第 35 卷 第 1 期
2020 年 2 月

天津科技大学学报
Journal of Tianjin University of Science & Technology

Vol. 35 No. 1
Feb. 2020

DOI:10.13364/j.issn.1672-6510.20190151
数字出版日期：2019-12-19；数字出版网址：http://kns.cnki.net/kcms/detail/12.1355.N.20191219.1130.006.html

人脸识别活体检测综述

杨巨成，代翔子，韩书杰，毛 磊，王 媛
（天津科技大学人工智能学院，天津 300457）

摘 要：由于人脸认证系统高安全性的需求，并且人脸容易受到照片、视频、面具等伪造攻击，进而导致人脸活体检测具有现实紧迫性. 近年来，研究人员在该领域进行了大量的研究，本文介绍目前人脸识别活体检测技术的国内外研究现状，并做相应的分析以及对未来该技术的展望.

关键词：人脸识别；伪造攻击；活体检测
中图分类号：TP301.6 **文献标志码**：A **文章编号**：1672-6510(2020)01-0001-09

On Liveness Detection through Face Recognition

YANG Jucheng，DAI Xiangzi，HAN Shujie，MAO Lei，WANG Yuan
（College of Artificial Intelligence，Tianjin University of Science & Technology，Tianjin 300457，China）

Abstract：Face liveness detection has great significance in face authentication systems due to its high security，but it is vulnerable to forgery attacks with photos，videos，masks，etc. In recent years，researchers have done a lot of work in this field. This paper reviews worldwide current researches on liveness detection technology in face recognition and analyses its prospect in the future.

Key words：face recognition；forgery attack；liveness detection

人脸识别技术是个人身份认证的重要工具，并且该技术拥有非接触式、成本低、方便快捷等特点，成为各种安全应用领域的最佳选择(例如社交媒体和智能手机访问控制、关键地点的边境管制和视频监控). 由于复制人脸非常容易实现，因此出现了很多针对人脸认证攻击的手段，主要包括人脸照片攻击[1]、人脸视频回放攻击[1]以及三维人脸模型攻击[2].

人脸识别系统中活体检测技术判断人脸图像是否为活体. 只有人脸图像被判定为活体的情况下，人脸身份认证才有效，否则就会被判定为非法攻击. 本文首先列举了 3 种常见的伪造攻击类型，再分析近十年的相关工作，并将活体的检测方法分为两大类：(1)基于描述子的分析方法，指根据描述子所描述的特征差异性区分活体与非活体人脸图像，比如纹理、运动、频率、颜色、形状等；(2)基于分类器的分析方法，指利用大量活体与非活体人脸数据作为训练样本，执行分类算法得到的活体判别模型. 继而归纳目前常见的几种公开数据集，分析其属性，包括人脸图像的采集设备、采集环境、采集方式等. 为了评价人脸活体检测方法的性能，本文详细介绍了人脸活体检测中常见的几种评价指标，分析几种主流方法的优缺点，包括利用传统的局部特征以及运动信息、深度学习方法等，指出未来人脸活体检测方法的发展趋势.

1 伪造攻击类型

图 1[3]是具有活体检测功能的人脸身份认证系统框架. 人脸识别系统通常会考虑以下 3 种伪造攻击类型：

(1) 人脸照片攻击：包括打印照片、弯曲打印照片模拟人脸运动以及切割眼部的打印照片[1].

(2) 人脸视频回放攻击：通过视频播放进行的攻

收稿日期：2019-05-20；修回日期：2019-08-30
基金项目：国家自然科学基金资助项目(61502338)
作者简介：杨巨成（1980—），男，湖北天门人，教授，jcyang@tust.edu.cn

击显示几乎与真实人脸活体具有相似的行为，具有许多有效用户运动的固有特征. 这种类型的攻击具有照片中未呈现的生理迹象，例如眨眼、人脸表情以及头部和嘴部的运动，并且可以使用平板电脑或大型智能手机轻松执行[1].

(3) 三维人脸模型攻击：在获得合法用户的人脸照片或人脸视频信息后，非法用户可以通过真人三维建模的方式得到合法用户的三维面具. 但是，面具的制造需要 3D 扫描和打印特殊设备，成本比其他类型攻击更加昂贵，其制作过程也更加困难[2].

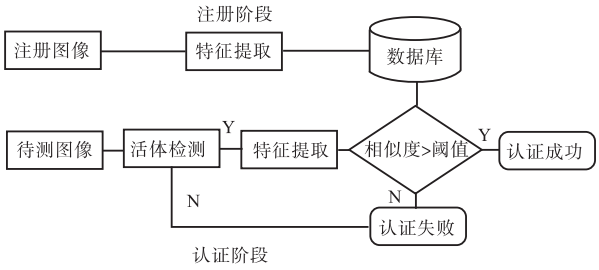


图 1　具有活体检测功能的人脸身份认证系统框架

Fig. 1　Framework of face recognition-based authentication system for liveness detection

2　针对人脸伪造攻击的主要方法

本文将针对人脸伪造攻击的活体检测方法归纳为两大类：一是基于描述子的分析方法，比如纹理、运动、频率、颜色、形状或反射率；二是基于分类器的分析方法，比如判别式、回归、距离度量以及启发式方法.

2.1　基于描述子的分析方法

2.1.1　基于纹理描述子的方法

打印照片中存在着活体中不存在的某种特有的纹理信息[4-5]. 纹理特征的差异性在活体和非活体中比较明显，有超过 80% 的研究方法都是单独使用纹理特征或者是利用纹理特征结合其他描述子. 不同的纹理描述子可以被用于检测人脸攻击，其中具有简单易算性的局部二值描述子(local binary pattens，LBP)算法[6]，常被用作特征描述的首要选择，很多研究者都是探究 LBP 或者基于 LBP 改进的方法[7-8]. LBP 是一种具有灰度、旋转不变性的纹理编码技术，通过将每个像素与其邻域进行比较，标记每个像素，将结果连接成二进制数. 邻域的数量、邻域半径和编码策略都是该方法的参数. 最后将最终计算的结果组织在直方图中以描述纹理. Tan 等[9]在 Lambertian 反射模型的基础上利用对数总差异(logarithmic total variation，LTV)方法对图像完成预处理，然后利用高斯差分(difference of Gaussian，DoG)滤波器对图像进行滤波，提取图像 DoG 特征，最后用改进的 Logistic 回归完成人脸真伪分类.

