基于神经网络的数字验证码识别研究

吕 刚[1,2],郝 平[1]

(1. 浙江工业大学 信息工程学院,浙江 杭州 310032; 2. 金华广播电视大学 理工学院,浙江 金华 321000)

摘要:验证码是网络上普遍采用的一种用于真人交互证明的有效方法.对验证码识别的研究有助于解决硬人工智能问题,促进人工智能领域的进步.现有的研究多是针对一种验证码,通过多种方法进行识别.这类方法对先验知识的依赖很大,识别方法对其他验证码不一定有效,或者需要大量调整来适应新的验证码.为了研究验证码识别算法的适应性问题,通过选取多个具有代表性的网站的验证码图像,基于分割法和 Hopfield 神经网络进行分析和试验,取得了较好的试验结果.试验结果表明:利用字符图像灰度信息和 Hopfield 网络可以有效的对可分割的验证码进行分类识别,算法有一定的适应性,并且仅需字符图像的灰度信息既可适应新的验证码,对先验知识的依赖少.

关键词:神经网络;验证码;伪逆规则;文字识别;分割

中图分类号:TP391.43 **文献标识码**:A **文章编号**:1006-4303(2010)04-0433-04

Research on recognition of CAPTCHA based on neural network

LÜ Gang[1,2], HAO Ping[1]

(1. College of Information Engineering, Zhejiang University of Technology, Hangzhou 310032, China;
2. College of Technology, Jinhua Radio and Television University, Jinhua Zhejiang 321000, China)

Abstract: CAPTCHA is a commonly adopted effective means for human interactive proofs on Internet. Study in CAPTCHA is helpful to solve hard AI problems. Current methods aim to recognize one type of CAPTACHA via multiple methods. These methods need a mass of prior knowledge and they maybe are not necessarily valid for other CAPTCHA or need massive adjustment to suit new CAPTCHA. In order to study the adaptive problems on recognition algorithm of CAPTCHA, several CAPTCHAs on the representative websites are selected. The recognition algorithm is analyzed and tested based on segmentation method and Hopfield neural network. The test results are good. The experimental results show that the gray information of character image and Hopfield network can be used to recognize the divisible CAPTCHA. This algorithm has a good adaptability. It can adapt the new CAPTCHA with the gray information of character image and it less depends on the prior knowledge.

Key words: neural network; authentication code; pseudo inverse; character recognition; segmentation

验证码(Completely automated public turing test to tell computers and humans apart, CAPTCHA)是网络上普遍采用的一种用于真人交互证明的有效方法.目前验证码主要有 Gimpy, Bongo, PIX 三大类[1],网络上流行的以 Gimpy 及其变形为主,Gimpy 是一种基于 OCR 的验证码, Google,

收稿日期:2009-02-15

作者简介:吕 刚(1978—),男,浙江金华人,硕士研究生,讲师,主要从事图像处理和模式识别研究,E-mail:lg2578@tom.com.

QQ,csdn. net 等网站采用的验证码均与此类似,这些验证码被用来防止自动注册、垃圾邮件、自动投票等. 验证码设计的一条基本规则是减少硬人工智能(hard AI)问题[2],即任何能通过验证码测试的程序都可以用来解决一个困难的未解决的人工智能问题[1]. 因此一个问题如果不能用计算机程序解决,则可以用做验证码,反之,如果这个验证码被破解,则是人工智能领域的一大进步.

