Advances in Applied Mathematics 应用数学进展, 2021, 10(11), 4006-4016
Published Online November 2021 in Hans. http://www.hanspub.org/journal/aam
https://doi.org/10.12677/aam.2021.1011426

Hans汉斯

基于Hopfield神经网络模型的验证码识别问题

张靖文，林萍芝，肖思佳，王浩华*

海南大学理学院，海南 海口

收稿日期：2021年10月23日；录用日期：2021年11月13日；发布日期：2021年11月25日

摘　要

为了避免恶意破解密码、刷票、论坛注水、黑客攻击等行为，验证码因此而生，它通过强制人机交互的方法来抵御机器自动化攻击。但准确识别验证码是当前还未完全解决的难题。本文的研究对象为四位数字的验证码，采用分割分析和Hopfield神经网络的方法对验证码识别及其精度进行分析。建立并训练Hopfield网络对验证码图像变换后的矢量进行模式识别，比对的结论表明，Hopfield神经网络算法可以得到比较好的测试结果，具有推广应用的价值。

关键词

灰度化，二值化，边缘检测分割，Hopfield神经网络，验证码识别

Hopfield Neural Network Based Approach to Recognizing the Verification Code

Jingwen Zhang, Pingzhi Lin, Sijia Xiao, Haohua Wang*

School of Sciences, Hainan University, Haikou Hainan

Received: Oct. 23rd, 2021; accepted: Nov. 13th, 2021; published: Nov. 25th, 2021

Abstract

In order to avoid malicious cracking of passwords, ticket brushing, forum water injection, hacking, etc., verification codes are born. It uses the method of forcing human-computer interaction to resist machine automation attacks. But accurately identifying the verification code is a difficult problem that has not yet been completely resolved. The research object of this article is a four-digit verification code. The method of segmentation analysis and Hopfield neural network is used to analyze the verification code recognition and its accuracy. Establish and train the Hopfield network to

*通讯作者。

文章引用: 张靖文, 林萍芝, 肖思佳, 王浩华. 基于 Hopfield 神经网络模型的验证码识别问题[J]. 应用数学进展, 2021, 10(11): 4006-4016. DOI: 10.12677/aam.2021.1011426

perform pattern recognition on the transformed vector of the captcha image. The conclusion of the comparison shows that the Hopfield neural network algorithm can get better test results and has the value of popularization and application.

Keywords

Gray Processing, Binarization, Edge Detection and Segmentation, Hopfield Neural Network, Verification Code Recognition

1. 引言

图像识别问题是人工智能领域上一个复杂的问题，其本质是图像被计算机分析和处理，对于不同种类的图像处理方式也会有所不同，是一种被开发出识别各种模式的目标和对象的技术。图像识别的种类繁多，验证码识别是其中一种，也是互联网上常用的真实人机交互验证的有效方法[1] [2]。

对于识别数字验证码这个问题，国内外众多学者进行了许多研究，李成建等[3]在识别数字验证码问题上使用了卷积神经网络算法；潘浩等[4]利用 Tesseract 引擎，在经过训练之后，能够分别识别简单和复杂的验证码；冯军军等[5]提出了一种多模块验证码识别方法，这种方法涉及 python3、selenium、PIL 等模块。但是这些算法着重研究模块化识别，考虑到常用的验证码有四位数字和字母验证码以及目前最新的汉字验证码，本文主要考察的验证码是由四位数字以及一些噪声组成的图片。本文先对数字验证码使用了如下预处理操作：灰度化、二值化和边缘检测分割。再通过中值滤波的方法去除噪点，将图片转变成 Hopfield 神经网络进行模式识别。这么做具有一定的抗干扰能力是因为其结合了神经网络的联想记忆功能。图形用户界面(GUI)测试结果表明，Hopfield 神经网络模型具有良好的稳健性。

