网上银行验证码研究与安全性分析

冯 杰,李旭伟
(四川大学 计算机学院,四川 成都 610065)

摘 要:验证码(CAPTCHA),是用于区别用户是人类还是机器的一种计算机自动程序。作为一种辅助手段,验证码在互联网安全领域扮演着很重要的角色。为了对网上银行验证码进行安全性评价,其过程包括三方面:验证码图像采集、图像预处理和图像识别。对国内网上银行验证码特点进行分析,采用最具可靠性的BP神经网络算法,选取其中具有代表性的验证码进行训练、识别。从识别结果中分析,通过所得到的识别率来评价国内网上银行验证码的安全有效性,并对网上银行验证码的生成给出一定的建议。

关键词:验证码;预处理;BP神经网络;网上银行
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2013)11-0144-04
doi:10.3969/j.issn.1673-629X.2013.11.036

Research and Security Analysis of Online Banking CAPTCHA

FENG Jie, LI Xu-wei
(College of Computer, Sichuan University, Chengdu 610065, China)

Abstract: CAPTCHA is an automatic computer program that determines a user is a human or a computer. As a supplementary measure, CAPTCHA plays a very important role in Internet security. In order to evaluate the safety of the online banking CAPTCHA, its process consists of three main areas, CAPTCHA image acquisition, image pre-processing and image recognition. Analyze the characteristics of domestic online banking CAPTCHA code, and then use the most reliable BP neural network algorithm to select the representative codes into training and identifying. From the recognition result of analysis, evaluate the safety and effectiveness of the domestic online banking CAPTCHA code, and give some suggestions to online banking CAPTCHA code generated by the obtained recognition rate.

Key words: CAPTCHA; pre-processing; BP neural network; online banking

0 引 言

CAPTCHA实质上是一幅图像,其上为一串随机产生的数字或符号,以及一些影响数字符号识别的干扰因素,以防止被电脑程序自动识别出来而使验证码失去其本来意义[1]。验证码图片的字符信息由人眼识别出来,再由人手动在网站的表单中输入来达到验证的目的,用户只有通过验证才能使用某些功能。对验证码识别的研究能促进计算机视觉和机器学习的发展,进一步认清人眼和机器视觉的区别。现在国内对验证码的研究主要集中在规范的数字或英文字符上,字符间既不粘连也不扭曲。由于不同网站采用的是不同的验证码生成规则,产生不同的干扰背景,因而无法做到统一的识别验证码[2]过程,即需要有针对性地识别某类验证码。

银行推出的网上银行业务,由于涉及到很多敏感的客户资料,其安全性要求也比较高,验证码作为网络账户安全性的保障手段之一,在网上银行中应用广泛。

所以对现有网上银行验证码的安全性研究就变得很有必要。

1 验证码识别流程与算法描述

文中选取十类具有代表性的网上银行验证码进行识别,通过识别率来评价其安全性。识别流程图如图1所示。

文中采用OSTU法和迭代法作为二值化处理方法,以BP神经网络算法作为训练测试方法。

1.1 OSTU法

最大类间方差法(OSTU)[3],是依据图像灰度特性,图像被分为两部分:目标部分和背景部分。

收稿日期:2013-01-22 **修回日期**:2013-04-27 **网络出版时间**:2013-08-28
基金项目:国家"863"高技术发展计划项目子课题(2002AA144020)
作者简介:冯 杰(1989-),男,硕士,研究方向为计算机网络与信息系统;李旭伟,副教授,硕士生导师,研究方向为计算机网络与信息系统。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20130828.0829.013.html

