

基于可区分性加权的模糊核说话人识别

林 琳, 王树勋, 陈 建

(吉林大学通信工程学院, 吉林长春 130022)

摘 要: 针对训练和识别语音数据较少的情况, 本文提出了一种新的说话人识别算法. 通过核映射, 在高维特征空间对说话人的语音特征进行模糊矢量量化. 为了增加说话人之间的可区分性, 提出了一种基于高维特征空间的码字矢量的权值分配方法, 对具有较强区分性的码字矢量分配较大的权值, 并将产生的权值和说话人的码书一起形成说话人数据库. 识别时, 提出一种模糊核加权最近邻近分类器, 在高维特征空间中对说话人进行匹配. 实验表明, 该算法在训练语音少于 8s, 识别语音为 1s 时, 能够得到较好的识别结果.

关键词: 说话人识别; 少量语音数据; 可区分性权值; 模糊核加权最近邻近分类器; 模糊核矢量量化

中图分类号: TN912.3 **文献标识码:** A **文章编号:** 0372-2112 (2008) 07-1446-05

A Fuzzy Kernel with Discriminative Weighted Method for Speaker Recognition

LIN Lin, WANG Shuxun, CHEN Jian

(College of Communication Engineering, Jilin University, Changchun, Jilin 130022, China)

Abstract: As to small amounts of training and test speech data, it proposed a new speaker recognition algorithm. By the kernel mapping, it used the fuzzy vector quantization to quantize the speakers' speech features in the high dimensional feature space. In order to improve the discriminations of different speakers, it presented a novel weights assignment method. It assigned the larger weight to the code vector with higher discriminative power. Then, it used the codebooks and weights to form the speakers' database. In the matching phase, it proposed a fuzzy kernel weighted nearest prototype classifier, which can identify different speakers in the high dimensional space. Experimental results show that when the training speech data is less than 8s, and test speech data is 1s, this algorithm can get good performance.

Key words: speaker recognition; small amounts of speech data; discriminative weighted value; fuzzy kernel weighted nearest prototype classifier; fuzzy kernel vector quantization.

1 引言

说话人识别是一种以语音对说话人进行区分, 从而进行身份鉴别与验证的技术. 目前, 大多数说话人识别系统仍然需要较长的语音文本以及大量的训练数据来建立话者模型. 尽管可以利用各种算法^[1]来减少系统的识别时间, 达到实用化, 但是对于那些只能获得少量说话人语音数据的应用场合, 这些系统就无能为力了. 因此利用尽可能少的训练和识别数据实现高性能的说话人识别, 更具有现实意义^[2]. 本文主要针对训练语音少于 8s, 识别语音为 1s 的说话人识别算法进行研究.

对于实时性要求较高、没有充分存储资源及计算资源可供利用的场合, 矢量量化法较高斯混合模型(Gaussian Mixture Model, GMM)能够得到更好的识别性能^[3]. 随着模糊集理论和模糊聚类方法的发展, 基于软划分的模糊 C-均值(Fuzzy C-Means, FCM)聚类的思想^[4,5]被引入到说话人识别中, 得到了优于矢量量化法的识别效

果. 然而, FCM 法对初值十分敏感, 容易陷入局部极小值, 为此文献[6~8]利用全局搜索技术对算法进行改进, 改善了说话人识别系统的性能. 由于 FCM 法假设样本为超球体分布, 对于非超球体数据结构不能奏效, 因此, 张铃华等^[9]在假设数据分布为超椭圆型的基础上, 提出了一种基于模糊超椭圆聚类的说话人识别算法, 进一步改善了说话人识别系统的性能. 但是说话人的语音特征分布复杂, 不能事先确定其具体的数据结构, 因此特定数据结构, 如超球型、超椭圆型数据分布的假设, 都不能对复杂说话人的语音特征分布进行更准确地描述. 因此, Lin. J^[10]在矢量量化中引入模糊核聚类的方法^[11], 通过非线性映射, 扩大了模式类之间的差异, 在训练语音和识别语音较少时, 得到较好的识别效果. 不同音素的研究表明, 语音信号的不同部分在不同说话人之间有唯一的区分特性, 也就是说, 说话人之间某些音的变化与其他音有明显的不同^[12]. 因此, 为了在少量训练和识别语音的情况下, 进一步增加说话人之间的可区