2.1.2　基于运动描述子的方法

运动描述子从两种不同的运动方法角度进行活体检测. 一种方法是检测和描述人脸变化，例如眨眼、人脸表情和头部旋转. Pan 等[10]使用条件随机场(conditional random fields，CRF)确定闭眼，从而检测到眨眼；除了局部动作检测外，检测和描述全局人脸运动. 而也有研究人员[11-12]利用光线流动(optical of lines，OFL)用于测量水平和垂直方向的人脸图像的时空变化. Bharadwaj 等[13]利用定向光流直方图(histogram of oriented optical flow，HOOF)和光学幅度直方图应用流(histogram of magnitudes of optical flows，HMOF)创建人脸运动方向和幅度的分级表示[14]过稀疏和低秩分解(robust alignment by sparse and low-rank，RASL)进行稳健对齐，尝试在多个帧中对齐人脸并测量非刚性运动[15]. 另一种方法是评估用户交互环境中的一致性. 鉴于此，Komulainen 等[16]提出了计算人脸和背景区域之间的运动相关性方法，Pinto 等[17]提出基于高斯混合模型(Gaussian mixture models，GMM)的传统背景差分法.

通过使用动态模式分解(dynamic mode decomposition，DMD)[18]探索帧序列内个体的人脸纹理，并通过在时间空间上移位的快照中的特征脸提取特征. DMD 与 LBP 技术结合使用作为纹理描述子，其用于捕获视频序列中活体人脸存在的证据，例如眨眼和嘴唇的运动. 图 2[10]中(a)、(b)、(c)图是活体一个完整的眨眼动作，(d)、(e)、(f)是活体分别对应检测眨眼动作的二值图像.

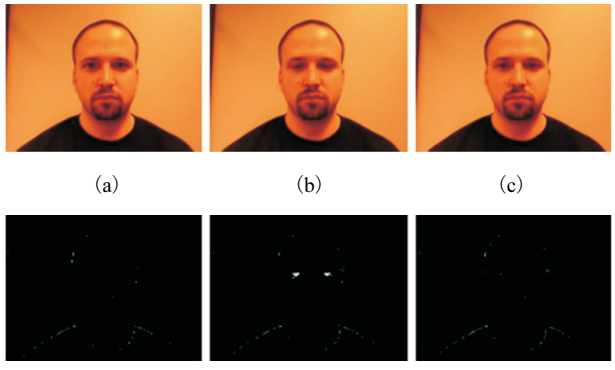
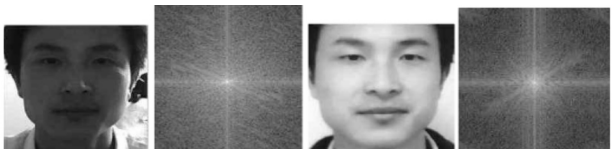


图 2　活体眨眼动作图像对应眼部的二值图像

Fig. 2　Binary images of living eyes with blinking movements

2.1.3　基于频率描述子的方法

频率描述子的方法是基于活体和非活体人脸图像在频域中的差异性提出的. Li 等[19]提出一种结合高频描述子和动态傅里叶频率描述子的方法分析人脸. 该方法基于两种特性：(1)照片是平面结构，所以产生高频分量应该小于活体人脸的成像；(2)因为脸部缺少表情变化，所以使得频率分量(即频率振幅的大小)的标准差较小. 根据这两种特性在人脸活体与非活体之间的差异性，促使很多研究者利用 2D 离散傅里叶变换或者 2D 快速傅里叶变换将图像从时域转换到频域[20−24]，然后利用 LBP 或者 HOG 等描述子进行一个特征表达. 图 3[20]中(a)图是活体及其傅里叶变换的频谱图，(b)图是非活体及其傅里叶变换的频谱图.



(a)　　(b)

图 3　活体和非活体图像在频域空间上的频谱图

Fig. 3　Spectrum of living and non-living images in the frequency domain

2.1.4　基于颜色描述子的方法

颜色描述子的方法是基于活体和非活体的颜色差异提出的. 在这种背景下，色频(CF)直方图用于描述图像中颜色的分布[25]，而且这些直方图被用作对图像的不同块计算 HOG 特征，即用 3 个 bin 编码具有最高像素数的像素每个颜色通道中的梯度幅度. 图像失真分析(IDA)[26−27]、图像质量评估(IQA)[28]和图像质量测量(IQM)[29]方法通过全局图像矩描述活体人脸图像. IDA 用于在 HSV 和 RGB 色彩空间提取特征，平滑光照强度. IQA 用于在人脸活体检测中最大化关键性能指标. IQM 旨在表明通过图像的质量评估用高斯滤波产生的最小值，以判断是否为非活体人脸图像. YCbCr 和 HSV 颜色空间在文献[30−31]中用作颜色描述子. 在文献[32]中，RGB 颜色空间的每个通道用于特征提取. 图 4[27]中(a)图是活体，(c)图是非活体，(b)、(d)图分别是对应(a)、(c)图的 HSV 颜色特征直方图分布.

2.1.5　基于形状描述子的方法

形状描述子的方法对于区分打印照片是非常有效的一种手段，因为活体人脸几何特征是无法在打印照片平面上重现的. 基于约束性的局部模型(CLM)的活体轮廓被用于检测视频流中的人脸关键点，然后这些人脸关键点被定义成一个稀疏的 3D 结构用于描述人脸的平面性[33].

