

文章编号:1001-9081(2006)11-2583-03

一种基于演化计算的在线手写签名验证算法实现

匡 韬¹, 郑建彬^{1,2}

(1. 武汉理工大学 信息工程学院, 湖北 武汉 430070; 2. 华中科技大学 电子与信息工程系, 湖北 武汉 430074)
(abigrat@126.com)

摘 要:提出了基于演化计算的在线手写签名验证算法。该算法将参考签名分割成曲线段,以一定长度的搜索窗在测试签名曲线上进行动态搜索,实现与参考签名曲线段自适应的动态分割与匹配。在算法中引进了演化计算中的分级和加速技术,使算法的搜索速度和匹配效果有了一定程度的提高。实验结果表明了该算法的有效性。

关键词:签名验证;演化计算;动态匹配

中图分类号: TP309; TP391 **文献标识码:** A

A new algorithm for dynamic handwriting signature verification based on evolutionary computation

KUANG Tao¹, ZHENG Jian-bin^{1,2}

(1. School of Information Engineering, Wuhan University of Technology, Wuhan Hubei 430070, China;
2. Department of Electronics and Information Engineering, Huazhong University of Science and Technology, Wuhan Hubei 430074, China)

Abstract: A new algorithm for dynamic handwriting signature verification was proposed based on evolutionary computation (EC). The reference signature curve was divided into segments firstly. The adaptive dynamic segmentation and match between reference signature curve and test signature curve were implemented by dynamic search on the test signature curve with a search window of certain width. The theories of classification and acceleration in the EC were adopted in the basic evolutionary approach, which improved the search efficiency and matching result to a certain extent. The validity of the algorithm is proved by the experiment results.

Key words: signature verification; evolutionary computation; dynamic match

0 引言

随着计算机科学技术的发展,电子商务以及网络应用也开始普及,实时准确的个人身份认证已经成为解决网络安全问题的一个重要方面。在线手写签名验证是一种基于生物特征的身份识别方法,该技术在模式识别、信号处理等领域都属前沿课题。

在线手写签名验证基于每个人签名的唯一性以及短期内不会改变的签名习惯。它通过计算机把手写签名的图像、笔顺、速度和压力等信息与真实签名样本进行对比,以实时鉴别手写签名的真实性。在很多发达国家已经立法承认签名的合法性,我国也于 2005 年 4 月 1 日出台了《电子签名法》,成为电子商务发展的重要里程碑。

签名验证算法主要有参数法和函数法两大类。比较有代表性的有:基于离散拉东变换和隐性马尔可夫相结合的模式^[1];利用 Gabor 滤波的相位进行时域偏移估计来进行签名验证的方法^[2]及基于自回归模型的签名认证方法^[3]。

然而,由于在线签名具有随意性,且将签名用函数表示十分复杂,因此,目前很难提出一个较好的评判签名相似度的准则,从而给比较测试签名和参考签名相似度带来很大困难,造成了各种特征提取和比较方法的效果都不尽如人意的现状。本文提出了一种新的签名相似度评判方法,以此作为准则来比

较测试签名和参考签名的相似程度,建立数学模型,并首次将演化计算的方法^[4]引入到签名的匹配识别中,利用了个体分级和加速搜索技术^[5],提高了算法效率,收到了较好的效果。

1 数学模型

1.1 问题的引出

签名验证的实现由硬件采集数据和软件验证共同完成。硬件采集设备是分辨率为 4096×4096 像素的手写板,首先通过其进行实时签名数据采集,包括 X 轴和 Y 轴的坐标信息。采样间隔时间 Δt 为 5ms,取采样时刻作为横坐标,分别以手写板上 X 轴和 Y 轴的数据为纵坐标建立坐标系。为便于查看,横坐标取实际采样时刻 $t/5$,单位是 ms;纵坐标单位是像素(全文同)。