分性, 本文提出了一种基于可区分性加权的模糊核说话人识别方法. 利用模糊核矢量量化在高维特征空间中对说话人的语音特征进行训练. 同时, 为了更好地利用说话人语音变化的差异性, 根据高维特征空间中不同参考模型之间的关系, 提出了一种新的权值分配方法. 这种方法不需要知道任何关于特征矢量和音素区分性能的先验知识, 就能适应给定数据库中特征矢量的统计特性. 然后, 利用产生的权值和说话人的码书形成说话人数据库. 在识别阶段, 提出了一种模糊核加权最近邻分类器的匹配方法. 由于说话人模型的训练和识别过程都是在高维特征空间中进行的, 同时增加了可区分性加权的思想, 使得说话人识别系统的性能进一步提高.

2 特征空间中的模糊最近邻分类器

设测试矢量集合 $X = \{x_k\}$, $k = 1, \dots, N$, 参考说话人的码书集合为 $V = \{V_1, V_2, \dots, V_q\}$, $q = 1, \dots, Q$, 其中第 q 个说话人码书 V_q 的第 i 个码字矢量为 $v_i(q)$, $q = 1, \dots, Q$, $i = 1, \dots, c$, 则计算矢量 x_k 与码书 V_q 之间的失真 $d(x_k, V_q)$, 最简单的方法就是定义 $d(x_k, V_q)$ 为矢量 x_k 与码书 V_q 中最临近码字之间的距离

$$d(x_k, V_q) = \min_{1 \leq i \leq c} d(x_k, v_i(q)) \quad (1)$$

这里使用欧式距离计算 $d(x_k, v_i(q))$.

由于算法中引入了模糊聚类的思想, 因此定义使模糊目标函数 $J_m(x_k, V_q)$ 最小的 $d(x_k, V_q)$ 为

$$d(x_k, V_q) = \min_u \sum_{i=1}^c u_{ik}^m(q) d^2(x_k, v_i(q)) \quad (2)$$

其中 $u_{ik}(q)$ 为矢量 x_k 隶属于码书 V_q 第 i 类的程度, 满足

$$0 \leq u_{ik}(q) \leq 1; \sum_{i=1}^c u_{ik}(q) = 1 \quad (3)$$

当模糊目标函数 $J_m(x_k, V_q)$ 最小时, $u_{ik}(q)$ 为

$$u_{ik}(q) = \left[\sum_{j=1}^c [d(x_k, v_i(q)) / d(x_k, v_j(q))]^{2/(m-1)} \right]^{-1} \quad (4)$$

将上式带入式(2), 得到模糊目标函数最小时, 矢量 x_k 与码书 V_q 之间的失真

$$d(x_k, V_q) = \left\{ \sum_{i=1}^c [d(x_k, v_i(q))]^{2/(m-1)} \right\}^{(1-m)} \quad (5)$$

如果引入核方法, 使用非线性映射 $\Phi(\cdot)$ 把输入模式矢量空间变换到一个高维特征空间, 则高维特征空间中, 矢量 x_k 与码书 V_q 之间的失真 $d_K(x_k, V_q)$ 可以表示为

$$d_K(x_k, V_q) = \left\{ \sum_{i=1}^c [d_K(x_k, v_i(q))]^{2/(m-1)} \right\}^{(1-m)} \quad (6)$$

$$d_K^2(x_k, v_i(q)) = K(x_k, x_k) - 2K(x_k, v_i(q)) + K(v_i(q), v_i(q)) \quad (7)$$

其中 $K(x_k, v_i(q))$ 为矢量 x_k 与 $v_i(q)$ 的核函数矩阵. 文中采用高斯核函数, 其中 σ 为高斯核宽度.