2003 年 Mori. G 和 Malik. J 利用形状上下文对 Gimpy 和 EZ-Gimpy 验证码进行了识别,识别率分别达到 33% 和 92%[2];2008 年 Yan. J 等对 Microsoft 的验证码进行了成功分割,并通过多分类器进行识别,识别率达到 60%[3];2005 年 Chellapilla. K 等研究表明单个的验证码字符可以很好的被计算机识别[4]. 国内学者对基于分割法的验证码识别也有一些研究,2007 年张淑雅等对 SMTH-BBS 验证码进行分割识别,分割结果采用分别采用 K 近邻分类器、BP 网络、SVM 进行识别,识别率均在 95% 以上[5]. 但是,目前对验证码识别的研究多是针对一种验证码,通过一种或多种方法进行识别. 这类方法对先验知识的依赖很大,识别方法对其他验证码不一定有效,或者需要大量调整来适应新的验证码. 为了研究验证码识别算法的适应性问题,通过选取多个具有代表性的网站的验证码图像,基于分割法和 Hopfield 神经网络进行分析和试验,取得了较好的试验结果. 试验结果表明:利用字符图像灰度信息和 Hopfield 网络可以有效的对可分割的验证码进行分类识别,算法有一定的适应性,并且仅需字符图像的灰度信息既可适应新的验证码,对先验知识的依赖少.

1 预处理

文中验证码图像来自多个不同的网站,包括数字和英文字母. 经过灰度化、二值化和分割等预处理操作划分为单个字符,再通过尺寸归一化为 18×12 像素的二值图像,然后以像素灰度值为特征转换成维数 216 的向量,提交 Hopfield 网络识别. 一般把从获得图像后到提交识别前的这段图像处理过程,称为图像预处理过程. 预处理的目的是获得更加适合识别的图像.

1.1 灰度化

在对 CSDN 网站验证码做识别研究的过程中发现,用传统方法灰度化后的图像亮度不能很好的保留原图亮度信息,目标像素和背景像素的亮度差受加权值的影响被缩小,灰度化后的图像有时候不适合做阀值分割,如图 1. 其中来源于 HSI 彩色空间中 I 分量的计算公式和来源于 NTSC 彩色空间中 Y 分量的计算公式[6]分别为

$$g(i,j)=\frac{R(i,j)+G(i,j)+B(i,j)}{3} \tag{1}$$

$$g(i,j)=0.11\times R(i,j)+0.59\times G(i,j)+0.3\times B(i,j) \tag{2}$$

基于灰度化的目的是做阀值分割,可以采用保留最小亮度(黑色)的方法,计算公式为

$$g(i,j)=\mathrm{Min}(R(i,j),G(i,j),B(i,j)) \tag{3}$$

试验证明,这种方法能最有效的保留字符和背景区的对比度信息,决定了下一步字符分割的成败,如图 1 所示.

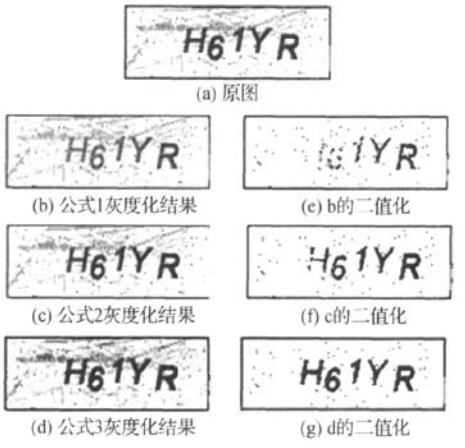

图 1 灰度化公式对比

Fig. 1 Comparison of graying formula

1.2 二值化

假设以 0 代表目标像素,1 代表背景色,则一幅灰度图的二值化[6]可以表述为

$$g(i,j)=\begin{cases}0, f(i,j)>T\\ 1, f(i,j)\leqslant T\end{cases} \tag{4}$$

其中,T 为一个确定的阀值. 可以采用最优阀值法(又叫最大类间方差法或 Otsu 法)计算阀值 T.

2 字符分割和归一化

输入神经网络识别的测试样本是单个字符,因此必须对验证码图像进行字符分割. 先用积分投影法获得字符区,然后再次用积分投影法对字符区进

行切分,得到单个的字符,如图 2 所示.

(a) 原图　(b) 灰度图　(c) 二值图　(d) 垂直投影图

图 2　积分投影分割示意图

Fig. 2　Integral projection segmentation demo

从垂直投影图中很容易找到明显的分割点,也可以采用求连通区的方法获得单个字符,对于阀值分割不干净的二值图,采用求连通区并过滤掉目标像素个数低于设定值的连通区,可以获得优于积分投影的识别效果.