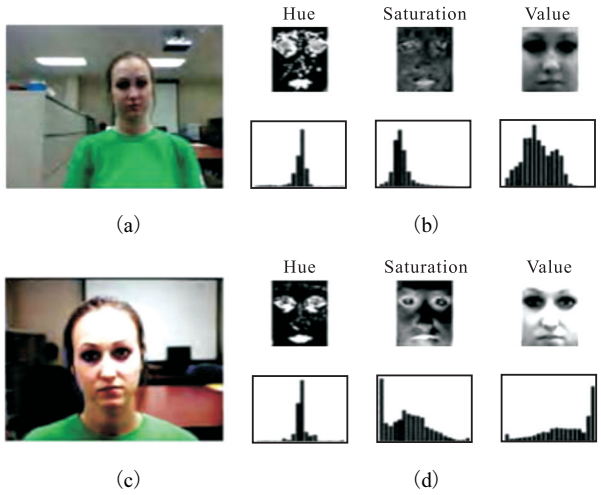


图 4　活体和非活体图像在 HSV 颜色空间中的分布

Fig. 4　Distribution of living and non-living images in HSV color space

2.1.6　基于反射率描述子的方法

考虑到活体和非活体的人脸图像在相同光照条件下表现不同，因而可以使用反射信息区分. 为了实现这一点，变分 Retinex 方法将输入图像分解为反射率和光照成分[34]，以便分析整个图像. 图 5[27]中(a)图是活体图像和检测到的反射特征图像，(b)图是非活体图像和检测到的反射特征图像；(c)图是(a)图中反射特征图像特征值分布图，(d)图是(b)图中反射特征图像特征值分布图.

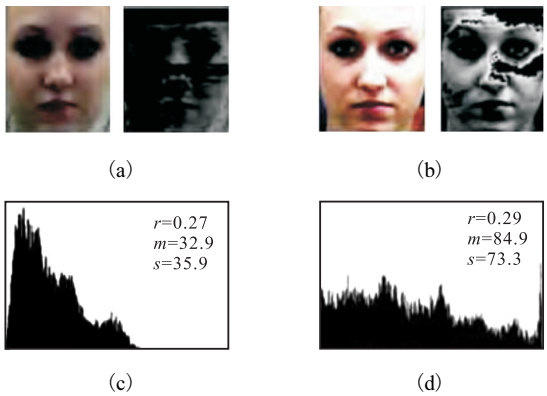


图 5　活体和非活体图像在反射特征中的分布

Fig. 5　Distribution of living and non-living images in reflex features

2.2　基于分类器的分析方法

2.2.1　基于判别器的方法

判别技术是通过最小化类内变化或最大化类间的变化区分不同的类别. 这种类型的分类器在过半数的分析工作中被使用研究.

支持向量机(SVM)是人脸图像活体检测中最常见的分类技术,性能优越. 为了实现区分目标,SVM需要找到最佳超平面,将活体和非活体人脸图像的特征分开. 当这些类不是线性可分时,需要使用不同的内核函数用于获得非线性分类器. 虽然线性SVM已经广泛用于不同的领域[35-37],并且径向基函数核[38-39]和直方图交叉核[40]也被应用于提高分类精度. 但是,这些研究并没有描述如何在实验中使用某种类型的SVM核函数.

除了SVM之外,还有一种常用的方法为线性判别分析(LDA)[41-42]. LDA能够明确地建模类间的差异,以解决分类任务,它的优势在于可有效降维,降低分类预测时间复杂度. 多层感知器(MLP)[16]用于评估人脸图像是否过度移动(手工平面打印照片)或没有移动(连接到媒体的平面打印照片攻击)有变化在N视频序列期间;神经网络(NN)[11]擅长学习隐式模式,它能够通过适当的训练去识别非活体的运动信息. NN的训练是使用标记数据集通过反向传播方式进行,该自动编码器被视为预训练过程.

2.2.2　基于卷积神经网络的方法

卷积神经网络(convolutional neural network, CNN)[43-51]方法能够自动提取图像的有效特征,完全避免了传统手工设计特征算法提取特征模式的单一性,并且能够保证特征的尺度不变性,旋转不变性. 近几年它被广泛应用在人脸图像有效识别特征提取中,用以进行人脸图像的活体判断. 这类方法在公开测试集上取得了显著的效果[52]. 但是,这类模型在训练中容易过拟合,导致在实际运用中,泛化能力差,在某些不稳定的真实场景效果不尽人意. 同时,这类方法对数据的覆盖度、数据量的大小要求较高. 图6是一个典型的基于卷积神经网络方法实现活体检测的模型流程图.

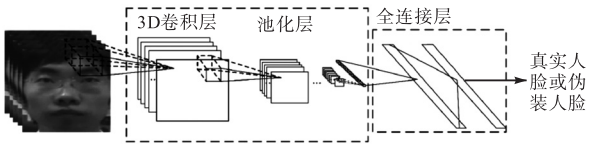


图6　基于3D卷积结构的活体检测网络

Fig. 6　Living detection network based on 3D convolution structure

2.2.3　基于距离度量的方法

距离度量的使用可以改善人脸活体检测系统的性能,它的目标是测量样本之间的差异性. 但是,这些方法通常需要一个穷举搜索完成分类任务,这可能导致大型参考数据集中的高成本. 卡方距离[53]和余弦距离[54-55]是常见的距离度量方式,它们用于计算一个待检测人脸和参考数据集合的累积距离,以此决定待测人脸属于活体人脸还是非活体人脸.

2.2.4　基于启发式的方法

启发式算法(heuristic algorithm)是相对于最优化算法提出的. 一个问题的最优算法求得该问题每个实例的最优解. 启发式算法可以这样定义:一个基于直观或经验构造的算法,在可接受的花费(指计算时间和空间)下给出待解决组合优化问题每一个实例的一个可行解,该可行解与最优解的偏离程度一般不能被预计.

目前比较通用的启发式算法一般有模拟退火算法(simulated annealing, SA)、遗传算法(genetic algorithm, GA)、蚁群算法(ant colony optimization, ACO)等.

