人脸活体检测综述

蒋方玲 [1,2] 刘鹏程 [1] 周祥东 [1]

摘 要 人脸活体检测是为了提高人脸识别系统安全性而需要重点研究的问题。本文首先从人脸活体检测的问题出发，分个体、类内、类间三个层面对人脸活体检测存在的困难与挑战进行了阐述分析。接下来，本文以算法使用的分类线索为主线，分类别对人脸活体检测算法及其优缺点进行了梳理和总结。之后，本文就常用人脸活体检测数据集的特点、数据量、数据多样性等方面进行了对比分析，对算法评估常用的性能评价指标进行了阐述，总结分析了代表性人脸活体检测方法在照片视频类数据集 CASIA-MFSD、Replay-Attack、Oulu-NPU、SiW 以及面具类数据集 3DMAD、SMAD、HKBU-MARsV2 上的实验性能。最后本文对人脸活体检测未来可能的发展方向进行了思考和探讨。

关键词 人脸活体检测, 计算机视觉, 人脸识别, 深度学习, 特征表达

引用格式 蒋方玲, 刘鹏程, 周祥东. 人脸活体检测综述. 自动化学报, 2019, **XX**(X): X−X

DOI 10.16383/j.aas.c180829

A Review on Face Anti-spoofing

JIANG Fang-Ling[1,2] LIU Peng-Cheng[1] ZHOU Xiang-Dong[1]

Abstract Face anti-spoofing is an important research field for ensuring the security of face recognition system. In this paper, we first discuss the difficulties and challenges in the development of face anti-spoofing. Then we take the classification clues utilized by the methods as the main line to review the achievements in the study of face anti-spoofing. Next, we analyze the characteristics, data volume and data diversity of commonly used face anti-spoofing datasets. The evaluation metrics of performances commonly used in algorithm evaluation are expounded. We summary and analyze the performances of representative face anti-spoofing methods on CASIA-MFSD,Replay-Attack,Oulu-NPU,SiW,3DMAD,SMAD and HKBU-MARsV2 datasets. Finally, we discuss the future development direction of face anti-spoofing.

Key words Face anti-spoofing, face recognition, computer vision, deep learning, feature representations

Citation JIANG Fang-Ling, LIU Peng-Cheng, ZHOU Xiang-Dong. A Review on Face Anti-spoofing. *Acta Automatica Sinica*, 2019, **XX**(X): X−X

人脸活体检测是指辨别当前获取的人脸图像是来自活体人脸还是假体人脸的过程，其中活体人脸指有生命的真实人脸，假体人脸指冒充真人身份的人脸仿冒品[1]。随着人脸识别技术的广泛应用，人脸活体检测作为保障人脸识别技术安全性的关键环节，逐渐成为计算机视觉、模式识别、人脸识别领域非常活跃的研究方向。

人脸活体检测研究具有重要的应用价值。深度学习的发展使人脸识别技术的性能有了质的提升，人脸识别技术具有自然、直观、易用等优点，目前已广泛应用于智能安防、公安刑侦、金融社保、智能家居、电子商务、人脸娱乐、医疗教育等领域，应用场景丰富，应用市场潜力巨大。然而，人脸识别技术的广泛应用亦使得人脸识别技术的安全性问题日益凸显。传统的人脸识别研究专注于整体识别性能的提升，如图 1 所示，整体处理流程一般包含人脸检测、人脸对齐、特征抽取、特征比对等环节，其并不判断当前获取的人脸图像是来自活体人脸还是假体人脸。随着智能手机和社交网络的蓬勃发展，不法分子收集合法用户的人脸图像，制作假体人脸的渠道广、成本低。文献 [2] 利用合法用户在社交网络上发布的照片轻松的经过了六个商业人脸识别系统 Face Unlock, FacelockPro, Visidon, Veriface,Luxand Blink 以及 FastAccess 的认证。目前人脸识别技术广泛应用于对安全性有高要求的人员身份鉴定场景，若不法分子利用传统人脸识别技术的这个安全性隐患，使用假体人脸成功冒用合法用户身份，从短期来看，侵犯了合法用户的权益，较大可能造成生命财产损失；从长远来看，亦会影响

收稿日期 2018-12-12 录用日期 2019-04-19
Manuscript received December 12, 2018; accepted April 19, 2019
国家重点研发计划 (2018YFC0808300), 中科院西部之光项目, 国家自然科学基金 (6180021609, 6180070559,61602433) 资助
Supported by National Key Research and Development Program of China(2018YFC0808300), CAS Light of West China Program, National Natural Science Foundation of China (6180021609, 6180070559,61602433)
本文责任编委 XXX
Recommended by Associate Editor XXX
1. 中国科学院重庆绿色智能技术研究院 重庆 400714 2. 中国科学院大学 北京 100049
1. Chongqing Institute of Green and Intelligent Technology, Chinese Academy of Sciences, Chongqing 400714, 2. University of Chinese Academy of Sciences, Beijing 100049

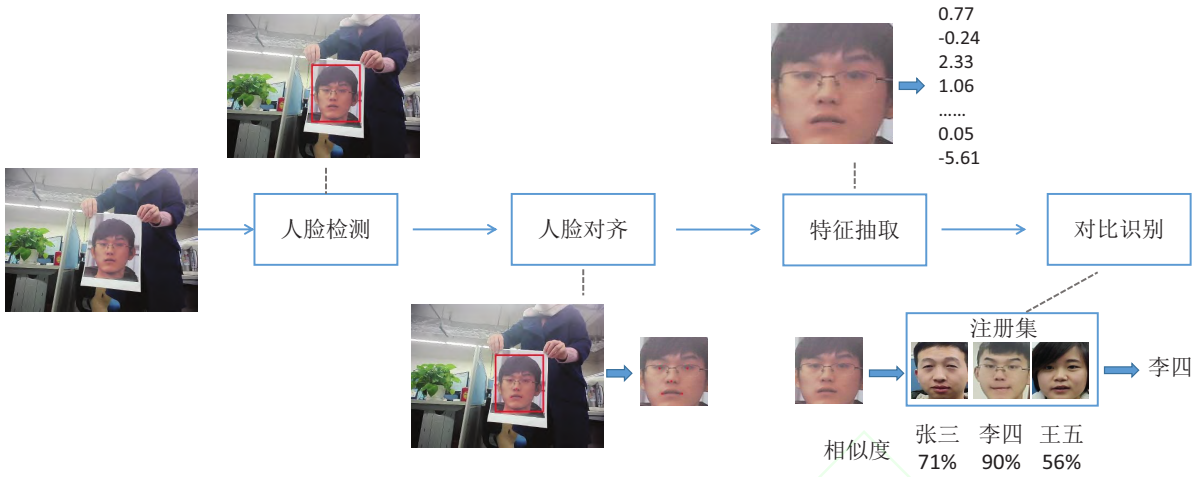


图 1 传统人脸识别技术的安全性缺陷

Fig. 1 Vulnerability of conventional face recognition system

人脸识别技术的进一步广泛深入应用。因此，如何准确识别活体人脸与假体人脸，保障人脸识别技术的安全性成为一个亟待解决的问题。

人脸活体检测研究具有重要的学术价值。近年来，国内外对人脸活体检测的研究活跃。瑞士 IDIAP 研究所，密歇根州立大学，OULU 大学，南洋理工大学，中国科学院自动化所，清华大学，上海交通大学等都有团队从事人脸活体检测的研究。CVPR(IEEE conference on Computer Vision and Pattern Recognition)、ECCV(Europe conference on Computer Vision)、IEEE Transactions on Information Forensics and Security 等重要国际会议期刊上发表的人脸活体检测相关论文数量大幅度增长。人类的智慧是无穷的，假体人脸亦是各种各样，层出不穷。通过寻找活体人脸与假体人脸之间的可区分线索，研究出准确率高、通用性强的人脸活体检测算法，不仅能够服务于人脸识别技术，对于类似的纹理分类，皮肤检测，掌纹、静脉、虹膜等生物识别领域亦能够提供思路启发。

鉴于人脸活体检测的重要研究价值，相关研究者对人脸活体检测方法进行了综述。文献 [3] 根据算法使用的技术对 2014 年前的人脸活体检测方法进行了综述。文献 [4-5] 对 2017 年已有的人脸活体检测方法进行了综述。这些文献详细列举了目前存在的假体人脸类别，对于假体人脸的特性所造成的人脸活体检测问题没有更深入的分析，而问题的剖析更有利于后期有效方法的提出。因此，有必要对假体人脸特性所造成的人脸活体检测的难点进行深入剖析。除此之外，这些文献主要对基于手工特征的方法进行了分析综述，对于基于深度学习的方法少有涉及。随着深度学习方法的发展，不少研究者提出了基于深度学习的人脸活体检测方法。相对于 2017 年前已有的人脸活体检测算法，近年来出现的基于深度学习的人脸活体检测算法很大程度上提升了人脸活体检测的性能。虽然目前基于深度学习的人脸活体检测算法也存在一定的问题，但是鉴于深度学习方法在人脸识别、物体分类等其他计算机视觉领域的应用经验，利用深度学习方法进行人脸活体检测的前景是可观的。因此，有必要对基于手工特征以及基于深度学习的人脸活体检测方法进行全面的综述和讨论，以期为进一步的人脸活体检测研究奠定一定的基础。

本文系统地综述了人脸活体检测相关研究进展，并对未来发展趋势进行了展望。本文首先从人脸活体检测的问题出发，从个体、类内、类间三个层面分析了假体人脸给人脸活体检测带来的难点和挑战，继而根据人脸活体检测算法的主要应用形式将主流算法分为交互式人脸活体检测与非交互式人脸活体检测两大类进行梳理和总结，详述了代表性方法的原理、优势与不足。之后，对人脸活体检测方面的主流数据库进行了整理，对数据库的特点、数据量、数据多样性方面进行了比较分析，对算法评估常用的性能评价指标进行了阐述，总结分析了代表性人脸活体检测方法在照片视频类数据集 CASIA-MFSD、Replay-Attack、Oulu-NPU、SiW 以及面具类数据集 3DMAD、SMAD、HKBU-MARsV2 上的性能数据，最后对人脸活体检测算法未来可能的发展方向进行了思考和探讨。

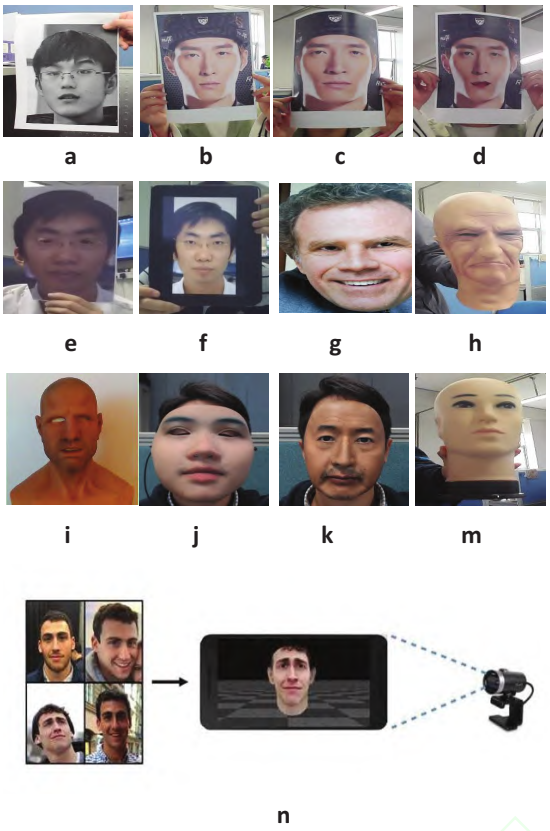


图 2　不同类别假体人脸示例

Fig. 2　Examples of spoofing faces

1　人脸活体检测的难点与挑战

人脸活体检测已经发展为保障人脸识别系统安全性的一个基本问题，逐渐成为了人脸识别整个处理流程中的一个重要环节，亦是一个非常具有挑战性的问题。目前常见的假体人脸有以下几种：

1) 照片类假体人脸

照片类假体人脸是指用照片纸、普通打印纸打印的黑白 (如图 2 a 所示) 、彩色人脸照片或者电子设备显示的电子照片。照片类假体人脸是二维人脸，有完整照片假体人脸 (如图 2 b,c 所示) 和挖去部分脸部区域的照片假体人脸 (如图 2 d,e 所示) 两类，挖去的区域通常是眼部 (如图 2 d 所示) 或者嘴部 (如图 2 e 所示) 区域。照片类假体人脸可以平铺在摄像头前 (如图 2 b 所示)，亦可弯曲的放在摄像头前 (如图 2 c 所示)。社交网络的发展使得假体人脸的制造者能够快速、方便的收集他人的人脸图像，打印机的普及也使得打印照片方便且成本低廉。因此，照片类假体人脸是最常见的假体人脸。

2) 视频类假体人脸

视频类假体人脸是指通过手机、平板电脑或者其他电子显示设备播放的预先录制好的人脸视频 (如图 2 f 所示)。这些视频通常包含眨眼、点头、抬头、张嘴、唇部微运动等一些动作信息，用于迷惑人脸识别系统。

3) 面具类假体人脸

面具类假体人脸是指各类材质的三维人脸面具。此类假体人脸通常有塑料、乳胶、硅胶材质的人脸面具、人脸模具等。塑料硅胶人脸面具有根据商家设计的人脸制作的面具 (如图 2 h,f 所示)，亦有根据用户提供的照片定制的人脸面具 (如图 2 j,k 所示)，其中图 2 j 的制作方是 ThatsMyFace(thatsmyface.com)，图 2 h 的制作方是 REAL-F(real-f.jp)。人脸模具指三维立体人头模块 (如图 2 m 所示)，一般不可以戴在脸上。

4) 合成的三维人脸模型类假体人脸

合成的三维人脸模型类假体人脸是指利用合法用户照片使用三维人脸软件合成的三维人脸模型 (如图 2 n 所示)。此类人脸模型通常以电子设备为媒介，通过电子设备显示后攻击人脸识别系统。

图 3　Replay-Attack 数据集中的假体人脸

Fig. 3　Spoofing faces of Replay-Attack

人脸活体检测的难点与挑战究其原因，主要是假体人脸以假乱真的高质量以及假体人脸的多种多样导致的，具体可以从个体、类内和类间三个层面来看。

个体：人脸活体检测的任务是要识别当前获取的人脸图像是否来自有生命力的活体人脸。基本解决思路是抽取活体人脸图像与假体人脸图像的差异作为分类线索。目前很多假体人脸的制造工艺优良，制造出来的假体人脸质量高，经人脸检测对齐处理后的假体人脸图像与活体人脸图像看起来非常相似。如图 3 所示，人眼几乎很难分辨出这些人脸图像不是采集于活体人脸而是照片类假体人脸。个体层次以假乱真的高质量使得人脸活体检测的难度大大增加。

类内：同一类别的假体人脸虽然有共同的本质特征，但是同一类别的不同假体人脸也存在着较大差异。假体材质、制造方式、制造者、外界环境的不同都会导致同类别的不同假体人脸的差异。比如说，照片类假体人脸的材质有打印纸、照片纸、电子显示屏等。面具的材质有塑料、乳胶、硅胶等。不同材