图 1 某签名图示

由于笔画造成的提笔落笔之间的时间间隔以及其他因素,采集数据为两条不连续的曲线,不连续的位置则表示了书写笔未接触到手写板或手写者提笔落笔的位置。为了便于处理,必须对其进行去零点、尺度归一化等预处理操作。图 1 是某个测试者的某一次试验签名。

收稿日期:2006-05-10;修订日期:2006-06-28 基金项目:国家自然科学基金资助项目(69672014)

作者简介:匡韬(1984-),男,湖北监利人,硕士研究生,主要研究方向:信息处理、模式识别; 郑建彬(1966-),男,湖北黄冈人,教授,博士研究生,主要研究方向:信号与信息处理、模式识别。

以图 1 中签名作为参考签名,同一测试者另一次签名作为测试签名,图 2 为两者曲线的对比效果,虽然两条曲线大部分极为相似,但由于时间的非线性,若直接对两条曲线进行整体对比和匹配尝试,将造成巨大的误差而无法达到预期效果。因此需要对原曲线进行处理再进行匹配识别。

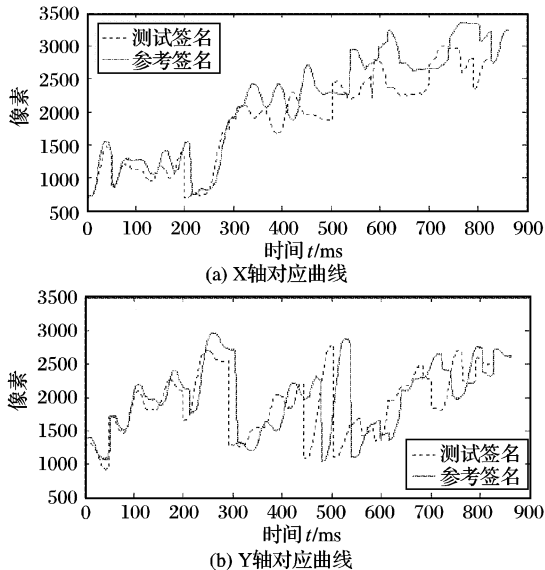


图 2 参考签名和测试签名 X 轴、Y 轴对应曲线对比

1.2 数学模型

为了从签名所采集的数据中提取数学特征并建立验证算法,以 X 坐标轴的信号数据为例,将测试签名曲线的对应函数记为 $f_1(x)$,参考签名曲线的对应函数记为 $f_2(x)$,这两条曲线是否匹配,可以根据两条曲线的相似度确定。

本文提出了一种新的相似度评判规则:相似度定义。给定函数 $f_1(x)$, $f_2(x)$, 称 $d(f_1, f_2) = \int_{c_0}^{c_1} |f_1(x) - f_2(x)| dx$ 为两个函数之间的距离, $[c_0, c_1]$ 为函数的定义域;如果对于给定的值 ε , 若 $d(f_1, f_2) \leq \varepsilon$, 则称 $f_1(x)$, $f_2(x)$ 相似, 否则称它们不相似。

事实上用区间 $[c_0, c_1]$ 上的函数的相似性来确定两条曲线是否匹配存在很大的误差。因此,需要对两条曲线进行分段,再进行逐段匹配。同时,由于签名时存在时间轴的非线性、书写位置的差异以及字体大小的局部变化,因此,分段匹配时必须对某段 $f_1^i(x)$ 进行平移及伸缩变换。经变换后,距离定义为:

$$d(f_1^i, f_2^j) = \int_{x_i}^{x_{i+1}} |kf_1^i(ax+b) + h - f_2^j(x)| dx \quad (1)$$

其中 k 和 h 分别是垂直方向上的伸缩比例和平移分量; a 和 b 分别是水平方向上的伸缩比例和平移分量。

2 算法实现

即使经过预处理后的签名数据仍然不能直接进行整段匹配,因此采取自适应动态分段匹配方式。

2.1 自适应动态分割

通常的分段方法并不能很好解决起始点的确定和最优匹配误差问题。如将 $f_1(x)$ 和 $f_2(x)$ 分别对应分成 N 段,将两条曲线所对应的分段一对一匹配,分段的准确性会直接影响到最后匹配结果。因此本文提出了自适应动态分割与匹配的方法,其优点是可以降低匹配结果对分段准确性的依赖程度,同时可以利用演化算法实现线段间的最优匹配。