2. 图像的预处理

如图 1，验证码为带噪声的数字，计算机无法直接识别和处理带有太多噪声的验证码，因此，就需要预处理验证码，首先将每个图像中的四个数字全部转化为单独分开的数字，再利用归一化把每个数字转为 7*5 的二值图像，然后根据灰度值把图像转化成维数为 35 的向量，最后把向量放入 Hopfield 网络进行识别。

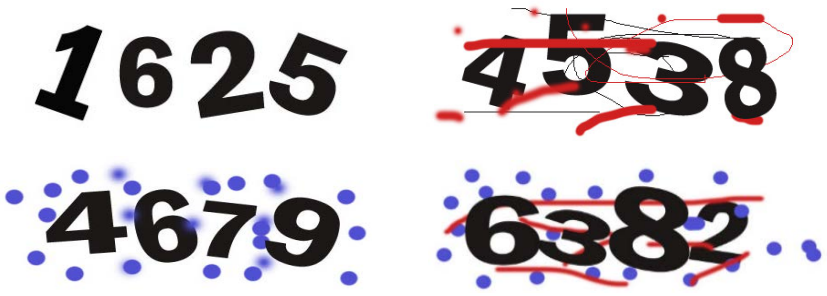


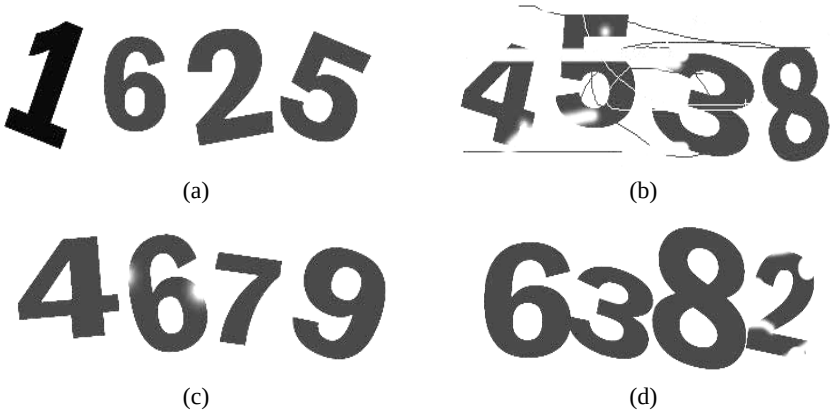
Figure 1. Digital verification code
图 1. 数字验证码

2.1. 灰度化

在对数字验证码图像做识别研究的过程中，如果想要让计算机更快速和有效的识别数字验证码图像，有一个步骤是不可省略的，那就是对彩色图像进行灰度化处理[6] [7]，阈值分割是灰度化处理的目的。计算阈值有很多的方法，本文考虑了最大亮度法，它的计算方法为：

$$g(i,j)=\mathrm{Max}\left(R(i,j),G(i,j),B(i,j)\right)$$

验证码图像经过灰度化后的结果如下图 2 所示：



(a) (b)

(c) (d)

Figure 2. Retain the grayscale results of the maximum brightness method
图 2. 保留最大亮度法的灰度化结果图

2.2. 二值化

设背景色用 0 表示，目标像素用 1 表示。则灰度图的二值化[8]可以表示为：

$$g(i,j)=\begin{cases}1 & f(i,j)>T\\ 0 & f(i,j)\le T\end{cases}$$

其中 T 指的是确定的阀值。

二值化的核心步骤就在于此阀值，本文采用最大类间方差法确定 T 的取值[7] [8]。

最大类间方差法是由 Otsu 在 1978 年提出的一种算法[7] [8]，这种算法一经提出就被广泛使用。定义类内方差 σ_w^2，类间方差 σ_β^2 和总体方差 σ_T^2，还定义了三个等价的标准度量：

$$\lambda=\frac{\sigma_\beta^2}{\sigma_W^2},K=\frac{\sigma_T^2}{\sigma_W^2},\eta=\frac{\sigma_\beta^2}{\sigma_T^2}$$