$$K(y, z) = \exp\left[-\frac{\|y, z\|^2}{2\sigma^2}\right] \quad (8)$$

对于给定的待识别语音特征矢量序列 $X = \{x_1, x_2, \dots, x_N\}$, 定义特征空间中矢量的平均量化失真为目标函数

$$J_m^\Phi(X, V_q) = \frac{1}{N} \sum_{k=1}^N d_K(x_k, V_q) \quad (9)$$

对于说话人辨认而言, 选择目标函数值 $J_m^\Phi(X, V_q)$ 最小的码书所对应的说话人作为系统的识别结果, 即

$$\text{Result} = \arg \min_{1 \leq q \leq Q} \left(J_m^\Phi(X, V_q) \right) \quad (10)$$

3 特征空间中的可区分性加权匹配

3.1 特征空间中的加权模糊目标函数

在利用码书对说话人进行表征时, 码书中不同的类别可以表示不同的声学单元, 因此如何利用不同音素之间区分能力的问题就转换成: ①如何对不同码书的码字矢量进行权值分配; ②如何在匹配过程中利用权值对目标函数进行计算. 针对上述两个问题, 本文首先提出了一种特征空间中加权目标函数的匹配方法. 下面来看一个例子. 图 1 给出了三个不同参考说话人的特征矢量分布情况, 其中分别使用“□”、“○”、“△”来表示三个说话人, 未知说话人的特征矢量用“★”来表示. 从图中可以看出, 未知说话人的特征矢量主要分布成三类: 右上角区域、左上角区域、右侧中间区域. 右上角区域包含所有参考说话人的码字矢量, 因此仅从这一区域无法判断未知说话人是来自哪个参考说话人, 可以说这一区域的参考说话人码字矢量没有区分性. 左上角区域相对好些, 从特征矢量的分布情况可知, 未知说话人不是来自说话人“△”, 这一区域的码字矢量区分性较右上角区域强些. 而右侧中间区域的码字矢量区分性最强, 可以明显地看出未知说话人是来自说话人“□”.

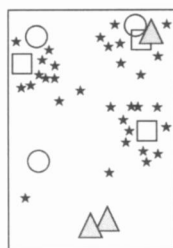


图 1 具有不同区分性码字矢量的图解

从图中可以看出, 未知说话人的特征矢量主要分布成三类: 右上角区域、左上角区域、右侧中间区域. 右上角区域包含所有参考说话人的码字矢量, 因此仅从这一区域无法判断未知说话人是来自哪个参考说话人, 可以说这一区域的参考说话人码字矢量没有区分性. 左上角区域相对好些, 从特征矢量的分布情况可知, 未知说话人不是来自说话人“△”, 这一区域的码字矢量区分性较右上角区域强些. 而右侧中间区域的码字矢量区分性最强, 可以明显地看出未知说话人是来自说话人“□”.

从上面的分析可知, 不同码字矢量其区分能力不同, 因此目标函数的定义中还应该考虑每个码字的区分能力, 定义特征空间中的加权模糊目标函数为

$$J_m^\Phi(X, V_q, W_q) = \left\{ \sum_{k=1}^N [f(w_{NN[x_k]}^\Phi) d_K(x_k, V_q)]^{2/(1-m)} \right\}^{(1-m)} \quad (11)$$

这里 $w_{NN[x_k]}^\Phi$ 是高维特征空间中与最临近码字相关的权值函数, 函数 f 是 $w_{NN[x_k]}^\Phi$ 的非增函数. 假设 $d_K(x_k, V_q)$ 不变, 当码字的区分能力较强时, $w_{NN[x_k]}^\Phi$ 值较大,

$f(w_{NN[x_k]})$ 值较小, 则得到的目标函数值较小. 反之, 当码字的区分能力较差时, 得到的目标函数值较大. 因此乘积 $f(w_{NN[x_k]}) d_K(x_k, V_q)$ 可以看作是一个将判决平面移向具有较强区分性码字的局部操作. 特征空间中的加权目标函数, 可以使那些同时属于多个说话人码字矢量的特征矢量、与任何码字矢量都不能进行很好匹配的离群点和噪声矢量对匹配结果产生较小的影响.

在加权模糊目标函数的设计中, 主要有两个问题需要解决: (1) 如何进行码字矢量权值的分配; (2) 函数 f 的选择. 由式(11)可知, 函数 f 是 $w_{NN[x_k]}$ 的非增函数, 因此在文中, 选择函数 f 为指数减函数

$$f(w) = e^{-\alpha w} \quad (12)$$

这里 $\alpha > 0$ 为衰减因子.