在人脸活体检测中典型利用启发式算法例子的有眨眼次数[10]、动作测量阈值[12]、平均像素比率阈值[24]和运动测量的加权[40],进行启发式判别的方法都是启发式学习的例子. 这种学习方式的显著缺点是易导致过拟合,因为启发式算法的局部最优值的陷入无法避免. 启发式,本质上是一种贪心策略,这也在客观上决定了不符合贪心规则的更好(或者最优)解都会错过.

3　公开数据库

NUAA数据集[9]是第一个用于评估人脸活体检测的数据集. 在不同环境和不同光照条件下,利用廉价摄像头,分别采集了3个不同时间段的数据,每个时间段间隔为两周. 其中伪造人脸的方式为平面或者弯曲打印照片.

Yale数据集[56]是在不同光照条件下采集的,该数据库通常用在评估纹理方法的人脸活体检测上. 伪造人脸的方式为打印照片.

Print-Attack数据集[57]的采集是通过向采集传感器显示真实用户的平面打印照两种方式:手持(即冒名顶替者用手拿照片)或固定支架. 伪造人脸的方式为打印照片.

Replay-Attack数据集[39]采集环境是在不同光照条件下进行的,其中伪造人脸方式包括打印照片和视频回放. 视频回放所用的设备又包括低分辨率的移动设备和1 024×768分辨率平板电脑.

Casia Face Anti-Spoofing 数据集[58]包含 7 种不同的攻击场景和 3 种不同的攻击类型. 伪造人脸的方式为平面照片、眼部被切割的打印照片以及视频回放.

Kose and Dugelay 数据集[59]的创建是通过 3D 结构光设备得到立体结构模型，然后利用 3D 打印机打印出 3D 面具得到的. 伪造人脸方式为面具.

3D Mask Attack 数据集[60]是通过 RGB-D 深度相机采集得到的，其中每个人都包括一张正脸和两张侧脸照片. 伪造人脸方式为面具.

MSU-MFSD 数据集[27]的组成包括两种数据类型，一种是通过视频帧截取出来的打印照片，另外一种是视频回放. 打印照片用的是彩色大尺度的纸张，同时视频回放的采集也是尽量保证采集环境的相似性. 伪造人脸方式为打印照片和视频回放.

UVAD 数据集[23,61]中伪造人脸是通过高清视频回放设备以每秒 30 帧的回放速度采集的，其中每段视频是在不同的光照以及不同的场景（室内或者室外）下拍摄得到的. 伪造人脸方式为视频回放.

Oulu-NPU 数据集[62]采集设备包含 6 种手机机型，采集环境包括 3 种光照环境和背景. 伪造人脸方式为打印照片和视频回放.

Siw 数据集[63]的组成包括两种数据类型，一种是通过 1 080 p 高清设备采集的，另外一种是打印照片. 采集环境包括光照、姿态、距离、表情这 4 个变量. 伪造人脸的方式为打印照片和视频回放.

CASIA-SURF 数据集[64]包含 RGB 图、深度图以及红外热力图像 3 种数据，主要用于多模态融合方法上. 伪造人脸方式包括打印照片和眼部被切割的打印照片.

数据集详情见表 1.

表 1　公开活体数据集

Tab. 1　Public living data set

年份	数据集	人数	真/伪样本数	攻击类型
2010	NUAA	15	5 105/7 509	打印照片
2011	Yale	10	640/1 920	打印照片
2011	Print-Attack	50	200/200	打印照片
2012	Replay-Attack	50	200/100	打印照片、视频回放
2012	Casia Face Anti-Spoofing	50	150/450	打印照片、视频回放、眼部切割照片
2013	Kose and Dugelay	20	200/198	面具
2013	3D Mask Attack	17	170/85	面具
2014	MSU-MFSD	35	70/210	打印照片、视频回放
2015	UVAD	404	808/16 268	视频回放
2016	Oulu-NPU	55	990/3 960	打印照片、视频回放
2018	Siw	165	4 478 段视频	打印照片、视频回放
2018	CASIA-SURF	1 000	21 000 段视频	打印照片、眼部切割照片

4　性能评价指标

常用的人脸活体检测性能评价指标主要评价识别错误，其类型主要有两类：一是非活体被作为活体接受数量 NFA（number of false acceptance），另外一种是活体被认为是非活体拒绝数量 NFR（number of false rejection）. 这两种错误类型在人脸活体检测系统中出现的可能性分别被称为错误接受率（false acceptance rate，FAR）和错误拒绝率（false rejection rate，FRR），这两种比率存在着反比例的关系. 受试者工作特征曲线（receiver operating characteristic curve，ROC）是通过同时计算 FAR 和 FRR 的值获得的，如图 7 所示. 被 ROC 包围的区域面积为曲线下面积（area under the curve，AUC），同时在 ROC 曲线上当 FAR 等于 FRR 的时候，这个点被称作等错误率（equal error rate，ERR），FAR 和 FRR 的均值被称为半错误率（half total error rate，HTER）. 精度（the overall accuracy，ACC）同时兼顾着活体和非活体各自的 FAR 和 FRR.

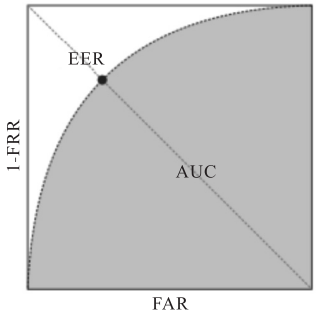


图 7　受试者工作特征曲线图

Fig. 7　Receiver operating characteristic curve

由于很多数据集中活体和非活体人脸图像数据

量并不是均衡的，所以用 ACC 分析可能会导致偏差. 其评估指标计算公式详见表 2.