质的同类别假体人脸成像时反射属性、纹理方面会存在较大差异。不同的打印机、不同的电子显示设备、不同的生成厂家及其制造方式都会导致同类别不同假体人脸在颜色分布、分辨率、外观质量等方面存在差异。同类别不同假体人脸的成像效果也会根据人脸识别系统的摄像头、外界环境的差异而多种多样。这些类内的差异给人脸活体检测算法带来了极大的困难。

类间：假体人脸的种类多种多样，具体来说其品类有照片、视频、面具之分，其材质有纸质、电子显示屏、塑料、硅胶之分，其结构有二维和三维之分。目前大部分人脸活体检测算法都是根据具体的假体人脸类型设计具体的算法。假体人脸的类间差异使得抽取有效而通用的特征同时去准确识别各类假体人脸与活体人脸的难度大大增加，给人脸活体检测算法带来了极大的挑战。不仅目前常见的假体人脸多种多样，随着假体人脸制造技术的发展，未来的假体人脸更是可能多种多样。人脸活体检测算法如何对这多种多样的未知假体人脸有效而通用更是一个有挑战的问题。

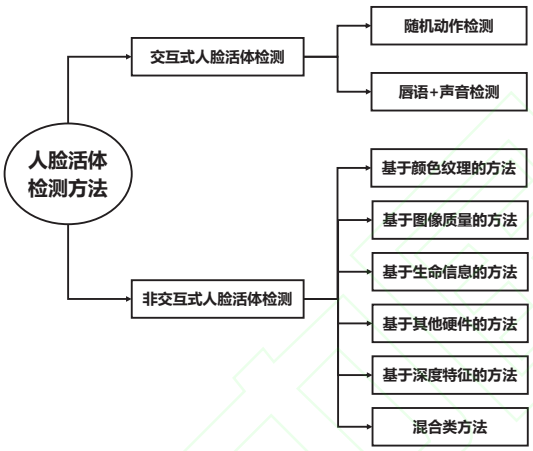


图 4 人脸活体检测方法分类

Fig. 4 Classification of face anti-spoofing methods

2 人脸活体检测方法

现有的人脸活体检测方法从多种不同的角度致力于将活体人脸图像与假体人脸图像区分开来。关于人脸活体检测方法的分类，根据不同的分类依据可以得到不同的分类体系。如以信号源为依据，可以分为基于可见光的人脸活体检测、基于红外的人脸活体检测、基于多光谱的人脸活体检测、基于光场相机的人脸活体检测、基于深度摄像头的人脸活体检测、基于可见光图像与语音混合的人脸活体检测。以输入信息的模态为依据，可以分为基于单帧图像的人脸活体检测、基于视频的人脸活体检测、基于三维深度坐标点的人脸活体检测、基于视频语音混合的人脸活体检测。人脸活体检测方法一般将人脸活体检测问题作为一个活体人脸图像和假体人脸图像的二分类问题来处理。分类问题的性能很大程度上由算法是否使用了区分性足够强的特征以及是否使用了合适的分类策略。考虑到特征的重要性，本文拟以人脸活体检测方法所利用的特征种类为线索详述各类人脸活体检测算法。本文根据当前主流人脸活体检测方法的应用形式，将其分为交互式人脸活体检测与非交互式人脸活体检测两大类，针对每类方法，进而以特征种类为线索，具体阐述各类人脸活体检测算法。整体分类体系如图 4 所示，表 1 对相应类别方法进行了概括性的对比分析。下面将对各类方法进行具体阐述。

2.1 交互式人脸活体检测

活体人脸的宿主是有生命力的人类。人类可以按照要求做出动作或者发出声音，但是假体人脸却难以做到。基于这个考虑，人们提出了交互式人脸活体检测方法。交互式人脸活体检测利用动作指令与用户交互，系统通过判断用户是否准确完成了指定动作来辨别摄像头前的人脸是活体人脸还是假体人脸[6−14]。常见的动作指令有点头、抬头、眨眼、闭眼、遮挡眼睛、扬眉、皱眉、笑脸、吐舌头、张嘴、朗读一段文字等。

早期的交互式人脸活体检测动作指令的设计是固定的，这使得预先录制完成动作指令的视频就能攻破这类人脸活体检测算法。为了解决这个问题，基于随机动作指令的交互式人脸活体检测应运而生。动作指令的随机性使得攻击者难以预先录制视频来攻破活体检测算法。交互式人脸活体检测算法的性能如检测准确率、检测时间很大程度上依赖于动作指令识别算法的性能。动作指令的识别是交互式人脸活体检测算法的核心部分。文献 [8] 对连续多帧人脸图像中的动作执行区域进行二值化处理，通过分析二值化图像的变化是否大于指定阈值来判断用户是否完成了随机指定的动作。文献 [10] 通过检测人脸嘴部区域的变化幅度进行唇语识别，辅以语音识别获取用户响应的语音信息共同判断用户是否按要求朗读了系统随机给出的语句。文献 [11] 抽取嘴部区域的光流特征继而用 SVM 进行分类来识别用户是否朗读了系统给出的一串数字。文献 [12] 指导用户完成随机表情动作，通过计算多帧图像的 SIFT 流能量值来判断用户是否完成了指定表情。

交互式人脸活体检测通过精心设计的交互动作，有效减弱了假体人脸类内类间差异对算法性能的影响，因此识别率高，通用性较好，目前被广泛应用于金融、医疗等实际业务场景中。交互式人脸活体检测需要从多帧图像中识别用户是否完成了动作，相对基于单帧的算法计算量大、所需时间长，而且其需要用户在指定区域内完成多个指定动作，检测过

表 1　主流人脸活体检测方法总览

Table 1　Brief overview of face anti-spoofing methods

一级类别	二级类别	分类特征	防范的假体人脸	算法优点	算法缺点
交互式人脸活体检测	基于随机动作的方法	用户配合的动作：点头、抬头、眨眼、闭眼、遮挡眼睛、扬眉、皱眉、笑脸、吐舌头、张嘴[8,12]	照片、视频	对二维类假体人脸准确率高，通用性强	需要用户配合，用户体验差；不能防止眼部、嘴部挖洞的面具攻击；适用范围窄；
	基于唇语声音混合的方法	朗读一个数字串、一段文字时的唇语与声音[10−11]			
非交互式人脸活体检测	基于纹理的方法	LBP、HOG、Gabor 等描述符从灰度图中抽取的灰度纹理特征[15−17,21,23,30−33]；LBP、LPQ 等描述符从 HSV，YCbCr 颜色空间图像中抽取的颜色纹理特征[20,35,41]；	照片、视频、面具	容易实现，计算量少，单张图片可预测结果，速度快	容易被拍摄设备、光照条件、图像质量影响；跨数据集通用能力不强；
	基于图像质量的方法	手工设计特征抽取图像镜面反射、颜色分布、清晰度方面的图像质量特征[45−47]	照片、视频	针对单类假体人脸的跨数据集通用能力相对强，速度快	需要根据假体人脸的类别设计具体特征，跨假体类型的通用能力不强；需要高质量图像；难以抵御高清哑光照片视频攻击；
	基于生命信息的方法	光流法、运动成分分解检测活体不自主的眨眼，脸部、唇部的微运动[50,53−54,58]	照片	对照片类假体人脸准确率高，通用性高	需要视频为输入；计算量大，速度慢；难以防范视频攻击；对假体制造的微运动鲁棒性不强；
		远程光学体积描记术 (rPPG) 信息检测待测对象是否具有心率[60−64]	面具	特定约束条件下准确率高	需要视频为输入；鲁棒性不强，受外界光照、个体运动的影响大；
	基于其他硬件的方法	近红外图像特征[66−72]；短波红外图像特征[73]；热红外图像特征[74]；400nm 至 1000nm 的多个波段图像特征[75−76]；光场图像信息[78−79]；深度图像信息[80−83]；	照片、视频、面具	准确率高	需要增加新的昂贵硬件；设备采集、处理图像的时间增加；
	基于深度特征的方法	从头训练 CNN 抽取深度特征分类[84−85,89]；利用预训练的 ResNet-50、VGG 等模型抽取特征[90−91,93]；深度特征与手工特征融合[91,97−99]；三维卷积抽取时空深度特征[109−110]；	照片、视频、面具	相对来说，准确率较高	模型参数多，计算量大，训练时间长；过拟合问题；对数据量和数据丰富性上有高要求；
	混合特征类方法	纹理信息和运动生命信息的混合[17−19,25,91,99,109,110,112−114]；纹理信息和人脸结构信息的混合[81,85,89,104,115]；人脸结构信息与运动生命信息的混合[101]；图像质量与运动生命信息的混合[97]；背景信息[27] 和其他特征的混合[84,86,90,93,104,109,113]；	照片、视频、面具	融合多特征的优点提升识别准确率和通用性	计算量、存储增大，相对识别时间增长；算法实现和维护的工作量增加；

程繁琐，对用户的限制和要求较高，用户体验不佳，违背了人脸识别技术方便自然识别的优点。除此之外，交互式人脸活体检测需要用户配合的特点决定了其只能用于用户主动配合的业务场景，不适用于视频监控人脸分析之类的用户处于自然行为状态的业务，应用范围相对窄。

2.2　非交互式人脸活体检测

非交互式人脸活体检测在用户无主动感知条件下辨别活体人脸和假体人脸，无需与用户进行交互。

非交互式人脸活体检测分析摄像头捕获的活体人脸图像和假体人脸图像间的差异来区分活体人脸和假体人脸。从利用的差异特征方面分析，非交互式人脸活体检测可以分为基于纹理的方法、基于图像质量的方法、基于生命信息的方法、基于其他硬件的方法、基于深度特征的方法、混合特征类方法。

2.2.1 基于纹理的方法

常见的基于纹理的方法主要关注照片、视频类攻击[15−35]，也有少量文献处理面具类攻击[36−38]。照片、视频中的人脸二次成像时面部的纹理会带有照片纸或者电子显示屏的纹理，和活体人脸皮肤的纹理有一定差异。照片类假体人脸不同的打印质量，视频类假体人脸显示设备不同的显示分辨率也会造成假体人脸的纹理与活体人脸不同。除此之外，活体人脸有复杂的三维立体结构，照片、视频类攻击是二维的平面结构，光在三维结构和二维结构表面不同的反射会形成脸部颜色明暗区域的差异。基于纹理的方法主要利用这些差异为线索进行活体人脸和假体人脸的分类。

LBP(Local Binary Patterns 局部二值模式)[39] 考虑了像素及其相邻像素间的关系，作为一种局部纹理描述符，能够抽取高判别力的纹理特征且理论简单、计算复杂度低，被广泛应用于基于纹理的人脸活体检测方法。鉴于 LBP 描述符的在人脸活体检测领域的基础地位，这里对 LBP 描述符简单的进行介绍。原始的 LBP 算子定义了一个 3*3 的矩阵邻域，以中心点像素值为阈值将邻域像素值二值化，邻域的像素值大于或者等于中心点像素则设为 1，邻域的像素值小于中心点像素则设为 0，之后以逆时针方向遍历邻域一周得到一个表示中心点的像素值二进制模式。图像中的每一个像素点按照此计算方法得到一个表示局部纹理信息的二进制模式。统计各个二进制模式出现的频率得到 LBP 直方图作为特征向量用于分类。3*3 的邻域设计使得原始的 LBP 描述符不能获取其他尺度的纹理信息，Ojala 等人采用圆形邻域扩充了 3*3 的矩阵邻域，使得其能够自定义使用指定半径圆上的指定个邻域点的信息。如此改进后却依然存在问题：同一尺度下的 LBP_{PR} 的各个模式出现的频率不均匀致使抽取的纹理特征效果不能让人满意，同时会产生 2^P 种不同的二进制模式，对计算和存储带来了挑战。为了解决这个问题，Ojala 等人提出了均匀 LBP。均匀 LBP 模式是指二进制串里从 0 到 1 或者从 1 到 0 的变化不超过 U 次。每一个均匀 LBP 模式分为独立的一类，非均匀的 LBP 模式全部归为一类。均匀 LBP 起到了降维的作用，改进计算效率的同时提升了特征抽取的效果。

文献 [15-17] 将采集的图像转化为灰度图之后抽取图像的灰度纹理信息用于活体人脸和假体人脸的分类，屏蔽了颜色光照因素的影响。文献 [15] 利用多个不同尺度的均匀 LBP 算子从灰度图的局部块以及全局图像中抽取纹理特征直方图，之后将所有特征直方图连接形成一个 531 维的特征直方图送入以 RBF 为内核的 SVM 分类器中进行活体人脸和假体人脸分类的训练和测试。基于灰度图的纹理分析算法对于高分辨率、纹理清晰的假体人脸图像比较有效，但是对于一些低分辨率的假体人脸图像，则很难分辨准确。一般用于制造照片视频假体人脸的打印机或者电子设备的色域是人眼可视色域的子集，其颜色没有人眼能感知的颜色丰富。因此，打印机或者电子设备制造的照片、视频类假体人脸在颜色分布上与活体人脸有一定差异。考虑到这个因素，文献 [20] 将图像从 RGB 颜色空间转化为 YCbCr 颜色空间，从亮度、色度通道抽取 LBP 纹理特征，结合颜色、纹理两方面的差异线索进行人脸活体检测。除了 LBP 特征，LBP 的一些变种如 tLBP[16]，dLBP[16]，mLBP[16]，CLBP[21]，CSLBP[21]，LBPV[22] 等也被用于抽取图像中的纹理信息。

除了 LBP 及其变种，研究者们也提出了诸多其他的特征描述符用于人脸活体检测纹理特征的抽取。文献 [23] 将人脸分成 12 个小块，利用局部相位量化 (Local Phase Quantization，LPQ) 抽取纹理特征。文献 [21,24] 利用二值化统计图像特征 (Binarized Statistical Image Features, BSIF) 抽取脸部局部块和脸部全局的纹理特征送入 SVM 用于分类。方向梯度直方图（Histogram of Oriented Gradient, HOG）计算局部区域的梯度方向直方图构成特征被用于分类[23,26−29]。文献 [28,31-32] 使用灰度共生矩阵（Gray-Level Co-occurrence Matrix，GLCM）[40] 统计像素间灰度值的分布规律抽取纹理特征。文献 [33-34] 利用 DOG 高斯差分函数（Difference of Gaussians，DOG）抽取纹理特征识别差光照条件下的活体人脸和假体人脸。文献 [15,26,32] 利用 Gabor 滤波器提取不同尺度不同方向上的纹理特征。文献 [41] 利用加速稳健特征 (Speeded-Up Robust Features,SURF) 从 HSV、YCbCr 颜色空间的图像中抽取颜色纹理特征。文献 [42] 利用一个附加的闪光灯以便拍摄的图像纹理更清晰，活体人脸图像和假体人脸的纹理差异更明显。不少研究者们混合使用多种特征描述符从图形中抽取特征，继而连接不同描述符的特征送入分类器 SVM 进行训练和测试，如 LPQ 与 LBP 混合[23,43],BSIF 与 LBP 混合[24]，HOG 与 LPQ 混合[44]，Gabor、LBP、GLCM 的混合[32]。不同特征的混合有利于人脸活体检测性