3.2 特征空间中权值的分配

假设 $v_i(q) \in V_q, q = 1, \dots, Q, i = 1, \dots, c$ 为第 q 个说话人的第 i 个码字矢量, 则在特征空间中可以表示为 $\Phi(v_i(q))$. 文中对每个码字的每个码字矢量分配一个权值, 则特征空间中第 q 个码字的权值矢量可表示为

$$\begin{aligned} W_q &= \{w(\Phi(v_1(q))), w(\Phi(v_2(q))), \dots, w(\Phi(v_c(q)))\} \\ \text{定义 } NN^{(t)}, t \neq q, t = 1, \dots, Q \text{ 为第 } q \text{ 个码字中第 } i \text{ 个码字的最近邻近码字的索引, 则 } \Phi(v_i(q)) \text{ 的权值为} \\ w(\Phi(v_i(q))) &= \frac{1}{\sum_{t=1, t \neq q}^Q (1/d_K(\Phi(v_i(q)), \Phi(v_{NN^{(t)}}(t))))} \\ &= \frac{1}{\sum_{t=1, t \neq q}^Q (1/d_K(v_i(q), v_{NN^{(t)}}(t)))} \quad (13) \end{aligned}$$

如果 $d_K(v_i(q), v_{NN^{(t)}}(t)) = 0$ 则 $w(\Phi(v_i(q))) = 0$

从上式可以看出, 计算码字矢量的权值首先要找到其它码字中该码字的最近邻近码字, 然后将它们之间的距离取倒数和, 再取反. 码字矢量的权值主要依赖于高维特征空间中该码字与其它码字中最近邻近码字之间的距离 $d_K(v_i(q), v_{NN^{(t)}}(t))$. 如果 $d_K(v_i(q), v_{NN^{(t)}}(t))$ 较大, 则计算得到的权值较大, 码字的区分能力较强, 反之, $d_K(v_i(q), v_{NN^{(t)}}(t))$ 较小, 则码字的区分能力较弱. 这是由于当待识别矢量分布在某个码字周围时, 如果码字与其它各码字的最近邻近码字距离较大, 就会使待识别矢量很容易被识别, 因此它具有较强的区分性, 反之, 如果码字与其它各码字的最近邻近码字距离较小, 则无法判断待识别矢量到底属于哪个码字, 码字的区分性较弱.

码字权值的形式实际上是在训练阶段的一种后处理计算, 它是在所有参考说话人的码字形成后确定的, 与说话人的码字一起形成说话人的数据库, 因此并没有增加匹配过程的计算量.

4 实验和结果分析

实验中采用的语音数据为 PKU-SRSC 语音数据库^[13], 进行与文本无关的说话人辨认实验. 从数据库中任选 20 个说话人(10 个男生和 10 女生)为合法用户, 使用每个说话人的 6 次录音数据, 其中每次录音的间隔为一周. 选择其中第一次录音的部分语音作为训练语音, 其余的所有语音作为识别语音, 每个识别语音约为 1s 左右. 提取 20 维的 Mel 倒谱系数及其一阶动态倒谱系数共 40 维, 去掉第一维, 将剩下的 39 维作为说话人的特征参数. 采用分裂法产生初始码书.

实验 1: 衰减因子对 α 识别结果的影响

在计算特征空间加权模糊目标函数时, 需要确定指数减函数的衰减因子 α 的大小, 因此利用用户第一次录音约 5s 的语音数据进行训练. 取码本容量为 8, 训练和识别模糊加权指数分别为 1.15 和 1.05. 根据文献^[10], 高斯核宽度 σ 取 4. 考察不同衰减因子 α 对算法识别性能的影响. 图 2 给出了在码本容量为 8 时, 系统错误率随衰减因子 α 的变化曲线.

