计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.210100181

基于多特征融合的人脸活体检测算法

栾 晓 李晓双
重庆邮电大学计算机科学与技术学院 重庆 400065
重庆邮电大学图像认知重庆市重点实验室 重庆 400065

摘 要 近年来,随着人脸识别系统的不断发展,各种假冒合法用户的欺骗手段不断出现。基于单一差异线索进行的活体检测,已经不能满足当前复杂环境下提高人脸活体检测方法性能的需求。基于此,文中提出多特征融合的方法,使用卷积神经网络从人脸图像的不同线索中学习多个特征来进行活体检测,深度图在空间上能够区分真假人脸之间的深度信息;光流图在时间上能够区分真假人脸之间的动态信息;残差噪声图根据真人脸的一次成像和假冒人脸的二次成像噪声成分的不同进行区分。文中融合3种特征,不仅利用空间、时间多维度线索弥补了单一线索的不足,同时也提高了模型的泛化能力。相比现有的方法,所提方法无论是在同一个数据库还是跨数据库的情况下,均有较好的实验结果。具体而言,所提方法在CASIA数据集、REPLAY-ATTACK数据集和NUAA数据集上的错误率分别为0.11%,0.06%和0.45%。

关键词:人脸识别;活体检测;多特征融合
中图法分类号 TP391.41

Face Anti-spoofing Algorithm Based on Multi-feature Fusion

LUAN Xiao and LI Xiao-shuang
College of Computer Science,Chongqing University of Posts and Telecommunications,Chongqing 400065,China
Chongqing Key Laboratory of Image Cognition,Chongqing University of Posts and Telecommunications,Chongqing 400065,China

Abstract In recent years,with the development of face recognition systems,various spoofing methods that impersonate legitimate users appear. Face anti-spoofing detection method based on a single clue no longer meets the requirements of current face recognition system under complex environment. Based on this,we propose to use a convolutional neural network to learn multi-feature from different clues of face images,and to fuse the depth map,the face optical flow map,and the residual noise map to perform liveness detection. The depth map can distinguish the depth information between real and fake faces in space,the optical flow map can distinguish the dynamic information between real and fake faces in time,the residual noise map is based on the one-time imaging of the real face and the fake face. The secondary imaging noise components are distinguished by different components,and the three features are merged to use space,time and multi-dimensional clues to make up for the shortcomings of a single clue,and also improve the generalization ability of the model. Compared with the existing methods,our method shows promising results both on the single database and cross-databases. Specifically,equal error rate (EER) of our method on databases of CASIA,REPLAY-ATTACK and NUAA can achieve 0.11%,0.06% and 0.45%,respectively.

Keywords Face recognition,Spoofing detection,Multi-feature fusion

1 引言

在过去的二十年中,人脸识别已经取得了长足的发展,然而面向现实的人脸识别系统仍然面临着诸多的挑战[1]。例如人脸活体检测,人脸活体检测指系统会根据摄像头捕捉到的人脸去辨别其是否为活体状态,通常可视为二分类问题。活体人脸图片和假冒人脸图片在图像纹理信息、图像光谱信息、图像运动信息、图像深度信息等方面都存在一定的差异。利用这些差异可以设计不同的活体检测方法,对真假人脸做出判断。近年来,人脸活体检测算法可以归类为3个方面:基于手工设计特征的方法、基于深度学习的方法和基于特征融合的方法[2-3]。

基于手工设计特征的方法包括基于纹理信息分析的方法[4-6]、基于深度信息的方法[7]、基于光谱信息的方法、基于运动信息的方法[8],以及其他特征的方法(如基于热红外图的方法[9]、基于图像质量的方法[10]和基于上下文线索的方法[11]等)。虽然基于手工设计特征的方法可以取得不错的精度,但也存在局限性,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。与手工设计特征的方法相比,深度学习的方法有更多的优势,它以数据驱动的学习方式更容易学习到一般性特征,能够应对复杂以及未知的欺骗手段,在模型的鲁棒性以及泛化能力上可以达到更好的效果。2014年Yang等[12]首次将卷积神经网络(Eonvolution Neural Network,CNN)应用于人脸活体检测,并且在论文中指出深度学习的方法相比手工特征,可以捕获更多的判别线索。此后,众多深度学习的方法不断涌现。例如,文献[13]提出引入迁移

基金项目:国家自然科学基金(61801068)
This work was supported by the National Natural Science Foundation of China(61801068).
通信作者:栾晓(luanxiao@cqupt.edu.cn)