自适应动态分割与匹配算法如下:

1) 只对参考签名曲线进行分段,既可依据某种特征进行分段,也可等长分段,还可以人工分段,例如将参考签名等长分割成 N 段。

2) 依据参考签名的分段,在测试签名曲线中在指定的搜索窗内进行动态搜索匹配,找到最优匹配点,实现对测试签名的分割。若 $d(f_1^i, f_2^j) \leq \varepsilon$, 则认为两曲线段相似; 否则, 认为两曲线段不相似。

3) 若 N 段中有多于 M 段相似 (M 为某一给定阈值, 且 $M \leq N$), 则可认为参考签名与测试签名匹配成功。从而, 签名验证问题转化为两签名间曲线段的匹配。

对曲线使用动态搜索分段匹配技术, 需要满足单调、连续的特点, 经过预处理后的曲线可近似视为满足上述要求。

2.2 签名匹配与相似度计算

首先对参考签名和测试签名曲线进行预处理, 并记下参考签名曲线上出现连续若干个零值的坐标。参考签名曲线按零点特征进行分割。具体方法为: 顺序读取 s_i 个参考签名数据, 记为 r_i , 若包含连续零值坐标记录则以该坐标为 r_i 的结束点。然后顺序读取 s_i 个测试签名数据, 记为 t_i 。在 t_i 段上以一定宽度的搜索窗 w_0 进行动态搜索, 得到最佳的两个匹配距离值: 最小距离值 z_{im} 和次小距离值 z_{in} 。设定匹配距离阈值为 z_η , 将 z_{im} 和 z_{in} 与 z_η 比较, 然后经过分析确定该段的匹配结果。如图 3 所示, 依次对各个曲线段进行匹配, 直到将所有曲线段匹配完毕。最后统计成功匹配的曲线段 M 在总的曲线段 N 中的比重 $\eta (\eta = M/N)$, 与设定的阈值 η_0 进行对比, 即可得到匹配的最终结果。

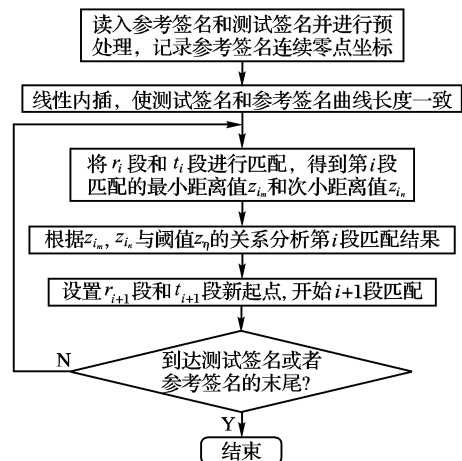


图 3 签名匹配流程

z_{im} 和 z_{in} 与 z_η 的比较分为三种情况:

1) 若均大于 z_η , 则表明匹配效果较差, 此时利用删除算子对 r_i 进行删除操作, 然后再次进行动态搜索匹配。若仍然不在阈值 z_η 范围内, 则舍弃第 i 段, 视为匹配失败; 若删除操作后满足阈值 z_η 则保留删除操作后的匹配结果。

2) 若均小于 z_η , 则需要利用后续的匹配结果决定选取其中之一作为本段的匹配结果。这样做的原因是签名匹配要求的是全局最优而非局部最优, 因此分别基于 z_{im} 和 z_{in} 进行后续匹配, 根据后续匹配效果来选取第 i 段的匹配结果, 而不直接选取 z_{in} 作为第 i 段的匹配结果。