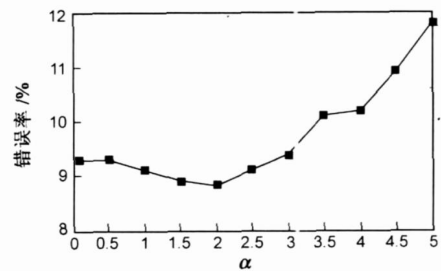


图 2 系统错误率随衰减因子 α 变化曲线图

从图 2 中可以看出, 当衰减因子 $\alpha < 2$ 时, 系统错误率随着 α 的减小而逐渐增大, 当 $\alpha \leq 0.5$ 时系统错误率趋于平稳; 当 $\alpha > 2$ 时, 系统错误率随着 α 的增大而增大; 当 $\alpha = 2$ 时, 系统错误率最小, 识别效果最好. 这主要是由于当 $\alpha \rightarrow \infty$ 时, 函数 f 的值趋于 0, 计算得到的特征空间中加权模糊目标函数 $J_m^\Phi(X, V_q)$ 值趋于 0, 此时说话人之间的可区分性减小, 因此导致识别效果的下降. 当 $\alpha \rightarrow 0$ 时, 函数 f 的值趋于 1, 此时特征空间中的加权模糊目标函数 $J_m^\Phi(X, V_q)$ 退化为没有进行加权的模糊目标函数, 因此取衰减因子 $\alpha = 2$.

实验 2: 不同方法误识率比较

为了验证特征空间中模糊区分性加权匹配方法的有效性, 将本文提出的区分性加权模糊核矢量量化 DWFQVQ (Discriminative Weighted Fuzzy Kernel Vector Quantization) 算法与文献^[10]算法进行比较. 使用 3s~8s 的训练语音, 1s 的识别语音, 比较两种算法在不同码本容量下的错误率, 如图 3 所示. 其中图 3(a)、(b)、(c) 分别代表码本容量为 16、32、64 时两种算法的错误率比较图, 横坐标表示训练语音的长度, 纵坐标表示系统得到

的错误率。从图中可以看出, DWFKVQ 算法在不同码本容量下, 使用 3s~ 8s 的训练语音, 都能得到较低的错误率, 可见特征空间中区分性加权匹配方法能够进一步增加说话人之间的可区分性, 提高系统的性能。

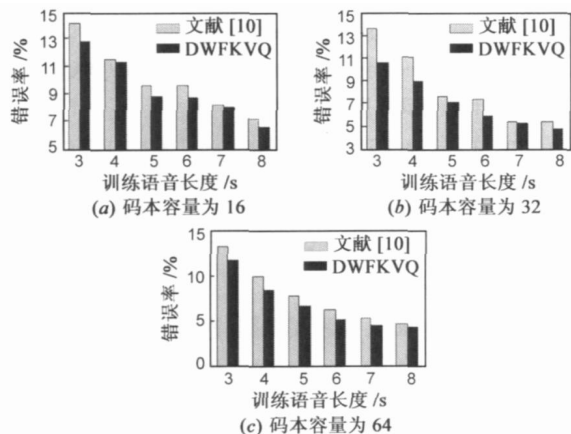


图 3 DWFKVQ 和文献 [10] 算法在不同码本容量时的错误率曲线

为了验证本文提出的算法在较短训练语音的情况下, 能够更好地描述说话人的特征分布, 将 DWFKVQ 算法与目前说话人识别中较流行的高斯混合模型(GMM)法进行比较。比较不同长度训练语音条件下两种算法的错误率, 这里取码本容量(高斯混合度)为 16 和 32, 训练语音长度为 3s~ 12s。高斯混合模型的初始参数使用随机初始值的 K-均值方法确定, 同时使用方差下限补偿训练数据不充足的条件, 对 GMM 进行 10 次训练和识别实验, 统计其平均的错误率, 错误率比较曲线如图 4 所示。其中图 4(a)和图 4(b)分别给出了码本容量为 16 和 32 时系统错误率的对比图。