能的提升，但是同时也增加了计算复杂度。

总体来说，基于纹理的方法计算量少，计算复杂度低，容易实现。基于纹理的方法着重利用纹理颜色方面的差异进行分类，要求输入图像的分辨率高，能够保存清晰的颜色纹理细节信息，对采集设备有高要求。采集条件如光照、摄像头质量的差异，假体人脸制造设备的差异造成的假体人脸类内差异皆会导致同类别假体人脸抽取的纹理模式不同，因此，基于纹理的方法普遍存在跨数据集通用性不够强的问题。文献 [35] 也利用丰富的实验验证了采集条件差异和假体人脸类间差异对于基于纹理的人脸活体检测算法的跨数据集通用性存在明显的削弱。

2.2.2 基于图像质量的方法

假体人脸的呈现需要一定的媒介，不管是照片纸、打印纸、电子设备、硅胶、塑料等各类媒介的材料属性与活体人脸的五官、皮肤材质都有差异。材质的差异会导致反射属性的差异，比如照片纸、手机显示屏会有一些镜面反射而活体人脸基本不会存在这种现象。假体人脸的制造工艺虽然优良，但是大部分假体人脸二次成像后的图像质量与活体人脸还是存在一定距离，比如说颜色分布的失真，假体人脸图像的模糊感等。基于图像质量的方法主要利用图像失真、反射属性方面的差异分辨真假人脸。

文献 [45] 设计了 25 种图像质量评估指标用于评估假体人脸的失真程度。文献 [46] 针对人脸活体检测设计了 14 种通用特征用于抽取图像质量方面的差异。文献 [47] 利用镜面反射、图像模糊、颜色分布等图像失真方面的分析提取了针对照片假体人脸的特征。图像的质量很大程度上依赖拍摄设备以及外界条件。低质量的拍摄设备以及差的光照等外界条件亦会使得活体人脸的图像存在失真的问题。文献 [48] 考虑了不同质量拍摄设备的影响，首先利用聚类的方法将图像以图像质量维度聚类，然后针对每一种质量等级的图像预训练一个基于图像质量特征的活体人脸和假体人脸分类指导模型，对于测试图像，首先判断其图像质量等级，利用回归的方法映射图像到其对应图像质量等级的分类指导模型，之后利用映射得到的分类指导模型进行活体人脸和假体人脸分类。文献 [49] 选取图像质量差异明显的人脸块用于人脸活体检测，他们首先将检测到的人脸图像分成小块，利用图像质量评价、图像强度分析等方法将小块人脸图像根据其判别能力进行排序，最后从判别能力强的小块人脸图像中抽取特征，送入 SVM、QDA 等分类模型中进行活体人脸和假体人脸分类。

基于图像质量的方法计算复杂度低，检测速度较快，有利于在线实时检测。此类方法使用了的一些通用的图像质量评估特征，能够较好的应对假体人脸的类内差异问题，对于单类假体人脸的跨数据通用能力相对较强。目前基于图像质量的方法主要关注于照片、视频类假体人脸的识别，对面具类假体人脸的研究较少。此类方法不能很好的应对假体人脸的类间差异，需要针对每一类假体人脸的特点设计其图像质量方面的特征，识别照片、视频类假体人脸的图像质量特征不能简单的迁移使用到面具类假体人脸的识别。算法虽然对于打印照片、手机显示的照片视频假体人脸比较鲁棒，但是难以准确识别一些高清哑光的照片、视频攻击[46]。从基于图像质量的方法的本质来看，其需要高质量的活体人脸和假体人脸图像作为输入以便能够抽取足够好的图像质量特征，对人脸图像采集设备要求高。

2.2.3 基于生命信息的方法

活体人脸和假体人脸之间一个明显的区别是活体有心跳、血液流动、眨眼、脸部肌肉不自主的微运动等生命特征，而大部分类别的假体人脸难以完美模仿此类生命特征。基于生命信息的方法主要利用这些生命特征方面的差异来进行活体人脸和假体人脸的分类。

文献 [50-51] 利用条件随机场检测输入图像序列中的人眼是否存在睁眼闭眼的切换来判断是否是活体人脸。文献 [52] 分析眼部区域多个尺度、多个方向的 Gabor 响应信号来判断是否存在眨眼行为。文献 [53] 分析活体人脸唇部不自主的微动作进行活体检测。此类利用眼睛和唇部信息的方法能够比较好的识别照片类假体人脸但是不能很好的识别视频、面具类假体人脸。活体人脸具有三维立体结构，其运动模式和照片、视频类二维假体人脸存在差异。文献 [54-56] 利用光流线 (Optical Flowof Lines, OFL) 从水平方向和垂直方向两个维度计算人脸图像的时空差异，获取人脸的运动信息来检测照片、视频之类的平面假体人脸攻击。文献 [57] 利用欧几里得运动放大的方法增强人脸不自觉的微运动信息并用 HOOG 算子抽取运动特征。文献 [58] 利用运动成分分解的方法从图形中分解出眨眼、唇部动作、脸部肌肉动作等运动信息用于活体检测。基于运动信息的检测方法利用了假体人脸难以模拟的生命特征，对于活体人脸和假体人脸来说差异大。同时，假体人脸的类内类间差异对于此类方法有效特征的抽取影响较少。在约束条件下，特征能够稳定抽取时此类方法检测准确率高，但是其需要人脸视频作为输入，计算量相对大，假体人脸的一些模拟微运动能够迷惑此类算法。

远程光学体积描记术 (Remote Photoplethysmography,rPPG)[59] 是一种利用普通摄像头拍摄的

人脸视频计算人体心率的方法。活体人脸面部有丰富的毛细血管，活体心脏跳动会导致血管中血液流量和流速的变化，而血流的变化又影响面部光线的吸收和反射情况，最后这种血液的变化就导致了人脸颜色的变化。通过抽取人脸毛细血管丰富区域的颜色变化即可得到心率的变化。活体人脸的宿主有心率，而假体人脸没有心率，利用这个线索，文献 [60-63] 利用 rPPG 信号检测待测对象是否具有心率并以此判断待测对象是否是活体人脸。文献 [64] 从图像的 R 和 G 通道中抽取血流信息来进行活体检测。此类抽取心率、血流信息的方法多用于三维面具类假体人脸的检测上，在良好不变光照条件下，待测对象保持姿态、表情不动的情况下方法准确率较高，但是它们的计算过程需要足够长的高清人脸视频以便能够抽取到足够好的 rPPG 信号，同时 rPPG 信号受外界环境光照、待测对象运动的影响大，方法鲁棒性不强。

2.2.4 基于其他硬件的方法

除了利用传统的可见光摄像头捕获人脸图像，研究者们也利用了其它多元化的硬件如红外摄像头、多光谱摄像头、光场相机、深度摄像头等捕获相应类型的人脸图像进行活体检测。

红外摄像头、多光谱摄像头 红外摄像头、多光谱摄像头是最常用的一种。不同波段的红外如近红外、短波红外、热红外都有相关研究工作。假体人脸的材质与活体人脸的皮肤、眼睛、嘴唇、眉毛等部位的材质不同，而材质的不同就会造成反射属性有差异。虽然假体人脸在可见光条件下看起来和活体人脸非常相似，但是在红外光谱下，活体人脸的皮肤、眼睛、鼻子等区域的看起来和假体人脸都有较大差异。一些研究者利用 Gabor、HOG、朗伯模型等抽取近红外摄像头图像中活体人脸和假体人脸的反射差异进行活体检测[66−72]。在近红外光谱下，照片和视频攻击与活体人脸的差异较大，此类方法准确率高，跨数据通用能力强，但是制作精良的面具却与活体人脸的差异较少。为了识别面具攻击，文献 [73] 利用短波红外来区分人脸皮肤和面具。热红外图像中包含了受测对象散发的热辐射信息。活体人脸有一定温度能够散发热辐射，但是照片、视频等假体人脸却不能散发此类信息。文献 [74] 利用热红外图像进行活体人脸以及照片、视频类假体人脸的分类。文献 [75-76] 利用了 400nm 至 1000nm 的多个波段图像来抽取反射特征区分活体人脸和照片攻击。

光场相机光场相机能够记录光在空间中的方向与位置等信息[77]，文献 [21,78-79] 利用光场相机拍摄光场照片用于人脸活体检测。原始的光场照片是由很多个小的微透镜图像组成的。随着焦距的不一样，微透镜图像表示不同的光分布。这些不同光分布的图像能够用于估计输入图像中深度的存在。文献 [78] 利用 LBP 从光场照片的两种可视化图像：微透镜图像和光场子孔径图像中抽取人脸边缘特征以及射线差异特征用于假体人脸与活体人脸的分类。

深度摄像头 活体人脸有复杂的三维立体结构，照片、视频类假体人脸却是二维平面结构。深度摄像头拍摄的深度图像能够记录下物体间的深度信息，三维活体人脸和二维假体人脸结构的差异导致人脸离深度摄像头的深度信息会存在较大差异。文献 [80-81] 利用 Kinect 与可见光摄像头录制人脸深度图和可见光图像，继而从人脸可见光图像和深度图中抽取纹理特征以及人脸结构特征进行活体人脸和照片、视频类假体人脸的分类。活体的三维人脸结构有明显变化的表面曲率，但是二维的假体人脸却没有。文献 [82] 利用三维扫描仪获取待测对象的三维模型，通过分析待测对象的表面曲率来判断三维活体人脸和二维假体人脸。面具类假体人脸虽然也有三维立体结构，但是因为工艺原因，大部分面具类假体人脸的三维结构还是没有活体人脸精细。基于几何属性的三维形状分析能够很好的刻画人脸的表面结构与形状。常用的几何属性包括主曲率、高斯曲率、平均曲率及其方差。文献 [83] 利用主曲率测量以及 meshSIFT 特征描述符从待测对象的三维人脸模型中抽取活体人脸和面具间的几何形状差异来进行活体人脸和面具假体人脸的分类。

基于其他硬件的方法利用的特征区分度大，假体人脸的类内差异对方法的影响较少，整体识别准确率高，但是其需要增加新的硬件，这不仅意味着新的昂贵的硬件投入，而且也意味着人脸识别系统的硬件改造，费时费力。新增硬件在一定程度上也会限制算法的使用范围，比如智能手机之类的移动端人脸活体检测可能会因为新增其他摄像头不方便而舍弃这种解决方案。

2.2.5 基于深度特征的方法

早期的人脸活体检测算法一般抽取手工设计的特征，继而利用 SVM、LDA 等分类器训练分类模型进行活体人脸和假体人脸的分类。手工设计特征作为浅层特征，表达能力一般，不能有效表征活体人脸和假体人脸之间的差异。深度学习方法能够抽取高层语义的特征表达，近年来大大提升了人脸识别、物体分类等计算机视觉任务的性能。随着深度学习方法的发展，人们也逐渐利用深度学习的方法来处理人脸活体检测的问题。基于深度特征的人脸活体检测方法一般融合考虑了多方面的信息进行活体人脸与假体人脸的分类，如颜色纹理、图像质量、背景边框信息、时序变化信息等。针对深度学习技术，数

据和网络模型训练至关重要，本节将从网络输入数据源和深度特征学习两个方面来分析基于深度特征的人脸活体检测方法。

网络输入数据源

最初人们借鉴深度学习方法在其他领域的应用方法，使用端到端的深度学习方法进行活体人脸和假体人脸分类。文献 [84] 利用五个卷积层、五个池化层、三个全连接层组成的卷积神经网络从包含不同尺度背景信息的可见光 RGB 人脸图像中抽取深度特征，并使用 Softmax 进行活体人脸和假体人脸的预测。由于假体人脸的类内类间差异大以及假体人脸的造价昂贵导致的人脸活体检测数据集中个体数量少、数据总量少、数据间的多样性不如常规的人脸识别数据集丰富的问题，方法的识别准确性和跨数据集通用性仍有待提高。

为了提取区分度更大的特征，研究者们对传统的 RGB 人脸图像进行各类处理，使得要利用的特征更加明显，之后再利用卷积神经网络抽取分类特征[85−87]。文献 [85] 将人脸图像从 RGB 颜色空间转换成 HSV，YCbCr 颜色空间并分割成小块，利用端到端的卷积神经网络从分割的小块图像中抽取特征进行分类。颜色空间转换让活体人脸和假体人脸的颜色纹理差异更明显。小块的分割一方面让卷积神经网络更专注于局部块的信息抽取，另一方面也从数据增强的角度提升了方法的性能。文献 [86] 将非线性扩散[88] 和卷积神经网络进行了结合。考虑到二维的假体人脸经非线性扩散后人脸五官的边界会退化而活体人脸则会保留边界信息，他们首先使用非线性扩散处理活体人脸和假体人脸图像，继而利用卷积神经网络从扩散后的图中抽取深度特征。文献 [87] 采取类似 rPPG 的思路，以心脏跳动会带来活体面部颜色的变化为差异线索，为图像中的每一个像素点进行频率分析，得到能够表征生命信息的相对高低能量值，之后利用卷积神经网络从人脸图像的这种能量表示图抽取分类特征进行分类。除了对 RGB 图像进行各类处理，研究者们也综合利用了其他硬件设备录制的图像。文献 [89] 利用卷积神经网络从常规的可见光人脸图像以及 Kinect 录制的人脸深度图中抽取特征用于活体人脸和假体人脸分类。深度图中包含的人脸结构信息对于三维活体人脸和二维假体人脸的高区分性有利于提升算法的准确率与通用性。

深度特征学习

深度学习的方法能否学习到有效而通用的特征很大程度上依赖数据量是否足够大，数据多样性是否丰富。人脸活体检测的小数据集问题导致基于深度学习的人脸活体检测方法容易陷入过拟合的困境。很多研究者们利用在其他数据更丰富的数据集上预训练深度神经网络模型的思路来解决过拟合的问题[90−93]。文献 [90] 首先在 ImageNet 上预训练 ResNet50 模型[94]，利用得到的模型从连续多帧人脸图像中抽取空间深度特征，之后将抽取的特征送入 Long Short-Term Memory (LSTM) [95] 中抽取帧间的时序变化信息用于活体人脸和假体人脸的分类。LSTM 与 CNN 的结合综合了双方从连续多帧人脸图像中抽取空间信息、时序信息的能力，利用预训练的残差网络模型减少了人脸活体检测数据集上过拟合的影响。文献 [93] 在 MSU Mobile Face Spoofing Database (MSU-MFSD)[47] 数据集上通过大量实验对比了 Inception-v3 、ResNet50，ResNet152 用于人脸活体检测的性能。实验中考虑了模型的深度、微调预训练模型或者从头训练、不同学习速率等方面的对比因素。

