计算机科学2002Vol. 29№. 11

一个在线手写签名身份认证系统的设计与实现*)

The Design and Implementation of An On-line Handwritten Signature Verification

杨 飞 沈 峰 袁余良 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)

Abstract With the development of computer network, Biometrics, as a kind of information security techniques, is thought more and more of. Handwritten signature verification is an effective one. This paper introduces the design and implementation of an on-line handwritten signature verification system which is based on dynamic programming matching algorithm and give a brief evaluation of its performance. The performance of the system is satisfying according to the experiment.

Keywords Biometrics ,Handwritten signature verification, Dynamic programming matching

1. 引言

由于传统的口令方式的身份认证策略不具有个人的特征,容易被窃取,因而安全性无法保障。所以基于生物认证技术的应用获得广泛推崇。生物认证技术是指基于人的生物学特征进行个人身份认证的研究领域,如视网膜或虹膜认证,指纹认证,人脸认证,语音认证,手写体签名认证等。

关于签名认证,根据数据的获取方法,可以分为两类:离线签名认证和在线签名认证。离线签名认证视签名为静态数字图像。在线签名认证使用特殊的硬件设备如数字手写板,记录笔的运动,签名被视为多通道数字信号。Nalwa[1]认为签名的动态信息(速度,加速度等)不如静态信息(字形信息)稳定,认证应该以字形信息为主。Hastie[6]曾使用隐马尔科夫模型(HMM)比较离线签名认证和在线签名认证,发现在线签名认证效果较好。

本文介绍一个在线手写签名身份认证(On-line Handwritten Signature Verification)系统的设计、实现及其性能评价。

2. 系统结构及处理流程

本系统包括6个模块:预处理模块、特征抽取模块、注册(Enroll)模块、匹配模块、阈值(Threshold)选择模块和验证模块,它们之间的关系及处理流程如图1所示。

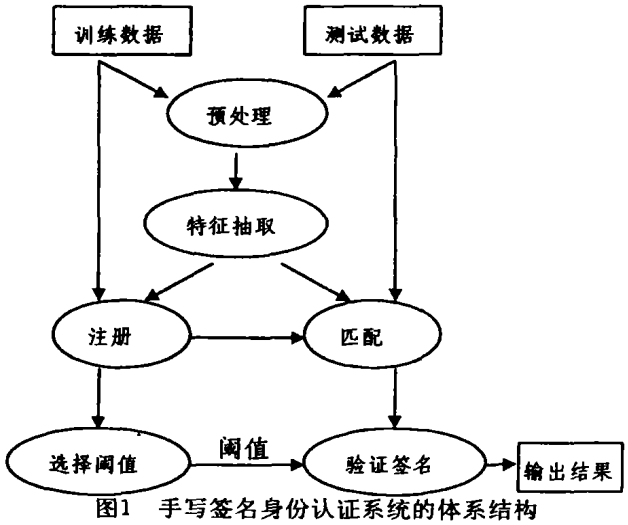

图1 手写签名身份认证系统的体系结构

3. 系统的实现及关键技术

在线手写签名身份认证的实现方法大致包括:基于匹配的方法[2],基于 Hidden Markov 模型的方法[5,7],神经网络方法[3],统计学方法等等。

本系统采用动态规划匹配算法,认证就是通过一定的验证策略辨别真伪的过程。

3.1 数据获取

本系统采用 WACOM 公司的数字手写板作为数据获取设备,以100Hz 或200Hz 采样频率(可设定)记录采样点的空间特征以及压力。从数字手写板获得的数据是一组多通道数字信号,我们称之为原始特征向量,表示为:(x_i, y_i, p_i, t_i), $i \in [1, N]$,其中 x, y 表示位置,p 表示压力,t 表示从第一个采样点开始计的时间。$p_1 \neq 0, p_N \neq 0; t_{i+1} - t_i = S, i \in [1, N-1]$,S 为采样间隔,是常量,本系统中 $S = 10ms$。

3.2 预处理

预处理包括三个步骤:重采样,规范化,平滑化[2]。

3.2.1 *重采样* 原始采样数据中包含了冗余信息,因此需要进行重采样。重采样是对所有的原始采样点按照一定的采样距离重新抽取的过程。本系统中采样距离为4,即从每4个原始采样点中抽取一个作为记录签名信息的特征点序列。为了使重采样后的特征点序列仍然符合等时间间隔的条件,我们采取的抽取方法是:假设原始特征点的下标为 $i, i = 0, 1, 2 \cdots$,取 $i \bmod 4 = 0$ 的特征点,并重新从0开始递增编号。原始特征向量是不适合直接拿来进行匹配的,必须扩展它,可以从原始特征向量中计算出局部特征和全局特征。原始特征向量是:(x_i, y_i, p_i), x, y 是经过旋转的坐标值,p 仍旧是压力值,常量 t 去掉。容易算出 x, y 两个方向的速率,可以把原始向量扩展为 $(x_i, y_i, vx_i, vy_i, p_i)$ 作为局部特征向量,vx, vy 分别是 x 方向和 y 方向的速率。全局特征包括:总笔划数,笔划总长度,签名时间,x 方向的平均速率,y 方向的平均速率,平均压力,x 方向速率方差,y 方向的速率方差,压力方差,于是得到一个9维的全局特征向量 $G = (g_1, g_2, \cdots, g_9)^T$。还可以计算许多其他全局特征[4]。