Hopfield 神经网络要求输入的格式一致. 因此需要将分割后的字符图像尺寸归一化为 18×12,然后逐行一维化为长度 216 的向量 $\boldsymbol{P}$.

3　Hopfield 网络设计

Hopfield 网络是一种递归网络,因为具有类似人脑联想记忆的能力,因此在字符识别领域有广泛的应用. 一个离散 Hopfield 网络可以表示为

$$\boldsymbol{a}(t+1)=\text{stalins}(\boldsymbol{W}\boldsymbol{a}(t)+\boldsymbol{b}),\boldsymbol{a}(0)=\boldsymbol{P} \quad (5)$$

其中,stalins 是对称饱和线性函数. Hopfield 网络没有与之相对应的学习规则(式(5)没有对权值 $\boldsymbol{W}$ 和偏置 $\boldsymbol{b}$ 进行调整). Hopfield 网络设计技术的关键在于选择权值矩阵 $\boldsymbol{W}$ 和偏置 $\boldsymbol{b}$ 以便使性能参数最小化.

字符识别问题可以看成是一个联想存储器,对于输入 p_q 产生输出 t_q,性能参数函数为

$$F(\boldsymbol{W})=\sum_{q=1}^{Q}\|t_q-\boldsymbol{W}p_q\|^2 \quad (6)$$

令,$\boldsymbol{T}=[t_1,t_2,\cdots,t_Q]$,$\boldsymbol{P}=[p_1,p_2,\cdots,p_Q]$. 则,式(6)可写为

$$F(\boldsymbol{W})=\|\boldsymbol{T}-\boldsymbol{W}\boldsymbol{P}\|^2 \quad (7)$$

如果 $\boldsymbol{P}$ 的逆存在,则 $\boldsymbol{W}=\boldsymbol{T}\boldsymbol{P}^{-1}$,实际应用中这是很少有可能的. 通常矩阵 $\boldsymbol{P}$ 的列向量是线性无关的,但 p_q 的维数 R 比 p_q 的向量个数 Q 要大(文中 R 为 216,Q 则小于 34),所以 $\boldsymbol{P}$ 不是一个方阵,不存在确切的逆. 使式(7)最小化的权值矩阵可由仿逆规则给出,即

$$\boldsymbol{W}=\boldsymbol{T}\boldsymbol{P}^{+} \quad (8)$$

当矩阵 $\boldsymbol{P}$ 的行数 R 大于其列数 Q,且 $\boldsymbol{P}$ 的列向量线性无关时,其仿逆为

$$\boldsymbol{P}^{+}=(\boldsymbol{P}^{\mathrm{T}}\boldsymbol{P})^{-1}\boldsymbol{P}^{\mathrm{T}} \quad (9)$$

这样就获得了网络的权值矩阵 $\boldsymbol{W}=\boldsymbol{T}(\boldsymbol{P}^{\mathrm{T}}\boldsymbol{P})^{-1}\boldsymbol{P}^{\mathrm{T}}$,偏置 $\boldsymbol{b}$ 初始化为 0 向量.

Hopfield 网络是递归网络,还存在假稳态,收敛性等问题. 试验中出现了假稳态、振荡收敛,通过增加输入模式可以避免;没有出现发散的情况.

4　试验与分析

选取 4 个不同网站的验证码图片进行识别,见图 3,其中 3 个是无粘连的纯数字验证码,另外一个是带复杂粘连的数字和字母结合的验证码(CSDN 网站的验证码).

(a) 一般网站　(b) 工行网银　(c) 农行网银　(d) csdn

图 3　验证码示例

Fig. 3　CAPTCHA demos

用 Hopfield 网络进行验证码识别的主要步骤如下:

(1) 从已知验证码图像中分割出足够的字符样本(每个字符 1－3 个样本)并归一化,用来构建 Hopfield 网络的训练样本.