除了利用预训练的模型外，研究者们也从训练方法方面进行了研究。文献 [80,89] 利用深度卷积神经网络抽取特征，之后利用 SVM 进行分类，在一定程度上可以降低过拟合的影响，提升算法性能。文献 [96] 针对人脸活体检测数据集数据量少的问题，提出了一种训练策略提高算法的通用能力。常规的深度学习模型训练方法是将训练集随机化排序一次后划分小批量数据集用于训练，文献 [96] 在模型的训练阶段每一次迭代都从整个训练集中随机的选取一个小批量数据用于训练，通过这种随机的选取小批量训练数据的方法减少过拟合的影响。一般的基于深度学习的人脸活体检测方法利用活体人脸和假体人脸的类别为标签，文献 [101] 认为简单的类别标签包含的信息过于简单，他们利用活体人脸和假体人脸的深度信息图以及 rPPG 信号为指导标签训练深度神经网络进行分类预测。深度信息图中蕴含了三维活体人脸和二维假体人脸的结构差异，rPPG 信号蕴含了活体人脸与假体人脸的生命信息差异，两种信息皆对活体人脸与假体人脸的区分度大。使用这两种信息明确的作为指导信息，有利于提升方法的通用性。假体人脸的种类多且类间差异大，为了减少类间差异对活体检测算法性能的影响，文献 [106] 针对照片和视频类攻击分别训练对应类别的 ResNet50 分类模型，然后利用堆栈泛化[107−108] 的方法训练一个模型组合不同类别假体人脸的分类模型。单类假体人脸分类模型减少了不同假体人脸间的差异对分类性能的影响，使模型专注于某一类假体人脸的分类，有利于模型性能的提高。使用堆栈泛化组合模型一方面能够进一步提高分类准确率，一方面也使得一个模型能够处理多种假体人脸，提升模型的通用性。

针对目前人脸活体检测算法跨数据集通用性不

强的问题，文献 [103] 引入领域自适应的方法进行活体人脸与假体人脸分类，提升深度模型的跨数据集通用性。文献 [102] 将贪婪深层字典学习用到了人脸活体检测。一般基于深度学习的方法利用二维的卷积神经网络抽取图像层面的信息，并没有利用到连续多帧人脸活体检测图像中的时序信息。文献 [109-110] 利用三维卷积神经网络[111] 从连续多帧人脸图像中抽取时空深度特征，相对于基于二维卷积神经网络的人脸活体检测方法，增加了时间维度的差异信息，更有利于提高算法的识别性能与通用性。

很多研究者们也将深度学习的方法和手工设计特征的方法进行了融合[91,97−99]，以结合两种方法的优点，减少过拟合的影响，提升算法性能。文献 [97] 将神经网络、shearlet、光流法进行了结合，设计了一个分层神经网络，融合学习图像质量以及运动信息用于人脸活体检测。他们首先利用 shearlet 抽取图像质量方面的特征，利用光流法从裁剪后的人脸以及包含背景的人脸图像中抽取光流幅度运动特征，然后将抽取的运动特征送入一个两层的神经网络中抽取分类特征进行分类。文献 [91] 将 CNN 与 LBP 结合起来，利用人脸活体检测数据集微调预训练好的 VGG-face 模型[100]，之后从微调的 VGG-face 模型抽取的卷积特征图中抽取 LBP 特征并送入 SVM 进行活体人脸和假体人脸的预测。文献 [98] 将 CNN 与 LBP-TOP 结合起来，利用 LBP-TOP 从卷积特征图中抽取时空特征，在减少过拟合情况的发生的同时，为活体检测算法增加了时间维度的分类线索。文献 [99] 将 CNN 与光流法进行了结合，学习连续多帧人脸图像中的动态纹理信息。他们首先利用一个预训练的 VGG 网络从每一帧图像中抽取卷积特征图，然后利用光流法计算每一个卷积特征图的微运动特征，最后在通道可分辨性约束下，从所有卷积通道的微运动特征中提取深层卷积动态纹理特征并送入 SVM 进行分类。文献 [104] 将微纹理描述符与 Single Shot MultiBox Detector (SSD)[105] 结合，首先在人脸检测的过程中同时进行活体人脸和假体人脸的分类，然后对于 SSD 给出的预测结果置信度高的人脸图像，取 SSD 的预测结果，对于 SSD 给出的预测结果置信度低的人脸图像，利用设计的微纹理描述符抽取纹理特征并送入 SVM 进行分类，取 SVM 的预测结果。方法利用深度学习方法与手工设计特征的方法组成的层级结构，融合了两类方法的判别能力提升活体人脸与假体人脸的识别性能。

总体来说，越来越多的研究者倾向于利用基于深度特征的人脸活体检测方法去解决人脸活体检测面临的问题。一些端到端的基于深度特征的方法相对于基于手工特征的方法实现起来更方便。基于深度特征的方法针对假体人脸个体以假乱真的高质量、类内类间差异、数据量少的问题从网络输入数据源和深度特征学习等方面做了相关研究，抽取的深度特征相对来说有效性和通用性较好，在公开数据集上，目前基于深度特征方法也取得了最好的性能，但是其模型参数多，训练时间长，计算量大，对数据量和数据丰富性上有较高要求。

2.2.6 混合特征类方法

基于单一差异线索进行活体人脸与假体人脸分类，可能会面临识别准确率以及算法通用性方面的瓶颈。为了提高人脸活体检测方法的性能，人们提出了融合多个差异线索进行人脸活体检测的方法，也就是混合特征类方法。常见的混合有纹理信息和运动生命信息的混合[17−19,25,91,99,109,110,112−114]，纹理信息和人脸结构信息的混合[81,85,89,104,115]，人脸结构信息与运动生命信息的混合[101]，图像质量与运动生命信息的混合[97]，背景信息[27] 和其他特征的混合[84,86,90,93,104,109,113] 等。照片、视频类假体人脸存在的边框等背景信息能够提供有效的分类线索，经常被融合利用到各类方法中。

为了利用时序上的微运动生命特征差异，文献 [17-19] 利用 Local Binary Patterns from Three Orthogonal Planes (LBP-TOP)[65] 从时空两个维度抽取动态纹理信息进行活体人脸与假体人脸的分类。LBP 主要抽取空间上的局部纹理信息，LBP-TOP 从时间维度扩充了传统的 LBP 从而可以抽取时空两方面的纹理信息。LBP-TOP 考虑了三个正交平面，传统 LBP 处理的 XY 平面，图像每一行沿时间轴形成的 XT 平面，图像每一列沿时间轴形成的 YT 平面。三个平面以中心点正交。XY 平面记录着空间纹理，XT 平面、YT 平面记录着动态纹理。计算每一个平面的 LBP 特征，然后连接三个平面的 LBP 特征形成 LBP-TOP 特征。文献 [17-19] 考虑了不同长度的时间窗口，抽取 LBP-TOP 动态纹理信息，继而利用以 RBF 为内核的 SVM 进行分类。类似于 LBP-TOP，研究者们也从时间维度扩充了 MLPQ 为 MLPQ-TOP，MBSIF 为 MBSIF-TOP 抽取动态纹理进行人脸活体检测[25]。文献 [112] 融合了深度神经网络抽取的深度纹理特征以及眨眼等运动生命信息。文献 [81] 利用 BSIF 描述符从图像全局以及眼睛等局部小块抽取了纹理和人脸结构造成的深度差异信息。

很多基于深度特征的人脸活体算法混合使用了多种分类特征[85,89,91,97,99,101,104,109−110]。文献 [104] 融合利用了颜色纹理信息、背景信息、人脸结构信息进行人脸活体检测。他们将人脸活体检测与人脸检测融合到一个步骤完成，利用上下文背景信息在给出人脸所在位置的矩形框时也进行活体人脸和假体人脸的判断。他们还设计了两个描述符：spatial pyramid coding micro-texture (SPMT)

表 2 主流人脸活体检测数据集总览

Table 2 Brief overview of face anti-spoofing datasets

数据集	年份	假体人脸	个体数	数据量	姿态、表情、光照等录制场景	录制设备与图像分辨率
NUAA[116]	2010	三种打印照片	15	12641 张图像	三个不同光照的外界环境	网络摄像头 - 可见光图像 640*480 像素;
Yale-Recaptured[33]	2011	LCD 屏显示的照片	10	2560 张图像	64 种不同光照	Kodak C813 8.2 与 Samsung Omnia i900 的摄像头 - 裁剪后的灰度图 64*64 像素;
Print-Attack Database[117]	2011	手持照片、固定照片	50	200 个视频	两种不同光照	可见光图像 苹果笔记本内置摄像头 -320*240 像素;
CASIA-MFSD[34]	2012	弯曲照片、挖眼照片、视频	50	600 个视频	室内光照	可见光图像 使用时间长的 USB 摄像头 -640*480 像素; 新 USB 摄像头 -480 *640 像素; Sony NEX-5 摄像头 -1920 *1080 像素;
Replay-Attack[16]	2012	手持或者固定的照片与视频	50	1300 个视频	两种不同光照	可见光图像 苹果笔记本内置摄像头 -320*240 像素;
MSU-MFSD [47]	2014	高分辨率照片与视频	35	280 个视频	一个场景	可见光图像 MacBook Air 13 内置摄像头 -640x480 像素 Google Nexus 5 前置摄像头 -720*480 像素
UVAD[31]	2015	6 种设备拍摄的人脸视频	404	17076 个视频	不同背景光照的室内室外场景	索尼摄像头 - 可见光图像 1366 *768 像素;
REPLAY-MOBILE[119]	2016	高分辨率照片与视频	40	1200 个视频	五种不同光照	iPad Mini2 (iOS) 以及 LG-G4 前置摄像头 - 可见光图像 720 * 1280 像素;
MSU-USSA [120]	2016	高分辨率照片与视频	1000	9000 张	一个场景	可见光图像 Google Nexus 5 前置摄像头 -1280 × 960 像素; 后置摄像头 -3264 × 2448 像素;
Oulu-NPU[121]	2017	照片与视频	55	5940 个视频	三种不同光照场景	六种智能手机的前置摄像头 - 可见光图像 1920 × 1080 像素;
SiW[101]	2018	高低两种分辨率的照片，弯曲照片与高分辨率视频	165	4478 个视频	活体人脸录制了距离、姿态、表情、光照差异	Canon EOST6, Logitech C920 摄像头 - 可见光图像 1920* 1080 像素;
GUC-LiFFAD [21]	2015	激光、喷墨打印的照片，iPad 显示的照片	80	4826 张图像	不同焦距的图像，室内室外场景	光场相机
Msspoof[122]	2016	可见光与近红外光谱的黑白照片	22	4704 张图片	7 种不同的室内室外环境	uEye 摄像头以及近红外滤波器 可见光与近红外图像 -1280*1024 像素;
EMSPAD[123]	2017	激光打印的照片，喷墨打印的照片	50	10500 张图像	2 个场景	多光谱摄像头七个波段的图像 裁剪对齐后 120*120 像素;
3DMAD[37]	2013	定制三维人脸面具	17	76500 张图像	3 种不同场景	Kinect 深度摄像头 - 深度图 640x480 像素; 可见光摄像头 - 可见光图像 640x480 像素;
HKBU-MARsV2[124]	2016	两种三维人脸面具	12	1008 个视频	7 种不同光照	可见光图像，三种传统摄像头： Logitech C920 网络摄像头 -1280*720 像素; 工业摄像头 -800*600 像素; Canon EOS M3-1280*720 像素； 可见光图像，4 种移动设备摄像头： Nexus 5, iPhone6,Samsung S7, Sony Tablet S；
SMAD[102]	2017	硅胶三维人脸面具	-	130 个视频	不同光照，不同录制背景环境	-
MLFP[125]	2017	挖去眼部的二维照片，乳胶三维人脸面具	10	1350 个视频	室内室外场景	Android 智能手机 - 可见光图像 1280 *720 像素; FLIR ONE 热像仪安卓版 - 热红外图像 640*480 像素; 微软 Kinect- 近红外图像 424 * 512 像素;

抽取微纹理方面特征，template face matched binocular depth (TFBD) 抽取人脸结构方面的特征。将 SMTP 和 SSD 结合起来，对于 SSD 预测结果置信度低的人脸图像抽取 SPMT 特征并利用 SVM 进行分类。除此之外，他们还将 SMTP 与 TFBD 结合起来，综合利用纹理与人脸结构方面的差异。从文献 [104] 的实验结果可以看出混合了各类特征的人脸活体检测算法有利于算法识别率的提升。

总的来说，混合特征类方法可以综合各类特征的优势，减少高质量假体人脸以及假体人脸的类内类间差异的影响，抽取高判别力的特征，提高算法的准确率和通用性，但是正因为其综合了多个不同的特征，算法实现和维护的成本增加，计算量也将增多，算法的处理时间相对会变长。

3 人脸活体检测数据集

数据集中数据的总量、数据类型的丰富程度、数据的采集设备、采集环境等都会影响人脸活体检测方法的性能。随着深度学习方法的发展，数据的重要性日益凸显。对于人脸活体检测，相关研究者们利用的分类特征多种多样，使用的数据集也都有自身的特点，从数据集的发展也能窥测出主流人脸活体检测方法使用的特征、防范的攻击类型、影响算法性能因素的处理等方面的发展。鉴于数据的重要性以及人脸活体检测数据集的多样性，本节我们对人脸活体检测方面的主流数据集分假体人脸类型进行阐述：照片视频类假体人脸活体检测数据集、面具类人脸活体检测数据集。综述的数据集大部分是公开数据集，少部分是不公开的数据集。在介绍不同的数据集时，主要从数据集的特点，数据集建设年份，数据集包含的活体人脸和假体人脸的个体数，图像大小，各类别样本数量，假体人脸类型，录制时考虑的光照、姿态、假体人脸材质等方面的影响因素等方面进行阐述，表 2 对主流人脸活体检测数据集进行了总览对比分析。

3.1 照片视频类人脸活体检测数据集

3.1.1 可见光照片视频类人脸活体检测数据集

NUAA[116] 数据集是第一个面向学术界免费公开的人脸活体检测数据集。NUAA 利用普通的网络摄像头在三个不同的环境下录制了 15 个个体的活体人脸与照片类假体人脸的图像。为了让活体人脸与假体人脸更相似，录制过程中要求活体人脸做到人脸正向面对摄像头，保持自然表情，不出现眨眼、头部微运动等情况。制作的假体人脸一共有三种：6.8cm x 10.2cm 与 8.9cm x 12.7cm 两种大小的照片纸上打印的彩色照片，普通 A4 打印纸上打印的彩色照片。数据集录制了正面平展照片，同时还对照片弯曲、沿水平轴旋转、垂直轴旋转等情况进行了录制。

Yale-Recaptured[33] 数据集为 LCD 屏幕显示的照片类假体人脸录制了一批多种光照条件下的数据。Yale Face Database B[14] 包含了 1 个个体 64 种不同光照下活体人脸数据。Yale-Recaptured 数据集利用三种 LCD 显示屏显示 Yale Face Database B 中 1 个个体 64 种光照条件下的 640 张照片人脸。整个数据集从假体人脸光照差异方面考验算法的有效性和通用性。

Print-Attack [117] 数据集是瑞士 Idiap 研究中心发布的关于打印照片类假体人脸的人脸活体检测数据集。Idiap 研究中心在人脸活体检测领域研究活跃，针对照片、视频、面具等不同类型的假体人脸发布了不同的数据集。Print-Attack 数据集在两种不同的光照条件下分别录制了手持照片、固定照片两种不同照片攻击模式的数据，其中照片是打印在 A4 打印纸上的彩色照片。

CASIA-MFSD[34] 数据集为活体人脸和照片、视频类假体人脸录制了低、中、高三种不同质量的视频数据。假体人脸包括完整的彩色照片假体人脸，挖去颜色的彩色照片假体人脸以及视频类假体人脸。照片类假体人脸在录制的过程中也录制了正面平展照片以及弯曲照片的情况。根据收集的数据，CASIA-MFSD 从图像成像质量、假体人脸类型方面设计了七种不同的测试协议用于验证人脸活体检测算法的性能。

