计算机应用研究
Application Research of Computers
ISSN 1001-3695,CN 51-1196/TP

《计算机应用研究》网络首发论文

题目：人脸识别活体检测研究方法综述
作者：邓雄，王洪春，赵立军，吴至友，皮家甜
DOI：10.19734/j.issn.1001-3695.2019.03.0106
收稿日期：2019-03-22
网络首发日期：2019-08-29
引用格式：邓雄，王洪春，赵立军，吴至友，皮家甜．人脸识别活体检测研究方法综述[J/OL]．计算机应用研究. https://doi.org/10.19734/j.issn.1001-3695.2019.03.0106

网络首发时间：2019-08-29 16:11:34
网络首发地址：http://kns.cnki.net/kcms/detail/51.1196.TP.20190828.1154.023.html

人脸识别活体检测研究方法综述 *

邓 雄[1a,2]，王洪春[1a,2]，赵立军[2,3]，吴至友[1a,2]，皮家甜[1b,2†]

(1. 重庆师范大学 a. 数学科学学院; b. 计算机与信息科学学院，重庆 401331; 2. 智慧金融与大数据分析，重庆市重点实验室，重庆 401331; 3. 马上消费金融股份有限公司，重庆 401331)

摘 要：人脸识别具有广泛的应用，但容易受到伪造的欺骗人脸攻击而影响安全性，设计检测准确率高、泛化能力强、满足实时性需求的活体检测方法是目前的研究重点。将现有的人脸活体检测研究方法分为基于手工设计特征表达的方法，基于深度学习的方法和基于融合策略的方法，介绍每类方法所包含的典型算法的基本思想、实现步骤及优缺点。最后对已公开的人脸活体检测数据库进行整理说明，对人脸活体检测的发展趋势以及还需要进一步解决的问题进行综述，为今后人脸活体检测的研究提供参考和借鉴。

关键词：人脸识别；活体检测；特征提取；深度学习；融合策略

中图分类号：TP37 doi: 10.19734/j.issn.1001-3695.2019.03.0106

Survey on face anti-spoofing in face recognition

Deng Xiong[1a,2], Wang Hongchun[1a,2], Zhao Lijun[2,3], Wu Zhiyou[1a,2], Pi Jiatian[1b,2†]

(1. *a. School of Mathematical Sciences, b. College of Computer & Information Science, Chongqing Normal University, Chongqing* 401331, *China*; 2. *Intelligent Finance & Large Data Analysis, With Key Laboratory in Chongqing, Chongqing* 401331, *China*; 3. *Mashang Consumer Finance Co, Ltd, Chongqing* 401331, *China*)

Abstract: Face recognition has a wide range of applications, but it is vulnerable to spoofing attacks that affect security. How to design a method with high detection accuracy, strong generalization ability, and satisfying real-time requirements is the focus of current research. The existing methods of face Anti-Spoofing are divided into methods based on hand-crafted descriptor, methods based on deep learning and methods based on fusion strategy. The basic ideas, implementation steps and advantages and disadvantages of typical algorithms contained in each method were introduced. Finally, the published databases of face Anti-Spoofing were collated and explained, the development trend of face Anti-Spoofing and the problems that still further need to be solved were summarized, which can provide reference for the future research of face Anti-Spoofing.

Key words: face recognition; face anti-spoofing; feature extraction; deep learning; Fusion strategy

0 引言

随着人类社会进入数字时代，计算机、互联网技术迅猛发展，生物识别技术也越来越多的被应用于身份认证。人脸识别技术因其安全性和非接触性等优点，在现有生物特征识别技术当中更容易被用户接受，已成为学术界和工业界的一个重点研究方向[1]。然而人脸识别系统容易受到非法用户的恶意攻击，这给系统的安全性能带来了很大的威胁。针对恶意攻击，设计一个检测精度高、耗时短、鲁棒性强、泛化能力强的人脸反欺骗系统至关重要。

人脸识别系统的反欺骗检测又称为人脸活体检测，而常见的欺骗攻击方式有照片攻击[2,3]、视频攻击[4,5]和 3D 面具攻击[6,7]。真实人脸图像在摄像头下直接获取，而欺骗人脸图像的获取需要两个过程(假人脸的制作及二次采集)，两者之间存在一定的差异，主要体现在图像纹理信息、深度信息、运动信息、光谱信息等方面。利用真实人脸与欺骗人脸图像的这些差异可以设计不同的活体检测方法，对真假人脸作出判断。

近年来，有关人脸活体检测问题的研究发展迅速，取得了许多有价值的研究成果，主要集中在三个方面：基于手工设计特征表达的方法、基于深度学习的方法和基于融合策略的方法。本文将分别对其进行阐述，分析各种方法的优缺点；对已公开的活体检测数据库进行整理说明；分析人脸活体检测的发展趋势以及还需要解决的问题。

1 基于手工设计特征表达的人脸活体检测方法

随着人脸识别技术的广泛应用，人脸活体检测也受到了广泛的关注，已经成为了相对独立的研究领域。对于目前人脸活体检测的方法还没有统一分类这一问题，本文根据人脸活体检测技术的发展历程，将现存的主要方法分为三大类：基于手工设计特征表达的方法，基于深度学习的方法和基于融合策略的方法。

1.1 基于图像纹理分析的方法

图像在采集过程中会损失一些信息，并伴随有各种噪声，两次采集的图像与一次采集的相比，纹理上会有一定的差异。欺骗人脸图像与真实人脸图像的微纹理差异主要来源于图像的局部高光、阴影变化以及模糊程度[8]，据此可以对真假人脸进行判断。

收稿日期：2019-03-22；**修回日期：**2019-05-07 **基金项目：**重庆市基础研究与前沿探索项目(cstc2018jcyjAX0470)、重庆市教委科技项目青年项目(KJQN201800521)、重庆师范大学人才引进项目(17XLB021)

作者简介：邓雄(1991-)，男，河南邓州人，硕士研究生，主要研究方向为不确定性推理和模式识别方面的研究；王洪春(1967-)，男，四川大竹人，教授，硕导，主要研究方向为不确定性推理和模式识别方面的研究；赵立军(1970-)，男，辽宁朝阳人，博士，主要研究方向为人工智能方向的研究；吴至友(1967-)，女，重庆人，教授，博导，主要研究非线性规划、最优化理论与算法；皮家甜(1990-)，男(通信作者)，湖北潜江人，博士，主要研究方向为计算机视觉、仿生双眼、SLAM 等方面的研究(pijiatian@cqnu.edu.cn).