为了避免过多的计算，通过简化下面的公式进行简化：

$$\sigma^2(T)=W_A(\mu a-\mu)^2+W_b(\mu b-\mu)^2$$

其中，σ^2 为两类间最大方差，W_A，W_b 分别为 A，B 类概率，μa，μb 为分别为 A，B 类平均灰度，μ 为平均灰度。

不同阈值会将图像分割成两个不同的部分，若 T 能使分成两部分的总方差 $\sigma^2(T)$ 取得最大值，那么该值就是最佳阈值。下图 3 是对原图利用上述方法后的对比。

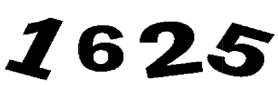
原图	最大类间法二值化
	
	
	
	

Figure 3. Maximum interclass method binarization
图 3. 最大类间法二值化

2.3. 中值滤波

噪声是识别数字验证码图像中的一个阻碍，它会大大降低计算机识别的准确性，因此需要对数字图像进行降噪处理。降噪效果的好坏会影响之后的处理，因此根据噪点的特点，本文使用中值滤波的方法去除噪声，主要利用高频噪声，孤立偏差大的特点进行的[9] [10]。几种常用的识别窗口如下图 4 所示，窗口的中心与确认识别的像素对齐。

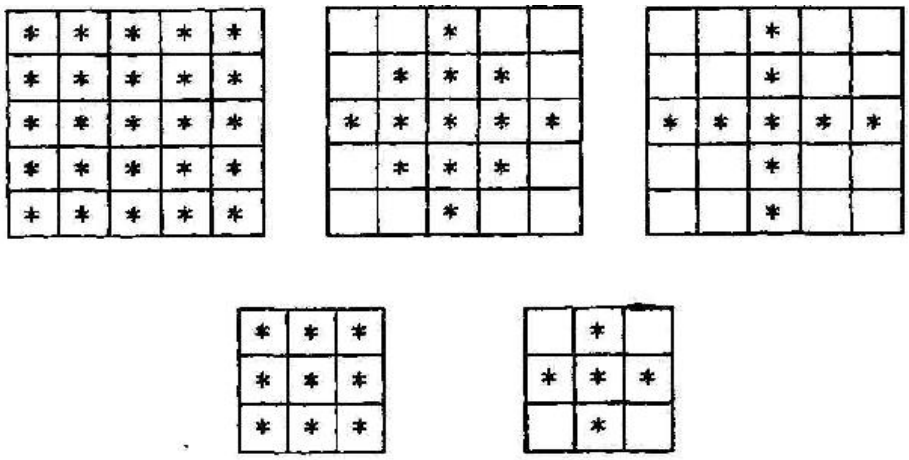


Figure 4. Gray value recognition window
图 4. 灰度值识别窗口

本文使用了图 4 中的 3*3 模板，过滤结果如图 5 所示。

从图 5 可以看出，第二组数字验证码的效果较好，消去了大量的噪点。与之相对比，由于另外三组验证码的噪点不是很多，因此滤波效果不明显，但总体来看，经过中值滤波后的图像上的噪点比未经过滤波图像上的噪点要少，且可以保护图像边缘，因此使用中值滤波效果较好。

二值化处理后的图片	中值滤波处理后的图片	参数
		3*3模板
		3*3模板
		3*3模板
		3*3模板

Figure 5. Median filter
图 5. 中值滤波

2.4. 字符串分割和归一化

神经网络识别的采样要求是单个字符，因此需要分割图像。采用有效的方法能提升识别的准确率。字符串分割的方法有多种，有积分投影法和边缘检测分割法[9] [10] [11]等，但利用积分投影法进行字符串的分割时，不同验证码的字符分割位置以及长度和宽度等存在差异，并且不同的字符还可能会相连，难以用简便的算法统一处理。为此，本文构造了基于图像边缘检测的分割方法。