Replay-Attack[16] 数据集的录制方式类似于 Print-Attack 数据集。相对于 Print-Attack 数据集，假体人脸新增了 iPhone 3GS 手机以及 iPad 显示的视频类假体人脸。

MSU-MFSD [47] 数据集考虑了人脸活体检测在移动端的应用场景，采用智能手机录制活体人脸和假体人脸的图像信息。采用佳能 550D 单反相机以及 iPhone 5S 后置摄像头拍摄高像素照片和视频作为假体人脸。视频类假体人脸采用了两种像素进行显示， iPad Air 显示的 2048 x 1536 像素的视频， iPhone 5S 显示的 1136 x 640 的视频。打印类照片假体人脸以 1200 x 600 的分辨率打印在 A3 的纸上。相比于之前的数据集中的假体人脸，MSU-MFSD 的假体人脸质量更高。

Unicamp Video-Attack data set (UVAD)[31] 数据集采用了 6 种不同的摄像头拍摄人脸视频用做假体人脸录制数据，之后利用 7 种不同的设备显示视频假体人脸用于攻击人脸识别系统。UVAD 从制作视频假体人脸的设备以及假体人脸的显示设备方面丰富了人脸活体检测数据集。

REPLAY-MOBILE[119] 数据集同样考虑到智能移动设备如智能手机和平板电脑的发展，利用 Nikon Coolpix P520 相机以及 LG-g4 智能手机后置摄像头拍摄高分辨率照片或者视频作为假体人脸。考虑到人脸活体检测在移动端的应用，数据集的录制也采用 IOS 和 Android 智能移动设备进行数据录制。假体人脸的显示也尽量屏蔽镜面反光的影响，采用了哑光电子显示屏和纸张显示视频或者照片。为了验证方法的通用性，REPLAY-MOBILE 数据集录制了 5 种不同的光照条件下的数据。

MSU-USSA[120] 数据集也是一个模拟假体人脸攻击智能手机中的人脸识别系统的数据集。MSU-USSA 的采集过程中考虑了背景环境、图像质量、图像采集设备、个体方面的多样性。MSU-USSA 从 Weakly Labeled Face 数据集选取了 100 个个体的图像用于数据集的录制，从个体、个体所在背景环境方面增加了人脸活体检测数据集的多样性。100 个活体人脸图像来自于互联网，所以其拍摄设备多种多样，从图像采集设备方面丰富了数据集。假体人脸类似于其他数据集，采用笔记本、平板电脑、智能手机、哑光照片纸显示。MSU-USSA 利用 Google Nexus 5 的前置摄像头与后置摄像头为假体人脸拍摄两种不同分辨率的图像，从图形质量、假体类别、假体质量方面丰富了数据集。

Oulu-NPU[121] 数据集在三个不同光照不同背景的场景下利用六种移动设备的前置摄像头录制了活体人脸和假体人脸的图像信息。打印照片类假体人脸由两个不同的打印机彩色打印而成。视频类假体人脸由两种不同的显示设备显示。Oulu-NPU 数据集录制过程中考虑了更多的变化因素用于验证人脸活体检测方法的有效性和通用性。

SiW[101] 收集了 165 个个体的活体人脸与假体人脸图像信息。活体人脸在录制的时候考虑了人脸与摄像头的距离、姿态、表情、光照方面的变化。打印照片类假体人脸考虑了高分辨率和低分辨率两种照片。视频类假体人脸采用了平板电脑、苹果手机、PC 机显示器、三星手机四种不同的设备显示。SiW 数据集在个体数以及活体人脸的变化方面增加了数据集的丰富性。

3.1.2 基于其他硬件的照片视频类人脸活体检测数据集

GUC-LiFFAD[21] 数据集是一个利用光场相机录制了不同焦距的光场图像的数据集，为利用光场图像差异的人脸活体检测算法提供数据支持。数据集利用喷墨打印机、激光打印机、第四代 iPad 平板电脑制作了高质量的打印照片与显示的电子照片。数据集收集了 80 个不同个体的活体人脸和假体人脸数据，个体差异方面相对来说更丰富。

Msspoof[122] 数据集录制了活体人脸和照片类假体人脸的可见光与近红外光谱图像数据。数据集使用的近红外波段是 800nm。对于活体人脸，Msspoof 数据集在七个不同的环境下录制了 5 张可见光与 5 张近红外光谱图像。对于假体人脸，Msspoof 数据集从之前录制的活体人脸的 5 张可见光与 5 张近红外光谱图像选取了看起来成像比较好的 3 张可见光与 3 张近红外光谱图像用于制造假体人脸。选取出来的 6 张图像均被打印成黑白照片。Msspoof 数据集分别为这 6 张照片录制了三种不同光照条件下的可见光与近红外光谱图像。

Extended Multispectral Presentation Attack Face Database (EMSPAD)[123] 数据集利用多光谱摄像头录制了 425nm, 475nm, 525nm, 570nm,625nm,680nm,930nm 7 个波段的图像。数据集录制的过程中考虑了距离的影响，选取了 1.52 米的录制对象与摄像头间距，以便能够收集高质量的多光谱图像。

3.2 面具类人脸活体检测数据集

3DMAD[37] 是最早的录制了三维人脸面具类假体人脸数据的人脸活体检测数据集。数据集使用的面具是由 ThatsMyFace.com 根据用户的一张正面人脸图像以及两张侧面人脸图像定制的三维塑料面具。考虑到假体人脸与活体人脸三维结构方面的差异，3DMAD 数据集不仅利用可见光摄像头录制了活体人脸与假体人脸的可见光图像，还利用了微软 Kinect 深度摄像头录制活体人脸与假体人脸的深度图像信息。

HKBU Mask Attack with Real World Variations Dataset Version 2 (HKBU-MARsV2)[124] 数据集也是一个三维人脸面具类假体人脸数据集。相比较于 3DMAD，HKBU-MARsV2 在假体人脸质量、录制数据的摄像头、外界光照条件等方面增加了数据多样性。假体人脸方面，数据集选取了两个公司的假体人脸：ThatsMyFace 制作的脸部表观质量稍低的三维面具以及 Real-F 制作的脸部表观质量高的三维人脸面具。录制数据的摄像头方面，数据集考虑了传统人脸识别系统以及智能移动设备上人脸活体检测的应用，选取了三种传统摄像头以及四种移动设备的摄像头录制活体人脸和假体人脸的数据。光照方面，数据集设计了六种不同的室内光照环境用于数据录制。

Silicone Mask Attack (SMAD)[102] 数据集是一个为活体人脸以及三维硅胶人脸面具录制了图像信息的数据集。硅胶人脸面具能更好的与人脸的眼睛、鼻子、嘴巴部位贴合，戴起来看起来更加真实。

硅胶人脸面具更接近现实应用中不法分子可能会使用的面具，从这个角度上看，SMAD 数据集更贴近现实情况。数据集在录制的过程中也考虑了不同的外界光照、背景等外界影响条件。

Multispectral Latex Mask based Video Face Presentation Attack(MLFP)[125] 数据集在可见光、近红外、热红外光谱下录制了多光谱的活体人脸和面具假体人脸数据。面具假体人脸使用了挖去眼部区域的二维照片以及三维的乳胶人脸面具。录制过程中选取了不同时段、室内室外不同地方的多个场景录制数据，在外界环境方面丰富了数据集。

从表 2 我们可以看出，早期人们关注照片视频类假体人脸的处理，逐渐发展为也关注面具类假体人脸的处理。早期人们关注 PC 端人脸活体检测，逐渐发展为关注 PC 端以及移动端的人脸活体检测，利用网络摄像头以及移动端多元化摄像头捕获人脸图像。人脸识别、物体分类等其他领域的大规模数据集多是从网络上收集不同人、不同摄像头、不同环境下拍摄的图像，而目前人脸活体检测的数据集都是约束状态下人工录制的，其数据集个体数、数据多样性远远不及人脸识别、物体分类等其他领域的数据集。

4 算法性能比较

4.1 性能评价指标

人脸活体检测算法的性能主要从单数据集测试以及跨数据集测试两方面进行衡量。单数据集测试是指训练集和测试集同属于一个数据集时算法的性能。跨数据集测试是指训练集和测试集不是同一个数据集时算法的性能。人脸活体检测算法的性能评价同时考虑活体人脸与假体人脸的识别率。常用的性能评价指标主要有两种：一种是 False Acceptance Rate(FRR)，False Rejection Rate (FAR)，Equal Error Rate (EER) 以及 Half Total Error Rate (HTER) 指标[16]，一种是生物识别防假体攻击方面的标准文件 ISO/IEC 30107-3[126] 提出的 Attack Presentation Classification Error Rate (APCER)，Bona Fide Presentation Classification Error Rate (BPCER) 以及 Average Classification Error Rate (ACER) 指标。

错误接受率 (False Acceptance Rate, FAR) 指算法把假体人脸判断成活体人脸的比率。错误拒绝率 (False Rejection Rate, FRR) 指算法把活体人脸判断成假体人脸的比率。FAR 与 FRR 的定义如公式 1，2 所示，其中 N_{s2l} 表示假体人脸判断为活体人脸的次数，N_s 表示假体人脸攻击总次数，N_{l2s} 表示活体人脸判断为假体人脸的次数，N_l 表示活体人脸检测总次数。不同的阈值可以得到不同的 FRR 以及 FAR 对，分别以 FRR 与 FAR 为横轴与纵轴即可绘制 ROC 曲线。利用开发集数据进行测试得到的 ROC 曲线上 FRR 等于 FAR 时，FRR 与 FAR 的均值即为等错误率 Equal Error Rate (EER)。以开发集上 FRR 等于 FAR 时的阈值为测试集上的阈值计算测试集 FRR 与 FAR 的均值，即为半错误率 Half Total Error Rate (HTER)。

表 3 CASIA-MFSD 与 Replay-Attack 数据集单数据集测试性能数据

Table 3 The performance of intra-test on CASIA-MFSD and Replay-Attack datasets

方法	CASIA-MFSD	Replay-Attack	
	EER(%)	EER(%)	HTER(%)
LBP[16]	18.2	13.9	13.8
DoG[34]	17.0	-	-
Motion Magn[57]	14.4	0.0	1.25
IDA[45]	32.4	-	15.2
LBP-TOP[17]	10.0	7.9	7.6
CNN[84]	7.4	6.1	2.1
DMD + LBP[58]	21.8	5.3	3.8
IDA and motion[97]	5.8	0.83	0.0
Colour LBP[20]	2.1	0.4	2.8
VLBC[118]	6.5	1.7	0.8
3D CNN [110]	5.2	0.16	0.04
FD-ML-LPQ-FS[43]	4.6	5.6	4.8
patch+depthCNN[85]	2.7	0.8	0.7
SURF[41]	2.8	0.1	2.2
PreDRS+LSTM[90]	1.22	1.03	1.18
ST Mapping[87]	1.1	0.78	0.80
DDGL[102]	-	1.3	0.0
LiveNet[96]	4.59	-	5.74
Color texture[35]	4.6	1.2	4.2
DSGN[106]	3.42	0.13	0.63
deep LBP[91]	2.3	0.1	0.9
3D CNN+geneloss[109]	1.4	0.3	1.2
SSD+SPMT [104]	0.04	0.04	0.06

利用开发集数据进行测试得到的 ROC 曲线上 FRR 等于 FAR 时，FRR 与 FAR 的均值即为等错误率 Equal Error Rate (EER)。以开发集上 FRR 等于 FAR 时的阈值为测试集上的阈值计算测试集 FRR 与 FAR 的均值，即为半错误率 Half Total Error Rate (HTER)。

$$FAR = \frac{N_{s2l}}{N_s} \tag{1}$$

$$FRR = \frac{N_{l2s}}{N_l} \tag{2}$$

Attack Presentation Classification Error Rate (APCER) 指假体人脸分类错误率。Bona Fide Presentation Classification Error Rate (BPCER) 指活体人脸分类错误率。Average Classification Error Rate (ACER) 指平均分类错误率，其定义如公式 3,4,5 所示：

$$APCER_{PAI} = \frac{1}{N_{PAI}} \sum_{i=1}^{N_{PAI}} (1 - Res_i) \quad (3)$$

$$BPCER = \frac{\sum_{i=1}^{N_{BF}} Res_i}{N_{BF}} \quad (4)$$

$$ACER = \frac{\max_{PAI=1...S}(APCER_{PAI}) + BPCER}{2} \quad (5)$$

N_{PAI} 是某一类别假体总的攻击次数。N_{BF} 是指活体人脸检测次数。若第 i 次检测判断为假体人脸则 Res_i 置为 1，若判断为活体人脸则置为 0。APCER 与 BPCER 同第一种评价指标中的 FAR 与 FRR 类似，但是 FAR 和 FRR 把所有类别的假体人脸混合在一起计算性能，$APCER_{PAI}$ 是为每一种类别的假体人脸计算 APCER，比如说照片类假体人脸、视频类假体人脸，最后活体检测算法总的 APCER 是所有类别假体人脸中最大的 $APCER_{PAI}$，也就是说识别率最差的那类假体人脸。EER 是指开发集上 APCER 与 BPCER 相等时 APCER 与 BPCER 的均值。ACER 是以等错误率对应的阈值为测试集的阈值计算的 APCER 与 BPCER 的均值。

单数据集的测试能够在一定程度上反映算法的性能，但文献 [127] 通过实验证明了很多在单数据集上性能优良的算法，在其他数据集上测试时，性能会急剧下降，算法的通用性不强。为了验证算法的通用性，他们提出了跨数据集测试的方法：以一个数据集的数据为训练集训练活体检测算法模型，以另一个数据集的数据为测试集测试活体检测算法模型的性能。目前大部分的跨数据集测试还都是集中在同类别假体人脸跨数据集测试的形式，对于跨数据集、跨假体人脸类别的测试还比较少。这也从侧面反映出目前人脸活体检测算法的通用性还有待提高。

4.2 主流算法性能比较

照片视频类数据集 CASIA-MFSD、Replay-Attack、Oulu-NPU、SiW 以及面具类数据集 3DMAD、SMAD、HKBU-MARsV2 是目前比较常用的基准数据集。表 3、表 4、表 5、表 6、表 7、表 8 以文献发表的年份为顺序总结了代表性的人脸活体检测方法在 CASIA-MFSD、Replay-Attack、Oulu-NPU、SiW、3DMAD、SMAD、HKBU-MARsV2 上报道的单数据集以及跨数据集测试性能数据。为了比较的公平性，表 3、表 4、表 5、表 7 中总结的方法