3.2.2 *规范化* 考虑到系统最终将应用于网络,网络上的输入设备各异,进行规范化是必要的。规范化包括缩放和旋转两个过程。

*)本课题获日本富士通公司国际合作研究资金资助。杨 飞、沈 峰、袁余良 硕士研究生,研究方向为人工智能和多媒体技术。潘金贵 教授,博士生导师,从事中间件、Agent 技术及多媒体信息处理技术等的研究。

缩放就是将所有的签名都纳入一个矩形(H,W)(H为高度,W为宽度)中。

第一步　计算签名的中心(μ_x,μ_y):$\mu_x=\frac{\sum_1^N x_i}{N}$,$\mu_y=\frac{\sum_1^N y_i}{N}$;$x_i,y_i$分别为签名第$i$个采样点的$x$坐标,$y$坐标。

第二步　以(μ_x,μ_y)为新的坐标原点重新计算各采样点的坐标:$x_i=x_i-\mu_x$,$y_i=y_i-\mu_y$。

第三步　计算签名的高度h和宽度w:

$h=y_{max}-y_{min}$,y_{max}和y_{min}分别为签名采样点的y坐标最大值和最小值;

$w=x_{max}-x_{min}$,x_{max}和x_{min}分别为签名采样点的x坐标最大值和最小值。

设经过缩放的高和宽分别为h'和w':IF$(H/W>h/w)$ THEN$\{h'=h*W/w,w'=W\}$ ELSE $\{h'=H,w'=w*H/h\}$

第四步　计算经过缩放的特征点坐标:$x_i=x_i*w'/w$,$y_i=y_i*h'/h$

旋转关键是计算旋转角度θ。可以通过求x坐标的标准方差σ_x的最大值计算θ,$\sigma_x=\sqrt{\frac{\sum_1^N x_i^{*2}}{N}}$,也就是求$\sum_1^N x_i^{*2}$的最大值,$x_i^*$即是旋转后的$x$坐标值,$x_i^*=x_i\cos\theta-y_i\sin\theta$,$y_i^*=x_i\sin\theta+y_i\cos\theta$,不妨设$-\frac{\pi}{4}<\theta<\frac{\pi}{4}$,则$\theta=\frac{1}{2}\arctan(\frac{2Q}{R-P})$,其中$P=\sum_1^N x_i^2$,$Q=\sum_1^N x_i*y_i$,$R=\sum_1^N y_i^2$。

3.2.3　平滑化　是为了去除设备不平滑造成的抖动,我们采用的是一种数字图像处理技术——高斯过滤器,一维的高斯过滤器定义为:$f_i=\frac{e^{-\frac{i^2}{2\sigma^2}}}{\sum_{j=-2\sigma}^{2\sigma}e^{-\frac{j^2}{2\sigma^2}}}$,其中$f_i$是位置$i$的过滤器的值,$\sigma$是过滤器的变量,本系统取2,原始坐标与过滤后坐标的关系是$x_i^{filtered}=\sum_{i=-2\sigma}^{2\sigma}f_i*x_{i+i}^{orig}$。特征向量的任何一维都要使用高斯过滤器进行过滤。

3.3　验证策略和阈值的选取

验证策略对系统性能是至关重要的。有三类策略:基于参考集的策略、基于模板的策略和混合策略。

生物认证技术的研究表明,即使同一个签名者也有几种不同的签名风格[2]。

基于参考集的验证策略是把注册的所有签名都保存起来组成一个参考集,验证时输入签名与参考集中每个签名分别比较,得出n个距离(n是参考集中签名的个数),然后设计一个n元函数,以得出的n个距离作为函数变量计算出函数值,最后将该值与阈值比较得出验证结果。通常采用的函数有三种:最小值函数(从n个变量中选取一个最小值作为函数值),平均值函数(计算出n个变量的算术平均值作为函数值),最大值函数(从n个变量中选取一个最大值作为函数值)。该策略实现难度不大,效果较好,被本系统采用。

基于模板的策略是从注册的所有签名数据计算出一个"平均签名"——模板,然后输入签名与模板比较得出一个距离,最后这个距离与阈值比较得出结果。这种策略的优势在于它的简单,对时间和空间的要求低,缺陷是抹杀了签名风格的多样性,因而效果一般。