$$(T) = W_a(\mu_a - \mu)^2 + W_b(\mu_b - \mu)^2 \quad (1)$$

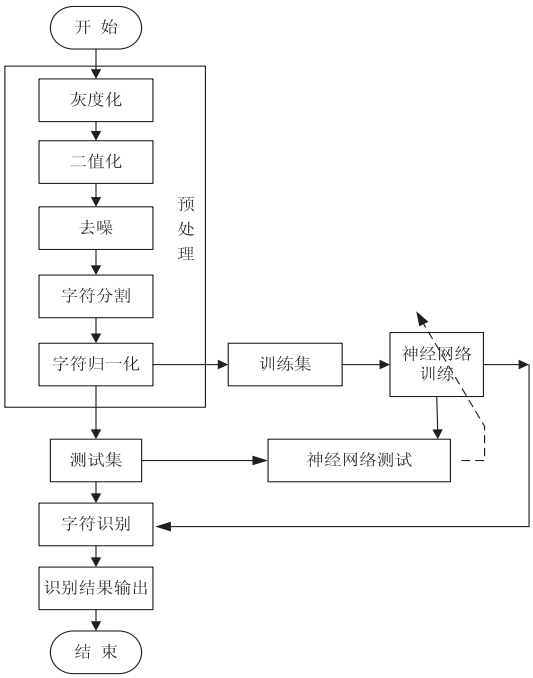

图 1　验证码识别流程图

对一幅 $M*N$ 像素的图像来说,最大类间方差算法如下:

(1) 首先计算图像总体灰度μ,遍历灰度图中所有像素,$n(i)$ 表示统计得到的灰度 i 的像素个数,计算式如式(2) 所示:

$$\mu = (1*n(1) + 2*n(2) + \cdots + i*n(i))/M*N \quad (2)$$

(2)T 为区分目标与背景的灰度值阈值,由该阈值,取得目标像素(灰度值小于 T) 占图像的比例, W_a 目标像素的平均灰度为μ_a,这两个参数计算如式(3) 和式(4) 所示:

统计灰度值小于 T 的像素点总数 w:

$$W_a = w/M*N \quad (3)$$

统计目标像素中灰度为 i ($i < T$) 的像素个数 $n(i)$,于是:

$$\mu_a = (1*n(1) + 2*n(2) + \cdots + i*n(i))/w \quad (4)$$

同理,获得背景像素占图像的比例 W_b,背景像素的平均灰度μ_b。

(3) 遍历 (2) 中的 T,当 T 最大时,即为最佳图像灰度阈值。

1.2　迭代法

算法描述如下[4]:

(1) 遍历图像每个像素点的灰度值,找出最小灰度值 $\text{Gray}_{\min}$ 及最大灰度值 $\text{Gray}_{\max}$;

(2)初始化阈值 $T = (\text{Gray}_{\min} + \text{Gray}_{\max})/2$;

(3)以 T 作为图像像素灰度值的分割点,分别求出灰度值大于 T 的所有像素的灰度平均值 average_h 和灰度值小于等于 T 的所有像素的灰度平均值 average_l ,取 $T_1 = (\text{average}_h + \text{average}_l)/2$ 作为新的阈值;

(4)比较 T 与 T_1,若 T 与 T_1 之间差的绝对值大于设定的差值(如 0.1),则把 T_1 赋予 T,继续跳转到第(3)步迭代,若它们间差值的绝对值小于设定的值,目的是使前后两次阈值相差几乎为 0,最终的 T 就是迭代所求的阈值。

1.3　BP 神经网络算法

BP(Back Propagation) 神经网络[5-7]是一种按误差逆向传播算法训练的多层前馈网络,网络拓扑结构包括输入层、输出层和隐含层,采用反向传播有监督学习方法,其学习规则按最速下降法,以反向传播信号的方式调整各层间权值和阈值,使实际输出和目标输出的误差平方和最小,这就是神经网络训练的实质。

算法描述如下:

(1)设置变量和参数,包括输入向量、输出向量、初始权值矩阵、学习速率;

(2)初始化,将随机产生的较小的非零向量赋予各个权值矩阵;

(3)随机的某一样本 p 取自于训练样本集中,将其信息输入网络;

(4)对输入信息,正向计算 BP 网络每一层的输出信息,再以此输出作为下层的输入;

(5)计算实际输出与期望输出之间的误差。判断是否满足误差要求,若满足转(8),否则转(6);

(6)迭代次数是否达到设定值,若达到,转(8),否则反向计算每层的权值和阈值(局部梯度);

(7)根据第(6)步计算的局部梯度修改权值矩阵;