1)Fourier 频谱分析

Fourier 变换是数字图像处理的基础，通过在时域和频域上的切换来图像来分析所提取的图像特征。Li 等人[9]在频域上对真假人脸进行判断。给出了两个设定：第一是照片相比于真实人脸，是一个平面结构，有更少的高频分量；第二是打印的人脸照片没有相对运动，在一定时间内没有明显变化。基于这两点，对真假人脸进行判断。此方法存在一定的不足，一方面，照片人脸的高频分量随着打印照片清晰度的提升而增多；另一方面，没有考虑图像的空间信息。

Fourier 频谱分析方法相对简单，但算法鲁棒性不强，易受图像分辨率和光照等的影响。在人脸图像清晰时，其 Fourier 频谱图的高频分量较多，反之越少，随着高清摄像头的普遍应用，其不足之处突显出来。

2)纹理特征方法

Freitas 等人[10]将空间信息、时间信息融合到一个称为三维正交平面局部二值模式(LBP-TOP)的描述符中，用于照片和视频欺骗攻击检测。Boulkenafe 等人[2]提出了一种基于颜色纹理分析的人脸活体检测方法。从单个图像通道中提取 LBP 直方图，将这些直方图连接起来形成最终描述符，具体流程如图 1 所示。为了分析哪个颜色空间更具区分性，此方法考虑了 RGB、YCBCR 和 HSV 这三个颜色空间。实验表明，基于颜色纹理的方法在检测各种攻击时优于灰度纹理的方法。Boulkenaf 等人[3]又重点研究了亮度和色度通道，并利用了颜色和纹理的联合信息。虽然在实验中取得了不错的结果，然而，微纹理描述子的层次较低，因此对光照变化和高质量的图像都很敏感。

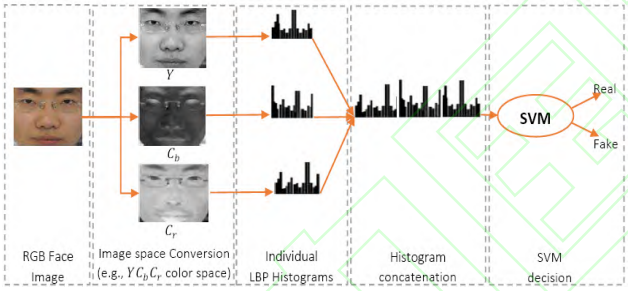

图 1　基于纹理分析方法流程图

Fig. 1　Texture analysis methodology flowchart

以上介绍的基于纹理特征的方法都是基于低层次的特征来分类的，这样不可避免的会影响模型的鲁棒性和泛化能力。由于低层次特征一般存在于高维空间，且易受到噪声等的干扰，不利于直接分类[11]。为了提高对图像内容的表达能力，并希望类内特征更相似而类间特征更有区别性，为了减少分类器训练与测试的计算量和存储空间，提高算法的识别效率和泛化能力，需要将低层次的特征通过一些编码算法表达为更具区分性、更加鲁棒的高层次特征。高层次的特征可以更好的表达整个图像的信息，便于分类。

Zhang 等人[12]提出了一种基于颜色纹理马尔可夫特征(color texture Markov feature, CTMF)和支持向量机递归特征消除(support vector machine recursive feature elimination, SVM-RFE)的人脸欺骗检测方案。作者分析了真实人脸与欺骗人脸的相邻像素差异，充分考虑了彩色通道之间的纹理信息。首先利用方向差分滤波器捕获真假人脸的纹理差异，这可以看做是 CTMF 的低层特征；然后利用马尔可夫过程对人脸纹理差异进行建模，形成低层特征的高层表示；最后利用 SVM-RFE 降维，使其适合于实时检测，在不同数据库上取得了较好的效果。同时 Zhang 等人对以往文献中忽略的彩色通道间的纹理相互信息也进行了研究。

基于图像纹理分析的反欺骗方法，算法简单，实时性高，成本低，然而随着高清摄像机的普及和高质量 3D 面具的应用，仅使用纹理信息已经不能满足需求，所以纹理信息往往需要和其他信息融合使用。

1.2　基于多光谱的活体人脸检测方法

真实人脸与欺骗人脸的材质不同，导致了成像系统反射率的巨大差异，在可见光环境下，该区别不是很显著，但在某些特定波段下会呈现出明显不同的反射特性，这为基于多光谱分析的活体检测方法提供了理论依据。可见光、近紫外光、近红外光等对人体没有危害且容易获取，在目前基于多光谱的活体检测方法中被经常使用。

Kim 等人[13]首先选取 685nm 和 850nm 这两个近红外波段光谱采集人脸图像，然后将这两个波段下的人脸皮肤反射数据投影到二维空间，并以此来对真假人脸进行判断。该方法存在的不足是需要采集目标与采集设备之间保持一定的距离，且人脸的额头区域要被拍摄到。这些要求影响用户体验，且由于检测对象单一而无法应对有针对性的欺骗攻击。

基于多光谱的方法具有检测精度高、检测范围广等优点；缺点是需要配备不同波段的主动光源，对设备的要求较高，从而增加了成本。

1.3　基于运动信息的方法

1)人机交互方法

真实人脸具有多样性的运动特征，如眨眼、张嘴、表情的变化等，而欺骗人脸很难模拟这样的运动，因此可以通过分析人脸区域是否存在这样的运动来判断真假。Singh 等人[14]利用眨眼和嘴部动作来进行活体判断。通过计算眼部区域的面积和牙齿的 HSV(hue, saturation, value)来判断眼睛是否睁开和嘴部是否张开。此外，还设计了一个人机交互系统，受试者根据该系统随机产生的短语提示作出动作，完成相关动作方可证明是真实人脸。基于人机交互的方法虽然能达到很高的识别率，不依赖纹理特征，对图像鲁棒性好，但需要受试者的高度配合，检测过程对用户不友好，检测时间较长。