表 2　评估参数

Tab. 2　Evaluation parameters

度量方法	含义	计算公式
FAR	错误接受率	$\mathrm{FAR}=\frac{\mathrm{NFA}}{\#\mathrm{Fake}}$
FRR	错误拒绝率	$\mathrm{FRR}=\frac{\mathrm{NFR}}{\#\mathrm{Real}}$
ERR	等错误率	$\mathrm{ERR}=(\mathrm{FAR}=\mathrm{FRR})$
HTER	半错误率	$\mathrm{HTER}=\frac{\mathrm{FAR}+\mathrm{FRR}}{2}$
ACC	精度	$\mathrm{ACC}=100\times(1-\mathrm{FAR})$
AUC	曲线下面积	$\mathrm{AUC}=\int_a^b f(x)\mathrm{d}x([a,b]\Rightarrow R)$

注：#Real 为样本集活体样本数；#Fake 为样本集非活体样本数.

5　主要方法性能比较

为验证模型在人脸活体检测任务上的鲁棒性和泛化能力，研究人员普遍利用了 3 大公开数据库 CASIA、Replay 以及 MFSD 做了相关基准测试：

LBP 方法[65]通过在 CASIA 上训练，在 Replay 测试上得到的半错误率为 47%. 这种方法的优点：一定程度上消除了光照因素带给人脸图像的噪声影响，并且该算子具有旋转不变性，特征维度低，计算速度快. 但是，由于训练样本和测试样本特征分布不一致，导致编码阈值很难设定.

LBP-TOP 方法[65]是在 LBP 的基础上增加一个维度信息——时间维度，这样有助于获取视频帧之间的运动信息，进而提高人脸活体的准确率. 但是，由于重新引入了新的输入维度信息，导致输出变成了一个高维度特征，从而计算量增加.

Motion 方法[65]主要通过获取人脸活体和非活体之间的微动作之间的差异作为评判标准. 因为主要是针对刚性运动，所以导致它对视频回放攻击或者照片抖动攻击这种非刚性攻击效果不好.

CNN 方法[66]提出了一种让计算机自动学习出模式特征的方法，并将特征学习融入到了建立模型的过程中，从而减少了人为设计特征造成的不完备性. 其中 Auxiliary 方法[63]使用空间和时间辅助信息的监督而不是二元监督，以便从人脸视频中更健壮地检测人脸伪造攻击. 这些辅助信息是基于我们关于现场和欺诈面部之间关键差异的领域知识获得的，其中包括两个视角：空间和时间. 其中空间就是图像的深度，而时间就是使用远距光体积描记术（remote photoplethysmography，rPPG）信号作为辅助监督. 而 De-Spoof 方法[47]启发于图像去噪和去抖动，无论是噪声图还是模糊图，都可看成是在原图上加噪声运算或者模糊运算，而去噪和去抖动就是估计噪声分布和模糊核，从而重构回原图，利用训练出的噪声模型去判别人脸活体图像. 但是，当实际场景中活体的人脸图质量并不是很高，而非活体人脸攻击图像的质量相对高时，这种方法很难去判别人脸活体与非活体. GFA-CNN[67]方法则是利用了风格迁移[68]减少不同域之间带来的影响. 这些 CNN 方法的不足是：都需要大量的数据作为支撑，并且训练判别模型也需要算力较大的硬件设备作为支持.

Color LBP[30]、Color Texture[30]以及 Color Surf[30]都是基于颜色域空间上利用不同的描述子去提取人脸活体与非活体图像特征的方法. 其缺点是针对面具攻击效果较差，对单个颜色特征的依赖性大，泛化能力也差.

不同方法在不同数据库上的训练测试半错误率的对比结果见表 3.

表 3　不同方法在不同数据库上的训练测试半错误率的对比　　%

Tab. 3　Comparison of half total error rate indicators in different training tests on different databases with different methods

方法	训练	测试	训练	测试	训练	测试	训练	测试	平均值
	CASIA	Replay	Replay	CASIA	MFSD	Replay	Replay	MFSD	
LBP	47.0		39.6		45.5		45.8		44.5
LBP-TOP	49.7		60.6		46.5		47.7		51.5
Motion	50.2		47.9		—		—		49.1
CNN	48.5		45.5		37.1		48.6		44.9
Color LBP	37.9		35.4		44.8		33.0		37.8
Color Texture	30.3		37.7		33.9		34.1		34.0
Color Surf	26.9		23.2		29.7		31.8		27.9
Auxiliary	27.6		28.4		—		—		28.0
De-Spoof	28.5		41.1		—		—		34.8
GFA-CNN	21.4		34.3		25.8		23.5		26.3

注：—表示未测试出.

由表 3 可以分析出：前半部分方法大多数都是基于人工设计特征提取算子 LBP 进行分析人脸图像，这种方法提取特征形式比较单一，无法有效提取更多的人脸活体判别信息. 而后半部分方法大多数是基于 CNN 提取人脸活体特征，提取形式相比较于传统人工设计特征提取算子更丰富；但是仍然不能很好地解决模型的泛化能力，故目前出现了很多利用人脸图像的其他信息辅助监督模型进行训练，以此达到更好的模型泛化性.

6 展　望

尽管人脸识别活体检测在公开数据集上取得了良好的效果，但是我们应该考虑与工业界实际情况相结合，尽量提高方法的泛化能力，以应对工业界各种复杂的场景.

首先，基于描述子的分析方法是从人脸识别技术引入到人脸活体检测中，在单个特定数据集上通常能得到较好的结果，但其性能会随着不同数据集的迁移逐渐衰减. 因此，设计专门用于人脸图像活体检测的解决方案是很有必要的，比如早期基于运动和反射率的方法. 这点在过去几年里似乎未被充分研究，但是深度学习可以学习到更抽象的语义特征，例如短期记忆网络（long short-term memory，LSTM）[69]和傅里叶卷积神经网络（Fourier CNN）[70].

第二，可以探索其他学习框架以提供不同关于如何解决这个问题的观点. 到目前为止，尚未有基于迁移学习或在线学习框架的活体识别方法，不过这类框架对于不同的数据集和流数据有更好的适应性.