学习的方法，Manjani 等[14]提出针对面具攻击的方法，以及 Gan 等[15]利用三维卷积神经网络(three-dimensional CNN，3DCNN)从短视频中提取连续视频帧的时空特征方法等。

基于特征融合的方法利用多种模态下的信息进行融合，目的是打破单个模态信息的局限性，提高活体检测的准确度。Tronc 等[16]提出一种融合纹理信息和运动信息的活体检测方法。Komulainen 等[17]对文献[16]中的方法加以改进，检测效率进一步得到提升。此外，Wang 等[7]利用深度信息和纹理信息，也取得了很好的效果。Tang 等[18]提出使用 CNN 从人脸图像的不同信息中学习多个深层特征(包括时间特征、颜色特征、局部特征等)来进行活体检测，同样取得了较好的效果。由此可见，融合不同特征不仅可以弥补单个模态信息的不足，提升检测效果，还可以提升算法的鲁棒性以及泛化能力。

近年来，深度学习在计算机视觉领域得到了广泛应用，深度特征相对于传统手工特征而言通用性更强，在公开的数据集上，目前基于深度学习的特征方法也取得了最好的性能，越来越多的研究者更倾向于利用深度特征学习算法去解决人脸活体检测面临的问题。此外，活体人脸与假冒人脸之间存在很大的差异，单一的特征差异具有一定的局限性，很难在复杂的环境中保证模型的高识别率以及鲁棒性。因此，可以利用深度学习的方法对数据进行特征的提取，再将多种模态的特征信息进行融合，利用融合后的特征差异进行分类，不仅有望提升识别精度，还可以提高算法的鲁棒性和泛化能力。基于上述分析，本文将采用深度学习算法结合特征融合的方式，来充分利用互补的信息，以得到最优的结果。

目前，基于人脸的活体检测方法使用的主要线索是深度信息、纹理信息和运动信息。由于大多数攻击都使用打印的照片或重放的视频，因此深度信息可能是有用的线索。Wang 等[7]将深度信息和文本信息相结合，使用局部二值模式(Local Binary Pattern，LBP)特征来表示 Kinect 捕获的深度图像，并使用 CNN 从 RGB(Red，Green，Blue)图像中学习纹理信息。此方法需要额外的深度摄像头，通常无法用于许多应用程序。与其相比，Atoum 等[19]不需要使用深度传感器来估计深度信息，而是将深度信息与从人脸区域提取的外观信息融合起来，以区分假脸和真脸。除深度信息外，纹理或运动信息也已广泛用于面部活体检测[20]。Smiatacz 等[22]计算人脸转动所产生的光流值，通过支持向量机(Support Vector Machines，SVM)对这些光流值进行训练和分类；Boulkenafet 等[20]使用不同的颜色空间来探索颜色纹理信息，并从每个空间通道提取 LBP 特征，然后将所有空间通道的 LBP 特征连接起来，输入支持向量机进行分类。

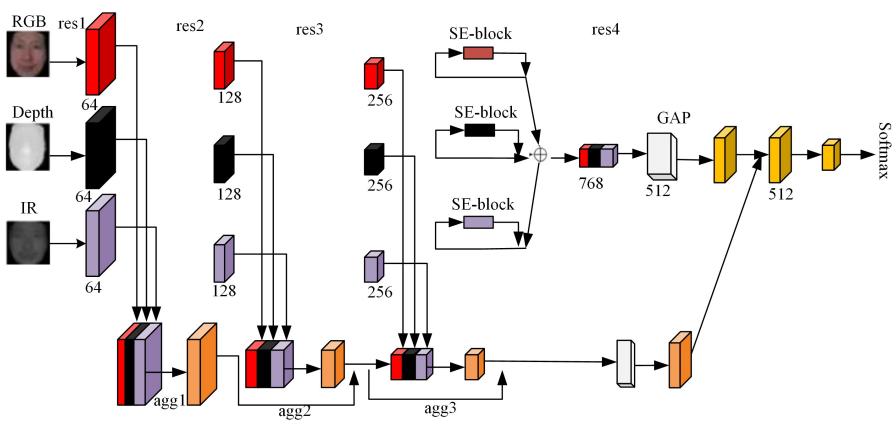
虽然现有的方法探索了人脸活体检测的各种信息，但它们大多只使用了面部的单一线索。尽管有些方法[7,17-19,21]探索了人脸的多个线索来进行活体检测，但它们只采用手工设计特征，具有一定的局限性。这种情况下需要一些辅助信息，本文利用人脸的时间信息、空间信息作为辅助信息，然后把时间信息、空间信息和纹理信息融合，用于人脸活体检测。