2.4.1. 边缘检测分割法

图像处理中的关键问题是边缘检测，目的是识别图像中光度变化明显的点[12] [13]。边缘指的是图像中物体与背景之间以及物体与物体之间灰度变化较大的所有点连接起来形成的线，数字图像中物体的边缘可利用灰度的不连续性来寻找，如果将一个边界定义为一组具有一定数量光强变化的点，则边缘检测就是计算光强变化的导数。因此，可以通过使用差分运算来定位对象的边缘，以获得信号的转换率。边缘是两个区域的边界，这是图像分割所依赖的重要定义。这个定义可以用来分割图像。为了解决图像分割问题，就需要识别图像的边缘以便于图像分割。

边缘检测算法的主要思想为：对一个连续的图像 $f(x,y)$，在位置 (x,y) 的梯度可以表示成一个矢量，假设用 G_x 和 G_y 来表示 $f(x,y)$ 沿着 x 方向和 y 方向的梯度，对 G_x 和 G_y 分别使用不同模板，然后将两个模板拼在一起，形成梯度算子。对图像使用微分运算，图像灰度变化较小时，计算出的微分值较小。微分值是否边缘点取决于阈值是否小于微分值，如果阈值小于微分值，则将该点定义为边缘点。

本文采用了以 Sobel 微分算子为基础的边缘检测分割的方法[12] [14]。

图 6 是四组验证码图像经过边缘检测后的结果图。

根据图 6，我们可以看出，经过边缘检测后的图像与之前的图像相对比少了很多的数据，也能起降噪的作用，并且保留了原图中的重要数据信息。

2.4.2. 归一化

由于 Hopfield 网络需要输入相同的格式，但切割后的字符大小存在差异，为了让识别的标准性和准确率更高，就需要把图像标准化，统一尺寸。因此需要将切割后的字符图像尺寸归一化为 7*5，然后逐行化为长度为 35 的一维向量 P。

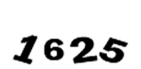
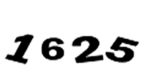
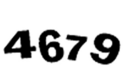
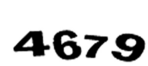
二值化后的图片	中值滤波后的图片	边缘检测后的图像
		
		
		
		

Figure 6. Image after edge detection
图 6. 边缘检测后的图像

3. Hopfield 网络识别模型的建立与验证

3.1. 神经网络的基本原理

Hopfield 网络全连接网络[13]。图 7 就很好地展示出了一个 Hopfield 网络，其中n是神经元的数量，V 是输入向量，U 是输出向量，W 是神经元之间的连接权值。在离散 Hopfield 网络中，是每个神经元仅有“1”与“−1”这两个可输出的状态值。可用向量$V=\{v_1,v_2,\cdots,v_n\}$表示当前神经元的状态，其中v_i表示第 i 个神经元的状态。由于神经元两两相连，因此两个不同神经元之间可以相互传递信息。

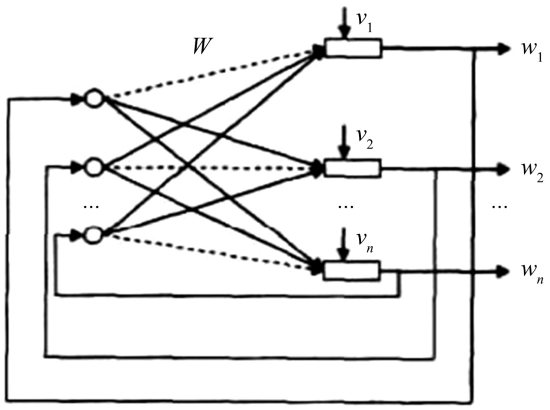


Figure 7. A fully interconnected network with feedback
图 7. 有反馈的全互联型网络

设一个 Hopfield 网络由 n 个神经元构成，V_i 和V_j 分别表示第 i，j 个神经元节点的状态，W 表示神经元 i 和 j 的连接权值，θ 表示神经元 i 的阈值。那么节点的能量可表示为：