3) z_{im} 和 z_{in} 之一满足 z_η 的限定要求。此时直接选取较小者, 作为第 i 段的匹配结果予以保留。

2.3 演化计算匹配算法

根据式(1)的定义,两个签名曲线之间的相似度转化为它们之间的距离。动态匹配的目的就是在区间 $[x_i, x_{i+1}]$ 上求出满足 $z_0 = \text{Min}(z) = \text{Min}(d(f_1^i, f_2^j))$ 的参数 k, h, a, b ,这也是整个算法的关键。但由签名问题得到的不是一个明确的函数表达式,对这样一类问题的优化十分困难。由于演化计算优化不需要具体的函数表达式,它只需要评价适应度值,因此本文提出了基于演化计算的签名验证算法。

选取个体 k, h, a, b 的适应度函数为 $d(f_1^i, f_2^j)$,即每一个个体都对应一个参考签名和测试签名曲线段之间的距离,该适应度越小,表示参与匹配的参考签名与测试签名曲线段距离越小,也就是个体越优良。

基于演化计算的签名验证算法步骤如下:

1) 在一定的种群规模 S 下,随机产生初始种群 $P(j)$, $j = 0$ 。其中每产生一个解均检验其是否满足约束条件。若是,则产生下一个解;否则重新产生直到满足约束条件。

2) 根据个体 k, h, a, b 的值,在各自的邻域随机产生 S 个子代。

3) 计算所有父代和遗传产生的子代的适应度值,根据适应度值对所有的个体进行分级,选取最优的 S 个个体组成新的群体 $P(j+1)$,替换种群 $P(j)$ 。当满足终止条件时,转步骤4);否则转到步骤2)。

4) 输出结果。

终止条件为演化世代数达到设定的最大世代数。

3 实例与分析

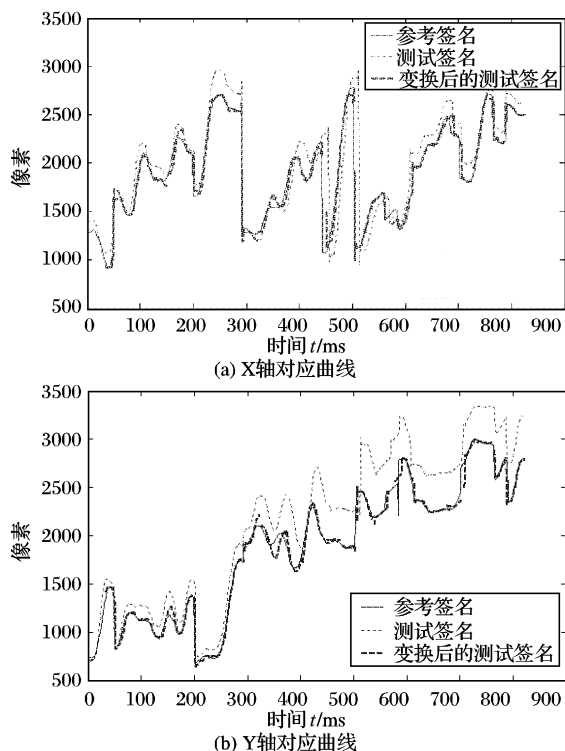


图4 测试签名和参考签名X,Y轴对应曲线匹配结果

选取出自同一签名者的某参考签名和测试签名作为实例分析。在实验过程中,在对参考签名曲线进行分割时,为了简化操作,通常选择等长分段方式,例如选择每段20点分割参考签名。通常,曲线在水平方向有较大非线性失真,但这种失真通常存在于某一个具体的曲线段中,因而可令 $\alpha = 1$,这时

只影响某一个曲线段的匹配,对其他段的影响较小,但却显著提高了演化计算的速度。由于在匹配过程中抛弃了匹配效果很差的点,因此每段曲线的点数 n_i 有可能并不相同,因此需要引入平均距离 $\bar{z}_0 = z_0/n_i$ 来衡量匹配是否成功,而 $\bar{\varepsilon}$ 则是平均距离对应的阈值。 l_{f_2} 为参考签名曲线段的长度, l_{f_1} 为与参考签名段对应的搜索范围内测试签名段的长度。