2)脸部光流估计

当一个物体在运动时，它在图像上对应点的亮度模式也在运动，光流可以表征这种图像亮度模式的运动[15]。三维人脸和二维人脸的运动模式存在差异，当人脸旋转摆动时，活体人脸因脸部各处运动不一致产生不同的光流，而照片人脸不同区域的运动基本一致，其产生的光流和活体人脸有较大差别。基于这些差异，可以使用光流信息进行真假人脸的判断。Smiatacz 等人[16]计算人脸转动所产生的光流值，通过 SVM 对这些光流值进行训练并分类。该方法较为简单，但对光照比较敏感，对视频攻击和 3D 面具攻击检测效果较差。

1.4　基于深度信息的方法

真实人脸是三维的，额头、眼睛、鼻尖等不同位置具有不同的深度信息，而照片人脸和视频人脸是二维的，不同点的深度信息相同，而且即使将照片进行折叠，也同样与真实人脸具有不同的深度信息，因此深度信息可以用来进行活体检测。

基于深度信息的活体检测方法可分为需要额外硬件的和不需要额外硬件的。对于第一种，Lagorio 等人[17]通过包含结构光的 3D 扫描仪获取大约 8000 个特征点的三维坐标，计算每个点的曲率和所有点的平均曲率，最后通过平均曲率进行真假人脸的判断。虽然实验取得了零错误拒绝率，但是人为将图片进行弯曲造成折痕时，效果并不理想。Wang 等人[18]结合 Kinect 相机的深度信息和从卷积神经网络中学习到的纹理特征进行真假人脸的判断，也取得了不错的结果。对于第二种，Wang 等人[19]利用一段视频或多张照片恢复出稀疏的三维人脸模型，并以此进行活体检测。首先从多个角度获取多张照片或视频，定位每一帧的关键点，然后选取关键帧并

从中恢复出 3D 结构，最后选取 3D 人脸的 45 个关键点的三维坐标联合起来作为特征向量，使用 SVM 进行分类。第二类方法对设备的要求不高，适用性较强，但是深度信息的计算精度普遍不高。

基于深度信息的人脸活体检测方法具有明显的优势：深度信息具有光照不变等特性，所以活体检测鲁棒性好；真实人脸深度图具有三维人脸的轮廓特征，与照片人脸和视频人脸的深度图有显著的差异；无须用户过多交互，对照片和视频攻击等具有较好的检测效果，但对于 3D 面具攻击的检测效果较差。基于深度信息分析的关键是如何得到深度图以及人脸特征点的三维深度坐标，利用单张图片或多张图片估计出的深度信息精度不高，想要得到较准确的深度信息则需要一些设备作为辅助。

1.5　其他方法

1)基于热红外成像分析

欺骗人脸不具有稳定的热信号，其热红外图像较为暗淡，大多情况下和真实人脸的热红外图有较大差异。Bhattacharjee 等人[20]首次对使用定制硅胶面具的欺骗攻进行了研究，同时提供了一个新的关于定制硅胶面具攻击数据库(CS-Mad)。因为面具的温度比人体低，所以真实人脸的热红外图像比较明亮，人脸面具的热红外图像比较黑暗，但是当攻击者戴上面具时，面罩可能会随着时间的推移而升温。基于热红外图像分析的方法具有较高的检测效率，对光照有较强的鲁棒性，但是对设备有一定的要求。

2)基于心率检测分析

光学体积描述术(Photoplethysmography, PPG)是利用光学的方法测量血流体积。利用这项技术能够获得诸如心率变化、血压、呼吸率、血氧饱和度、供血量、自主神经功能等信息，它们一般都是接触式的。用摄像头进行非接触式的心率测量，一般称之为 remote-PPG(rPPG)。真实人脸和照片人脸中提取的心率在频域上有不同的分布，利用这一点可以判断真假人脸。

Li 等人[4]第一个将 rPPG 应用到活体检测中。输入多帧视频，首先提取心率特征，若判别结果是活体，则由于屏幕视频中人脸心率分布与活体相近，需要进一步提取 LBP 颜色纹理特征来区分活体/屏幕攻击。具体流程如图 2。

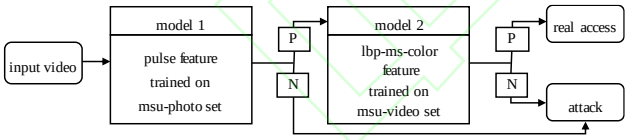

图 2　级联策略结构图

Fig. 2　Cascade policy structure diagram

Liu 等人[6]认为虽然现有的基于 rPPG 的方法在交叉数据库中都取得了很好的效果，但当 rPPG 信号受到噪声污染时，它们可能不够健壮，为此提出了一种新的特征—rPPG 对应特征(rPPG correspondence feature, CFrPPG)，用于从有噪声的 rPPG 信号中准确地识别心跳残迹。为了克服全局干扰，提出了一种在 CFrPPG 特征中引入全局噪声的学习策略，所提出的特征不仅优于基于 rPPG 的 3D 面具攻击方法，而且能够处理弱光和摄像机运动的实际场景。

由于 rPPG 的算法鲁棒性一般，所以计算的心率特征的判别性能还不能保证，往往需要级联其他的特征和分类器来实现活体检测。

3)基于图像质量分析

Galbally 等人[21]提出了一种通过对图像质量度量中的 25 个显著因素进行分析来对图像质量进行评价。受文献[21]的启发，Wen 等人[22]提出了一种基于图像失真分析(image distortion analysis, IDA)的人脸欺骗检测算法。首先提取四种不同的特征(镜面反射、模糊度、色矩和颜色多样性)，形成 IDA 特征向量；然后对于不同人脸欺骗攻击(如照片攻击和视频攻击)训练的多个 SVM 分类器组成一种集成分类器，用于区分真假人脸；最后将该方法应用到基于投票的视频多帧人脸欺骗检测中，取得了不错的结果。同时还收集了一个用于人脸反欺骗的数据库(MSU MFSD)。当图像质量较高的时候，此方法容易被欺骗。

4)基于情景分析

上下文线索对活体检测也很有用。Komulainen 等人[23]通过检测场景中的欺骗攻击介质来进行人脸欺骗攻击检测。Yan 等人[24]融合多个上下文线索，如背景一致性和场景移位等。然而，基于这些简单线索的系统很容易被欺骗，因此它们往往不单独使用。

