Computer Science and Application 计算机科学与应用, 2022, 12(7), 1871-1876
Published Online July 2022 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2022.127187

Hans汉斯

基于卷积神经网络的人脸活体检测模型研究

周沛松[1,2]

[1]河北地质大学信息工程学院，河北 石家庄
[2]智能传感物联网技术河北省工程研究中心，河北 石家庄

收稿日期：2022年6月24日；录用日期：2022年7月22日；发布日期：2022年7月29日

摘 要

针对以往身份验证系统容易被攻击活体欺诈的问题，提出了一种基于深度学习的活体检测算法。主要包括：1) 通过图像增强技术对现有少量真实和欺诈图像进行平移、旋转、翻转等几何变换自制数据集，用于模型训练、验证及测试。2) 针对现有算法对光照条件不足的照片识别准确率较低的问题，提出了一种基于照片的活体检测模型。通过检测照片中的人脸区域，并针对人脸区域中的像素、纹理以及人脸特征差异进行活体和非活体二分类预测。实验结果表明，本文提出的算法在光照条件不足的图像中准确率达到86%。同时与以往模型相比，在保证模型预测精度的基础上减少了参数的数量。

关键词

活体检测，深度学习，卷积神经网络，目标检测，计算机视觉

Research on Face *in Vivo* Detection Model Based on Convolutional Neural Network

Peisong Zhou[1,2]

[1]School of Information Engineering, Hebei University of Geosciences, Shijiazhuang Hebei
[2]Intelligent Sensing Internet of Things Technology Hebei Engineering Research Center, Shijiazhuang Hebei

Received: Jun. 24th, 2022; accepted: Jul. 22nd, 2022; published: Jul. 29th, 2022

Abstract

Aiming at the problem that previous identity verification systems are easy to be attacked by vivisection fraud, a vivisection detection algorithm based on deep learning was proposed. It mainly includes: 1) Self-made data sets for translation, rotation and reversal of a small number of existing real and fraudulent images by using image enhancement technology for model training, verifica-

文章引用: 周沛松. 基于卷积神经网络的人脸活体检测模型研究[J]. 计算机科学与应用, 2022, 12(7): 1871-1876.
DOI: 10.12677/csa.2022.127187

tion and testing. 2) Aiming at the problem of low recognition accuracy of existing algorithms for photos with insufficient illumination conditions, a photo-based *in vivo* detection model is proposed. By detecting the face region in the photo, we predict the difference of pixel, texture and face feature in the face region by living and non-living dichotomies. Experimental results show that the accuracy of the proposed algorithm reaches 86% in images with insufficient illumination conditions. At the same time, compared with the previous models, the number of parameters is reduced on the basis of ensuring the prediction accuracy of the model.

Keywords

***In Vivo* Detection, Deep Learning, Convolutional Neural Network, Target Detection, Computer Visio**

1. 引言

活体检测主要指的是针对图像中的人脸区域进行识别分类的过程，其最终只有活体和非活体两类返回结果，因此也可看作一种二分类任务。其中非活体图像即攻击欺诈图像，其可以通过生物仿真技术和图像生成对抗网络得到，能够对人脸识别等诸多应用场景下造成安全隐患[1]。随着近些年人们对活体检测技术的研究逐渐深入，以及其本身具有的重要经济与研究价值，目前活体检测研究已成为计算机视觉和模式识别领域的热点研究方向。其在银行信贷、社区安防、在线教育等诸多应用场景中，都获得了诸多应用和实际落地的项目。

现有的活体检测算法往往通过传统设计滑动窗口的方式对活体和非活体进行检测，该方法不仅无法保证算法的泛化能力，且需要依靠人工提取图像特征的方式进行编码，很大程度上增加了算法的时间开销并降低了精度。本文提出了一种基于卷积神经网络的活体检测算法，其通过深度神经网络自动提取图像特征的方式进行编码，能够有效提高模型的精度并减少参数的数量，从而降低时间开销。同时使用 DropOut 以一个概率值丢弃参数传递过程中的一部分参数，从而能够有效增强模型在未测试过的图像数据集上的泛化能力。

2. 现有技术

目前的活体检测算法中在解决该任务时，往往使用深度学习的方式设计损失函数，并使用传统的方式提取图像特征。其大致可分为：1) 直接使用二元交叉熵监督的方式；2) 利用辅助任务使用像素级监督。

第一种方法中包括：Li 等人(2004)提出了基于傅里叶谱分析的方法，主要假设为真实人脸图像比打印照片图像包含的高频成分多。Tan 等人(2010)利用基于变分 Retinex 的方法和高斯差分(difference of Gaussian, DoG)的滤波器提取人脸图像的潜在反射特征，然后训练稀疏低秩双线性判别模型进行分类。