第三，活体检测目前还没有统一公认的大型数据集. 多场景、多人物、多光照等更具有泛化性的大型数据集有助于算法的快速进步，对于讨论该领域的如过拟合、多类别攻击等复杂问题能起到重要的推动作用. 因此，亟待构建大型人脸识别活体检测数据集.

最后，可进一步考虑多模态活体检测方法. 因为必须同时伪造多个生物识别特征，所以多模态生物识别系统不太可能被非活体伪造. 出于这个原因，很多方法是通过融合两个或更多人类特征解决非活体的问题. 考虑到这一点，人脸识别技术可以被视为一种特殊情况，因为多模态可以利用多种人脸特征（例如纹理、形状和温度）避免伪造攻击. 如今，不同的有效设备能够捕获图像的颜色、深度和红外线，同时在价格上比较有优势. 这些设备可用于减弱当前的人脸伪造攻击影响，并在将来有可能实际地运用到工业界中.

参考文献：

[1] 孙霖，潘纲. 人脸识别中视频回放假冒攻击的实时检测方法[J]. 电路与系统学报，2010，15(2)：39–46.

[2] 谷小婧，付传卿，顾幸生. 基于面部生命特征的 3D 假面欺骗攻击检测方法[J]. 系统仿真学报，2016，28(2)：361–368.

[3] 许晓. 基于深度学习的活体人脸检测算法研究[D]. 北京：北京工业大学，2016.

[4] 吴继鹏. 基于纹理特征的 2D-3D 人脸活体检测关键技术研究[D]. 厦门：集美大学，2017.

[5] 吴继鹏，蔡国榕，陈水利，等. 基于 FS-LBP 特征的人脸活体检测方法[J]. 集美大学学报：自然科学版，2017，22(5)：65–72.

[6] Ojala T，Pietikäinen M，Harwood D. A comparative study of texture measures with classification based on featured distributions[J]. Pattern Recognition，1996，29(1)：51–59.

[7] Maatta J，Hadid A，Pietikainen M. Face spoofing detection from single images using texture and local shape analysis[J]. IET Biometrics，2012，1(1)：3–10.

[8] Maatta J，Hadid A，Pietikainen M. Face spoofing detection from single images using micro-texture analysis[C]// IEEE. 2011 International Joint Conference on Biometrics（IJCB）. New York：IEEE，2011：6117510.

[9] Tan X，Li Y，Liu J，et al. Face liveness detection from a single image with sparse low rank bilinear discriminative model[C]//ECCV. European Conference on Computer Vision. Berlin：Springer，2010：504–517.

[10] Pan G，Sun L，Wu Z，et al. Eyeblink-based anti-spoofing in face recognition from a generic webcamera[C]//IEEE. 2007 IEEE 11th International Conference on Computer Vision. New York：IEEE，2007：4409068.

[11] Feng L，Po L M，Li Y，et al. Integration of image quality and motion cues for face anti-spoofing：A neural network approach[J]. Journal of Visual Communication & Image Representation，2016，38：451–460.

[12] Kollreider K，Fronthaler H，Bigun J. Verifying liveness by multiple experts in face biometrics[C]//IEEE. 2008 IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops. New York：IEEE，2008：4563115.

[13] Bharadwaj S，Dhamecha T I，Vatsa M，et al. Computationally efficient face spoofing detection with motion magnification[C]//IEEE. 2013 IEEE Conference on

Computer Vision and Pattern Recognition Workshops. New York: IEEE, 2013: 6595861.

[14] Chingovska I, Yang J, Lei Z, et al. The 2nd competition on counter measures to 2D face spoofing attacks[C]// IEEE. 2013 International Conference on Biometrics (ICB). New York: IEEE, 2013: 6613026.

[15] Yan J, Zhang Z, Lei Z, et al. Face liveness detection by exploring multiple scenic clues[C]//IEEE. 2012 12th International Conference on Control Automation Robotics & Vision (ICARCV). New York: IEEE, 2012: 6485156.

[16] Komulainen J, Hadid A, Pietikainen M, et al. Complementary countermeasures for detecting scenic face spoofing attacks[C]//IEEE. 2013 International Conference on Biometrics (ICB). New York: IEEE, 2013: 6612968.

[17] Pinto A, Pedrini H, Schwartz W, et al. Face spoofing detection through visual codebooks of spectral temporal cubes[J]. IEEE Transactions on Image Processing, 2015, 24(12): 4726–4740.

[18] Tirunagari S, Poh N, Windridge D, et al. Detection of face spoofing using visual dynamics[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(4): 762–777.

[19] Li J, Wang Y, Tan T, et al. Live face detection based on the analysis of Fourier spectra[J]. Proceeding of SPIE, 2004, 5404: 296–303.

[20] Kim G, Eum S, Suhr J K, et al. Face liveness detection based on texture and frequency analyses[C]//IEEE. 2012 5th IAPR International Conference on Biometrics (ICB). New York: IEEE, 2012: 6199760.

[21] Phan Q T, Dang-Nguyen D T, Boato G, et al. Face spoofing detection using LDP-TOP[C]//IEEE. 2016 IEEE International Conference on Image Processing (ICIP). New York: IEEE, 2016: 7532388.

[22] Pinto A S, Pedrini H, Schwartz W R, et al. Video based face spoofing detection through visual rhythm analysis[C]//IEEE. 2012 25th SIBGRAPI Conference on Graphics, Patterns and Images. New York: IEEE, 2012: 6382760.

[23] Pinto A, Schwartz W R, Pedrini H, et al. Using visual rhythms for detecting video-based facial spoof attacks[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(5): 1025–1038.

[24] Garcia D C, De Queiroz R L. Face-spoofing 2D-detection based on Moiré-pattern analysis[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(4): 778–786.

[25] Schwartz W R, Rocha A, Pedrini H. Face spoofing detection through partial least squares and low-level descriptors[C]//IEEE. 2011 International Joint Conference on Biometrics (IJCB). New York: IEEE, 2011: 6117592.