以上所述方法都是基于人工设计的特征，对于人脸活体检测，虽然有些能达到较好的识别率，但也存在不足之处，如检测效果依赖特征的提取和表达，算法鲁棒性能和泛化能力有限等。

2　基于深度学习的人脸活体检测方法

随着深度学习在计算机视觉领域的广泛应用，其以数据驱动方式学习到的特征有手工设计的特征无法比拟的优势。此外，它有学习到更多一般性特征的潜力，以适用各种欺骗类型，这对于提高算法的鲁棒性和泛化能力都有益。

Yang 等人[25]首次提出将卷积神经网络(CNN)用于人脸欺骗检测，文献[26, 27]提出了直接修改网络结构的方法，进一步提高了检测精度。Manjani 等人[28]提出了一种基于深度学习的方法用于面具攻击检测。Gan 等人[29]利用三维卷积神经网络(3DCNN)从短视频中提取连续视频帧的时空特征来识别人脸欺骗攻击。Li 等人[30]介绍了一种基于深层卷积神经网络(deep part convolutional neural network, DPCNN)的人脸反欺骗方法。把每个卷积核看做一个局部滤波器，从人脸区域的关键部分提取特征，基于强响应区域，从 DPCNN 中提取深层特征作为局部描述符来区分真假人脸。与第一篇关于人脸反欺骗的工作[25]相比，DPCNN 具有更深层次的体系结构，利用了深层特征而不仅仅是全连接层。最后值得注意的是，当有大量的训练图像可供训练时，深度学习可以获得更好的效果。

Atoum 等人[31]提出了一种基于两流 CNN 的人脸反欺骗方法，用于照片和视频攻击检测。第一个 CNN 是端到端训练的，并给每个随机提取的图像块分配一个分数，而整个人脸图像用分数的平均值来计算；第二个 CNN 用来估计人脸图像的深度图，并根据估计的深度图为人脸图像提供一个真实性评分。该方法从人脸局部图像块中提取局部特征和从整个人脸图像中提取深度特征，最后通过这两个 CNN 的分数融合给出最终真假人脸的判断，具体流程如图 3 所示。

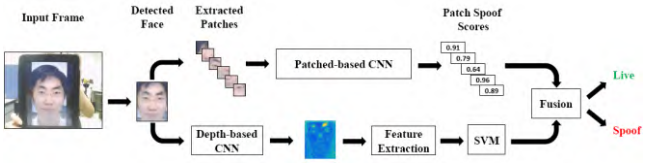

图 3　两流 CNN 结构图

Fig. 3　Architecture of the proposed face anti-spoofing approach

针对 3D 面具欺骗攻击，根据真实人脸与 3D 面具表现出不同的动作行为，而不同的动态信息通常存在于微妙的纹理层次上，传统的手工设计的纹理方法无法完全区分这些动态信息，Shao 等人[32]提出了一种反 3D 面具欺骗的方法，它从细粒度的深卷积特征中学习鲁棒的动态纹理信息。此外，为了获得一个更具辨别力的动态纹理特征，进一步将通道识别

约束引入特征学习过程，以赋予具有强判别性的特征通道更大的权重。

Liu 等人[33]指出把活体检测看成二分类问题，直接让 DNN 去学习，这样学出来的特征信息缺乏普遍性和判别性。针对这些问题，作者将二分类问题换成带目标性的特征监督问题，提出了一个深度模型，它使用空间和时间的辅助信息来进行视频攻击检测，如图 4 所示。从空间的角度来看，真实人脸是三维的而纸张(或屏幕)人脸是二维的；从时间的角度来看，真实人脸可以检测到正常的 rPPG 信号而欺骗人脸却不能。为了实现这两种监督，作者设计了一个网络架构，采用 CNN-RNN 模型对人脸图像训练得到深度图，并对 rPPG 信号进行序列监控得到心率统计量。最后深度信息和 rPPG 统计量融合，以区分真假人脸，取得了很好的结果。

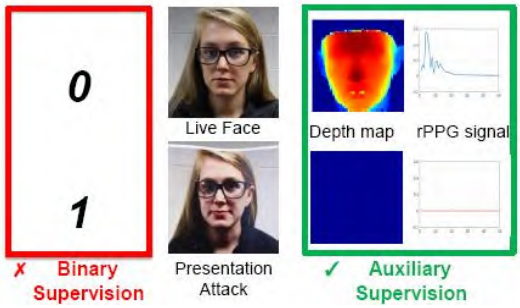

图 4　真实人脸与欺骗人脸在深度图像和 rPPG 信号方面的差异

Fig. 4　The difference between real face and deceptive face in depth image and rppg signal

Wang 等人[34]认为文献[33]存在一些不足，首先，使用非刚性配准层去除脸部表情和姿态的影响，忽略了非活体脸部不同表情与姿态的不自然变化；其次，仅利用单帧图像来预测深度，忽略了多帧间的空间微变化可以帮助重构深度图，即利用多帧信息理论上会比单帧更好地重构深度图。基于上面两点，提出利用多帧间的动态信息和深度信息进行人脸活体检测的方法。

学习空间和时间特征比较困难，因为需要大量的训练数据，而缺乏泛化的情况可能更加普遍。为此，Li 等人[35]从空间和时间两个维度出发，对深度特征表示进行了广义的研究，提出了一种人脸欺骗检测框架。首先，通过基于交叉熵损失的增强样本训练来初始化一个带有数据增强策略的 3DCNN 结构来完成欺骗检测任务。为了获得一个更鲁棒、更泛化的 3DCNN 模型，通过引入正则化机制来解决其泛化不足的问题，该机制的重点是在训练过程中提高分类精度，并通过调整不同领域训练样本的特征分布距离，可以无缝地学习广义特征，从而使网络能够进一步探测未知或不同条件下的欺骗攻击。该框架充分利用了深度学习的表征能力和领域泛化的特点，实现了人脸欺骗检测。

一些基于 CNN 的方法，如 Inception[36]和 ResNet[37]，在图像分类问题上表现出了优异的性能。Nagpal 等人[38]对 CNNs 的反人脸欺骗性能进行了评价，使用 Inception 和 ResNet 架构在不同的环境下进行人脸欺骗检测，取得了良好的效果。同时在实验中对网络的深度、权值初始化与微调、学习速率等问题进行了研究。