(2) 训练 Hopfield 网络.

(3) 把测试用验证码图像分割成单个字符并归一化,得到测试样本(单个字符).

(4) 提交到训练好的网络中进行识别.

试验结果见表 1.

表 1　验证码识别试验数据

Table 1　Result of recognition experiment

类别	模板数/个	Hopfield 识别率/%	预处理正确率/%	分割正确率/%
一般网站	10	100	100	100
工行网银	20	96	100	90
农行网银	12	80	较好	94
CSDN	34	42	82	68

通常情况下,用 Hopfield 网络进行验证码识别只需要 10 个数字(0－9)的模板. 工行网银验证码有简单的字体变化,通过适当增加模板(20 个),可以提高识别率;CSDN 验证码是数字和字母混合的验证码,没有数字 0 和字母 o,共需要 34 个模板. 测试样本数为 50 个,因为样本是随机产生的,样本数已能够代表一般情况.

一般网站的背景干扰通过合理的灰度化和 Otsu 阀值分割(二值化)可以去除的很干净,预处理正确率很高. 工行网银的背景和前景较一致,Otsu 阀

值的灰度值偏大. 笔者选用了一个较小的固定阀值，使得预处理正确率达到 100%；分割正确率为 90%，有两个样本因简单粘连导致无法分割，还有 3 个样本因为和边框粘连造成过分割. 实际的识别率为 96%，Hopfield 网络对过分割的 3 个样本获得了正确的识别结果，可见 Hopfield 具备一定的联想记忆的能力，能够从残缺的字符中恢复出整个字符的信息. 农行网银和工行网银类似，但背景和前景的灰度值更加接近，增大了预处理难度. 这里预处理正确率表示为较好，而不是一个具体的值，表示预处理结果都有一定程序的干扰不能完全除去. 最后分割得到的字符有幅度 20%左右的噪声干扰和位移干扰，有 3 个样本存在过分割. Hopfield 网络的识别率为 80%，20%的噪声干扰对 Hopfield 网络影响很小，但字符位移干扰对 Hopfield 网络影响明显. CSDN 验证码的难度主要在复杂粘连，分割法识别的效果不如人意.

5 结 论

基于积分投影分割和 Hopfield 神经网络建立了一套验证码识别的一般化算法，介绍了 Hopfield 网络的原理和实现. 通过实验验证了在验证码字符可分割的情况下，该算法具有训练简单，仅需少量先验知识，识别正确率高、适应性好的优点. 在字符粘连的情况下，如果提高粘连字符分割的正确率是下一步研究的方向.

参考文献：

[1] AHN L V, BLUM M, LANGFORD J. Telling humans and computers apart (automatically) or How lazy cryptographers do AI[R]. Pennsylvania, USA: CMU Press, 2002.

[2] MORI G, MALIK J. Recognizing objects in adversarial clutter: breaking a visual CAPTCHA[C]//Computer Vision and Pattern Recognition. IEEE Computer Society Conference on. New York, USA: IEEE Press, 2003(1): 134-141.

[3] YAN J, AHMAD A S E. A Low-cost attack on a microsoft CAPTCHA[C]//Proceedings of the 15th ACM Conference on Computer and Communications Security. New York, USA: ACM Press, 2008: 543-554.

[4] CHELLAPILLA K, LARSON K, SIMARD P, et al. Computers beat humans at single character recognition in reading-based Human Interaction Proofs[C]//In Proceedings of the Second Conference on Email and Anti-Spam. CA, USA: Stanford University, 2005.

[5] 张淑雅，赵一鸣，赵晓宇，等. 认证码字符识别方法的研究[J]. 宁波大学学报：理工版，2007，12(4)：0429-0433.

[6] GONZALEZ R C, WOODS R E, EDDINS S L. 数字图像处理(MATLAB 版)[M]. 阮秋琦，译. 2 版. 北京：电子工业出版社，2007.