第二种方法主要包括：Peixoto 等人(2011)提出结合 DoG 滤波器和标准稀疏 Logistic 回归模型在极端光照条件下的人脸活体验证算法。之后，Maata 等人(2011)提出根据局部二值模式(LBP)特征进行人脸活体验证。de Freitas Pereira 等人(2012)使用时空纹理特征来检测欺诈攻击，具体而言，提出一种称为三正交平面的局部二值模式(LBP from three orthogonal planes, LBP-TOP)算子，将时间和空间信息结合起来作为一个统一的描述子。

3. 基于 CNN 的活体检测算法

由于以往的算法中，对于光照条件不足的情况下不能很好的对图像进行识别，且模型在未见过的测试图像上往往泛化性能不足[2]。针对以上问题提出了一种基于卷积神经网络的活体检测算法，算法的总体设计流程如图 1 所示。其次，本文针对实验数据集不足的问题，自制了实验所需数据集。

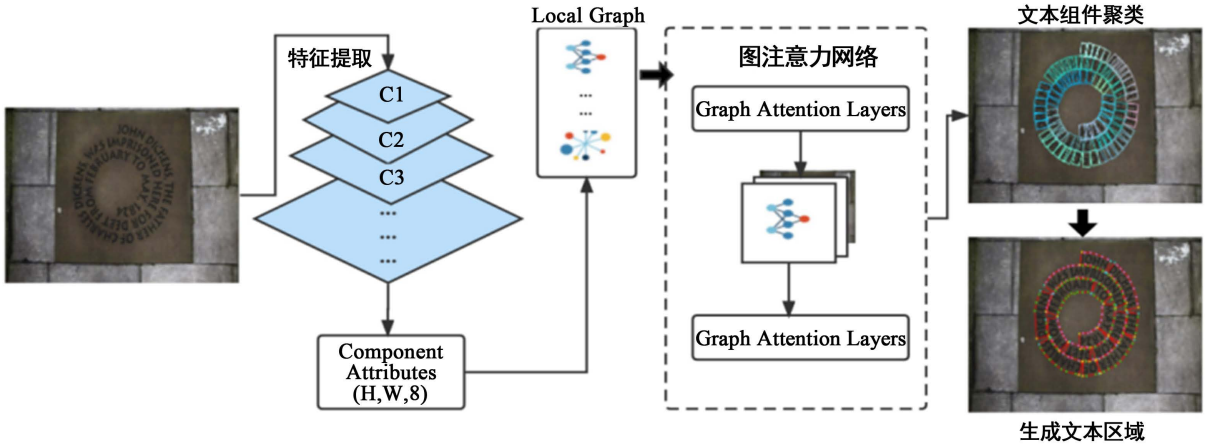

Figure 1. Algorithm flow chart
图 1. 算法流程图

共 3500 张图像，包括训练集和验证集，使用 Keras 框架中的 ImageDataGenerator 方法进行数据增强，主要是对图像进行旋转、翻转、平移、倾斜等图像处理操作的方式，能够达到对少量图像数据进行充分扩充的目的。通过变换前后图像四个顶点之间的对应关系来自动求解仿射矩阵 M 如公式(1)所示：

$$M = cv2.getAffineTransform(pos1, pos2) = \begin{pmatrix} a_{11} & a_{12} & 0 \\ b_{21} & b_{22} & 1 \end{pmatrix} \tag{1}$$

本文算法主要包括：数据预处理、权值初始化、人脸检测、模型优化和保存、训练及验证等步骤，最终将本文算法在服务器中部署实现算法的真实落地。其中，在模型训练阶段尝试了 MobileNet V2、VGG-16、ResNet 50 等不同的卷积神经网络，最终经过不断的测试及验证使用 MobileNet V2 网络作为模型的主干网络[3]。

因其相对与以往的卷积神经网络来说，大量的减少了模型参数，具有轻量化的结构和功能，能够有效减少模型训练及预测所需时间。在模型初始化阶段，由于图像中的像素以及纹理存在差异和不同，因此直接对整张人脸图像进行识别和预测难以达到预期的效果[4]。因此使用 Opencv 框架中级联分类器检测输入图像中的人脸区域并保存，进一步通过检测到的人脸图像进行后续的模型训练和预测。实验结果表明，通过人脸检测的截取到的人脸图像训练得到的模型，其准确率和泛化性能要远高于使用整张人像图片训练得到的模型[5]。本文算法的伪代码如下算法 1。