目前普遍使用的提取人脸的时间信息有两种。一种是基于人机交互的方法，Singh 等[8]利用眨眼和嘴部动作来进行人脸的活体检测。通过计算眼部区域的面积和牙齿周围 HSV(Hue，Saturation，Value)来判断眼睛是否睁开和嘴部是否张开，基于人机交互的方法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。第二种就是本文采用的脸部光流的方法，光流法利用图像序列中的像素强度的时域变化和相关性来确定各自像素位置的“运动”，从图像序列中得到各个像素点的运行信息，一般采用高斯差分滤波器、LBP 特征和支持向量机进行数据统计分析。同时，光流场对物体运动比较敏感，利用光流场可以统一检测眼球移动和眨眼。这种活体检测方式可以在不需要人机交互的情况下实现盲测，体验感较好。

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，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。

残差噪声图启发于图像去噪和图像去抖动，无论是噪声图还是模糊图，都可看成是在原图上进行加噪声运算或者模糊运算，以实现去噪和去抖动，其本质是估计噪声分布和模糊核，从而重构回原图。Liu 等[23]采用噪声来区分活体类型和假冒类型，实验结果较好。

2019 年 Parkin 等[24]利用近红外图、真彩图和深度图提出了一种多模态融合方法，模型如图 1 所示，该方法的模型基于经典的 ResNet18[25]做基础网络骨架，加入了 SENet[26]模块。SENet 的核心思想在于通过网络根据损失函数去学习特征权重，使得采用有效的特征图权重大、无效或效果小的特征图权重小的方式来训练模型能达到更好的结果。该方案在 2019 年人脸防伪检测挑战赛上一举夺魁。



注：GAP 全局平均池化；⊕级联

图 1 基于近红外图、真彩图和深度图融合的活体检测网络流程图[24]

Fig. 1 Outline of a network based on the fusion of near-infrared images，color images and depth images[24]

但是，上述方案存在一些局限性：首先，在公开的数据集方面，同时包含近红外图、真彩图和深度图的数据集较少，该方法不能进行大量的对比实验。其次，在特征选取方面，近红外图和深度图在该方法中都是通过额外的设备进行采集，产生了额外的开销且近红外图受环境光的影响较大，不同的光照环境下提取的特征图差异可能较大。另外，对于高质量的假冒图片，在纹理上很接近活体真彩图，提取的特征差异不大。最后，该方法的训练测试数据都是来自于 CASIA-SURF 数据集[27]，没有进行跨数据集的对比实验，未能充分验证该方法的泛化性能。基于此，本文考虑使用不需要专业设备进行采集就能获得的残差噪声图、深度图和光流图作为图 1 的输入，来进行多个深层特征的融合，并分别在同一个数据集和跨数据集上验证本文方法的效果。

2　本文方法

受到文献[24]的启发，本文提出利用残差噪声图、深度图和光流图 3 种特征的人脸图像活体检测算法。具体而言，该算法是从不同纹理空间中学习基于纹理的特征，从图像序列中学习时间特征，从深度特征中学习 3D 特征，考虑到多个特征之间具有互补性，深度图和光流图可以作为残差噪声图的辅助信息，我们进一步提出了一种采用残差噪声图、深度图和光流图融合特征的策略。下文依次介绍如何提取残差噪声图、光流图和深度图，然后将 3 种特征融合。

2.1　提取噪声图

根据重采样导致假冒人脸会出现的条带效应和摩尔纹等噪声现象，可以将一幅图像分解为代表图像本质成分的低频分量和代表噪声成分的高频分量。获取图像的低频分量，使用低通滤波，如均值滤波、高斯滤波、导向滤波等对图像进行滤波即可，本文使用高斯滤波对图像进行操作，如式(1)所示：

$$B=f(I) \tag{1}$$

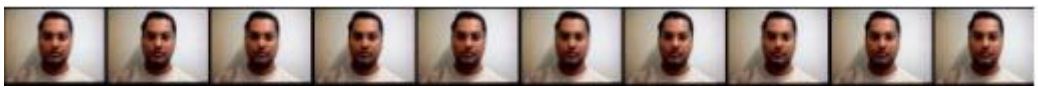
其中，I 表示要分解的图像，$f(I)$表示低通滤波操作，B 为提取低频分量后使用原图像减去低频分量，即为噪声图，如式(2)所示：

$$D=I-B \tag{2}$$

其中，D 表示提取的噪声图，此种分解方法为加性分解，活体人脸和假冒人脸可以通过得到的噪声图进行二分类。图 2 给出了活体和假冒人脸类型的残差噪声图。从图中可以看出，假冒人脸在二次成像的过程中会比活体人脸一次成像产生更多的摩尔条纹[28]和模糊效果。