为了推动人脸反欺骗技术的发展，Zhang 等人[39]发布了一个大规模、多模式人的脸反欺骗数据库，包含 1000 人，有三种模式(即 RGB、深度和红外)，是目前公共数据库中在主题多样性、数据规模和数据模式等方面最大的数据库。此外，还提出了一种新的多模态融合方法，对所涉及的三种模式进行有效的融合，通过对模型相关的特征进行加权，选择信息更丰富且对每一种模式有用的特征进行融合，模型结构如图 5 所示。最后在所提出的数据库上进行了大量实验，验证了其泛化能力。

总之，深度学习方法与传统的需要手工设计特征描述符的方法相比，具有自身的优越性。

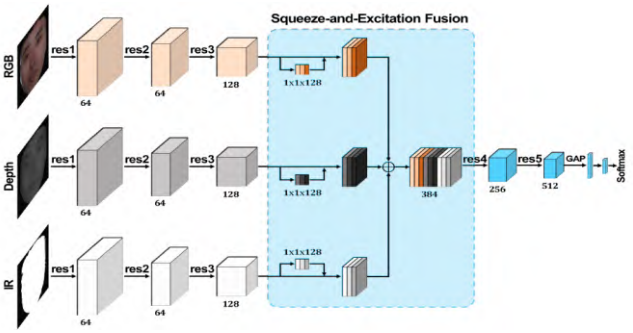

图 5　算法结构图

Fig. 5　Algorithm structure diagram

3　基于融合策略的人脸活体检测方法

传统的模式分类算法一般基于手工设计的特征，经过特征提取算法得到原始的特征数据，如 GIST 特征、HOG 特征、SIFT 特征、颜色特征等。一种特征一般只对图像部分特性的变化较为敏感，而对其他特性的变化不敏感，因此这些特征数据往往存在较小的类内方差和较大的类间方差。当两类图像在某种特征敏感特性上差异不大时，基于单一特征训练的分类器很难给出正确的分类[40]。基于深度学习的模式分类算法同样面临这样的问题。因此，为了提高活体检测算法的鲁棒性和泛化能力，需要把不同的信息进行融合。按照一定的方法将这些互补的信息融合，不仅可以提高识别精度，还可以提高算法的鲁棒性能和泛化能力。

3.1　融合策略简介

模式分类问题的解决过程一般包含数据预处理、特征提取、分类器设计等环节，每个环节都有对应的融合方法，分别为数据融合、特征融合、分类器融合，分类器融合又称为决策层的融合。数据融合发生在最底层，优点是保留了原始数据的所有信息，在深度学习领域被广泛使用，主要表现在数据集的扩充，缺点是原始数据含有大量的冗余信息和噪声，不利于计算；分类器融合发生在高层语义层次，算法简单高效，对分类精度和泛化能力有一定的提升，但是高层的融合不可避免的会造成原始数据信息的丢失，具有一定的局限；特征融合发生在中层，数据特征保留了显著的、必要的信息，既降低了原始数据的冗余和噪声，又比决策层的融合有更充分的数据信息，数据量和数据维度适中。不同的融合策略包含一些具体的方法，如图 6 所示。

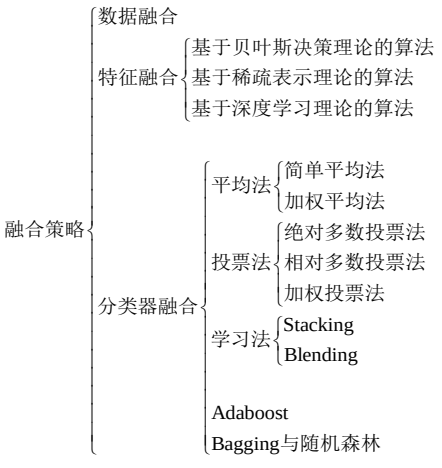

图 6　融合方法分类

Fig. 6　Classification of fusion strategy

上面介绍的融合方法各有利弊，需要根据具体的应用情形选择合适的融合策略。

3.2　基于融合策略的活体检测方法

Tronci 等人[41]提出一种融合纹理信息和运动信息的活体检测方法。Yan 等人[42]提出使用三种不同的特征相融合进行活体检测：非刚性运动、人脸背景一致性、图像条纹效应。Komulainen 等人[43]对文献[41]提出的方法加以改进，检测效率进一步得到提升。Wang 等人[19]结合深度信息和纹理信息，利用 LBP 特征来表达 Kinect 相机捕获的深度图像，并使用 CNN 从 RGB 图像学习纹理信息。

为了提高人脸反欺骗方法的泛化能力，Feng 等人[44]提出了一种基于分层神经网络的多信息融合框架，该框架融合图像质量信息和运动信息。首先利用剪切波变换进行人脸图像质量评价，提供了比常用的 LBP 更好的图像质量描述符；然后利用神经网络分别从剪裁的面部区域和整个场景的原始光流信息中学习基于运动的活体特征；最后提出基于分层神经网络的瓶颈特征融合策略对图像质量特征和运动特征进行融合，与原始特征融合策略、分数融合策略相比，瓶颈特征融合策略获得了更好的效果。

针对跨数据库测试的鲁棒性问题，Patel 等人[45]提出了一种鲁棒的反欺骗攻击方法，该方法整合了深层纹理特征和像眨眼这样的面部运动特征。欺骗图像在人脸和非人脸区域存在纹理失真，从对齐的面部图像和整个图像中分别学习深层纹理特征；然后使用一种基于帧差的方法进行眨眼检测，最后采取投票决策的方式融合两种方法，当两种方式都判断为真人脸时则认为真。

Song 等人[46]介绍了三种方法。首先，设计 SPMT(spatial pyramid coding micro-texture)特征来描述局部的外观信息；其次，利用 SSD(single shot multibox detector)这一深度学习框架来挖掘上下文信息，进行端到端的人脸欺骗攻击检测；最后，设计 TFBD(template face matched binocular depth)特征来描述人脸的立体结构。此外，还设计了两种融合方式，第一种将 SPMT 与 SSD 在决策级联融合，通过实验证明了局部外观特征与上下文信息之间的互补性；第二种将 SPMT 与 TFBD 相结合，证明了外观特征与立体结构信息之间的互补性。