首先在设定的取值范围内随机产生 k, h, b ,构成一个初始群体。将个体的适应度值 z 进行排序、分级,由每个个体的级别确定该个体下一代的搜索范围。

在所有的个体经过规定的世代数的演化后,可以得到最优解,这个解就是最小距离 z_0 ,通过比较 \bar{z}_0 与所设定的阈值 $\bar{\varepsilon}$,可以判断出该测试样本曲线段是否能与参考签名曲线段匹配。

程序运行时的参数设置如下:种群规模 $S = 20$;运行代数 50 ; $0.9 \leq k \leq 1.1$; $-1000 \leq h \leq 1000$; $0 \leq |l_{f_2} - l_{f_1}|$; 搜索窗宽度 $w_0 = 10$; $\bar{\varepsilon} = 70$; $\eta_0 = 85\%$ 。

图4是测试签名和参考签名在X轴和Y轴方向上对应曲线的匹配结果。

X, Y轴方向上的曲线一共有27段,匹配成功的段数都为26。每一分段对应的 k, h, b ,最小距离 z_0 ,平均距离 \bar{z}_0 如表1所示。匹配率为 $\eta = 26/27 = 96.30\%$,可以认为测试签名与参考签名是同一个人的签名。

表1 X轴对应曲线分段匹配参数及结果

段号	b	k	h	距离	结果	段号	b	k	h	距离	结果
1	3	0.902	56	43.0949	Y	15	4	0.921	-161	29.1797	Y
2	0	0.915	53	56.2946	Y	16	1	0.934	-184	18.8672	Y
3	0	0.918	18	27.2730	Y	17	0	1.088	-580	18.6678	Y
4	1	0.965	-109	7.5249	Y	18	1	0.907	-217	18.1540	Y
5	0	0.911	-19	34.5403	Y	19	2	0.906	-244	27.3538	Y
6	0	0.919	-29	38.8586	Y	20	10	0.979	-358	57.1196	Y
7	0	0.906	-18	56.7801	Y	21	1	1.02	-432	6.3760	Y
8	1	0.939	-31	16.4210	Y	22	6	0.909	-136	4.8814	Y
9	1	0.912	-15	10.7924	Y	23	0	1.093	-595	65.3803	Y
10	0	1.025	-217	19.3025	Y	24	3	0.901	20	41.7885	Y
11	0	0.919	13	37.2802	Y	25	0	0.973	-255	7.4729	Y
12	0	0.905	-98	66.8480	Y	26	0	1.092	-742	37.8192	Y
13	0	0.906	-161	104.8960	N	27	0	0.909	-161	47.8385	Y
14	0	0.927	-75	28.6037	Y						

实验选择了10个实验者,每人提供了30个签名。为保证签名风格的一定变化,签名数据分多次在不同时间录入。实验表明,针对签名曲线的特征采取不同的长度分段,将更有利于匹配率的提高。两次采取不同固定长度对测试签名进行分段,得到的匹配成功率分别为87%和83.32%,调整其中匹配失败的签名的分段长度,则成功率可以达到99.97%,误识率0,误拒率0.03%。

4 结语

本文提出了一种新的评判签名相似度的准则,建立了数学模型,首次将演化计算的方法引入到签名验证中来,利用演化算法来处理难以用函数描述的签名匹配和验证问题。在演化算法中利用了分级加速技术,大大加快了搜索速度,使签名验证算法运算结果得到较大提高,基本上达到了令人满意的效果。
(下转第2588页)