$$E_i=-\left(\sum_{j\neq 1}^{n}w_{ij}v_i-\theta_i\right)v$$

因此，网络整体能量的函数表示如下：

$$E_i = -\frac{1}{2}\sum_{i=1}^{n}\sum_{j\neq i}^{n} w_{ij}v_i v_j + \sum_{i=1}^{n}\theta_i v_i$$

设一个 Hopfield 网络由 n 个神经元构成的，在 t 时刻，记第 i 个神经元接收来自剩下 $n-1$ 个神经元输入值的总和为 $u_i(t)$。在 $t+1$ 时刻，如果第 i 个神经元的输出值 $v_i(t+1)$ 是符号函数作用于 $u_i(t)$ 中的某个阈值时，则该神经元称为活跃神经元。此迭代步骤为：

步骤 1：将 i 作为随机选择的一个神经元；

步骤 2：计算选中神经元 $i(1\le i\le n)$ 的总输入

$$u_i(t) = \sum_{j\neq i}^{n} w_{ij}v_i - \theta_i \ ;$$

步骤 3：根据 $u_i(t)$ 值大小，改变神经元的状态

$$\text{if} \quad (u_i(t)) \ge 0$$

$$\text{then} \quad v_i(t+1) = 1$$

$$\text{else} \quad v_i(t+1) = 0 \ ;$$

步骤 4：除神经元 i 以外的其他神经元 j 状态不发生改变；

步骤 5：转到(1)，循环至网络稳定为止。

Hopfield 网络具固定的稳定状态，权矩阵 W 可以根据网络的学习求得，再利用计算的方法进行联想。对于给出的 M 个模式，可以使用 Hebb 规则进行学习。

$$W_{ij} = \begin{cases} 0 & i = j \\ \sum_{k=1}^{M} v_i(k)v_j(k) & i \neq j \end{cases}$$

依照上述的法则求得权矩阵后，就已经把这 M 个模式存入到网络的连接权中。

3.2. Hopfield 神经网络建立

3.2.1. 输入样本的设计

对每个数字图像进行数字化处理，并将数字图像转换为神经网络可以处理的输入值和输出值，这样就得到输入样本。

0~9 中的每个数可以用带布尔值的 7*5 矩阵表示。比如“0”可以表示为：

$$r0 = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}.$$

每个数字都可以用 7*5 = 35 个元素组成一个行矩阵，再将 10 个数字均被定义成输入向量，每个数字的输入向量都有 35 个元素，全部数字组成一个 10*35 输入向量矩阵 alphabet。把这 10 个数字输入到变量 Number 中，变量成为网络的输入样本矩阵：