(a)活体人脸

(b)活体人脸残差噪声图



(c)假冒人脸

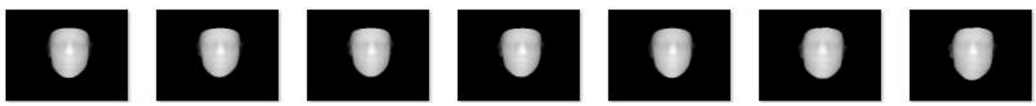
(d)假冒人脸残差噪声图

图 2　残差噪声图

Fig. 2　Residual noise maps

2.2　提取深度图

深度图是用于表示 3D 图特征的 2D 图，本文利用位置映射网络 PRNet[29]来实现，活体人脸用 PRNet 生成深度图，假冒人脸用全黑的平面图来训练。活体和假体人脸的深度图如图 3 所示，由图可知真实的人脸是三维立体的，而伪造人脸的图片仅仅是一个平面，由此来区分和筛选真实和假冒人脸图。



(a)活体深度图

(b)假冒人脸深度图

图 3　活体和假冒人脸深度图

Fig. 3　Depth maps of live and spoof faces

2.3　提取光流图

Lucas-Kanade(L-K)光流法最初于 1981 年由 Lucas 等提出[30]。L-K 光流法是一种两帧差分的稀疏光流估计算法，它假设在一个小的空间邻域内运动矢量保持不变，即光流在像素点的邻域是一个常数，然后使用加权最小二乘法对邻域中的所有像素点求解基本的光流方程。光流场对物体运动比较敏感，而真实人脸的眼部在姿势校正和眨眼过程中与照片产生不一样的光流，利用 L-K 算法计算输入视频序列中相邻两

帧的光流场，求得光流幅值，得到幅值较大的像素点数所占的比重，本文采用 L-K 光流法提取的活体人脸和假冒人脸如图 4 所示，真实人脸和假冒人脸在做眨眼运动时，真人脸比假冒人脸能得到不一样的光流值，以此可以区分真实人脸和假冒人脸。

(a) 活体人脸光流图

(b) 假冒人脸光流图

图 4 人脸光流图

Fig. 4 Optical flow images of different faces

2.4 特征融合

从上述分析得到的 3 种特征图中，残差噪声图虽然可以从二次成像的噪声图中区分出真实人脸和假冒人脸，但是该特征图需要高质量图片，并且该特征容易受到光照的影响；提取真假人脸的深度图受光照的影响较小，但是容易受到视频的欺骗；光流场对物体运动比较敏感，利用光流场可以统一检测眼球移动和眨眼。这种活体检测方式可以在不需要人机交互的情况下实现盲测，体验感较好。光流图和深度图可以从时间和空间上提取人脸的不同特征，同时还包含一些额外的有用信息用于活体检测，基于此考虑，残差噪声图从纹理上提取特征。活体检测技术主要有两种，一种是传统的人工特征模式识别方法，另一种则是近几年兴起的深度学习方法，后者被证实在多个测试数据集上性能远超前者，因此传统的人工特征识别活体检测方法基本被淘汰。但是本文从人工特征模式识别方法中获得灵感，由于活体检测不管是真人还是假人，它们在训练和测试数据集中的数据分布都存在较大差距，我们不应该直接用人工模式处理后的特征进行活体检测，因此，本文结合人工特征和神经网络学习到的特征，提高算法的泛化能力。

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。Zhang 等[25]介绍了一种用于多模态人脸活体检测方法。该方法使用 ResNet-18[25]作为骨架分别处理这 3 种模式，然后从每个分支的最后一层对特征进行重新加权，以选择信息量更大的通道特征，同时抑制信息量较少的特征，将重新加权的特征连接起来，并通过另外两个残差块进行处理，最后全局平均池化和两个连续的全连接层构成了网络结构。文献[24]把该方法加以改进作为网络框架，本文也采用该网络结构作为基本框架来融合这 3 种特征。