(8)判断是否还有新的输入,是则转(3),否则结束。

2　验证码图像预处理

十家网上银行分别以 $B_1, B_2, B_3, B_4, B_5, B_6, B_7, B_8, B_9, B_{10}$ 表示。除 B_1 外其余验证码都做灰度化处理[8]。二值化处理分别采用 OSTU 法和迭代法,其关键在于选择和确定合适的阈值,选取其中最优组合,结果如表 1 所示。

即使二值化后大部分噪点已经去除,但部分干扰噪点仍需要去噪方法处理[9],以免对后续步骤有所干扰。下一步工作即是对图片进行分割,根据各家银行的特点,采用不同的分割方法,如垂直投影、连通域分割等。由于分割后的图片大小不一,需要对每个字符图片进行归一化处理,大小为 12 * 16。结果如表 2 所示。

表 1 验证码最终二值化后示例

银行		网上银行验证码示例			
B_1	固定阈值 173	8124	1367	6417	5599
B_2	迭代法	kA7h	n8p2	567d	nbh8
B_3	迭代法	E9K6	BB6D	RLV4	UHFQ
B_4	ostu 法	KER4	XVMR	76ZB	VJ8R
B_5	迭代法	3pu4	k37b	8nka	x7hk
B_6	固定阈值 94	ek6m	kvwm	nesg	dcn4
B_7	ostu 法	ENNZ	NAN9	PSNA	GD32
B_8	迭代法	bN3dD	eXUDm	fbHeh	3LSRS
B_9	固定阈值 105	FTASF	C3YPK	VY547	QNA7B
B_{10}	ostu 法	fqn4n	famea	h62d4	hX47d

表 2 经归一化后验证码字符示例

银行	网上银行验证码示例
B_1	8124 1367 6417 5599
B_2	kA7h n8p2 5 7d nbh8
B_3	E9K6 BB6D RLV4 UHFQ
B_4	KER4 XVMR 76ZB VJ8R
B_5	3pu4 k37b 8nka x7kh
B_6	ek6m kVWm nesg dCn4
B_7	ENNZ NAN9 PSNA GD32
B_8	bN3dD eXUDm fbHeh 3LSRS
B_9	FTASF C3YPK VY547 QNA7B
B_{10}	fqn4n famea h62d4 hX47d

3 验证码字符样本训练

3.1 特征提取

逐像素特征提取法[10]：对每个字符图像全扫描，像素值表示黑色时，特征值取 1，像素值表示白色时，特征值取 0，每个像素点进行特征值表示就形成一个特征向量矩阵。

3.2 特征提取 BP 神经网络结构设计

BP 网络的结构设计主要是确定输入层、输出层、隐含层各层节点个数及各层之间传递所需要的传输函数。输入层输入信息，隐含层和输出层对其进行处理，得到一个输入信息和输出结果的映射。

(1)输入层节点数确定：根据样本字符特征向量矩阵维数确定输入层的节点数。在文中，由于归一化后的图像大小为 12×16，可确定输入层输入节点数为 192 个。

(2)输出层节点数选择：此节点数取决于网上银行验证码分割后的字符数量，由于每家银行所采用的规则不同，分割出来的字符类别数也就不同，因此无法最终确定输出层节点数。表 3 所示为字符类别数作为输出节点数以及所产生的字符类别数不同的原因。

表 3 网上银行验证码字符类别统计

银行名称	图片字符数	字符类别数	原因
B_1	4	9	数字
B_2	4	30	数字、大写字母
B_3	4	28	数字、大写字母
B_4	4	26	数字、大写字母
B_5	4	24	数字、大写字母
B_6	4	20	数字、大写字母
B_7	4	24	数字、大写字母
B_8	5	50	数字、大、小写字母
B_9	5	28	数字、大写字母
B_{10}	5	24	数字、大写字母

(3)隐含层节点数选择：此节点数的确定没有固定的规律，通常是凭借经验或实验过程中寻找到的最佳值。通常情况下，隐含层节点数越大，训练的时间就越长；但如果节点数太少，容错性也会越差，即测试样本对它的识别能力越低。文中采用式(5)进行设计：

$$n = \sqrt{n_i + n_0} + a \tag{5}$$

式中，n 表示所求隐层节点数；n_i 为输入层节点数；n_0 为输出层节点数；a 为 1 ~ 10 之间的任一常数。文中 a 取值为 5。

(4) 传递函数选择：采用 Sigmoid 型函数。

Sigmoid 函数：它是一种非线性函数，将任意输入值压缩至(0,1) 或(－1,1) 的范围内。其表达式为：

$$y = f(s) = \frac{1}{1 + e^{-s}} \tag{6}$$

(5) 学习率选择[11]：学习率设置不应过大，否则可能出现系统不稳定；但也不能太小，过小会增加网络训练时间，进而导致网络的收敛速度变慢。学习率在 0.01 ~ 0.8 范围内选取最佳。文中选取学习率为 0.5。