混合策略是上面两种策略的综合。它先分析出注册签名的签名风格,再按风格将签名分类,将每一种签名风格的签名做成模板,下面的验证过程与基于参考集的验证策略相同。该策略优点是兼顾了验证效果和时空要求,缺点是难度较大。

除了验证策略,系统还需要一个验证的标准,这个标准就是阈值。有两类阈值:通用阈值,签名者相关的阈值。

顾名思义,通用阈值就是从所有签名者的签名计算出一个平均距离作为系统的阈值,所有签名者输入的签名都通过这个阈值验证。

通用阈值没有考虑到不同签名者各自的特征。某些签名者具有比较稳定的书写风格,而另一些的书写风格变化较大,对于前者,阈值应该比较小,对于后者,阈值应该相对大一点,因此如果使用签名者相关的阈值,会取得更佳的认证效果。签名者相关的阈值有三种取法,分别是取参考集内所有签名间距离的最小值、平均值、最大值。本系统取平均值。

为了提高系统的效率和性能,本系统先用全局特征进行一次筛选,再用局部特征进行验证。

3.4　匹配

本系统采用经典的动态规划匹配算法(Dynamic Programming Matching)。图2是动态规划表,行号表示输入签名特征点序列,列号表示参考签名的特征点序列,score(i,j)表示到达(i,j)的匹配路径的得分。

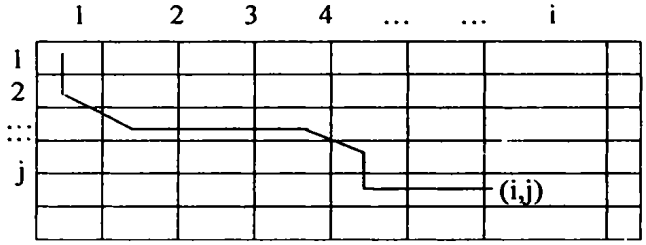

图2　动态规划表

算法如下:

$A=\frac{score(i-1,j)+dist(i,j)}{path(i-1,j)+1}$　$B=\frac{score(i-1,j-1)+dist(i,j)}{path(i-1,j-1)+1}$

$C=\frac{score(i,j-1)+dist(i,j)}{path(i,j-1)+1}$,$path(0,0)=0$

IF min(A,B,C)==A THEN {score(i,j)=score(i−1,j)+dist(i,j);path(i,j)=path(i−1,j)+1;}

ELSE IF min(A,B,C)==B THEN {score(i,j)=score(i−1,j−1)+dist(i,j);path(i,j)=path(i−1,j−1)+1;}

ELSE {score(i,j)=score(i,j−1)+dist(i,j);path(i,j)=path(i,j−1)+1;}

每个特征点都是一个五维向量(x_i,y_i,vx_i,vy_i,p_i),$dist(i,j)$是参考签名的第i个特征点到输入签名的第j个特征点的欧几里得距离。$path(i,j)$是从(0,0)到(i,j)的最佳匹配路径的长度。

(下转第75页)

4. 性能评价

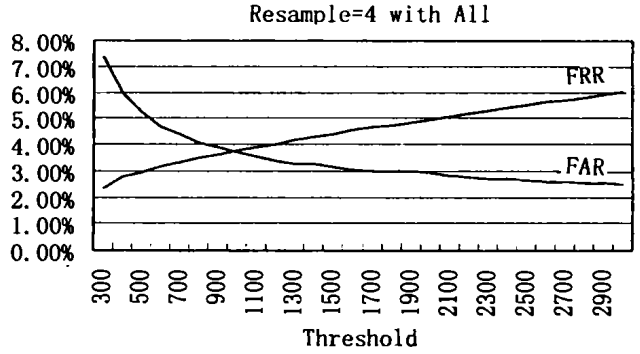

图3　Threshold--FAR&FRR 曲线

此步骤是在投影合并完相同频繁项后，在具有相同当前项名的二元频繁项组之间进行操作，是一个简单的分类问题。而且在投影后，得出的二元频繁项组的个数本身就大大小于投影前频繁项的个数(事务个数)，因此，相对于 FP-tree 构造算法，这部分开销是值得的和可以忽略的。

总结 通过以上的分析和研究表明：如果我们将 PFP-tree 构造算法(算法3)和 FP-growth 算法(算法2)结合起来进行频繁模式挖掘，可以有效地提高数据挖掘的性能，具有良好的可伸缩性。这主要体现在以下三个方面：

1. 运用投影和树结构技术，可以将一个大型数据库压缩到一个高密度的、更小的数据结构(PFP-tree)中，能有效地避免重复扫描数据库的昂贵代价；而且在构造 PFP-tree 的过程中，算法的性能不受数据库大小的影响。