在深度学习的强大表现能力的激励下，Tang 等人[47]提出使用 CNN 从人脸图像的不同信息中学习多个深层特征来进行活体检测。利用卷积网络从图像序列中学习时间特征，从不同颜色空间中学习颜色特征，从局部图像块中学习局部特征，每个 CNN 学习过程都由一个二分类的 softmax 分类器来监督。考虑到所有的特征都是互补的，进一步提出了一种整合所有特征的策略：将每个 CNN 的 softmax 函数输出的类别概率作为类别概率向量连接起来，输入 SVM 进行分类，模型结构如图 7 所示。

融合不同的信息可以弥补彼此的不足，从而克服单个线索的局限性，使活体检测的效果得到明显的提升，同时对于提高算法的鲁棒性和泛化能力也意义重大。

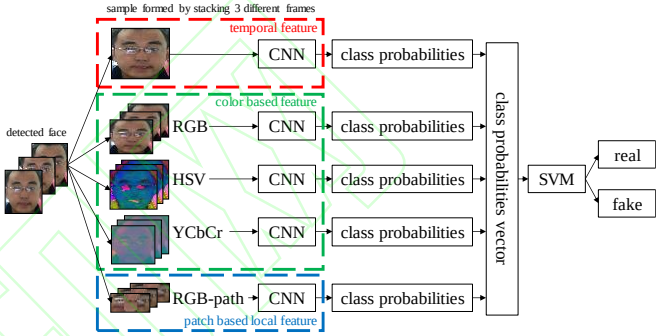

图 7　算法结构图

Fig. 7　Algorithm structure diagram

4　人脸活体检测数据库

为了满足人脸活体检测研究的需要，许多大学和研究所制作了人脸活体检测的数据库。已公布数据库的介绍如表 1 所示。

表 1　已公布人脸活体检测数据库及对比

Tab. 1　Comparison of published face liveness detection database

dataset	year	of subjects	of videos	camera	types	spoof attacks
NUAA[48]	2010	15	12614*	VIS	RGB	print
Print-Attack[49]	2011	50	1300	phone/laptop	RGB	print, replay
Replay-Attack[50]	2012	50	1200	VIS	RGB	print, replay
CASIA-FASD[51]	2012	50	600	VIS	RGB	print, replay
3DMAD[52]	2013	17	255	VIS/Kinect	RGB/depth	3D mask
MUS-MFSD[22]	2015	35	440	phone/laptop	RGB	print, replay
Replay-Mobil[7]	2016	40	1030	VIS	RGB	print, replay
Msspoof[5]	2016	21	4704*	VIS/NIR	RGB/IR	print
Oulu-NPU[53]	2017	55	5940	VIS	RGB	print, replay
SiW[33]	2018	165	4620	VIS	RGB	print, replay
CASIA-SURF[39]	2018	1000	21000	RealSense	RGB/depth/IR	print, replay

注：*表示此数据库仅含有图片不包含视频段

5　分析与讨论

本文通过对现有人脸活体检测方法进行分类、分析和比较，发现人脸活体检测在以下几个方面还亟待进一步研究：

1)特征编码技术的研究。

图像分类效果依赖于图像特征提取算法。基于手工设计特征的方法中，从图像中直接提取的特征大都是底层次的特征，一般存在于高维空间并含有大量的冗余与噪声，不利于直接分类。特征编码算法可以将底层特征转换为高层特征，能更好的描述整个图像的信息。高层特征不仅方便分类，而且对于算法鲁棒性和泛化能力的提升都很重要。如何设计编码算法使得高层特征更加具有代表性、简约性、鲁棒性成为核心研究问题。

2)深度学习框架的研究。

人脸活体检测要实现实时性需求，就需要设计一些针对性强的轻量型网络，避免网络结构的冗余；另一方面，图像分类基于图像特征的提取和表达，好的特征对于活体检测意义重大，深度学习可以学习到一些手工无法提取的特征，而如何根据不同的信息设计有监督的特征学习框架仍是目前研究的重点。

3)融合策略的研究。

真实人脸与欺骗人脸在很多方面都有差异，只关注其中

的一点差异很难保证模型的高识别率和鲁棒性，所以好的检测方法需要融合多角度的互补信息。目前常用的融合策略有特征级的融合、决策级的融合等。如何根据实际需求选取适当的信息，以及针对这些互补的信息设计相应的融合策略也是目前需要进一步研究的。

6 结束语

人脸识别系统容易受到欺骗攻击，给系统的安全性能带来挑战。如何设计一个检测精度高、耗时短、鲁棒性强、泛化能力强的人脸反欺骗系统成为目前的研究热点。本文详细介绍了人脸活体检测的研究方法，重点对基于手工设计特征的方法和基于深度学习的方法进行了分类和综述，提供了较为完整的现状分析，并且对已公开的活体检测数据库进行整理说明，最后对人脸活体检测中还需要进一步解决的问题进行了分析和说明。

随着深度传感器越来越多的应用于移动设备，基于 RGB-D 图像的人脸识别和活体检测算法值得进一步的研究。针对目前包含深度图的数据库非常有限的问题，本文作者接下来将利用 Kinect 相机采集一个包含 RGB 图像和深度图像的用于人脸活体检测的数据库，该数据库不仅包含照片攻击、视频攻击、3D 面具攻击，而且会考虑光照、距离、角度以及面部表情等因素；然后利用深度学习算法分别从 RGB 图和深度图中提取特征，进行特征级的融合，并选择合适的分类器对真假人脸进行判断。后续工作将在特征提取、特征融合和分类器设计等层面逐一展开。

参考文献：

[1] Lu J, Liong V E, Wang G, *et al.* Joint Feature Learning for Face Recognition [J]. IEEE Trans on Information Forensics and Security, 2017, 10 (7): 1371-1383.

[2] Boulkenafet Z, Komulainen J, Hadid A. Face antispoofing based on color texture analysis [C]// Proc of IEEE International Conference on Image Processing (ICIP) . Piscataway, NJ: IEEE Press, 2015: 2636-2640.

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

[4] Li Xiaobai, Komulainen J, Zhao Guoying, *et al.* Generalized face anti-spoofing by detecting pulse from face videos [C]// Proc of IEEE 23rd International Conference on Pattern Recognition (ICPR) . Piscataway, NJ: IEEE Press, 2016: 4239-4244.