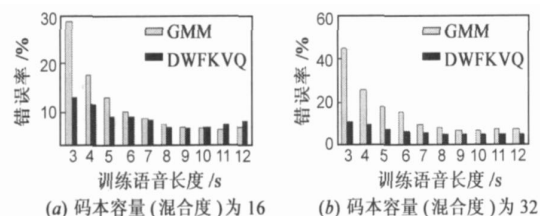


图 4 DWFKVQ 和 GMM 在不同码本容量时的错误率曲线

从图 4 中可以看出, 在码本容量(混合度)为 16 时, 当训练语音少于 10s 时, 由于基于统计特性的 GMM 在训练数据较少时, 模型参数的估计偏差会大大增加, 因此本文的方法优于 GMM 法。随着训练语音的增长, GMM 模型参数的估计更加准确, 因此在训练语音大于等于 10s 时, GMM 法优于本文算法。尽管训练语音增长能够增加 GMM 模型的估计精度, 但随着混合度的增加, 估计每个混合度的特征个数相对减少, 因此, 在码本容量(混合度)为 32 时, 本文算法在使用 3s~ 12s 的训练语音都能得到较 GMM 法更优的识别结果。可见, 本文提出的算法在训练语音少于 10s 时的说话人系统中体现出

了较强的优势。

5 结论

提出了一种可区分性加权的模糊核说话人识别算法。使用模糊核矢量量化对说话人的语音特征进行训练, 增加了语音特征模式的线性可分性概率。为了更好地利用说话人语音变化的差异性, 提出了一种高维特征空间码字权值的分配方法, 对具有较强区分性的码字矢量分配较大的权值, 并将产生的权值和说话人的码书一起形成说话人数据库。识别时, 在特征空间中进行模型与识别矢量之间的可区分性加权匹配。通过实验, 研究了算法中衰减因子 α 与系统错误率之间的关系。在与文献[10]算法、GMM 算法分别进行的对比实验中, 本文算法在训练语音小于 8s, 识别语音为 1s 的情况下, 均能得到较好的识别效果, 验证了算法的有效性。本文的算法在码本容量为 32, 训练语音约 8s, 识别语音约 1s 时, 其误识率可以达到 4.8%, 可见该算法在短语音说话人识别系统中能够得到较好的识别结果。尽管如此, 但是当训练语音为 3s, 识别语音为 1s 时, 系统的识别效果还不是很理想, 因此如何利用说话人的语音数据对说话人进行可区分性训练, 从而进一步提高短语音说话人识别系统的性能, 还是一个待解决的问题。

参考文献:

- [1] Tomi Kinnunen, Evgeny Karpov, Pasi Fäntti. Real Time speaker identification and verification[J]. IEEE Transactions on Audio, Speech, and Language Processing, 2006, 14(1): 277- 288.
- [2] Yang Yao yuan, Chen Wei, Lu Yur dong, . etc. Research of speaker identification based on little training data[A]. Proceeding of the 3rd International Conference on Machine Learning and Cybernetics[C]. Shanghai: IEEE Press, 2004. 26- 29.
- [3] Matsui T, Furui S. Comparison of text independent speaker recognition methods using VQ-distortion and discrete/ continuous HMMs[A]. Proceeding of IEEE International Conference on Acoustic, Speech, Signal Processing[C]. San Francisco: IEEE Press, 1991. 11- 157- 160.
- [4] Tran D, Wagner M, Van Le T. A proposed decision rule for speaker recognition based on fuzzy c means clustering[A]. 5th International Conference on Spoken Language Processing, IC-SLP' 98[C]. Sydney Australia: Australian Speech Science and Technology Association, Incorporated (ASSTA), 1998. 755 - 758.
- [5] 吴晓娟, 韩先花, 聂开宝. 模糊 C-均值(FCM)聚类算法与矢量量化法相结合用于说话人识别[J]. 电子与信息学报, 2002, 24(6): 845- 849.