3.4 可区分性

因为在签名验证阶段,许可证 W, PK_A, PK_B 一定要用到,因此代理盲签名与一般签名是可以区分的。

3.5 盲性

定理 1 本文提出的基于身份的代理盲签名具有盲性。

证明 根据定义 1^[12], 设 \bar{A} 是签名人或一个控制签名人的 PPT 算法, 通过密钥 / 公钥提取获得了基于身份信息的密钥 / 公钥对。

如果 \bar{A} 得到 \perp , 则容易看出 \bar{A} 能以 $1/2$ 的概率在游戏中赢。

现在考虑 \bar{A} 获得 $\sigma(m_i), \sigma(m_{1-b})$ 的情形。对于 $i = 0, 1$, 设 K'_i, h'_i, S'_i 为在签名发行过程中交换的数据, 将 $(K_0, S_0), (K_1, S_1)$ 交给 \bar{A} 。这时, 有足够的理由说明, 存在两个因子 (t_1, t_2) , 对于每一个 $i, j \in \{0, 1\}$, 能够将 K'_i, h'_i, S'_i 映射到 K_j, S_j 。我们进行如下定义:

$$\begin{aligned} S'_i &= (S_j - t_2 P_{pub}) t_1^{-1}, t_1 = h_1^{-1} h_j \\ K'_i &= t_1 \hat{e}(P, P_{pub})^{t_2} \\ &= [\hat{e}(P, S'_i)(PK_A + PK_B, P_{pub})^{H_3(H_1(W))h'_i}]^{t_1} \hat{e}(P, P_{pub})^{t_2} \\ &= [\hat{e}(P, (S_j - t_2 P_{pub}) t_1^{-1})(PK_A + PK_B, P_{pub})^{H_3(H_1(W))h'_i}]^{t_1} \end{aligned} \quad (11)$$

表 1 我们的方案与其他方案的性能比较

方案	生成代理密钥	签名	验证
文献[9] 方案	$2P_a + 4P_m + 1M_u G_2 + 1E_x G_2 + 4A_d + 1H_s$	$2P_a + 6P_m + 5A_d + 2H_s$	$3P_a + 1P_m + 1M_u G_2 + 1E_x G_2 + 1A_d + 2H_s$
文献[10] 方案	$1P_a + 2P_m + 1E_x G_2 + 1A_d + 4H_s$	$1P_a + 6P_m + 5A_d + 3H_s$	$1P_a + 1M_u G_2 + 1E_x G_2 + 1A_d + 2H_s$
我们的方案	$1P_a + 2P_m + 1E_x G_2 + 1A_d + 4H_s$	$5P_m + 1M_u G_2 + 3E_x G_2 + 2A_d + 1H_s$	$1P_a + 1M_u G_2 + 1E_x G_2 + 1A_d + 1H_s$

从各种操作的计算来看, P_a 计算最耗时, 然后是 P_m 。从表 1 中可以看出我们的方案的计算复杂度大约为 $2P_a + 7P_m$ 数量级, 文献[9] 的方案计算复杂度大约为 $7P_a + 11P_m$ 数量级, 文献[10] 的修正方案的计算复杂度大约为 $3P_a + 8P_m$ 数量级。因此, 我们的方案比文献[9] 的方案效率高得多, 同时比文献[10] 的修正方案的效率也高。

5 结语

本文结合代理签名和盲签名, 利用双线性映射, 构造了一种高效的基于身份的代理盲签名方案。分析表明, 该方案不仅能满足代理盲签名所要求的所有性质, 而且其效率也优于文献[9, 10]。基于身份的代理盲签名在电子现金和电子投票等领域将发挥重要的作用。

参考文献:

- [1] MAMBO M, USUDA K, OKAMOTO E. Proxy signature: delegation of the power to sign messages[J]. IEICE Transactions on Fundamentals, 1996, E792A(9): 1338 - 1353.
- [2] CHAUM D. Blind signature for untraceable payments [A]. Advances in Cryptology: Crypto'82[C]. Berlin, 1982. 199 - 203.
- [3] 谭作文, 刘卓军, 唐春明. 基于离散对数的代理盲签名[J]. 软件

$$\begin{aligned} &\hat{e}(P, P_{pub})^{t_2} \\ &= \hat{e}(P, S'_i)(PK_A + PK_B, P_{pub})^{H_3(H_1(W))h'_i t_1} \\ &= \hat{e}(P, S'_i)(PK_A + PK_B, P_{pub})^{H_3(H_1(W))h_j} = K_j \end{aligned}$$