$$\text{Number} = [r1, r2, r3, r4, r5, r6, r7, r8, r9, r10].$$

3.2.2. 输出样本的设计

输出样本定义为 10*10 单位矩阵。对于每个数字输入，输出在其行的相应位置为 1，在其余位置为 0。利用下面的 MATLAB 命令能简单实现：

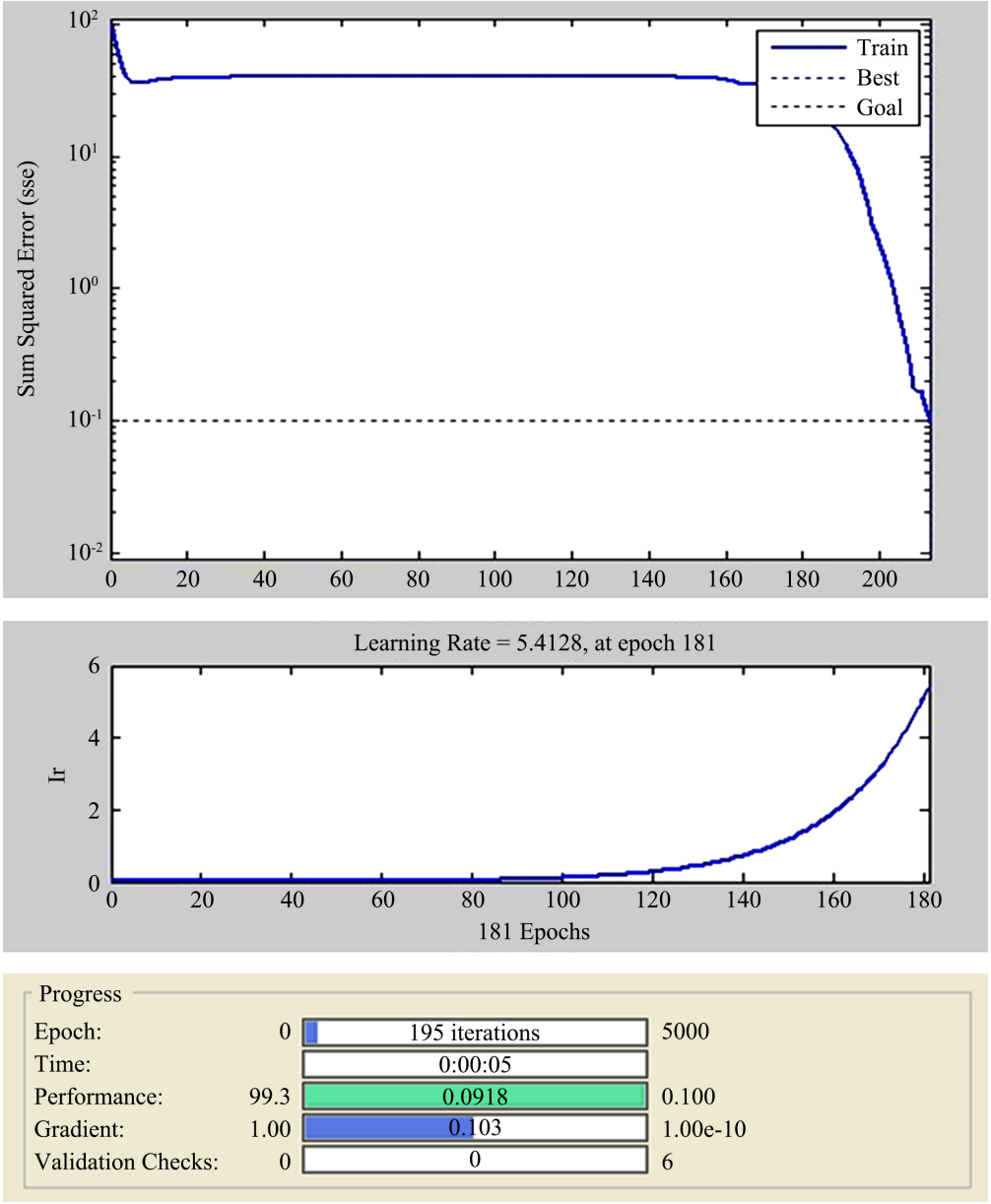


Figure 8. The sum of error squares and the change in learning rate
图 8. 误差平方和及学习速率的变化图

Targets = eye (10)。

每输入一个数字，网络就可以输出一个向量。

3.2.3. 网络结构的设计

根据上文可知，神经网络需要输入 35 个神经元和输出 10 个神经元[14] [15]。建立 BP 网络的必要条

件是确定隐层和隐层神经元的数目，本文所用的 BP 网络只有一个隐层，隐层神经元的个数必须经过多次重复实验才能确定一个合适的值，一种比较好的方法就是：每次调试时，为了加快误差下降的速率，只增加 1 或 2 个神经元。根据这种方法，经过测试，最终选定 10 个神经元作为隐含层神经元的数量。