（责任编辑：刘 岩）

《浙江工业大学学报》荣获“第四届华东地区优秀期刊”称号

2009 年 11 月在上海举行了第四届华东地区优秀期刊评选。经华东地区优秀期刊评审委员会最终评定，《浙江工业大学学报》荣获“第四届华东地区优秀期刊”称号。

此次评选活动由华东地区六省一市新闻出版局联合主办，旨在发挥优秀期刊在期刊出版事业中的示范作用，带动华东地区期刊整体质量提高，推动期刊出版繁荣发展。我省共有 33 种期刊被评为华东地区优秀期刊，其中包括 4 种普通高等学校学报。

浙江工业大学学报编辑部

基于神经网络的数字验证码识别研究

作者： 吕刚， 郝平， L(U) Gang， HAO Ping
作者单位： 吕刚,L(U) Gang(浙江工业大学,信息工程学院,浙江,杭州,310032;金华广播电视大学,理工学院,浙江,金华,321000)， 郝平,HAO Ping(浙江工业大学,信息工程学院,浙江,杭州,310032)
刊名： 浙江工业大学学报 ISTIC PKU
英文刊名： JOURNAL OF ZHEJIANG UNIVERSITY OF TECHNOLOGY
年，卷(期)： 2010,38(4)
被引用次数： 3次

参考文献(6条)

1. AHN L V;BLUM M;LANGFORD J Telling humans and computers apart(automatically)or How lazy cryptographers do AI 2002

2. MORI G;MALIK J Recognizing objects in adversarial clutter:breaking a visual CAPTCHA 2003

3. YAN J;AHMAD A S E A Low-cost attack on a microsoft CAPTCHA 2008

4. CHELLAPILLA K;LARSON K;SIMARD P Computers beat humans at single character recognition in readingbased Human Interaction Proofs 2005

5. 张淑雅;赵一鸣;赵晓宇 认证码字符识别方法的研究[期刊论文]-宁波大学学报(理工版) 2007(04)

6. GONZALEZ R C;WOODS R E;EDDINS S L;阮秋琦 数字图像处理(MATLAB版) 2007

本文读者也读过(10条)

1. 朱绍文. 陈光喜. Zhu Shaowen. Chen Guangxi 一种简单的基于字符形状的验证码识别技术[期刊论文]-桂林电子科技大学学报2010,30(1)

2. 贾磊磊. 陈锡华. 熊川. JIA Lei-lei. CHEN Xi-hua. XIONG Chuan 验证码的模糊识别[期刊论文]-西昌学院学报(自然科学版)2010,24(1)

3. 吕刚 带干扰的验证码识别研究[学位论文]2009

4. 文晓阳. 高能. 夏鲁宁. 荆继武. WEN Xiao-yang. GAO Neng. XIA Lu-ning. JING Ji-wu 高效的验证码识别技术与验证码分类思想[期刊论文]-计算机工程2009,35(8)

5. 苏磊. 马良. SU LEI. MA LIANG 形状上下文在验证码识别中的应用[期刊论文]-微计算机信息2007,23(35)

6. 李颖 Web验证码的生成与识别[学位论文]2008

7. 潘大夫. 汪渤. PAN DAFU. WANG BO 一种基于外部轮廓的数字验证码识别方法[期刊论文]-微计算机信息2007,23(25)

8. 基于神经网络的网络验证码识别研究[期刊论文]-计算机工程与科学2009,31(12)

9. 唐娅琴. Tang Yaqin 验证码的设计与破解探讨[期刊论文]-计算机与数字工程2010,38(5)

10. 陈福忠 面向WEB代理的验证码图片识别[学位论文]2007

引证文献(3条)

1. 景国彬. 丁网萍 浅谈误差逆传播神经网络的网站验证码识别研究[期刊论文]-信息通信 2012(2)

2. 胡光中. 欧阳鸿志 基于PIL的验证码快速识别框架的研究[期刊论文]-计算机与现代化 2012(5)

3. 吕刚. 郝平 基于权值模板和监督学习的验证码识别[期刊论文]-计算机与现代化 2010(12)