表 4 OULU 数据集单数据集测试性能数据

Table 4 The performance of intra-test on OULU dataset

协议	方法	APCER(%)	BPCER(%)	ACER(%)
1	GRADIANTex[129]	7.1	5.8	6.5
1	CPq[129]	2.9	10.08	6.9
1	GRADIANT[129]	1.3	12.5	6.9
1	Auxiliary[101]	1.6	1.6	1.6
1	Noise Modeling[128]	1.2	1.7	1.5
1	TDI[130]	2.5	0.0	1.3
2	GRADIANT[129]	3.1	1.9	2.5
2	GRADIANTex[129]	6.9	2.5	4.7
2	MixedFASNet[129]	9.7	2.5	6.1
2	Auxiliary[101]	2.7	2.7	2.7
2	Noise Modeling[128]	4.2	4.4	4.3
2	TDI[130]	1.7	2.0	1.9
3	GRADIANT[129]	2.6±3.9	5.0±5.3	3.8±2.4
3	GRADIANTex[129]	2.4±2.8	5.6±4.3	4.0±1.9
3	MixedFASNet[129]	5.3±6.7	7.8±5.5	6.5±4.6
3	Auxiliary[101]	2.7±1.3	3.1±1.7	2.9±1.5
3	Noise Modeling[128]	4.0±1.8	3.8±1.2	3.6±1.6
3	TDI[130]	5.9±1.0	5.9±1.0	5.9±1.0
4	GRADIANT[129]	5.0±4.5	15.0±7.1	10.0±5.0
4	GRADIANTex[129]	27.5±24.2	3.3±4.1	15.4±11.8
4	Massy HNU[129]	35.8±35.3	8.3±4.1	22.1±17.6
4	Auxiliary[101]	9.3±5.6	10.4±6.0	9.5±6.0
4	Noise Modeling[128]	5.1±6.3	6.1±5.1	5.6±5.7
4	TDI[130]	14.0±3.4	4.1±3.4	9.2±3.4

表 5 SiW 数据集单数据集测试性能数据

Table 5 The performance of intra-test on SiW dataset

评价协议	方法	APCER(%)	BPCER(%)	ACER(%)
1	Auxiliary[101]	3.58	3.58	3.58
1	TDI[130]	0.96	0.50	0.73
2	Auxiliary[101]	0.57±0.69	0.57±0.69	0.57±0.69
2	TDI[130]	0.08±0.14	0.21±0.14	0.15±0.14
3	Auxiliary[101]	8.31±3.81	8.31±3.80	8.31±3.81
3	TDI[130]	3.10±0.81	3.09±0.81	3.10±0.81

表 6 3DMAD、SMAD 与 HKBU-MARsV2 数据集单数据集测试性能数据

Table 6 The performance of intra-test on 3DMAD,SMAD and HKBU-MARsV2 datasets

方法	3DMAD	SMAD	HKBU-MARsV2	
	HTER(%)	HTER(%)	EER(%)	HTER(%)
LBPs[38]	0.1	20.8	22.5	24.0±25.6
deep and color[37]	0.95	-	-	-
IDA motion[97]	0	-	-	-
Color texcure[20]	-	-	23.0	23.4±20.5
videolet agg[114]	0	20.4	-	-
GrPPG[60]	7.94	-	16.4	16.1±20.5
LBP-TOP[102]	-	21.5	-	-
DBN[102]	0.5	19.2	-	-
DDGL[102]	0	13.1	-	-
CFrPPG[63]	6.82±12.1	-	4.04	4.42±5.1

表 7 跨数据集测试性能数据 HTER(%)

Table 7 The performance of inter-test between CASIA-MFSD and Replay-Attack

训练	CASIA-MFSD	Replay-Attack
测试	Replay-Attack	CASIA-MFSD
LBP [127]	55.9	57.6
Motion [127]	50.2	47.9
Motion Magn[57]	50.1	47.0
LBP-TOP[127]	49.7	60.6
CNN [84]	48.5	45.5
Color LBP [20]	30.3	37.7
texture+Motion[112]	12.4	31.6
FD-ML-LPQ-FS[43]	50.25	42.59
ST Mapping[87]	35.05	40.22
SURF [41]	26.9	23.2
DDGL[102]	22.8	27.4
Noise Modeling[128]	28.5	41.1
DeepImg+rPPG[101]	27.6	28.4
Domain Adapt[103]	27.4	36.0
Color texture[35]	9.6	39.2
LiveNet[96]	8.39	19.12

表 8 3DMAD 与 HKBU-MARsV2 数据集间跨数据集测试性能数据 HTER(%)

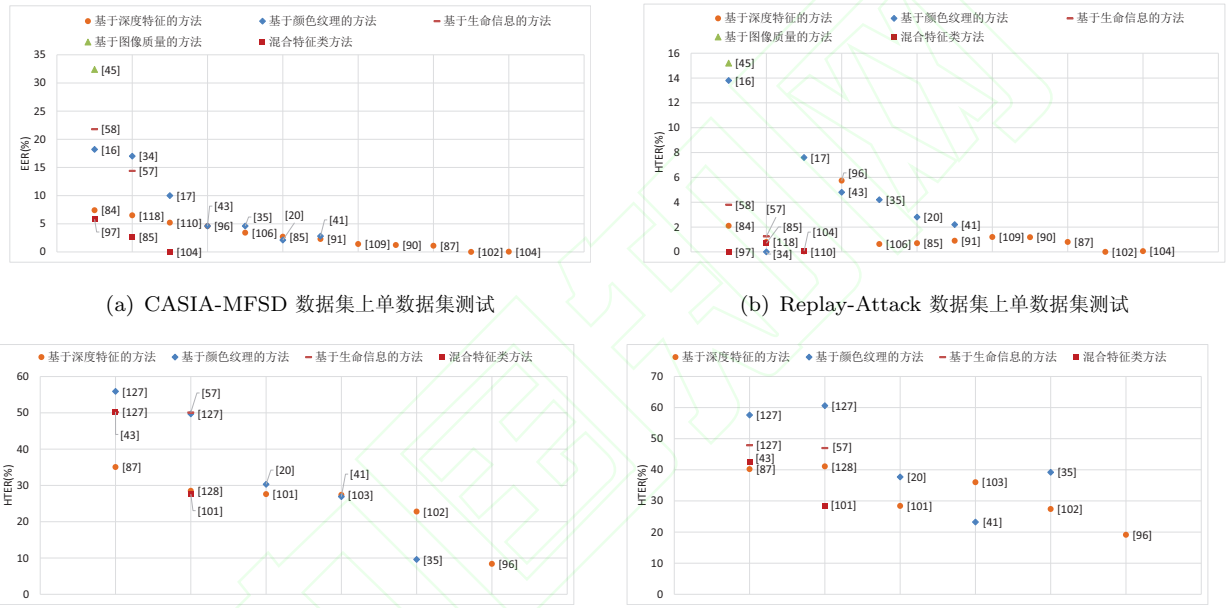
Table 8 The performance of inter-test between 3DMAD and HKBU-MARsV2

训练	3DMAD	HKBU-MARsV2
测试	HKBU-MARsV2	3DMAD
Color texcure[20]	40.1±7.8	47.7±5.4
LBPs[38]	53.0±3.6	32.8±11.5
pretrain CNN[63]	50.0±0.0	50.0±0.0
GrPPG[60]	24.3±7.1	15.7±6.8
CFrPPG[63]	2.51±0.1	2.55±0.1

在每个数据集上使用的是相同的官方给出的评价协议。3DMAD、SMAD、HKBU-MARsV2 面具类数据集中的个体数比较少，方法性能的评价通常采用交叉验证。表 6 中 3DMAD 数据集上的不同方法在进行交叉验证时训练集与测试集的数据比例稍有差异。表 6 中 SMAD 与 HKBU-MARsV2 数据集上的方法分别采用文献 [102]，文献 [63] 中的测试协议。表 8 中 3DMAD 与 HKBU-MARsV2 数据集间跨数据集测试采用文献 [63] 中的测试协议。从表 3

我们可以看出许多方法在 Replay-Attack 数据集上性能较好，但是在 CASIA-MFSD 数据集上却不能得到类似 Replay-Attack 数据集上的性能。CASIA-MFSD、Replay-Attack 的假体人脸类别都是照片类假体人脸和视频类假体人脸。这种性能差异也表明假体人脸类内差异大，对算法的性能有较大影响。随着深度学习方法的应用，同一种人脸活体检测方法抽取的特征更加通用，两个数据集间的性能差异逐渐减少。从表 4 中 Oulu-NPU 数据集上的性能测试数据中我们可以看出协议 4 的指标值明显高于其他三个协议，这表明不同的数据集录制设备造成的类内差异对于方法的性能影响较大。表 7，表 8 列出的皆是同类别假体人脸数据集间的跨数据集测试性能数据，较高的半错误率也告诉我们类内差异对人脸活体检测方法性能有较大影响。人脸活体检测方法的通用性仍有很大的提升空间。

图 5 针对表 3 与表 7 中人脸活体检测方法的 EER 或者 HTER 性能数据分类别进行了展示。从图 5 中我们可以大致看出目前常见的各类方法的性能发展水平。相对于其他类别的方法，基于纹理的方法、基于深度特征的方法、混合特征类方法的研究相对较多。无论是单数据集测试还是跨数据集测试，基于深度特征的方法以及混合特征类方法的性能是最好的。我们相信这两类方法的研究也将是未来的发展趋势。



(a) CASIA-MFSD 数据集上单数据集测试

(b) Replay-Attack 数据集上单数据集测试

(c) 跨数据集测试：训练集 (CASIA-MFSD)，测试集 (Replay-Attack)

(d) 跨数据集测试：训练集 (Replay-Attack)，测试集 (CASIA-MFSD)

图 5　各类人脸活体检测方法性能分布图

Fig. 5　Performance comparison of different category of face anti-spoofing methods

5　未来可能的发展方向

人脸活体检测方法的研究已经取得了一系列的进展，研究重心从交互式人脸活体检测方法逐渐转移到非交互式人脸活体检测方法，从手工设计特征的方法逐渐转移到基于深度学习的方法，从基于可见光图像的方法也逐渐发展为基于多元化图像的方法。从目前人脸活体检测方法的不足以及人脸活体检测业务的发展需要来看，人脸活体检测研究未来可能的发展方向主要有：

5.1　面具类假体人脸的识别

照片、视频类假体人脸制作起来方便简单，也是最常见的假体人脸，目前大部分的活体检测方法主要防范照片、视频类假体人脸的攻击。而目前针对面具类假体人脸的活体检测方法研究还不是很多。三维人脸面具的制造工艺复杂、成本高，但是三维人脸面具相对于二维的照片、视频类假体人脸，无论从颜色纹理还是人脸结构上都与活体人脸更为相似。常规的基于颜色纹理、图像质量、微运动、人脸结构等方面分类线索的方法处理面具类假体人脸的

时候，性能都会大打折扣。对于智能安防、通关安检类的公共场合，不法分子一般不会选择使用照片、视频攻击人脸识别系统，而是更倾向于使用面具进行伪装来攻击人脸识别系统。因此，研究如何有效的分辨活体人脸和面具类假体人脸对于人脸活体检测多场景的实际应用具有重要意义。

5.2 通用性问题研究

目前活体检测方法抽取的特征泛化能力不强，算法也不能很好的处理与训练数据不是同一个数据集的测试数据，不管是训练集中见过的假体人脸类别还是训练集中没有见过的假体人脸类别。究其原因是假体人脸的类内类间差异大。不同的假体人脸制造工艺，不同的数据集录制设备，不同的外界环境都会影响算法的性能。这些差异信息是人脸活体检测应用环境中确切存在的，也是人脸活体检测算法实际应用中无法回避的问题。如何提取泛化能力强的特征，灵活应对这些现实差异，提高活体检测算法单类别假体人脸的跨数据集通用性以及跨假体人脸类别、跨数据集的通用性都是值得研究的问题。

5.3 未见过假体人脸的自适应处理

目前主流的人脸活体检测算法都是观察活体人脸和假体人脸的分类线索，抽取分类特征，之后利用分类模型进行活体人脸与假体人脸的分类。大部分方法只对训练数据中见过的假体人脸有效。对于训练数据中没有见过的假体人脸，其性能则会下降。然而对于人类来说，即使之前只见过照片类假体人脸，第一次见到面具类假体人脸的时候也可以判断出面具类假体人脸不是活体人脸。人类大脑可能掌握了活体人脸的一些本质属性，对于未见过的假体人脸类别能够自适应识别。人类的智慧是无穷的，人脸活体检测的研究者们难以完全预测他人即将制造出什么样式的新的假体人脸。对于新出现的假体人脸，类似于打补丁似的完善活体检测方法则永远会慢人一步，给不法分子留下攻破人脸识别系统的机会。研究类似于人类大脑，对于未见过的新型假体人脸快速自适应识别的人脸活体检测算法具有重要的价值。

5.4 更大更全面数据集的建立

从十元左右制造成本的照片纸打印的彩色照片到成本上万的定制人脸面具，各类假体人脸的高成本使得人脸活体检测的数据集基本都存在个体少、样本少、数据的多样性不够丰富的问题。目前大部分常见的活体检测数据集要么是专门针对照片、视频类二维假体人脸的，要么是专门针对面具类三维假体人脸。数据集中包含的假体类别比较单一。计算机视觉领域的人脸识别、物体识别等子领域的数据集都远比人脸活体检测的数据集数据量大、数据多样性更丰富。随着深度学习方法的发展，数据在算法研究中的地位越来越重要。数据量大、数据多样性更丰富有利于基于深度学习的方法能够抽取有效而通用的分类特征。如何集结资源，以最少的成本建立一个数据量更大，个体数更多，假体人脸类型更全面，影响算法性能的姿态、表情、光照、录制设备等因素更多的数据集是值得思考和挑战的问题。

目前大部分的人脸活体检测数据集都是约束状态下比如正面人脸、自然表情录制的，而非约束条件下人脸活体检测研究需要的非约束状态下的活体人脸和假体人脸数据集也急需建立。

5.5 适应人脸活体检测的深度学习方法研究

深度学习的方法的使用让人脸活体检测算法的性能有了一定的提升，但是人脸活体检测数据集的问题导致深度学习方法在人脸活体检测领域使用的过程中经常会出现过拟合，抽取的特征通用性不够强的问题。目前人们提出了微调在其他大数据集上预训练的模型，设计特定的训练方法，深度特征与手工特征融合等方法来减少过拟合问题的影响，提高基于深度学习方法的准确率和通用性。根据现有的数据现状，研究适合人脸活体检测的深度学习方法是一个重要的研究方向。

5.6 非约束状态下的人脸活体检测研究

目前人脸活体检测研究集中在约束状态下的人脸活体检测。交互式人脸活体检测方法要求用户在指定距离内按照提示完成指定交互动作。目前主流的非交互式人脸活体检测方法虽然不需要用户交互，但是检测的整个过程基本要求人脸是正面脸，脸部不出现表情变化、姿态变化，人脸在规定距离内以便能够采集到足够好的待分析图像。约束状态下的人脸活体检测只能在特定的业务场景中使用，比如手机解锁、用户登录之类的用户能够处于约束状态的场景，应用范围窄，不能满足视频监控人脸活体检测之类用户处于自然状态的应用场景的需求。研究用户处于自然状态，可能存在姿态变化、部分遮挡、光照变化等影响的情况下的有效人脸活体检测方法具有非常重要的意义。有效而鲁棒的非约束状态下的人脸活体检测方法更有利于人脸活体检测方法大规模的实际应用，提高人脸识别技术的安全性。

6 结论

人脸活体检测在生物识别研究中具有重要的学术价值与实际应用价值。目前人脸活体检测的研究活跃，但同时也存在不少困难与挑战。本文从假体人脸的特性出发，分析了目前人脸活体检测