网络接受的输入向量应该为布尔向量，但是实际上，接收到的输入向量并不是布尔向量，这是因为存在一定的误差。为了避免这样的误差给实验带来不便，就需要设计的网络有一定的容错能力。可以设置噪声的均值为 0 并且标准偏差小于或等于 0.2，这样网络就有一定的容错能力辨别输入向量。

把该网络设计成两层的 BP 网络结果，这样能够识别数字。在隐含层和输入层之间的神经元传递使用 logsigmoid 函数，这个函数输出的值为布尔值，再将输出的值输入到输入层中。

3.2.4. 初始化

首先生产 10 个样本数据，让它们每个能代表 0~9 中的每个数，再构造双层网络，本文使用了 newff 函数，再定义第一隐含层权值 WI 和 B1 初始值，本文采用初始化的 nwlog.m 函数，用随机数选取后一层的初始值。这便是对 hopfield 网络的初始化过程。

3.3. 无噪声网络训练

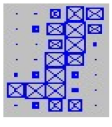
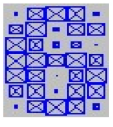
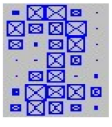
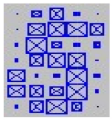
上述设计的网络没有抗干扰的能力，为了使其具备这个能力，就需要对网络进行训练，经过训练的网络能正确的处理由于错误输入导致的问题。如果能得到一个可以识别带有噪声的输入值的网络，就能把干扰噪声数字化处理转换成有均值的随机值。

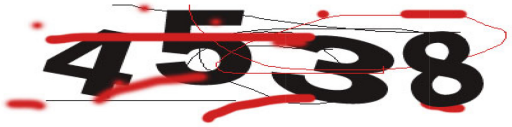
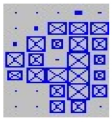
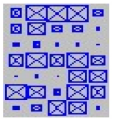
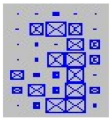
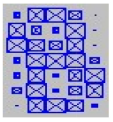
为了训练一个具有低平方误差和理想输入的网络，本文的无噪声训练采用学习速度快捷、附加动量因子的 BP 算法[14] [15]。

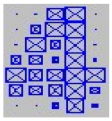
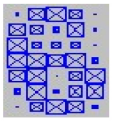
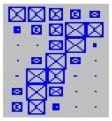
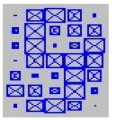
图 8 表现了在网络训练过程中，误差平方和、学习速度在各个学习阶段的变化。从图 8 中可以看到，网络的稳定性会随着学习次数的增加而提高。从图中还可以看出，在学习次数大约为 196 次时，我们设计的神经网络会达到稳定状态。

3.4. 网络测试

在网络测试中，通过 GUI 界面，来提高交互性。得到的测试结果分别如下图 9 所示。

原始图像				
神经网络的输入字符				
分出的单个字符特征				
模式识别的结果	1	6	2	0

滤波后的图像				
神经网络的输入字符				
分出的单个字符特征				
模式识别的结果	7	0	0	8

滤波后的图像				
神经网络的输入字符				
分出的单个字符特征				
模式识别的结果	4	6	7	0

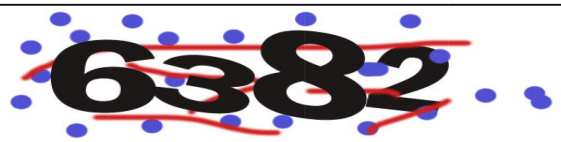
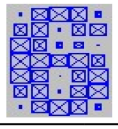
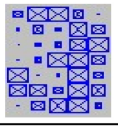
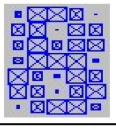
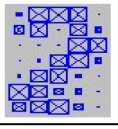
滤波后的图像				
神经网络的输入字符				
分出的单个字符特征				
模式识别的结果	6	1	8	7

