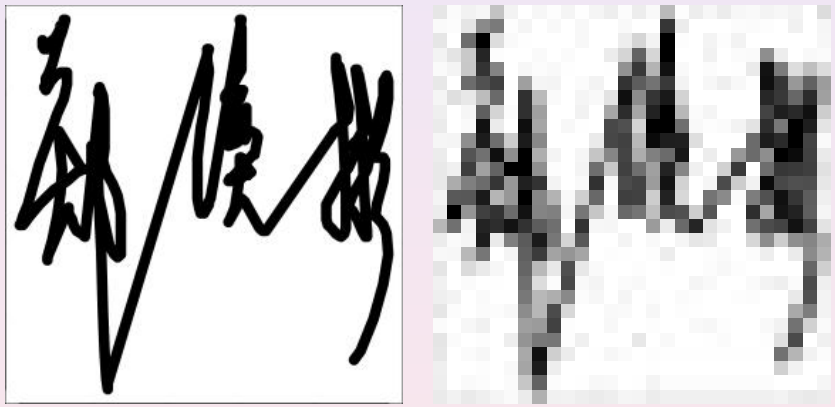


Figure 6：三种不同方差情况签名在不同模型下roc曲线对比

卷积神经网络模型已经取得了较好的识别结果，但目前发现主要问题有如下两个：

- 训练速度随着网络结构复杂度的提高而变慢
- 从图片的压缩角度来看，签名失真情况较明显



(a) 压缩前　　(b) 压缩后

Figure 7：失真情况

CAPITAL OF STATISTICS
PROFESSION, HUMANITY & INTEGRITY
IT大咖说 知识共享平台

- 先对轨迹序列$x(t), y(t)$进行拟合，再对拟合估计得到的参数进行卷积神经网络处理
- 该处理方法有两个好处：
  - 拟合的过程中，是考虑了时间序列中的时间信息，亦即相较于静态的图片识别，对参数进行卷积神经网络实际上是考虑了时间信息
  - 在实际处理过程中，自由度不需过高，已经对原始签名有较好的拟合效果；从而减小了输入空间，加快了训练模型的时间

CAPITAL OF STATISTICS PROFESSION, HUMANITY & INTEGRITY
IT大咖说 知识共享平台

Table 3 : 不同模型的时间对比

	spline+CNN	CNN
运算时间	10～20min	90～120min

Table 4 : 不同模型的识别效果对比

模型		spline+CNN	CNN
正样本方差小 负样本方差小	TPR	0.832(0.227)	0.971(0.044)
	FPR	0.224(0.149)	0.000(0.000)
正样本方差小 负样本方差大	TPR	0.915(0.100)	1.000(0.000)
	FPR	0.441(0.302)	0.000(0.000)
正样本方差大 负样本方差大	TPR	0.907(0.059)	0.935(0.106)
	FPR	0.304(0.259)	0.036(0.062)

结论

- 本次研究的方法较好了处理了在线签名识别问题，并发现了样本结构、网络结构对模型识别效果的影响
- 提出了综合利用时间信息的方法，利用时间信息确实对效果的提升有帮助
- 先利用拟合的方法对轨迹数据进行预处理，能有效的加快模型的训练速度

其他可行的方法：

- 使用专门针对时间序列的循环神经网络（RNN）来对签名数据进行处理
- 尽量减少模型训练样本的使用：如使用两样本配对、三样本配对等选取模板样本的方法；另外，用于处理仅有正样本的SVDD分类方法

- Gabe Alvarez, Blue Sheffer, and Morgan Bryant. Offline signature verification with convolutional neural networks.
- Luiz G Hafemann, Robert Sabourin, and Luiz S Oliveira. Learning features for offline handwritten signature verification using deep convolutional neural networks. Pattern Recognition, 70:163 – 176, 2017.
- Matthew D Zeiler, Graham W Taylor, and Rob Fergus. Adaptive decon- volutional networks for mid and high level feature learning. In Computer Vision (ICCV), 2011 IEEE International Conference on, pages 2018 – 2025. IEEE, 2011.
- Alan McCabe, Jarrod Trevathan, and Wayne Read. Neural network-based handwritten signature verification. Journal of computers, 2008, 3:9 – 22,.

- Luiz G Hafemann, Robert Sabourin, and Luiz S Oliveira. Written dependent feature learning for offline signature verification using deep convolutional neural networks. In Neural Networks (IJCNN), 2016 International Joint Conference on, pages 2576 – 2583. IEEE, 2016.
- Ronny Martens and Luc Claesen. On-line signature verification by dynamic time-warping. In Pattern Recognition, 1996., Proceedings of the 13th International Conference on, volume 3, pages 38 – 42. IEEE, 1996.
- Maged M M Fahmy. Online handwritten signature verification system based on DWT features extraction and neural network classification [J]. Ain Shams Engineering Journal, 2010 , 1 (1) :59-70
- 王星.非参数统计[M]. 北京：清华大学出版社，2014.10.

谢谢大家