的难点，以人脸活体检测算法利用的分类特征为主线，详细阐述了人脸活体检测领域的主流算法，探讨了各类方法主要利用的特征、防范的假体人脸类型、优缺点，就领域内常用的各个数据集的特点、数据量、数据多样性等方面进行了对比分析，阐述了常用的算法性能评价指标并总结分析了代表性人脸活体检测方法在照片视频类数据集 CASIA-MFSD、Replay-Attack、Oulu-NPU、SiW 以及面具类数据集 3DMAD、SMAD、HKBU-MARsV2 上的性能数据。以此为基础，本文对人脸活体检测未来可能的研究方向进行了分析与展望。我们相信人脸活体检测所面临的问题必将能在理论上与实践上得到更好的解决，人脸活体检测的应用也将推动人脸识别技术、生物识别技术更广泛、更深入的应用。

References

1 Ministry of Public Security of the People's Republic of China. Ga/T1212-2014 Face recognition application in security systems–testing methodologies for anti-spoofing. 2014
(中华人民共和国公安部. Ga/T1212-2014 安防人脸识别应用防假体攻击测试方法. 2014)

2 Li Y, Xu K, Yan Q, Li Y J, Deng R H. Understanding osn-based facial disclosure against face authentication systems. In: Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security. Kyoto, Japan: ACM, 2014. 413−424

3 Chakraborty S, Das D. An overview of face liveness detection. *arXiv preprint arXiv:1405.2227*, 2014

4 Souza L, Pamplona M, Oliveira L, Papa J. How far did we get in face spoofing detection?. *Engineering Applications of Artificial Intelligence*, 2017, **72**: 368−381

5 Ramachandra R, Busch C. Presentation attack detection methods for face recognition systems: a comprehensive survey.*Computing Surveys*, 2017, **50**(1): 8

6 Zheng H R, Chu Y P, Pan X, Zhao X M. A intrusive vedio face anti-spoofing method and system based on face pose control. China: 201510764681, 2015-11-11
(郑河荣, 褚一平, 潘翔, 赵小敏. 基于人脸姿态控制的交互式视频活体检测方法及其系统. 中国: 201510764681, 2015-11-11)

7 Xue P R, Bu X S, Wang J F. A face anti-spoofing method and system based on pose recognition. China: 201611129097, 2016-12-09
(薛炳如, 卜习栓, 王金凤. 一种基于动作识别的活体人脸识别方法及系统. 中国: 201611129097, 2016-12-09)

8 Wang X J, Chen Y B. A face anti-spoofing method and system. China: 201310384572, 2013-08-29
(王先基, 陈友斌. 一种活体人脸检测方法与系统. 中国: 201310384572, 2013-08-29)

9 Xu G Z, Liu M, Yin P L, Lei B J, Li C L. A face anti-spoofing method and apparatus based on activity state of eyes. China: 201510472931, 2015-08-05
(徐光柱, 刘鸣, 尹潘龙, 雷帮军, 李春林. 基于人眼区域活动状态的活体检测方法和装置. 中国: 201510472931, 2015-08-05)

10 Wang R J, Li J L, Ni H, Wu Y J, Huang F Y. A face recognition method and system. China: 201510319470, 2015-06-11
(汪铖杰, 李季檩, 倪辉, 吴永坚, 黄飞跃. 人脸识别方法及识别系统. 中国: 201510319470, 2015-06-11)

11 Kollreider K, Fronthaler H, Faraj M I, Big ü n J. Real-time face detection and motion analysis with application in "liveness" assessment. *IEEE Transactions on Information Forensics and Security*, 2007, **2**(3): 548−558

12 Ng E S, Chia Y S. Face verification using temporal affective cues. In: Proceedings of the 21st International Conference on Pattern Recognition. Tsukuba Science City, Japan: IEEE, 2012. 1249−1252

13 Chetty G, Wagner M. Liveness verification in audio-video authentication. In: Proceedings of the 10th Australian International Conference on Speech Science and Technology. Sydney, Australia: Australian Speech Science and Technology Association Inc, 2004. 358−363

14 Frischholz R W, Werner A. Avoiding replay-attacks in a face recognition system using head-pose estimation. In: Proceedings of IEEE International Workshop on Analysis and Modeling of Faces and Gestures. Nice, France: IEEE, 2003. 234−235

15 Määttä J, Hadid A, Pietikäinen M. Face spoofing detection from single images using micro-texture analysis. In: Proceedings of International Joint Conference on Biometrics. Colorado State, USA: IEEE, 2011. 1−7

16 Chingovska I, Anjos A, Marcel S. On the effectiveness of local binary patterns in face anti-spoofing. In: Proceedings of the 11th International Conference of the Biometrics Special Interes Group. Darmstadt, Germany: IEEE, 2012. 1−7

17 de Freitas Pereira T, Komulainen J, Anjos A, De Martino J M, Hadid A, Pietikäinen M, et al. Face liveness detection using dynamic texture. *EURASIP Journal on Image and Video Processing*, 2014, **2**(1): 4

18 de Freitas Pereira T, Anjos A, De Martino J, Marcel S. Lbp- top based countermeasure against face spoofing attacks. In: Proceedings of Asian Conference on Computer Vision. Daejeon, Korea: Springer, 2012. 121−132

19 Komulainen J, Hadid A, Pietikäinen M. Face spoofing detection using dynamic texture. In: Proceedings of Asian Conference on Computer Vision. Daejeon, Korea: Springer, 2012. 146−157

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

21 Raghavendra R, Raja K B, Busch C. Presentation attack detection for face recognition using light field camera. *IEEE Transactions on Image Processing*, 2015, **24**(3): 1060−1075

22 Kose N, Dugelay J L. Classification of captured and recaptured images to detect photograph spoofing. In: Proceedings of International Conference on Informatics, Electronics and Vision. Dhaka, Bangladesh: IEEE, 2012. 1027−1032

23 Yang J W, Lei Z, Liao S C, Li S Z. Face liveness detection with component dependent descriptor. In: Proceedings of International Conference on Biometrics. Madrid, Spain: IEEE, 2013. 1−6

24 Raghavendra R, Busch C. Robust 2d/3d face mask presentation attack detection scheme by exploring multiple features and comparison score level fusion. In: Proceedings of 17th International Conference on Information Fusion. Salamanca, Spain: IEEE, 2014. 1−7

25 Arashloo S R, Kittler J, Christmas W. Face spoofing detection based on multiple descriptor fusion using multiscale dynamic binarized statistical image features. *IEEE Transactions on Information Forensics and Security*, 2015, **10**(11): 2396−2407

26 Maatta J, Hadid A, Pietikainen M. Face spoofing detection from single images using texture and local shape analysis. *IET biometrics*, 2012, **1**(1): 3−10

27 Komulainen J, Hadid A, Pietikainen M. Context based face anti-spoofing. In: Proceedings of IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems. Washington, DC, USA: IEEE, 2013. 1−8

28 Schwartz W R, Rocha A, Pedrini H. Face spoofing detection through partial least squares and low-level descriptors. In: Proceedings of International Joint Conference on Biometrics. Washington, DC, USA: IEEE, 2011. 1−8

29 Yang J W, Lei Z, Yi D, Li S Z. Person-specific face antispoofing with subject domain adaptation. *IEEE Transactions on Information Forensics and Security*, 2015, **10**(4):797−809

30 da Silva Pinto A, Pedrini H, Schwartz W, Rocha A. Video-based face spoofing detection through visual rhythm analysis. In: Proceedings of 25th SIBGRAPI Conference on Graphics, Patterns and Images. Minas Gerais, Brazil: IEEE, 2012. 221−228

31 Pinto A, Schwartz W R, Pedrini H, de Rezende Rocha A. Using visual rhythms for detecting video-based facial spoof attacks. *IEEE Transactions on Information Forensics and Security*, 2015, **10**(5): 1025−1038

32 Waris M A, Zhang H L, Ahmad I, Kiranyaz S, Gabbouj M. Analysis of textural features for face biometric antispoofing. In: proceedings of the 21st European Signal processing Conference. Marrakech, Morocco: IEEE, 2013. 1−5

33 Peixoto B, Michelassi C, Rocha A. Face liveness detection under bad illumination conditions. In: proceedings of 18th IEEE International Conference on Image Processing. Melbourne, Australia: IEEE, 2011. 3557−3560

34 Zhang Z W, Yan J J, Liu S F, Lei Z, Yi D, Li S Z. A face antispoofing database with diverse attacks. In: proceedings of International Conference on Biometrics. New Delhi, India: IEEE, 2012, 26−31

35 Boulkenafet Z, Komulainen J, Hadid A. On the generalization of color texture-based face anti-spoofing. *Image and Vision Computing*, 2018, **77**: 1−9

36 Kose N, Dugelay J L. Countermeasure for the protection of face recognition systems against mask attacks. In: proceedings of 10th IEEE International Conference and Workshops on Automatic Face and Gesture Recognition. Shanghai, China: IEEE, 2013. 1−6

37 Erdogmus N, Marcel S. Spoofing in 2d face recognition with 3d masks and anti-spoofing with kinect. In: proceedings of IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems. Washington, DC, USA: IEEE, 2014. 1−6

38 Erdogmus N, Marcel S. Spoofing face recognition with 3d masks. *Transactions on Information Forensics and Security*, 2014, **9**(7): 1084−1097

39 Ojala T, Pietikainen M, Maenpaa T. Multiresolution gray-scale and rotation invariant texture classification with local binary patterns. *Transactions on Pattern Analysis and Machine Intelligence*, 2002, **24**(7): 971−987

40 Haralick R M, Shanmugam K, Dinstein. Textural features for image classification. *Transactions on Systems, Man, and Cybernetics*, 1973, (6): 610−621

41 Boulkenafet Z, Komulainen J, Hadid A. Face antispoofing using speeded-up robust features and fisher vector encoding. *IEEE Signal Processing Letters*, 2017, **24**(2): 141−145

42 Chan P P, Liu W W, Chen D, Yeung D S, Zhang F, Wang X Z, et al. Face liveness detection using a flash against 2d spoofing attack. *Transactions on Information Forensics and Security*, 2018, **13**(2): 521–534

43 Benlamoudi A, Aiadi K E, Ouafi A, Samai D, Oussalah M. Face antispoofing based on frame difference and multilevel representation. *Journal of Electronic Imaging*, 2017, **26**(4): 043007

44 Mohan K, Chandrasekhar P, Jilani S. Object face liveness detection with combined hoglocal phase quantization using fuzzy based svm classifier. *Indian Journal of Science and Technology*, 2017, **10**(3)

45 Galbally J, Marcel S, Fierrez J. Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition. *Transactions on Image Processing*, 2014, **23**(2): 710−724

46 Galbally J, Marcel S. Face anti-spoofing based on general image quality assessment. In: Proceedings of 22nd International Conference on Pattern Recognition. Stockholm, Sweden: IEEE, 2014. 1173−1178

47 Wen D, Han H, Jain A K. Face spoof detection with image distortion analysis. *Transactions on Information Forensics and Security*, 2015, **10**(4): 746−761

48 Li H L ,Wang S Q, Kot A C. Face spoofing detection with image quality regression. In: Proceedings of 6th International Conference on Image Processing Theory Tools and Applications. Oulu, Finland: IEEE, 2016. 1−6

49 Akhtar Z, Foresti G L. Face spoof attack recognition using discriminative image patches. *Journal of Electrical and Computer Engineering*, 2016, **2016**: 14−28

50 Pan G, Sun L, Wu Z H, Lao S H. Eyeblink-based anti-spoofing in face recognition from a generic webcamera. In: Proceedings of IEEE 11th International Conference on Computer Vision. Rio de Janeiro, Brazil: IEEE, 2007. 1−8

51 Sun L, Pan G, Wu Z H, Lao S H. Blinking-based live face detection using conditional random fields. In: Proceedings of International Conference on Biometrics. Seoul, Korea: Springer, 2007. 252−260

52 Li J W. Eye blink detection based on multiple gabor response waves. In: Proceedings of International Conference on Machine Learning and Cybernetics. California, USA: IEEE, 2008. 2852−2856

53 Kollreider K, Fronthaler H, Faraj M I, Bigun J. Real-time face detection and motion analysis with application in "liveness" assessment. *Transactions on Information Forensics and Security*, 2007, **2**(3): 548−558

54 Bao W, Li H, Li N, Jiang W. A liveness detection method for face recognition based on optical flow field. In: Proceedings of International Conference on Image Analysis and Signal Processing. Cairo, Egyptpages: IEEE, 2009. 233−236

55 Kollreider K, Fronthaler H, Bigun J. Verifying liveness by multiple experts in face biometrics. In: Proceedings of IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops. Alaska, USA: IEEE, 2008. 1−6

56 Kollreider K, Fronthaler H, Bigun J. Non-intrusive liveness detection by face images. *Image and Vision Computing*, 2009, **27**(3): 233−244

57 Bharadwaj S, Dhamecha T I, Vatsa M, Singh R. Computationally efficient face spoofing detection with motion magnification. In: Proceedings of Conference on Computer Vision and Pattern Recognition Workshops. Oregon, USA: IEEE, 2013. 105−110

58 Tirunagari S, Poh N, Windridge D, Iorliam A, Suki N, Ho A T. Detection of face spoofing using visual dynamics. *Transactions on Information Forensics and Security*, 2015, **10**(4): 762−777

59 Poh M Z, McDuff D J, Picard R W. Advancements in noncontact, multiparameter physiological measurements using a webcam. *Transactions on Biomedical Engineering*, 2011, **58**(1): 7−11

60 Li X B, Komulainen J, Zhao G Y, Yuen P C, Pietikäinen M. Generalized face anti-spoofing by detecting pulse from face videos. In: Proceedings of 23rd International Conference on Pattern Recognition. Cancun, Mexico: IEEE, 2016. 4244−4249

61 Nowara E M, Sabharwal A, Veeraraghavan A. Ppgsecure: Biometric presentation attack detection using photopletysmograms. In: Proceedings of 12th IEEE International Conference on Automatic Face and Gesture Recognition. Washington, DC, USA: IEEE, 2017. 56−62

62 Hernandez-Ortega J, Fierrez J, Morales A, Tome P. Time analysis of pulse-based face anti-spoofing in visible and nir. In: Proceedings of Conference on Computer Vision and Pattern Recognition Workshops. Salt Lake City, Utah, USA: IEEE, 2018. 544−552

63 Liu S Q, Lan X Y, Yuen P C. Remote photoplethysmography correspondence feature for 3d mask face presentation attack detection. In: Proceedings of the European Conference on Computer Vision. Munich, Germany: IEEE, 2018. 558−573

64 Wang S Y, Yang S H, Chen Y P, Huang J W. Face liveness detection based on skin blood flow analysis. *Symmetry*, 2017, **9**(12): 305

65 Zhao G Y, Pietikainen M. Dynamic texture recognition using local binary patterns with an application to facial expressions. *Transactions on Pattern Analysis and Machine Intelligence*, 2007, **29**(6): 915−928

66 Yi D, Lei Z, Zhang Z W, Li S Z. Face anti-spoofing: multi-spectral approach. *Handbook of Biometric Anti-Spoofing*. Berlin: Springer, 2014

67 Kim Y S, Na J, Yoon S, Yi J. Masked fake face detection using radiance measurements. *Journal of the Optical Society of America A*, 2009, **26**(4): 760−766

68 Zhang Z W, Yi D, Lei Z, Li S Z. Face liveness detection by learning multispectral reflectance distributions. In: Proceedings of International Conference on Automatic Face and Gesture Recognition and Workshops. Santa Barbara, CA, USA: IEEE, 2011. 436−441