Figure 9. Test result
图 9. 测试结果

4. 小结

验证码的自动识别归根到底是人工智能的问题，这里主要考察数字验证码的识别问题，采用的是Hopfield 神经网络与模式识别的研究方法。神经网络模型本身发展并不成熟，一些基础的理论也有待完善，拥有自身固有的优缺点[16]。由图 9 可以看出，本模型有一定的识别价值。但是其正确率有待提高，特别是数字验证码识别的难点主要体现在 3、5、9 身上，因为这些字符特征很相近，再加上一些随机性的干扰，很容易将其误识，这也是符合常理的。另外，在进行网络训练时，应保证对充足的样本来进行训练。对于含噪声的数字样本的识别问题，值得进一步研究。

基金项目

海南省自然科学基金(120RC451)，国家自然科学基金(11761025, 11961018, 11901114)，广东省教育厅青年创新人才类(2017KQNCX081)，广州市科技创新一般项目(201904010010)，中山大学广东省计算科学重点实验室开放课题基金资助(2018001)，海南省研究生创新科研课题项目(Hys2020-108)。

参考文献

[1] 王斌君, 王靖亚, 杜凯选, 韩宇. 验证码技术的攻防对策研究[J]. 计算机应用研究, 2013, 30(9): 2776-2779.

[2] 文晓阳, 高能, 夏鲁宁, 荆继武. 高效的验证码识别技术与验证码分类思想[J]. 计算机工程, 2009, 35(8): 186-188+191.

[3] 李建成, 李富城, 刘建芳. 基于卷积神经网络的数字验证码识别研究[J]. 电子设计工程, 2019, 27(17): 107-111.

[4] 潘浩, 李兰. 基于 Tesseract 引擎样本训练的验证码识别[J]. 信息与电脑(理论版), 2020, 32(1): 138-139+142.

[5] 冯军军, 王海沛, 陈新华. 基于 Python3 的极验验证码识别的研究[J]. 电脑知识与技术, 2019, 15(22): 37-39.

[6] 陈广秋, 王冰雪, 刘美, 刘广文. 基于结构信息相似度的线性投影灰度化算法[J]. 2020, 57(4): 877-884.

[7] 陈海峰, 丁丽丽. 二值化图像的灰度处理算法研究[J]. 电脑与电信, 2019(7): 34-38.

[8] 李治江, 丛林. 基于朴素贝叶斯理论的彩色图像二值化研究方法[J]. 数字印刷, 2020(1): 17-21.

[9] 钟彩, 杨兴耀. 车牌定位与车牌分割技术研究[J]. 电脑知识与技术, 2018, 14(2): 172-173.

[10] 张萍. 基于 MATLAB 的汽车牌照自动识别技术研究[J]. 自动化技术与应用, 2019, 38(11): 132-135+149.

[11] 皇甫磊磊, 阎瑞兵, 赵晓晓. 离散 Hopfield 神经网络在车牌识别系统中的应用[J]. 信息与电脑(理论版), 2018(17): 81-84.

[12] 徐展彧. 一种基于卷积神经网络的验证码识别方法[P]. 中国, CN110276357A. 2019-09-24.

[13] 张圣洁, 秦祎晗, 刘奕慧, 郭玮. 用于验证码识别的神经网络模型的构建方法和装置[P]. 中国, CN107360137A. 2017-11-17.

[14] 吕霁. 基于神经网络的验证码识别技术研究[D]: [硕士学位论文]. 泉州: 华侨大学, 2015.

[15] 李世成, 东野长磊. 基于卷积神经网络的验证码识别[J]. 软件, 2020, 41(4): 173-177.

[16] 杨晓帆, 陈廷槐. 人工神经网络固有的优点和缺点[J]. 计算机科学, 1994, 21(2): 23-26.