3 实验结果

3.1 数据集和评估协议

本文在 NUAA[31]、CASIA[32] 和 REPLAY-ATTACK[33] 3 个公开数据集上对人脸活体检测算法进行了实验。

3.1.1 NUAA 数据集

NUAA 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 3 个不同的环境下采集了 15 个个体的活体人脸和假冒人脸的数据，活体人脸是在人脸上一次采集的数据图片，假冒人脸是对照片进行二次采集或者多次采集。为了让活体人脸与假冒人脸更相似，在采集过程中统一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。采集的假冒人脸数据一共分为 3 种：6.8 cm×10.2 cm 与 8.9 cm×12.7 cm 两种大小的照片纸上打印的彩色照片，以及普通 A4 打印纸上打印的彩色照片。数据集录制了正面平展照片，同时对照片弯曲、沿水平轴旋转、垂直轴旋转等情况进行了录制。

3.1.2 CASIA 数据集

CASIA 包含 600 个真实访问和欺骗攻击尝试的录像，这些录像来自 50 个真正的受试者，对应于 20 个训练对象和 30 个测试对象。通过使用具有 3 种不同相机分辨率的设备来采集活体面部和假冒面部。该测试集可以分为 3 类(包含 7 个场景)：图像质量测试(低质量、正常质量、高质量)，假冒人脸测试(扭曲的照片攻击、剪切照片攻击、视频攻击)，整体测试。

3.1.3 REPLAY-ATTACK 数据集

Replay-Attack 数据集共有 1 300 个视频，包括 50 个人。每段视频至少 9 s，所用的摄像头是 Macbook 笔记本电脑的网络摄像头，分辨率为 320 * 240。视频被保存为 Mov 格式，每秒 25 帧。光照条件有两种：一种是受控制的，另一种是不受控制的。受控条件是办公室光照，关闭窗帘，背景相同；不受控条件是办公室光照关闭，打开窗帘，背景复杂。

3.1.4 评估协议

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。跨数据集测试指训练集和测试集不是来源于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冒人脸的识别率。评估指标采用文献[34]中提到的评估方式，在 CASIA 以及 REPLAY-ATTACK 数据集上进行评估。本文采用的主要有错误接受率(False Acceptance Rate，FAR)，错误拒绝率(False Rejection Rate，FRR)，等错误率(Equal Error Rate，EER)以及半错误率(Half Total Error Rate，HTER)。

FAR 指算法把假冒人脸判断成活体人脸的比率。FRR 指算法把活体人脸判断成假冒人脸的比率。FAR 与 FRR 的计算式如下：

$$FAR=\frac{N_{s2l}}{N_s} \tag{3}$$

$$FRR=\frac{N_{l2s}}{N_l} \tag{4}$$

其中，N_{s2l} 表示假冒人脸判断为活体人脸的次数，N_s 表示假冒人脸攻击的总次数，N_{l2s} 表示活体人脸判断为假冒人脸的次数，N_l 表示活体人脸检测的总次数。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，ROC 曲线上 FRR 与 FAR 相交处即为 EER。HTER 是 FAR 与 FRR 和的一半。

3.2 实验设置

本文所有代码都在 PyTorch 中实现，并且模型在 NVIDIA 1080Ti 上进行了训练。我们对每个模型进行了 30 轮的训练，初始学习率为 0.01，每一次处理 128 张图片。针对测试训练模型采用了相同的学习策略。为了证明本文算法的有效性，将其与以下主流算法进行对比。传统特征方法有 LBP[32]，用于角点检测的 DoG[32] (difference of gaussian)，二

维空间到三维空间的拓展的 LBP-TOP[33]（local binary patterns from three orthogonal planes），颜色纹理的方法[20]（color texture）等；基于深度学习的方法有 CNN[12]，3DCNN[14]，一种基于双流 CNN 的人脸反欺骗方法 Patch＋DepthCNN[19]；还有基于特征融合的方法[35]，即采用 RNN（Recurrent Neural Network）模型对人脸图像训练得到深度图，并对远程光电体积描记法（Remote Photoplethysmography，rPPG）信号进行序列监控得到心率统计量，然后进行特征融合。