69 Sun X D, Huang L, Liu C P. Context based face spoofing detection using active near-infrared images. In: Proceedings of 23rd International Conference on Pattern Recognition. Cancun, Mexico: IEEE, 2016. 4262−4267

70 Sun X D, Huang L, Liu C P. Multispectral face spoofing detection using vis–nir imaging correlation. *International Journal of Wavelets, Multiresolution and Information Processing*, 2018, **16**(02):1840003

71 Kose N, Dugelay J L. Reflectance analysis based countermeasure technique to detect face mask attacks. In: Proceedings of 18th International Conference on Digital Signal Processing. Santorini, Greece: IEEE, 2013. 1−6

72 Dowdall J, Pavlidis I, Bebis G. Face detection in the near-ir spectrum. *Image and Vision Computing*, 2003, **21**(7): 565−578

73 Steiner H, Kolb A, Jung N. Reliable face anti-spoofing using multispectral swir imaging. In: Proceedings of International Conference on Biometrics. Halmstad, Sweden: IEEE, 2016. 1−8

74 Kant C, Sharma N. Fake face recognition using fusion of thermal imaging and skin elasticity. *International Journal of Computer Science and Communications* , 2013, **4**: 65−72

75 Raghavendra R, Raja K B, Marcel S, Busch C. Face presentation attack detection across spectrum using time-frequency descriptors of maximal response in laplacian scale-space. In: Proceedings of 6th International Conference on Image Processing Theory Tools and Applications. Oulu, Finland: IEEE, 2016. 1−6

76 Raghavendra R, Raja K B, Venkatesh S, Busch C. Face presentation attack detection by exploring spectral signatures. In: Proceedings of IEEE Conference on Computer Vision and Pattern Recognition Workshops. Hawaii, USA: IEEE, 2017. 672–679

77 Adelson E H, Wang Y A . Single lens stereo with a plenoptic camera. *Transactions on Pattern Analysis and Machine Intelligence*, 1992,**1**(2): 99−106

78 Kim S, Ban Y, Lee S. Face liveness detection using a light field camera. *Sensors*, 2014, **14**(12): 22471−22499

79 Xie X H,Gao Y, Zheng W S, Lai J H, Zhu J Y. One-snapshot face anti-spoofing using a light field camera. In: Proceedings of Chinese Conference on Biometric Recognition. Shenzhen, China: Springer, 2017. 108−117

80 Wang Y, Nian F D, Li T, Meng Z J, Wang K Q. Robust face anti-spoofing with depth information. *Journal of Visual Communication and Image Representation*, 2017, **49**: 332−337

81 Raghavendra R, Busch C. Novel presentation attack detection algorithm for face recognition system: Application to 3d face mask attack. In: Proceedings of IEEE International Conference on Image Processing. Paris, France: IEEE, 2014. 323−327

82 Lagorio A, Tistarelli M, Cadoni M, Fookes C, Sridharan S. Liveness detection based on 3d face shape analysis. In: Proceedings of International Workshop on Biometrics and Forensics. Lisbon, Portugal: IEEE,2013. 1−4

83 Tang Y H, Chen L M. 3d facial geometric attributes based anti-spoofing approach against mask attacks. In: Proceedings of IEEE International Conference on Automatic Face and Gesture Recognition. Washington, DC, USA: IEEE, 2017. 589−595

84 Yang J W, Lei Z, Li S Z. Learn convolutional neural network for face anti-spoofing. *arXiv preprint arXiv:1408.5601*, 2014

85 Atoum Y, Liu Y J, Jourabloo A, Liu X M. Face anti-spoofing using patch and depth-based cnns. In: Proceedings of IEEE International Joint Conference on Biometrics. Denver, Colorado, USA: IEEE, 2017: 319−328

86 Alotaibi A, Mahmood A. Deep face liveness detection based on nonlinear diffusion using convolution neural network. *Signal, Image and Video Processing*, 2017, **11**(4): 713−720

87 Lakshminarayana N N, Narayan N, Napp N, Setlur S, Govindaraju V. A discriminative spatio-temporal mapping of face for liveness detection. In: Proceedings of IEEE International Conference on Identity, Security and Behavior Analysis. New Delhi, India: IEEE, 2017. 1−7

88 Perona P, Malik J. Scale-space and edge detection using anisotropic diffusion. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 1990, **12**(7): 629−639

89 Li L, Feng X Y, Boulkenafet Z, Xia Z Q, Li M M, Hadid A. An original face anti-spoofing approach using partial convolutional neural network. In: Proceedings of 6th international conference on Image processing theory tools and applications. Oulu, Finland: IEEE, 2016. 1−6

90 Tu X K, Fang Y C. Ultra-deep neural network for face anti-spoofing. In: Proceedings of International Conference on Neural Information Processing. Guangzhou, China: Springer, 2017. 686−695

91 Li L, Feng X Y, Jiang X Y, Xia Z Q, Hadid A. Face anti-spoofing via deep local binary patterns. In: Proceedings of IEEE International Conference on Image Processing. Beijing, China: IEEE, 2017. 101−105

92 Lucena O, Junior A, Moia V, Souza R, Valle E, Lotufo R. Transfer learning using convolutional neural networks for face anti-spoofing. In: Proceedings of International Conference Image Analysis and Recognition. Montreal, Canada: Springer, 2017. 27−34

93 Nagpal C, Dubey S R. A performance evaluation of convolutional neural networks for face anti spoofing. *arXiv preprint arXiv:1805.04176*, 2018

94 He K M, Zhang X Y, Ren S Q, Sun J. Deep residual learning for image recognition. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. Las Vegas, USA: IEEE, 2016. 770−778

95 Hochreiter S, Schmidhuber J. Long short-term memory. *Neural computation*, 1997, **9**(8): 1735−1780

96 Rehman Y A U, Po L M, Liu M Y. Livenet: Improving features generalization for face liveness detection using convolution neural networks. *Expert Systems with Applications*, 2018, **108**: 159−169

97 Feng L T, Po L M, Li Y M, Xu X Y, Yuan F, Cheung T C H, Cheung K W. Integration of image quality and motion cues for face anti-spoofing: A neural network approach. *Journal of Visual Communication and Image Representation*, 2016, **38**: 451−460

98 Asim M, Zhu M, Javed M Y. CNN based spatio-temporal feature extraction for face anti-spoofing. In: Proceedings of 2nd International Conference on Image, Vision and Computing. Chengdu, China: IEEE, 2017. 234−238

99 Shao R, Lan X Y, Yuen P C. Deep convolutional dynamic texture learning with adaptive channel-discriminability for 3d mask face anti-spoofing. In: Proceedings of IEEE International Joint Conference on Biometrics. Denver, Colorado, USA: IEEE, 2017. 748−755

100 Parkhi O M, Vedaldi A, Zisserman A. Deep face recognition. In: Proceedings of British Machine Vision Conference. Swansea, UK: BMVA Press, 2015. 41.1−41.12

101 Liu Y J, Jourabloo A, Liu X M. Learning deep models for face anti-spoofing: Binary or auxiliary supervision. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. Salt Lake City, USA: IEEE, 2018. 389−398

102 Manjani I, Tariyal S, Vatsa M, Singh R, Majumdar A. Detecting silicone mask-based presentation attack via deep dictionary learning. *IEEE Transactions on Information Forensics and Security*, 2017, **12**(7): 1713−1723

103 Li H L, Li W, Cao H, Wang S Q, Huang F Y,Kot A C. Unsupervised domain adaptation for face anti-spoofing. *IEEE Transactions on Information Forensics and Security*, 2018, **13**(7): 1794−1809

104 Song X, Zhao X, Fang L J, Lin T W Discriminative representation combinations for accurate face spoofing detection. *Pattern Recognition*, 2019, **85**: 220−231

105 L W, Anguelov D, Erhan D, Szegedy C, Reed S, Yang F C, et al. SSD: Single shot multibox detector. In: Proceedings of European Conference on Computer Vision. Amsterdam, The Netherlands: Springer, 2016. 21−37

106 Ning X, Li W J, Wei M L, Sun L J, Dong X L. Face anti-spoofing based on deep stack generalization networks. In: Proceedings of International Conference on Pattern Recognition Applications and Methods. Funchal, Madeira, Portugal: SCITEPRESS, 2018

107 Wolpert D H. Stacked generalization. *Neural networks*,1992, **5**(2): 241−259

108 Ting K M, Witten I H. Stacked generalization: when does it work? In: Proceedings of the Fifteenth International Joint Conference on Artifical Intelligence. Nagoya, Japan: Morgan Kaufmann Publishers Inc,1997. 866−871

109 Li H L, He P S, Wang S Q, Rocha A, Jiang X H, Kot A C. Learning generalized deep feature representation for face anti-spoofing. *IEEE Transactions on Information Forensics and Security*, 2018, **13**(10): 2639−2652

110 Gan J Y, Li S L, Zhai Y K, Liu C Y. 3d convolutional neural network based on face anti-spoofing. In: Proceedings of International Conference on Multimedia and Image Processing. Wuhan, China: IEEE, 2017. 1−5

111 Tran D, Bourdev L, Fergus R, Torresani L, Paluri M. Learning spatiotemporal features with 3d convolutional networks. In: Proceedings of the IEEE International Conference on Computer Vision. Washington, DC, USA: IEEE, 2015. 4489−4497

112 Patel K, Han H, Jain A K. Cross-database face antispoofing with robust feature representation. In: Proceedings of Chinese Conference on Biometric Recognition. Chengdu, China: Springer, 2016. 611−619

113 Tronci R, Muntoni D, Fadda G, Pili M, Sirena N, Murgia G, et al. Fusion of multiple clues for photo-attack detection in face recognition systems. In: Proceedings of International Joint Conference on Biometrics. Washington, DC, USA: IEEE,2011. 1−6

114 Siddiqui T A, Bharadwaj S, Dhamecha T I, Agarwal A, Vatsa M, Singh R, et al. Face anti-spoofing with multifeature videolet aggregation. In: Proceedings of International Conference on Pattern Recognition. Cancun, Mexico: IEEE, 2016. 1035−1040

115 Kose N, Dugelay J L. Mask spoofing in face recognition and countermeasures. *Image and Vision Computing*, 2014, **32**(10):779−789

116 Tan X Y, Li Y, Liu J, Jiang L. Face liveness detection from a single image with sparse low rank bilinear discriminative model. In: Proceedings of European Conference on Computer Vision. Crete, Greece: Springer, 2010. 504−517

117 Anjos A, Marcel S. Counter-measures to photo attacks in face recognition: a public database and a baseline. In: Proceedings of International Joint Conference on Biometrics. Washington, DC, USA: IEEE, 2011. 1−7

118 Zhao X C, Lin Y P, Heikkilä J. Dynamic texture recognition using volume local binary count patterns with an application to 2d face spoofing detection. *IEEE Transactions on Multimedia*, 2018, **20**(3): 552−566

119 Costa-Pazo A, Bhattacharjee S, Vazquez-Fernandez E, Marcel S. The replay-mobile face presentation-attack database. In: Proceedings of International Conference of the Biometrics Special Interest Group. Darmstadt: IEEE, 2016. 1−7

120 Patel K, Han H, Jain A K. Secure face unlock: Spoof detection on smartphones. *IEEE transactions on Information Forensics and Security*, 2016, **11**(10): 2268−2283

121 Boulkenafet Z, Komulainen J, Li L, Feng X Y, Hadid A. Oulu-npu: A mobile face presentation attack database with real-world variations. In: Proceedings of IEEE International Conference on Automatic Face and Gesture Recognition. Washington, DC, USA: IEEE, 2017. 612−618

122 Chingovska I, Erdogmus N, Anjos A, Marcel S. Face recognition systems under spoofing attacks. *Face Recognition Across the Imaging Spectrum*. Berlin: Springer, 2016

123 Raghavendra R, Raja K B, Venkatesh S, Cheikh F A, Busch C. On the vulnerability of extended multispectral face recognition systems towards presentation attacks. In: Proceedings of IEEE International Conference on Identity, Security and Behavior Analysis. New Delhi, India: IEEE, 2017. 1−8

124 Liu S Q, Yang B Y, Yuen P C, Zhao G Y. A 3d mask face anti-spoofing database with real world variations. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops. Las Vegas, USA: IEEE, 2016. 100−106

125 Agarwal A, Yadav D, Kohli N, Singh R, Vatsa M, Noore A. Face presentation attack with latex masks in multispectral videos. In: Proceedings of Computer Vision and Pattern Recognition Workshops. Hawaii,USA: IEEE, 2017. 275−283

126 ISO/IEC JTC 1/SC 37 Biometrics, Information technology – biometric presentation attack detection – part 1: Framework, International Organization for Standardization 2, 2016

127 de Freitas Pereira T, Anjos A, De Martino J M, Marcel S. Can face anti-spoofing countermeasures work in a real world scenario? In: Proceedings of International Conference on Biometrics. Madrid, Spain: IEEE, 2013. 1−8

128 Jourabloo A, Liu Y J, Liu X M. Face de-spoofing: Anti-spoofing via noise modeling. *arXiv preprint arXiv:1807.09968*, 2018

129 Boulkenafet Z, Komulainen J, Akhtar Z, Benlamoudi A, Samai D, Bekhouche S E, et al. A competition on generalized software-based face presentation attack detection in mobile scenarios. In: Proceedings of 2017 IEEE International Joint Conference on Biometrics. Denver, Colorado, USA: IEEE, 2017.688−696

130 Wang Z Z, Zhao C X, Qin Y X, Zhou Q S, Lei Z. Exploiting temporal and depth information for multi-frame face anti-spoofing. *arXiv preprint arXiv:1811.05118*, 2018

蒋方玲 中国科学院重庆绿色智能技术研究院博士研究生. 2012 年获得天津大学计算机科学与技术专业硕士学位. 主要研究方向为人脸活体检测, 计算机视觉与模式识别.
E-mail: jiangfangling@cigit.ac.cn
(**JIANG Fang-Ling** Ph. D. candidate at the Chongqing Institute of

Green and Intelligent Technology, Chinese Academy of Sciences. She received her master degree from Tianjin University in 2012. Her research interest covers face anti-spoofing, computer vision, and pattern recognition.)

刘鹏程 中国科学院重庆绿色智能技术研究院助理研究员. 2016 年获得中国科学院自动化研究所工学博士学位. 主要研究方向为人脸识别、跨领域图像识别.
E-mail: liupengcheng@cigit.ac.cn
(**LIU Peng-Cheng** Research assistant at the Chongqing Institute of Green and Intelligent Technology, Chinese Academy of Sciences. He received his Ph. D. degree from Institute of Automation, Chinese Academy of Sciences in 2016. His research interest covers face recognition and cross-domain image recognition.)

周祥东 中国科学院重庆绿色智能技术研究院副研究员. 2009 年获得中国科学院自动化研究所工学博士学位. 主要研究方向为文字识别、文档分析、人脸识别.
E-mail: zhouxiangdong@cigit.ac.cn
(**ZHOU Xiang-Dong** Associate professor at the Chongqing Institute of Green and Intelligent Technology, Chinese Academy of Sciences. He received his Ph. D. degree from Institute of Automation, Chinese Academy of Sciences in 2009. His research interest covers handwriting recognition, ink document analysis, and face recognition. Corresponding author of this paper.)