[5] Chingovska I, Erdogmus N, Anjos A, *et al.* Face recognition systems under spoofing attacks [C]. Proc of Face Recognition Across the Imaging Spectrum. Cham: Springer, 2016: 165–194.

[6] Liu Siqi, Lan Xiangyuan, and Yuen P C. Remote photoplethysmography correspondence feature for 3d mask face presentation attack detection [C]// Proc of the European Conference on Computer Vision (ECCV) . Cham: Springer, 2018: 558–573.

[7] Costa-Pazo A, Bhattacharjee S, Vazquez-Fernandez E, *et al.* The replay-mobile face presentation-attack database [C]// Proc of IEEE International Conference of the Biometrics Special Interest Group (BIOSIG) . Piscataway, NJ: IEEE Press, 2016: 1–7.

[8] 黄建恺. 人脸识别的活体检测技术研究 [D]. 武汉：华中师范大学, 2018. (Huang Jiankai. Research on living detection technology of face recognition [D]. Wuhan: Central China Normal University, 2018.)

[9] Li Jianwei, Wang Yunhong, Tan Tieniu, *et al.* Live face detection based on the analysis of fourier spectra [C]// Proc. SPIE 5404, Biometric Technology for Human Identification. [S. I.] : [s. n.] , 2004: 296-303.

[10] de Freitas Pereira T, Anjos A, De Martino J M, *et al.* Lbp-top based countermeasure against face spoofing attacks [C]// Proc of Asian Conference on Computer Vision (ACCV) . Berlin: Springer, 2013: 121-132.

[11] 向程渝. RGB-D 图像分类的特征提取与分类算法 [D]. 湖南：湘潭大学, 2017. (Xiang Chengyu. Research on feature extraction and classification method of RGB-D images [D]. Xiangtan: Xiangtan University, 2017.)

[12] Zhang Lebing, Peng Fei, Qin Le, *et al.* Face spoofing detection based on color texture markov feature and support vector machine recursive feature elimination [J]. Journal of Visual Communication and Image Representation, 2018 (51): 56-69.

[13] Kim Y, Na J, Yoon S, *et al.* Masked fake face detection using radiance measurements [J]. Journal of the Optical Society of America A, 2009, 26 (4): 760-766.

[14] Singh A K, Joshi P, Nandi G C. Face Recognition with Liveness Detection using Eye and Mouth Movement [C]// Proc of International Conference on Signal Propagation and Computer Technology (ICSPCT) . Piscataway, NJ: IEEE Press, 2014: 592-597.

[15] 尹文泽. 基于面部信息分析的活体检测系统研究与实现 [D]. 北京：北京邮电大学, 2017. (Yin Wenze. Study and implementation of an anti-spoofing system based on facial information analysis [D]. Beijing: Beijing University of Posts and Telecommunications, 2017.)

[16] Smiatacz M. Liveness Measurements Using Optical Flow for Biometric Person Authentication [J]. Metrology and Measurement Systems, 2012, 19 (2): 257-268.

[17] Lagorio A, Tistarelli M, Cadoni M, *et al.* Livensss detection based on 3D face shape analysis [C]// Proc of International Workshop on Biometrics and Forensics (IWBF) . Piscataway, NJ: IEEE Press, 2013: 1-4.

[18] Wang Tao, Yang Jianwei, Lei Zhen, *et al.* Face liveness detection using 3D structure recovered from a single camera [C]// Proc of International Conference on Biometrics (ICB) . Piscataway, NJ: IEEE Press, 2013: 1-6.

[19] Wang Yan, Nian Fudong, Li Teng, *et al.* Robust face anti-spoofing with depth information [J]. Journal of Visual Communication and Image Representation, 2017, (49): 332-337.

[20] Bhattacharjee S, Mohammadi A, and Marcel S. Spoofing deep face recognition with custom silicone masks [C]// Proc of IEEE the 9th International Conference on Biometrics Theory, Applications and Systems (BTAS) . Piscataway, NJ: IEEE Press, 2018.

[21] Galbally J, Marcel S, Fierrez J. Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition [J]. IEEE Trans on Image Processing, 2014, 23 (2): 710-724.

[22] Wen Di, Han Hu, Jain A K. Face spoof detection with image distortion analysis [J]. IEEE Trans on Information Forensics and Security, 2015, 10 (4): 746-761.

[23] Komulainen J, Hadid A, Pietikainen M. Context based face anti-spoofing [C]// Proc of IEEE the 6th International Conference on Biometrics: Theory, Applications and Systems (BTAS) . Piscataway, NJ: IEEE Press, 2013: 1-8.

[24] Yan Junjie, Zhang Zhiwei, Lei Zhen, *et al.* Face liveness detection by exploring multiple scenic clues [C]// Proc of IEEE the 12th International Conference on Control Automation Robotics & Vision (ICARCV) . Piscataway, NJ: IEEE Press, 2012: 188-193.

[25] Yang Jianwei, Lei Zhen, and Li S Z. Learn convolutional neural network for face anti-spoofing [J]. arXiv preprint arXiv: 1408. 5601,

2014.

[26] Tu Xiaokang. and Fang Yuchun. Ultra-deep neural network for face anti-spoofing [C]// Proc of International Conference on Neural Information Processing. Cham: Springer, 2017: 686-695.

[27] Lucena O, Junior A, Moia V, *et al.* Transfer learning using convolutional neural networks for face antispoofing [C]// Proc of International Conference Image Analysis and Recognition. Cham: Springer, 2017: 27-34.

[28] Manjani I, Tariyal S, Vatsa M, *et al.* Detecting silicone mask based presentation attack via deep dictionary learning [J]. IEEE Trans on Information Forensics and Security, 2017, 12 (7): 1713 – 1723.

[29] Gan Junying, Li Shanlu, Zhai Yikui, *et al.* 3d convolutional neural network based on face anti-spoofing [C]// Proc of IEEE the 2nd International Conference on Multimedia and Image Processing (ICMIP) . Piscataway, NJ: IEEE Press, 2017: 1–5.

[30] Li Lei, Feng Xiaoyi, Boulkenafet Z, *et al.* An original face anti-spoofing approach using partial convolutional neural network [C]// Proc of IEEE the 6th International Conference on Image Processing Theory, Tools and Applications (IPTA) . Piscataway, NJ: IEEE Press, 2016: 1–6.