Wu Xiao juan, Han Xian hua, Nie Bao kai. Speaker recognition using fuzzy C-mean clustering algorithm and vector quantization

- Algorithm[J]. Journal of Electronics and Information Technology, 2002, 24(6): 845–849. (in Chinese)
- [6] 王成儒, 王金甲. 模糊 G 均值聚类新算法在说话人辨认中的应用[J]. 计算机工程与应用, 2003, 39(27): 94–95, 140. Wang Cheng ru, Wang Jin jia. Novel algorithm of fuzzy G-mean clustering for speaker identification[J]. Computer Engineering and Applications, 2003, 39(27): 94–95, 140. (in Chinese)
- [7] 董国华. 一种改进的聚类算法及其在说话人识别上的应用[J]. 微机计算机信息(测控自动化), 2004, 20(9): 134–136. Dong Guo hua. A modified clustering algorithm and its application for speaker recognition[J]. Control & Automation, 2004, 20(9): 134–136. (in Chinese)
- [8] 林琳, 王树勋. 基于遗传模糊聚类分析的说话人识别方法及其仿真研究[J]. 系统仿真学报, 2006, 18(8): 2338–2341. Lin Lin, Wang Shu xun. A speaker recognition method based on genetic fuzzy clustering analysis and its simulation study[J]. Journal of System Simulation, 2006, 18(8): 2338–2341. (in Chinese)
- [9] 张玲华, 杨震, 郑宝玉. 基于模糊分类器及多层前馈神经网络混合结构的说话人辨认[J]. 通信学报, 2005, 26(11): 68–75. Zhang Hua lin, Yang Zhen, Zheng Bao yu. Hybrid architecture based on fuzzy classifier and multiplayer feed forward neural network for speaker identification[J]. Journal of Communication, 2005, 26(11): 68–75. (in Chinese)
- [10] Lin Lin, Wang Shu xun. A kernel method for speaker recognition with little data[A]. The 8th International Conference on Signal Processing(ICSP'06)[C]. Beijing: IEEE Press, 2006. 1: 716–719.
- [11] Wu Zhong dong, Xie Wei xin, Yu Jiarping. Fuzzy c-means clustering algorithm based on kernel method[A]. Computational Intelligence and Multimedia Application(ICCIMA2003)[C]. Xi'an: IEEE Press, 2003. 49–54.
- [12] Tomi kinnunen, Pasi Fänti. Speaker discriminative weighting method for VQ based speaker identification[A]. Proc. 3rd International Conference on Audio and Video Based Biometric Person Authentication (AVBPA)[C]. Halmstad, Sweden: Springer, 2001. 150–156.
- [13] 吴玺宏. 一个面向说话人识别的汉语语音数据库[OL]. <http://nlpr.web.ia.ac.cn/english/irds/chinese/sinobiometricspdf/wuxihong.pdf>, 2002.

作者简介:



林琳女, 1979年7月出生于辽宁省大连市. 2007年获得吉林大学通信工程学院博士学位. 现为吉林大学通信工程学院讲师. 主要研究方向为说话人识别、语音信号处理、DSP技术.
E-mail: go_onlin@yahoo.com.cn

王树勋 (见本期第 1328 页)

(上接第 1472 页)

- [11] S D Galbraith, K Harrisons, D Soldera. Implementing the Tate pairing[A]. In Algorithmic Number Theory 5th International Symposium, LNCS 2369[C]. Berlin: Springer, 2002. 324–337.
- [12] The pairing based Crypto Lounge[OL]. <http://planeta.terra.com.br/informatical/paulobarreto/pblounge.htm>
- [13] 吴问娣, 曾吉文. 一种无证书的环签名方案和一个基于身份的多重签名方案[J]. 数学研究, 2004, 39(2): 44–52. Wu Wendi, Zeng Jiwen. A Certificateless Ring Signature Scheme and an ID Based Multisignature Scheme from Multilinear Forms[J]. Journal of Mathematical Study, 2004, 39(2): 44–52. (Chinese Source)
- [14] Xinyi Huang, Willy Susilo et al. On the Security of Certificateless Signature Scheme from Asiacypt 2003[A]. 4th international conference, CANS 2005. LNCS 3810[C]. Berlin: Springer, 2005. 13–25.
- [15] Sherman S M Chow et al. Identity Based Threshold Ring Signature[A]. In Proc. ICISC 2004, LNCS 3506[C]. Berlin: Springer, 2005. 218–232.
- [16] M Au, J Chen, J Liu et al. Malicious KGC attacks in certificateless cryptography[A]. In Proc. Asiaccs 2007[C]. ACM Press, 2007. 302–311. <http://eprint.iacr.org/2006/255/>.