3.3　实验结果与讨论

3.3.1　单个数据集实验结果分析

为了评估本节提出算法的检测性能，本节在 CASIA、REPLAY-ATTACK 和 NUAA 数据集上进行实验分析，最终结果如表 1 和表 2 所列。

表 1　在 CASIA 与 REPLAY-ATTACK 数据集上的实验结果

Table 1　Results of intra-test on CASIA and Replay-Attack

（单位：%）

Algorithm	CASIA EER	REPLAY-ATTACK EER
LBP[32]	18.2	13.9
DoG[32]	17.0	—
Motion Magn[36]	14.4	0.0
LBP-TOP[33]	10.0	7.9
CNN[12]	7.4	6.1
DMD＋LBP[37]	21.8	5.3
IDA and motion[38]	5.8	0.83
Color LBP[39]	2.1	0.4
VLBC[40]	6.5	1.7
3D CNN[14]	5.2	0.16
FD-ML-LPQ-FS[41]	4.6	5.6
Patch＋DepthCNN[19]	2.7	0.8
SURF[42]	2.8	0.1
PreDRS＋LSTM[43]	1.22	1.03
ST Mapping[44]	1.1	0.78
LiveNet[45]	4.59	—
Color texture[32]	4.6	1.2
DSGN[46]	3.42	0.13
Deep LBP[47]	2.3	0.1
3D CNN ＋geneloss[48]	1.4	0.3
Our method	0.11	0.06

表 2　在 NUAA 数据集上的实验结果

Table 2　Results on NUAA dataset

（单位：%）

Algorithm	EER
CF＋HOG＋HSC＋GLCM- PLS[49]	8.20
LBP＋Gabor Wavelets＋HOG-SVM[50]	1.10
LBPV-x^2[51]	11.97
LBP＋LPQ＋HOG- SVM[52]	1.90
MLPQ-TOP＋MBSIF-TOP- KDA[53]	1.80
LBP[32]	1.80
Our method	**0.45**

总结得出，LBP，LPQ（Local Phase Quantization）等描述符从 HSV，YCbCr 颜色空间图形中抽取的颜色纹理特征虽然很重要，但是该方法易受到光照、图像分辨率等的影响，在视频攻击的情况下效果差；光流法需要以视频为输入，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；基于深度特征的方法模型参数多，计算量大，训练时间长，易过拟合，且对数据量和数据丰富性有高要求。本文利用多个深层特征融合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，本文方法在 CASIA 数据集、REPLAY-ATTACK 数据集和 NUAA 数据集上的错误率分别为 0.11%，0.06%和 0.45%，验证了该算法能取得较好的实验结果。

3.3.2　跨数据集实验结果

为了进一步验证本文算法在跨数据集训练和测试时的泛化能力，本节进行了跨数据集测试。实验包括两个部分，实验 1 指在 CASIA 数据集上进行训练，在 REPLAY-ATTACK 数据集上进行测试；实验 2 指在 Replay-Attack 数据集上进行训练，在 CASIA 数据集上进行测试，本文算法与其他算法的对比结果如表 3 所列。

表 3　跨数据集上的实验结果对比

Table 3　Results of inter-teston CASIA and Replay-Attack

（单位：%）

Algorithm	HTER（CASIA for training and Replay-Attack for testing）	HTER（Replay-Attack for training and CASIA for testing）
LBP[32]	55.9	57.6
Motion[54]	50.2	47.9
LBP-TOP[33]	50.1	47.0
CNN[12]	48.5	45.5
Color LBP[38]	30.3	37.7
Texture＋Motion[55]	12.4	31.6
FD-ML-LPQ-FS[41]	50.25	42.59
ST Mapping[43]	35.05	40.22
Noise Modeling[23]	28.5	41.1
DeepImg＋rPPG[35]	27.6	28.4
Domain Adap[56]	27.4	36.0
Color texture[21]	9.6	39.2
Our method	**30.0**	**32.11**

在活体检测数据集中，分别在相同的条件（照明、温度和头部姿势）下收集了训练数据和测试数据。因此，在数据库内部的人脸活体检测中的出色表现是显而易见的。但是，相同的算法在跨数据库测试中难以正确分辨出活体或者假冒。跨数据库人脸活体检测测试中其他算法性能下降的原因是，测试数据库中的条件（光照、头部姿势）与训练数据库完全不同。但是，与其他最新方法相比，本文算法在跨数据库中半错误率分别为 30%和 32.11%，证明本文的算法有较好的鲁棒性。

3.3.3　消融性实验结果

为了验证这 3 种特征的实验结果，本文还做了消融性测试，用于观察每种特征的贡献度。实验结果如图 5 所示。

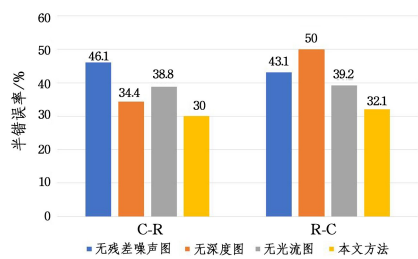


图 5　消融性实验结果

Fig. 5　Results of ablation experiment

图 5 中，C-R 表示在 CASIA 数据集上训练，在 REPLAY-ATTACK 上测试，而 R-C 表示在 REPLAY-ATTACK 上训练，在 CASIA 上测试。实验结果表明，3 种特征融合比两种特征融合取得了更好的结果，说明融合不同的特征信息可以弥补单一信息的不足，能有效地提高活体检测的准确率，降低错误率，在跨数据集实验中也可以得到较好的实验结果，在 REPLAY-ATTACK 数据集上，噪声图和光流图的贡献度更大