[31] Atoum Y, Liu Yaojie, Jourabloo A, *et al.* Face anti-spoofing using patch and depth-based cnns [C]// Proc of IEEE International Joint Conference on Biometrics (IJCB) . Piscataway, NJ: IEEE Press, 2017: 319–328.

[32] Shao Rui, Lan Xiangyuan, and Yuen P C. Deep convolutional dynamic texture learning with adaptive channel discriminability for 3d mask face anti-spoofing [C]// Proc of IEEE International Joint Conference on Biometrics (IJCB) . Piscataway, NJ: IEEE Press, 2017: 748–755.

[33] Liu Yaojie, Jourabloo A, and Liu Xiaoming. Learning deep models for face anti-spoofing: Binary or auxiliary supervision [C]// Proc of IEEE Conference on Computer Vision and Pattern Recognition (CVPR) . Piscataway, NJ: IEEE Press, 2018: 389-398.

[34] Wang Zezheng, Zhao Chenxu, Qin Yunxiao, *et al.* Exploiting temporal and depth information for multi-frame face anti-spoofing [J]. arXiv preprint arXiv: 1811. 05118, 2018.

[35] Li Haoliang, He Peisong, Wang Shiqi, *et al.* Learning generalized deep feature representation for face anti-spoofing [J]. IEEE Trans on Information Forensics and Security, 2018, 13 (10): 2639-2652.

[36] Szegedy C, Liu Wei, Jia Yangqing, *et al.* Going deeper with convolutions [C]// Proc of The IEEE Conference on Computer Vision and Pattern Recognition (CVPR) . Piscataway, NJ: IEEE Press, 2015: 1-9.

[37] He Kaiming, Zhang Xianyu, Ren Shaoqing, *et al*. Deep residual learning for image recognition [C]// Proc of The IEEE Conference on Computer Vision and Pattern Recognition (CVPR) . Piscataway, NJ: IEEE Press, 2016: 770–778.

[38] Nagpal C, and Dubey S R. A performance evaluation of convolutional neural networks for face anti spoofing [J]. arXiv preprint arXiv: 1805. 04176, 2018.

[39] Zhang Shifeng, Wang Xiaobo, Liu Ajian, *et al.* CASIA-SURF-A Dataset and Benchmark for Large-scale Multi-modal Face Anti-Spoofing [J]. arXiv preprint arXiv: 1812. 00408, 2018.

[40] 刘渭滨，邹智元，邢薇薇. 模式分类中的特征融合方法 [J]. 北京邮电大学学报，2017，40 (4): 5-12. (Liu Weibin, Zou Zhiyuan, Xing Weiwei. Feature fusion methods in pattern classification [J]. Journal of Beijing University of Posts and Telecommunications, 2017, 40 (4): 5-12.)

[41] Tronci R, Muntoni D, Fadda G, *et al.* Fusion of multiple clues for photo-attack detection in face recognition systems [C]// Proc of IEEE International Joint Conference on Biometrics (IJCB) . Piscataway, NJ: IEEE Press, 2011: 1-6.

[42] Yan Junjie, Zhang Zhiwei, Lei Zhen, *et al.* Face liveness detection by exploring multiple scenic clues [C]// Proc of IEEE the 12th International Control Automation Robotics & Vision (ICARCV) . Piscataway, NJ: IEEE Press, 2012: 188-193.

[43] Komulainen J, Hadid A, Pietikäinen M, *et al*. Complementary countermeasures for detecting scenic face spoofing attacks [C]// Proc of IEEE International Conference on Biometrics (ICB) . Piscataway, NJ: IEEE Press, 2013: 1-7.

[44] Feng Litong, Po Laiman, Li Yuming, *et al.* Integration of image quality and motion cues for face anti-spoofing: A neural network approach [J]. Journal of Visual Communication and Image Representation, 2016, (38): 451–460.

[45] Patel K, Han Hu, and Jain A K. Cross-database face anti-spoofing with robust feature representation [C]// Proc of Chinese Conference on Biometric Recognition (CCBR) . Cham: Springer, 2016: 611–619.

[46] Song Xiao, Zhao Xu, Fang Liangji, *et al.* Discriminative Representation Combinations for Accurate Face Spoofing Detection [J]. Pattern Recognition, 2019, (85): 220–4231.

[47] Tang Yan, Wang Xing, Jia Xi, *et al.* Fusing Multiple Deep Features for Face Anti-spoofing [C]// Proc of Chinese Conference on Biometric Recognition (CCBR) . Cham: Springer, 2018: 321-330.

[48] Tan Xiaoyang, Li Yi, Liu Jun, *et al.* Face liveness detection from a single image with sparse low rank bilinear discriminative model [C]// Proc of European Conference on Computer Vision (ECCV) . Berlin: Springer, 2010: 504–517.

[49] Anjos A and Marcel S. Counter-measures to photo attacks in face recognition: a public database and a baseline [C]// Proc of IEEE International Joint Conference on Biometrics (IJCB) . Piscataway, NJ: IEEE Press, 2011.

[50] Chingovska I, Anjos A, and Marcel S. On the effectiveness of local binary patterns in face anti-spoofing [C]// Proc of IEEE Proceedings of the International Conference of Biometrics Special Interest Group (BIOSIG) . Piscataway, NJ: IEEE Press, 2012.

[51] Zhang Zhiwei, Yan Junjie, Liu Sifei, *et al.* A face anti-spoofing database with diverse attacks [C]// Proc of IEEE the 5th IAPR International Conference on Biometrics (ICB) . Piscataway, NJ: IEEE Press, 2012: 26–31.

[52] Erdogmus N, Marcel S. Spoofing in 2d face recognition with 3d masks and anti-spoofing with kinect [C]// Proc of IEEE 6th International Conference on Biometrics: Theory, Applications and Systems (BTAS) . Piscataway, NJ: IEEE Press, 2013: 1-6.

[53] Boulkenafet Z, Komulainen J, Li Lei, *et al*. Oulu-npu: A mobile face presentation attack database with real-world variations [C]// Proc of IEEE the 12th International Conference on Automatic Face & Gesture Recognition. Piscataway, NJ: IEEE Press, 2017: 612–618.