盲因子总是存在且能满足式(11)的定义, 因此即使有无限能力的 \bar{A} 能成功决定 b 的概率仍为 $1/2$ 。

综合两种情形, \bar{A} 赢的概率为 $1/2$, 因此本文提出的基于身份的代理盲签名具有盲性。

4 性能分析

下面将我们提出的方案和文献[9] 的方案以及经过修正的文献[10] 的方案从计算复杂性方面进行比较, 并将结果总结在表 1 中。表 1 中有关符号的定义如下: P_a 表示双线性映射中的对操作, P_m 表示 G_1 上的标量乘, A_d 表示 G_1 上的点加操作, $M_u G_2$ 表示 G_2 上的乘操作, $E_x G_2$ 表示 G_2 上的指数运算, H_s 表示哈希函数。考虑到双线性对 $\hat{e}(P, P_{pub}), \hat{e}(PK_A, P_{pub}), \hat{e}(PK_A + PK_B, P_{pub})$ 可提前进行计算, 因此我们的方案中考虑计算复杂性时对相关双线性对进行了预计算, 文献[9] 的方案以及经过修正的文献[10] 的方案同样考虑了预计算。

学报, 2003, 14 (11): 1931 - 1935.

- [4] 王蜀洪, 王贵林, 鲍丰, 等. 对一个基于离散对数代理盲签名的密码分析[J]. 软件学报, 2005, 16 (5): 911 - 915.
- [5] AWASTHI AK, LAL S. Proxy blind signature scheme [J]. JFCR Transaction on Cryptology, 2005, 2(1): 5 - 11.
- [6] SHAMIR A. Identity - based cryptosystems and signature schemes [A]. Crypto'84, LNCS 196[C], Berlin, 1984. 47 - 53.
- [7] BONEH D, FRANKLIN M. Identity-based encryption from the weil pairing [A]. Crypto 2001, LNCS 2139[C], 2001. 213 - 229.
- [8] BONEH D, LYNN B, SHACHAM H. Short signature from the weil pairing [A]. Asiacrypt 2001, LNCS 2248[C], 2001. 514 - 532.
- [9] ZHENG D, HUANG Z, CHEN KF, *et al.* ID-based proxy blind signature [A]. ANNA 2004[C]. IEEE Computer Society, 2004, 2. 380 - 383.
- [10] LANG WM, TAN YM, YANG ZK *et al.* A new efficient ID-based proxy blind signature scheme [A]. ISCC 2004[C]. IEEE Computer Society, 2004, 1. 407 - 411.
- [11] HESS F. Efficient identity based signature schemes based on pairings [A]. SAC 2002, LNCS 2596[C], 2003. 310 - 324.
- [12] ZHANG F, KIM K. ID-based blind signature and ring signature from pairings [A]. Asiacrypt 2002, LNCS 2501[C], 2002. 533 - 547.

(上接第 2585 页)

参考文献:

- [1] COETZER J, HERBST BM, DU PREEZ JA. Offline Signature Verification Using the Discrete Radon Transform and a Hidden Markov Model [J]. EURASIP Journal on Applied Signal Processing, 2004, 2004(4): 559 - 571.
- [2] YI Y, LEE C, KIM J. Online Signature Verification Using Temporal Shift Estimated by the Phase of Gabor Filter [J]. IEEE Transactions on Signal Processing, 2005, 53(2): 776 - 783.

- [3] MOHANKRISHNAN N, PAULIK MJ, KHALIL M. On-line signature verification using a nonstationary autoregressive model representation [A]. IEEE International Symposium on Circuits and Systems [C], 1993. 2303 - 2306.
- [4] 潘正君, 康立山, 陈毓屏. 演化计算 [M]. 北京: 清华大学出版社, 1997.
- [5] 王小平, 曹立明. 遗传算法——理论、应用与软件实现 [M]. 西安: 西安交通大学出版社, 2002.