2. 基于 PFP-tree 的挖掘采用频繁模式增长的方法，避免了迭代产生大量候选项集的代价。

3. 采用对频繁项进行分割和分而治之的方法来挖掘频繁模式，将繁重的挖掘任务分解为一组小的多的任务——对各个频繁项的条件模式树的挖掘，能有效地减少搜索空间。

目前，对基于 FP-tree 挖掘的研究包括基于 SQL、高伸缩性的 FP 树结构的研究与应用，基于约束的频繁模式挖掘，以及运用该项技术来挖掘序列模式[12]、最大模式[13]和部分频率[14]等相关领域。如何将改进的 PFP-tree 方法运用到这些研究领域以及如何与实际的工业、商业大型数据相结合，则是我们进一步研究的方向。

参 考 文 献

1 Agrawal R, Srikant B. Fast algorithms for mining association rules. In VLDB'1994. 487～499

2 Grahne G, Lakshmanan L, Wang X. Efficient mining of constrained correlated sets. In ICDE'2000

3 Klemettinen M, et al. Finding interesting rules from large sets of discovered association rules. In CIKM'1994. 401～408

4 Lent B, Swami A, Widom J. Clustering association rules. In ICDE'1997. 220～231

5 Ng E, Lakshmanan L V S, Han J, Peng A. Exploratory mining and pruning optimizations of constrained associations rules. In SIGMOD'1998. 13～24

6 Park J S, Chen M S, Yu P S. An effective hash-based algorithm for mining association rules. In SIGMOD'1995. 175～186

7 Sarawagi S, Thomas S, Agrawal R. Integrating association rule mining with relational database systems. Alternatives and implications. In SIGMOD'1998. 343～354

8 Savasere A, Omiecinski E, Navathe S. An efficient algorithm for mining association rules in large database. In VLDB'1995. 432～443

9 Srikant R, Vu Q, Agrawal R. Mining association rules with item constraints. In KDD'1997. 594～605

10 Han Jiawei, Kamber M(加). 数据挖掘概念与技术. 机械工业出版社，2001. 158～161

11 Han Jiawei, Pei Jian, Yin Yiwen. Mining Frequent Patterns without Candidate Generation. http://www.cs.sfu.ca/～peijian/personal/publications

12 Agrawal R, Srikant S. Fast algorithms for mining association rules. In VLDB'1994. 487～499

13 Bayardo R J. Efficiently mining long patterns from databases. In SIGMOD'1998. 85～93

14 Han J, Pei J, Yin Y. Mining partial periodicity using frequent pattern trees: [CS Tech. Rep. 99-10]. Simon Fraser University, July 1999

(上接第125页)

评价一个签名认证系统的性能需要分析两种错误率：FRR (False Reject Rate)——真实签名被系统错误拒绝的比例和 FAR(False Accept Rate)——伪造签名被系统错误接受的比例[2]。通常，一个系统的性能用 EER(Equal Error Rate)——FRR 与 FAR 相等时的值来评价。本系统测试了3345个伪笔签名和584个亲笔签名，得到图3所示的测试结果。

从测试结果看，本系统的 ERR 在4%之下，FAR 和 FRR 的最小值均接近2%，性能是令人较为满意的。

5. 进一步的工作

签名者的签名风格是随时间变化的。如果参考集保持不变，系统性能会随时间下降，因此有必要对参考集更新。一种办法是用户主动地更新，但这样安全性较差。最好是系统自动更新，最简单的更新策略是把最早的参考签名替换掉，但这不是最佳策略。参考集的更新策略是一个值得进一步研究的有趣的课题。

另外什么是最佳的特征集，全局特征与局部特征怎样结合都需要进一步的研究。

参 考 文 献

1 Nalwa V S. Automatic on-line signature verification. Proceedings of the IEEE, 1997, 85: 215～239

2 Griess F D. Project Report: On-line Signature verification. May 2000

3 Dullink H, et al. Implementing a DSP Kernel for Online Dynamic Handwritten Signature Verification Using the TMS320 DSP Family. Dec. 1995

4 Lee L L, et al. Reliable on-line human signature verification systems. IEEE Transactions on Pattern Analysis and Machine Intelligence, 1996, 18: 643～647

5 Yang L, et al. Application of hidden markov models for signature verification. Pattern Recognition, 1995, 28(2): 161～170

6 Wirtz B. Stroke-based time warping for signature verification. In: Proc. of the Intl. Conf. on Document Analysis and Recognition, 1995, 1: 179～182

7 Dolfing J, et al. On-line signature verification with hidden markov models. In: Intl. Conf. on Pattern Recognition, vol. 2, IEEE, 1998, 2: 1309～1312

8 Hastie t, et al. A model for signature verification: [tech. rep]. AT&T Laboratories, Feb. 1992