模型训练阶段中，主要通过真假人脸图片中的纹理以及像素值之间的差异来得到最终的预测结果[6]。本文算法中使用卷积层提取图像中的特征，包括 64 × 64、32 × 32 等不同大小的卷积核，通过 1 和 3 的步长使用卷积运算得到每一个感受野的平均特征值。使用 Softmax 激活函数将连续型的神经元参数映射成离散型变量，作为激活层将模型中的卷积层和全连接层相连接[7]。Softmax 函数是深度学习中的一类常用于实现分类任务的数学函数。其往往加在网络中的后端层中，将连续型的神经元映射成一个 N 维的向量，经过 Softmax 函数计算输出的每一个神经元都对应着一个分类的标签，也是现在分类任务中一种最经常使用的激活函数，其数学计算流程如图 2 所示。

算法 1：live detect suggestion algorithm

Input：A 3-channel RGB image
Output：A tensor of 40 channels
1：提取图像人脸区域特征
2：沿上下边缘划分矩形文本组件，得到P_1和P_2
3：V← P1-P2
4：p = sum(sin(v_i)) i=0,...,n
5：if p≥0then
6：P_1是上部，P_2是下部
7：else
8：P_2是上部，P_1是下部
9：width ← 0.5 × width
10：height ← 1.3 × height
11：输入图片至FPN网络
12：得到F_1
13：CR ← conv1×1(conv$_{3\times3}$(F_1))
14：Fn← CR concat F_1

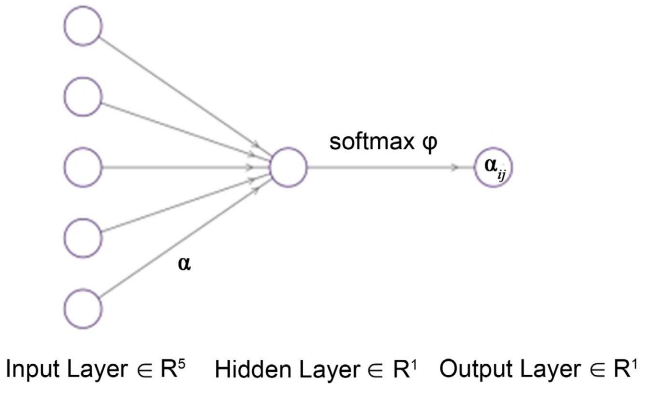

Figure 2. Neural network structure
图 2. 神经网络结构

为增强模型在未见过的测试图像上的泛化能力，使用 Dropout 防止模型出现过拟合现象[8]。Dropout 采用将每一个隐藏层传递过程中以一个概率随机丢弃任意一部分神经元，这样能够减小模型对神经元之间传递的依赖，进而实现避免出现过拟合的现象[9]。Dropout 公式表示如下：

$$\begin{aligned} r_j^{(l)} &= Bernoulli(p) \\ \tilde{y}^{(l)} &= r^{(l)} * y^{(l)} \\ z_i^{(l+1)} &= w_i^{(l+1)} \tilde{y}^{(l)} + b_i^{(l+1)} \\ y_i^{(l+1)} &= f\left(z_i^{(l+1)}\right) \end{aligned} \tag{2}$$

4. 实验结果分析

4.1. 实验环境

硬件环境：CPU：4 Cores；操作系统：Ubuntu 20.04 磁盘：150G GPU：NVIDIA RTX1500
编程环境：Pycharm；
环境配置：Keras2.1；python3.7；OpenCV；Pytorch3.6

4.2. 实验数据集

本实验采用自制数据集进行实验，通过使用 keras 框架中的图像增强方法，以平移、旋转、翻转等几何变换方式对少量的真、假人脸图像扩充至 3500 张用于模型的训练[10]。其中，用于攻击的欺诈图像使用手机、ipad 等工具翻拍所得到，均包括了完整的人脸区域。

4.3. 实验结果

为了验证关系推理网络在实现活体检测任务中的有效性，我们在 Total-Text，CTW1500 和 MSRA-TD500 上以及自制的数据集上进行了对比实验。表 1 显示了三个数据集上的实验结果。为了减少数据对实验结果的影响，我们采用 SynthText 进行预训练模型，然后在 Total-Text 和 CTW1500 上进行微调。由于 MSRA-TD500 由英语和中文组成，因此我们使用 ICDAR2017-MLT 对我们的网络进行准确率、召回率等评价指标进行测试和评价，结果如表 1 所示：

Table 1. Test results on open datasets
表 1. 在公开数据集上的检测结果

Datasets	Batch-size	R P H
CTW1500	12	71% 79% 75.2%
TD500	8	70% 72% 69.54%
Total-text	4	68.9% 74% 70%