一些，而在 CASIA 中，噪声图和深度图的贡献度更大，说明不同特征对于不同数据集的判别能力不一样，这也表明多个深层特征融合的必要性，证明该特征融合算法具有较好的鲁棒性。

结束语 本文提出了一种多特征融合的算法，该算法可以综合提取残差噪声图、人脸光流图和深度图特征的优势，解决单一线索进行活体检测的局限性问题，减少高质量人脸的类内差异大的影响，提取高判别力的特征，提高算法的准确率和通用性。目前基于人脸图像的活体检测方法存在提取的特征泛化能力不强、由于类内差异大导致算法性能下降、难以处理跨数据集的情况(无论是训练集中已知的人脸类别还是训练集中未知的人脸类别)。不同的采集设备、不同的外界环境都会影响算法的性能，这些是人脸活体检测算法实际应用中无法回避的问题，因此如何提取泛化能力强的特征，以及如何提高活体检测算法在跨数据集的通用性仍是值得研究的问题。

参 考 文 献

[1] LI X X, LING R H. Overview of occlusion face recognition: from subspace regression to deep learning[J]. Chinese Journal of Computers, 2017, 9(2): 634-639.

[2] WU W F N, LING X. Blind color image quality assessment base on color characteristics[J]. Computer Science, 2017, 44(6A): 151-156.

[3] DENG X, WANG H C, ZHAO L J, et al. A review of the research methods of face recognition anti-spoofing detection[J]. Application Research of Computers, 2020, 37(9): 2579-2585.

[4] ZHONG R, WU H Y, HE Y. Fast face recognition algorithm based on local fusion feature and hierarchical incremental tree [J]. Computer Science, 2018, 45(22): 308-313.

[5] MA Y K, WU L F, JIAN M, et al. An adversarial sample generation algorithm for face anti-spoofing detection[J]. Journal of Software, 2019, 30(2): 469-480.

[6] DE FREITAS PEREIRA T, ANJOS A, DE MARTINO J M, et al. LBP- TOP based countermeasure against face spoofing attacks[C]// Asian Conference on Computer Vision. Springer, Berlin, Heidelberg, 2012: 121-132.

[7] WANG Y, NIAN F, LI T, et al. Robust face anti-spoofing with depth information[J]. Journal of Visual Communication and Image Representation, 2017, 49: 332-337.

[8] SINGH A K, JOSHI P, NANDI G C. Face recognition with liveness detection using eye and mouth movement-[C]// Proceedings of the 2014 International Conference on Signal Propagation and Computer Technology. Piscataway: IEEE, 2014: 592-597.

[9] BHATTACHARJEE S, MOHAMMADI A, MARCEL S. Spoofing deep face recognitionwith custom silicone masks[C]// Proceedings of the IEEE 9th International Conference on Biometrics: Theory, Applications and Systems. Piscataway: IEEE, 2018: 1-7.

[10] GALBALLY J, MARCEL S, FIERREZ J. Image quality assessment for fake biometric detection: application to iris, fingerprint, and face recognition[J]. IEEE Transactions on Image Processing, 2014, 23(2): 710-724.

[11] KOMULAINEN J, HADID A, PIETIKÄINEN M. Context based face anti-spoofing[C]// Proceedings of the IEEE 6th International Conference on Biometrics: Theory, Applications and Systems. Piscataway: IEEE, 2013: 1-8.

[12] YANG J, LEI Z, LI S Z. Learn convolutional neural network for face anti-spoofing[J]. arXiv: 1408.5601, 2014.

[13] LUCENA O, JUNIOR A, MOIA V, et al. Transfer learning using convolutional neural networks for face anti-spoofing[C]// Proceedings of the 2017 International Conference Image Analysis and Recognition, LNCS 10317. Cham: Springer, 2017: 27-34.

[14] MANJANI I, TARIYAL S, VATSA M, et al. Detecting silicone mask-based presentation attack via deep dictionary learning[J]. IEEE Transactions on Information Forensics and Security, 2017, 12(7): 1713-1723.