[26] Kim I, Ahn J, Kim D. Face spoofing detection with highlight removal effect and distortions[C]//IEEE. 2016 IEEE International Conference on Systems, Man, and Cybernetics (SMC). New York: IEEE, 2016: 7844907.

[27] Wen D, Han H, Jain A K. Face spoof detection with image distortion analysis[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(4): 746–761.

[28] Galbally J, Marcel S. Face anti-spoofing based on general image quality assessment[C]//IEEE. 2014 22nd International Conference on Pattern Recognition. New York: IEEE, 2014: 6976921.

[29] Kose N, Dugelay J L. Countermeasure for the protection of face recognition systems against mask attacks[C]//IEEE. 2013 10th IEEE International Conference and Workshops on Automatic Face and Gesture Recognition (FG). New York: IEEE, 2013: 6553761.

[30] Boulkenafet Z, Komulainen J, Hadid A. Face anti-spoofing based on color texture analysis[C]//IEEE. 2015 IEEE International Conference on Image Processing (ICIP). New York: IEEE, 2015: 7351280.

[31] Boulkenafet Z, Komulainen J, Hadid A. Face spoofing detection using colour texture analysis[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(8): 1818–1830.

[32] Lakshminarayana N N, Narayan N, Napp N, et al. A discriminative spatio-temporal mapping of face for liveness detection[C]//IEEE. 2017 IEEE International Conference on Identity, Security and Behavior Analysis (ISBA). New York: IEEE, 2017: 7947707.

[33] Wang T, Yang J, Lei Z, et al. Face liveness detection using 3D structure recovered from a single camera[C]//IEEE. 2013 International Conference on Biometrics (ICB). New York: IEEE, 2013: 6612957.

[34] Kose N, Dugelay J L. Reflectance analysis based countermeasure technique to detect face mask attacks[C]//IEEE. 2013 18th International Conference on Digital Signal Processing (DSP). New York: IEEE, 2013: 6622704.

[35] Kose N, Dugelay J L. Mask spoofing in face recognition and countermeasures[J]. Image and Vision Computing, 2014, 32(10): 779–789.

[36] Komulainen J, Hadid A, Pietikainen M. Context based face anti-spoofing[C]//IEEE. 2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS). New York: IEEE, 2013: 6712690.

[37] 罗浩. 人脸识别中的活体检测方法研究[D]. 长沙: 湖

南师范大学，2015.
[38] de Freitas Pereira T，Anjos A，de Martino J M，et al. LBP-TOP based countermeasure against face spoofing attacks[C]//Springer. Asian Conference on Computer Vision. Berlin：Springer，2010：121–132.
[39] Chingovska I，Anjos A，Marcel S. On the effectiveness of local binary patterns in face anti-spoofing[C]//IEEE. 2012 BIOSIG-Proceedings of the International Conference of Biometrics Special Interest Group（BIOSIG）. New York：IEEE，2012：6313548.
[40] Kollreider K，Fronthaler H，Bigun J. Non-intrusive liveness detection by face images[J]. Image and Vision Computing，2009，27（3）：233–244.
[41] 曹喻. 活体人脸检测技术研究[D]. 厦门：集美大学，2014.
[42] Erdogmus N，Marcel S. Spoofing face recognition with 3D masks[J]. IEEE Transactions on Information Forensics and Security，2014，9（7）：1084–1097.
[43] Li L，Feng X，Boulkenafet Z，et al. An original face anti-spoofing approach using partial convolutional neural network[C]//IEEE. 2016 Sixth International Conference on Image Processing Theory，Tools and Applications（IPTA）. New York：IEEE，2016：7821013.
[44] Patel K，Han H，Jain A K. Secure face unlock：Spoof detection on smart phones[J]. IEEE Transactions on Information Forensics & Security，2016，11（10）：2268–2283.
[45] 龙敏，佟越洋. 应用卷积神经网络的人脸活体检测算法研究[J]. 计算机科学与探索，2018，12（10）：1658–1670.
[46] 甘俊英，李山路，翟懿奎，等. 基于 3D 卷积神经网络的活体人脸检测[J]. 信号处理，2017，33（11）：1515–1522.
[47] Jourabloo A，Liu Y，Liu X. Face De-spoofing：Anti-spoofing via Noise Modeling[M]. Berlin：Springer，2018.
[48] Rehman Y A U，Po L M，Liu M，et al. Face liveness detection using convolutional features fusion of real and deep network generated face images[J]. Journal of Visual Communication and Image Representation，2019，59：574–582.
[49] Graves A，Schmidhuber J. Framewise phoneme classification with bidirectional LSTM and other neural network architectures[J]. Neural Networks，2005，18（5/6）：602–610.
[50] Tu X，Zhao J，Xie M，et al. Learning generalizable and identity-discriminative representations for face anti-spoofing[EB/OL]. （2019–01–17）[2019–08–30]. https://arxiv.org/abs/1901.05602.
[51] Yang J，Lei Z，Li S Z. Learn convolutional neural network for face anti-spoofing[EB/OL]. （2014–08–24）[2019–08–30]. https://arxiv.org/abs/1408.5601.
[52] 蒋尚达. 基于视频的活体人脸检测算法研究[D]. 成都：电子科技大学，2018.
[53] Kose N，Dugelay J L. Classification of captured and recaptured images to detect photograph spoofing[C]//IEEE. 2012 International Conference on Informatics，Electronics & Vision（ICIEV）. New York：IEEE，2012：6317336.
[54] Bashier H K，Lau S H，Han P Y，et al. Face spoofing detection using local graph structure[C]// Advances in Intelligent Systems Research. International Conference on Computer，Communications and Information Technology. Atlantis：Atlantis Press，2014：11089.
[55] Housam K B，Lau S H，Pang Y H，et al. Face spoofing detection based on improved local graph structure[C]//IEEE. 2014 International Conference on Information Science & Applications（ICISA）. New York：IEEE，2014：6847399.
[56] Peixoto B，Michelassi C，Rocha A. Face liveness detection under bad illumination conditions[C]//IEEE. 2011 18th IEEE International Conference on Image Processing. New York：IEEE，2011：6116484.
[57] Anjos A，Marcel S. Counter-measures to photo attacks in face recognition：A public database and a baseline[C]//IEEE. 2011 International Joint Conference on Biometrics（IJCB）. New York：IEEE，2011：6117503.
[58] Zhang Z，Yan J，Liu S，et al. A face antispoofing database with diverse attacks[C]//IEEE. 2012 5th IAPR International Conference on Biometrics（ICB）. New York：IEEE，2012：6199754.
[59] Kose N，Dugelay J L. Shape and texture based countermeasure to protect face recognition systems against mask attacks[C]//IEEE. 2013 IEEE Conference on Computer Vision and Pattern Recognition Workshops. New York：IEEE，2013：6595862.
[60] Erdogmus N，Marcel S. Spoofing in 2D face recognition with 3D masks and anti-spoofing with Kinect[C]//IEEE. 2013 IEEE Sixth International Conference on Biometrics：Theory，Applications and Systems（BTAS）. New York：IEEE，2013：6712688.
[61] Kong K，Hei X，Zeng T，et al. A countermeasure against face-spoofing attacks using an interaction video framework[C]//IEEE. 2017 IEEE 3rd Information Technology and Mechatronics Engineering Conference（ITOEC）.
（下转第 17 页）