(6) 训练方法选择[12]：文中采用学习率可变的动量 BP 算法对网络进行训练，作为对最速下降法的改进，动量 BP 算法引入了动量因子 $\eta(0 < \eta < 1)$：

$$x(k+1) - x(k) = \eta[x(k) - x(k-1)] + a(1-\eta)\frac{\partial E(k)}{\partial x(k)} \tag{7}$$

式中，k 为迭代次数；a 为学习率；η 为动量因子；$x(k)$ 为第 k 次迭代每层的权值矩阵；$\frac{\partial E(k)}{\partial x(k)}$ 为在第 k 次迭代后输出误差对每层权值矩阵的梯度向量。

(7) 其他参数设置：初始权值和阈值为 0 ~ 1 之间随机数，目标误差值 0.01，动量因子取默认值 0.9。

3.3 样本训练

以 B_6 银行为例，进行样本训练，选取 1 000 张验

证码图片,600 张作为训练样本集,经过预处理取得可用字符图片 2 294 张,然后经过 13 011 次迭代,最终达到目标误差 0.01,训练完成。如图 2 所示为 BP 神经网络训练的变化曲线图。

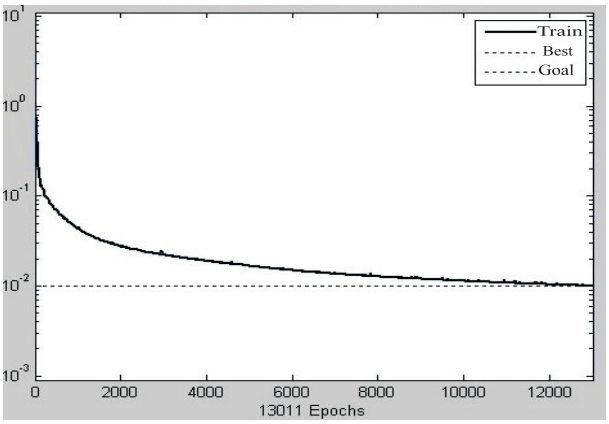

图 2　B_6 网上银行验证码 BP 神经网络训练结果

4　验证码字符测试

在测试中引入两个指标来评判网上银行验证码识别效果。

(1)单字符识别率:正确识别的单个字符数占单个字符数总数的百分比。

(2)整张验证码识别率:整张验证码图像正确识别占待识别验证码图像总数的百分比。

以前期训练的样本,对每家网上银行验证码都进行测试,最终的单字符识别率和整张验证码图像的识别率如表 4 所示。

表 4　基于 BP 神经网络的识别结果

银行	图片数	字符数	单字符/%	整张/%
B_1	100	4	99.4	97.6
B_2	100	4	95.7	83.9
B_3	200	4	99.6	98.4
B_4	200	4	96.3	86.0
B_5	200	4	95.2	82.1
B_6	200	4	94.6	80.1
B_7	200	4	98.5	94.1
B_8	200	5	86.1	47.3
B_9	100	5	94.8	76.6
B_{10}	100	5	91.2	63.1

5　结束语

通过分析识别结果,可以看出目前国内网上银行登录系统所使用的验证码都比较简单,容易通过机器破解,其安全性并不高,用户账户安全存在很大隐患。因此国内网上银行验证码是网上银行登录安全领域的一个薄弱环节,需在验证码验证环节加强安全性研究,使用安全性更高的验证码[13]。

良好的验证码应体现在以下两个方面:

(1)安全的健壮性,保证人眼可以识别的前提下,机器难以识别。

(2)用户的友好性,即最大限度地降低人验证码输入的繁琐程度和识别难度。

要达到机器难以识别的目的,需要给验证码加入适当干扰。给出如下建议:

(1)现有网上银行验证码字符个数都是固定的,通常为 4 个或 5 个,因此可以选择生成随机的字符的个数,字符数目的不确定将加大机器识别的难度;字符位置不固定,每个字符在整张图片中的相对位置不固定,在整体上减小了机器识别的可能性。

(2)对验证码添加干扰时,在不干扰人眼识别的前提下,尽量让字符颜色和干扰背景颜色相近,让干扰和字符类似,以此来增加机器前期预处理的难度。

(3)要尽量利用用户擅长而机器不擅长的特点来进行验证码生成,使字符粘连或对字符做较大的变形,若只在干扰背景上做过多复杂和花哨的东西,人眼都不易识别,自然也就失去了验证码设计的初衷。

参考文献:

[1] Imsamai M, Phimoltares S. 3D CAPTCHA: a next generation of the CAPTCHA[C]//Proc of 2010 international conference in information science and applications. Seoul, Korea: [s. n.], 2010.

[2] 陈福忠. 面向 WEB 代理的验证码图像识别[D]. 南京:南京理工大学,2007.

[3] Ostu N. A threshold selection method from gray-level histogram[J]. IEEE trans on systems man cybernetic, 1978(8):62-65.

[4] Due T Ø, Toffin T. Evaluation of binarization methods for document images[J]. IEEE transactions on pattern analysis and machine intelligence, 1995, 7(3):312-315.

[5] 胡振稳. 基于 BP 神经网络的车牌模糊识别的研究[D]. 武汉:武汉理工大学,2007.

[6] 付先珺. 基于 RPROP 人工神经网络对验证码识别的研究与实现[D]. 重庆:重庆大学,2011.

[7] 张月琴,刘　翔,孙先洋. 一种改进的 BP 神经网络算法与应用[J]. 计算机技术与发展,2012,22(8):163-166.

[8] Bernse J. Dynamic thresholding of gray-level images[C]// Proceedings of the eighth international conference on pattern recognition. Paris: [s. n.], 1986:1251-1255.

[9] 潘大夫,汪　渤. 一种基于外部轮廓的数字验证码识别方法[J]. 微计算机信息,2007,23(9-1):256-258.

[10] 张　伟. 基于人工神经网络的标签字符识别系统[D]. 长春:吉林大学,2006.

[11] 闫　栋. 车牌识别系统及其硬件实现的研究[D]. 西安:长

(下转第 160 页)

应用,并分角色对多种不同的信息进行分类访问与管理,分角色实现信息服务系统的功能,如图 3 所示。

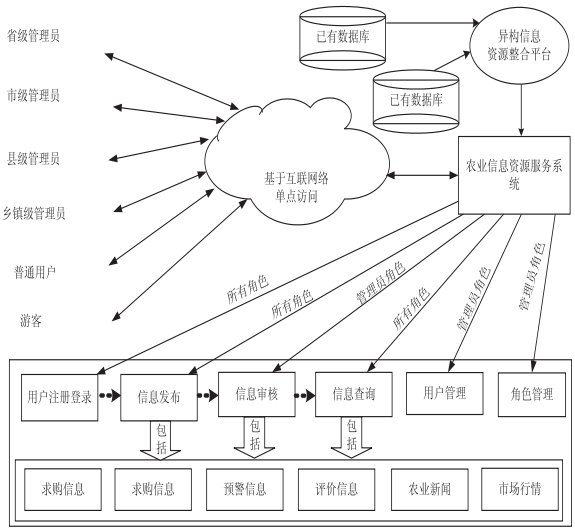

图 3 分角色实现农业信息服务系统

由图 3 可知:

①设计多级角色与权限:分为管理员权限(省级、市级、县级、乡镇级管理员角色)、普通用户角色及游客角色,各角色访问与角色相应的功能模型并完成不同的模块所要求的功能。如管理员实现审核、浏览、发布信息及授权功能等。

②所有角色用户注册登录后都可以发布信息(供应信息、求购信息、预警信息、市场行情、评价信息、农业新闻等),信息发布后需要发布者所在区域的管理员审核该信息(图 3 中的虚线箭头表示发布与审核之间的先后工作流关系),发布的信息经地区管理员审核后才允许被其他用户查询(但发布者自己可随时查看所发布的服务)。