模型训练过程及结果如图 3 和图 4 所示：

```
Training
Epoch 1/2
1875/1875 [==============================] - ETA: 0s - loss: 0.1005 - accuracy: 0.9686
Epoch 00001: loss improved from inf to 0.10055, saving model to lenet5_membrane.hdf5
1875/1875 [==============================] - 45s 24ms/step - loss: 0.1005 - accuracy: 0.9686
Epoch 2/2
1873/1875 [==============================>.] - ETA: 0s - loss: 0.0385 - accuracy: 0.9889
Epoch 00002: loss improved from 0.10055 to 0.03854, saving model to lenet5_membrane.hdf5
1875/1875 [==============================] - 46s 24ms/step - loss: 0.0385 - accuracy: 0.9889

Testing
313/313 [==============================] - 2s 5ms/step - loss: 0.0283 - accuracy: 0.9911

test loss:  0.028327286243438721
```

Figure 3. Model training process
图 3. 模型训练过程

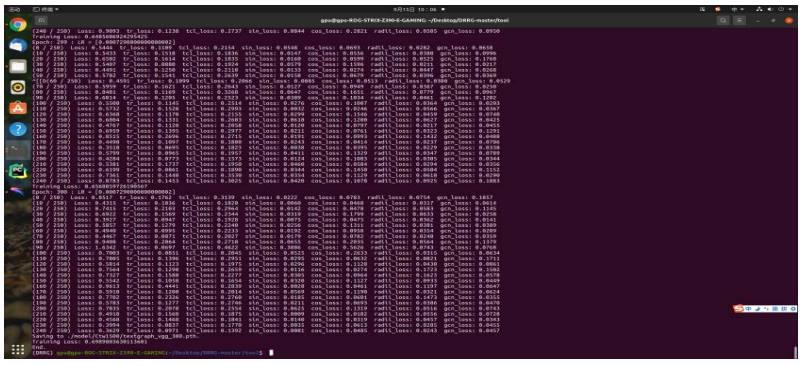

Figure 4. Model training results
图 4. 模型训练结果

5. 结论

本论文针对以往在银行信贷等应用场景中的攻击活体检测问题，提出了一种基于图片纹理和分辨率差异的活体检测算法，经过在自制数据集上的实验表明，提出的方法能够实现很好的效果并能在保证模型准确率不变的前提下，减小模型参数能够有效减少模型的预测所需时间。下一步的计划是，探索基于视频流的活体检测方法，并尝试在高分辨率的攻击图像上训练检测模型，测试实验的效果，同时进一步提高模型的容错率和泛化性能。

参考文献

[1] Detti, A.H., Jemei, S., Morando, S., *et al.* (2017) Classification Based Method Using Fast Fourier Transform (FFT) and Total Harmonic Distortion (THD) Dedicated to Proton Exchange Membrane Fuel Cell (PEMFC) Diagnosis. 2017 *IEEE Vehicle Power and Propulsion Conference* (*VPPC*), Belfort, 11-14 December 2017, 1-6. https://doi.org/10.1109/VPPC.2017.8331040

[2] Pavlidis, I., Khatri, A., Buddharaju, P., *et al.* (2018) Biofeedback Arrests Sympathetic and Behavioral Effects in Distracted Driving. *IEEE Transactions on Affective Computing*, **1**, 37-48.

[3] 宋云博. 基于级联网络的目标检测与实例分割算法研究[D]: [硕士学位论文]. 大连: 大连海事大学, 2020.

[4] Jaderberg, M., Simonyan, K., Vedaldi, A. and Zisserman, A. (2016) Reading Text in the Wild with Convolutional Neural Networks. *IJCV*, **116**, 1-20.

[5] Sieber, M., Siedersberger, K.H., Siegel, A., *et al.* (2021) Automatic Emergency Steering with Distracted Drivers: Effects of Intervention Design. *IEEE International Conference on Intelligent Transportation Systems*, Chicago, 1 March 2021, 31-40.

[6] Raviteja, S. and Shanmughasundaram. R. (2021) Advanced Driver Assitance System (ADAS). *Second International Conference on Intelligent Computing and Control Systems* (*ICICCS*), Chicago, 4 October 2021, 55-62.

[7] 王飞, 王林, 张儒良, 等. 基于融合FPN和Faster R-CNN的行人检测算法[J]. 数据采集与处理, 2019(3): 530-537.

[8] 顾鑫, 王海涛, 汪凌峰, 等. 基于不确定性度量的多特征融合跟踪[J]. 自动化学报, 2019, 37(5): 550-559.

[9] 郭玥秀, 杨伟, 刘琦, 等. 残差网络研究综述[J]. 计算机应用研究, 2020, 37(5): 1292-1297.

[10] 曹仰杰, 贾丽丽, 陈永霞, 等. 生成式对抗网络及其计算机视觉应用研究综述[J]. 中国图象图形学报, 2018, 23(10): 1433-1449.