yeast genes involved in higher alcohol and ester metabolism during beverage fermentation[J]. European Food Research and Technology, 2011, 233(5): 721–729.

[11] Pires E J, Teixeira J A, Brányik T, et al. Yeast: The soul of beer's aroma: A review of flavour-active esters and higher alcohols produced by the brewing yeast[J]. Applied Microbiology and Biotechnology, 2014, 98(5): 1937–1949.

[12] 杨小兰，罗正明，胡仕屏，等. 降低高浓啤酒发酵中高级醇含量的研究[J]. 食品科学，2011，32(9)：188–192.

[13] Eden A, Nedervelde L V, Drukker M, et al. Involvement of branched-chain amino acid aminotransferases in the production of fusel alcohols during fermentation in yeast[J]. Applied Microbiology Biotechnology, 2001, 55(3): 296–300.

[14] Donaton M C, Holsbeeks I, Lagatie O, et al. The *Gap1* general amino acid permease acts as an amino acid sensor for activation of protein kinase A targets in the yeast *Saccharomyces cerevisiae*[J]. Molecular Microbiology, 2010, 50(3): 911–929.

[15] Omura F, Fujita A, Miyajima K, et al. Engineering of yeast Put4 permease and its application to lager yeast for efficient proline assimilation[J]. Bioscience Biotechnology Biochemistry, 2005, 69(6): 1162–1171.

[16] Chiva R, Baiges I, Mas A, et al. The role of *GAP1* gene in the nitrogen metabolism of *Saccharomyces cerevisiae* during wine fermentation[J]. Journal of Applied Microbiology, 2009, 107(1): 235–244.

[17] Gietz R D, Schiestl R H. High-efficiency yeast transformation using the LiAc/SS carrier DNA/PEG method[J]. Nature Protocols, 2007, 2(1): 38–41.

[18] 张翠英，林雪，孙溪，等. 敲除 *MIG1* 同时过表达 *MAL62* 面包酵母的发酵性能[J]. 天津科技大学学报，2014，29(3)：1–5.

[19] 张艳英，肖冬光，张翠英，等. *BAT2* 缺失酿酒酵母基因工程安全菌株的构建及其杂交育种[J]. 食品与发酵工业，2012，38(1)：36–40.

[20] 中华人民共和国国家质量监督检验检疫总局，中国国家标准化管理委员会. GB/T 4928—2008 啤酒分析方法[S]. 北京：中国标准出版社，2008.

责任编辑：郎婧

（上接第 9 页）

New York: IEEE, 2017: 8122453.

[62] Boulkenafet Z, Komulainen J, Li L, et al. OULU-NPU: A mobile face presentation attack database with real-world variations[C]//IEEE. 2017 12th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2017). New York: IEEE, 2017: 7961798.

[63] Liu Y, Jourabloo A, Liu X. Learning deep models for face anti-spoofing: Binary or auxiliary supervision[C]//IEEE. 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition. New York: IEEE, 2018: 8578146.

[64] Zhang S, Wang X, Liu A, et al. A dataset and benchmark for large-scale multi-modal face anti-spoofing [EB/OL]. (2018–12–02)[2019–08–30]. https://arxiv.org/abs/1812.00408.

[65] de Freitas Pereira T, Anjos A, De Martino J M, et al. Can face anti-spoofing countermeasures work in a real world scenario[C]//IEEE. 2013 International Conference on Biometrics (ICB). New York: IEEE, 2013: 6612981.

[66] Pratt H, Williams B, Coenen F, et al. FCNN: Fourier convolutional neural networks[C]//Springer. Joint European Conference on Machine Learning and Knowledge Discovery in Databases. Berlin: Springer, 2017: 786–798.

[67] Nikisins O, George A, Marcel S. Domain adaptation in multi-channel autoencoder based features for robust face anti-spoofing[EB/OL]. (2019-07-09)[2019-08-30]. https://arxiv.org/abs/1907.04048.

[68] Laurensi R I A, Menon L T, Penna N. M C O, et al. Style rransfer applied to face liveness detection with user-centered models[EB/OL]. (2019-07-16)[2019-08-30]. https://arxiv.org/abs/1907.07270.

[69] Liu Y, Stehouwer J, Jourabloo A, et al. Deep tree learning for zero-shot face anti-spoofing[EB/OL]. (2019-04-05)[2019-08-30]. https://arxiv.org/abs/1904.02860.

[70] Zhang P, Zou F, Wu Z, et al. FeatherNets: Convolutional neural networks as light as feather for face anti-spoofing[EB/OL]. (2019–04–22)[2019–08–30]. https://arxiv.org/abs/1904.09290.

责任编辑：郎婧