针对图 3,文中基于 Windows XP,采用 java 语言、SQL Server2008 数据库、B/S 结构和三层软件架构(UI 表现层,BLL 业务逻辑层、DAL 数据访问层)进行相应的软件开发。

3 结束语

文中分析了农业信息资源共享与服务的现状及存在的问题,并针对农业信息资源建立中存在的分布式资源难以共享的问题,提出农业信息资源共享与信息服务的实施步骤,设计农业资源整合平台与信息服务系统,促进农业信息的共享与服务,辅助行政部门、农民或企业的决策支持。与文中提出的资源整合平台与信息服务系统紧密相关的一些建议如下:

(1)进一步建立和完善农业信息化基础设施、农业信息资源大型数据库与农业专家系统,不断应用高新信息技术(如物联网技术与遥感技术等)加强农业信息通道建设。

(2)逐渐形成多渠道采集农业信息机制,包括对种植业、畜牧、水产、农垦、农机、农业科技教育、农产品市场等领域采用多渠道、规范化采集与报送机制。

参考文献:

[1] Ali J, Kumar S. Information and communication technologies (ICTs) and farmers' decision-making across the agricultural supply chain[J]. International journal of information management, 2011, 31(2): 149-159.

[2] Mokotjo W, Kalusopa T. Evaluation of the agricultural information service (AIS) in Lesotho[J]. International journal of information management, 2010, 30(4): 350-356.

[3] 胡恒洋,刘苏社,张俊峰,等. 关于现代农业建设的认识和政策建议[J]. 宏观经济管理,2007(2):24-27.

[4] 梁 媛,王书华. 努力建构农村信息服务公共平台[J]. 中国国情国力,2008(1):38-41.

[5] 吴华刚. 推进福建农村科技信息服务体系建设的对策研究[J]. 情报探索,2010(7):55-56.

[6] 劳飞娟. 基层农业信息化服务体系建设的现状及对策初探[J]. 广西农学报,2010,25(1):96-98.

[7] 龚秀萍. 加快农业信息化服务体系建设构建云南社会主义新农村[J]. 安徽农学通报,2007,13(1):25-27.

[8] 王智芹. 依托信息化促进安徽新农村建设探讨[J]. 农业图书情报学刊,2009,21(12):11-14.

[9] 李习文,梁春阳,张玉梅. 宁夏新农村信息化建设的基本经验与存在的问题[J]. 宁夏社会科学,2009(2):64-67.

[10] 谷 莘. 关于推进农业与农村信息化建设的几点思考[J]. 农业图书情报学刊,2007(8):38-41.

[11] Muñoz-Gea J P, Malgosa-Sanahuja J, Manzanares-Lopez P, et al. Implementation of traceability using a distributed RFID-based mechanism[J]. Computers in industry, 2010, 61(5): 480-496.

[12] Zhang Peiyun, Xie Rongjian. Distributed heterogeneous information integration based on services composition[J]. Information-an international interdisciplinary journal, 2011, 14(12): 3941-3948.

[13] 谢荣见,张佩云,汪张林,等. 基于 Web 服务的虚拟企业信息集成研究[J]. 情报理论与实践,2007,30(4):520-523.

[14] 翟 梦,朱勤东. 基于 SOA 的福建交通地理信息公共服务平台建设[J]. 计算机技术与发展,2012,22(6):171-174.

(上接第 147 页)

安大学,2011.

[12] 张 华. 基于分类 BP 网络的车牌识别技术研究[D]. 太原:中北大学,2011.

[13] 文晓阳,高 能,荆继武. 论坛验证码技术的安全性分析[C]//全国计算机安全学术交流会论文集. 北京:中国计算机学会计算机安全专业委员会,2007:113-117.

网上银行验证码研究与安全性分析

作者： 冯杰， 李旭伟， FENG Jie， LI Xu-wei
作者单位： 四川大学 计算机学院,四川 成都,610065

刊名： 计算机技术与发展
ISTIC
英文刊名： Computer Technology and Development
年，卷(期)： 2013(11)