[15] GAN J, LI S, ZHAI Y, et al. 3D convolutional neural network based on face anti-spoofing[C]// Proceedings of the 2nd International Conference on Multimedia and Image Processing. Piscataway: IEEE, 2017: 1-5.

[16] TRONCI R, MUNTONI D, FADDA G, et al. Fusion of multiple clues for photo-attack detection in face recognition systems [C]// Proceedings of the 2011 IEEE International Joint Conference on Biometrics. Piscataway: IEEE, 2011: 1-6.

[17] KOMULAINEN J, HADID A, PIETIKÄINEN M, et al. Complementary countermeasures for detecting scenic face spoofing attacks[C]// Proceedings of the 2013 IEEE International Conference on Biometrics. Piscataway: IEEE, 2013: 1-7.

[18] TANG Y, WANG X, JIA X, et al. Fusing multiple deep features for face anti-spoofing[C]// Proceedings of t-he 2018 Chinese Conference on Biometric Recognition, LNCS 10996. Cham: Springer, 2018: 321-330.

[19] ATOUMY, LIU Y, JOURABLOO A, et al. Face anti-spoofing using patch and depth-based CNNs[C]// 2017 IEEE International Joint Conference on Biometrics. IEEE, 2017: 319-328.

[20] BOULKENAFET Z, KOMULAINEN J, HADID A. Face spoofing detection using color texture analysis[J]. IEEETransactions on Information Forensics and Security, 2016, 11(8): 1818-1830.

[21] FENG L, PO L M, LI Y, et al. Integration of image quality and motion cues for face anti-spoofing: A neural net-work approach [J]. Journal of Visual Communication and Image Representation, 2016, 38: 451-460.

[22] SMIATACZ M. Liveness Measurements Using optical flow for biometric person authentication[J]. Metrology and Measurement Systems, 2012, 19(2): 257-268.

[23] JOURABLOO A, LIU Y J, LIU X M. Face de-spoofing: anti-spoofing via noise modeling[C]// European Conference on Computer Vision. 2018: 6-7.

[24] PARKIN A, GRINCHUK O. Recognizing multi-m-odal face spoofing with face recognition networks[C]// Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops. 2019: 1617-1623.

[25] HE K M, ZHANG X Y, REN S Q, et al. Deep residual learning for image recognition[C]// Proc of The IEEE Conference on Computer Vision and Pattern Recognition. Piscataway, NJ: IEEE Press, 2016: 770-778.

[26] HU J, SHEN L, SUN G. Squeeze-and-excitation networks[C]// Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. 2018: 7132-7141.

[27] ZHANG S, WANG X, LIU A, et al. A dataset and benchmark for large-scale multi-modal face anti-spoofing[C]// Proceedings of the IEEE Conference on Computer Visionand Pattern Recognition. 2019: 919-928.

[28] GARCIA D C, DE QUEIROZ R L. Face-spoofing 2D-detection based on moire-pattern analysis[J]. IEEE Transactions on In-

formation Forensics and Security,2015,10(4):778-786.
[29] FENG Y,WU F,SHAO X,et al. Joint 3d Facereconstruction and dense alignment wit. position map regression network [C]// European Conference on Computer Vision. 2018:557-574.
[30] BAKER S,MATTHEWS I. Lucas-Kanade 20 years on:A unifying framework[J]. International Journal of Computer Vision, 2004,56(3):221-255.
[31] TAN X Y,LI Y,LIU J,et al. Face liveness detection from a single image with sparse low rank bilinear discriminative model [C]// Proceedings of European Conference on Computer Vision. Crete,Greece:Springer,2010:504-517.
[32] ZHANG Z W,WAN J J,LIU S F,et al. A face antispoofing database with diverse attacks[C]// Proc of IEEE the 5th IAPR International Conference on Biometrics. Piscataway, NJ: IEEE Press,2012:26-31.
[33] CHINGOVSKA I,ANJOS A,MARCEL S. On the effectiveness of local binary patterns inface anti-spoofing[C]// Proceedings of the 11thInternational Conference of the Biometrics Special Interest Group. Darmstadt,Germany:IEEE,2012:1-7.
[34] JIANG F L,LIU P C,ZHOU X D. A Review on face anti-spoofing[J]. Acta Automatica Sinica,2019,11(5):1-24.
[35] LIU Y,JOURABLOO A,LIU X. Learning deep models for face anti-spoofing:Binary or auxiliary supervision[C]// Proceedings of the IEEE Conference Oncomputer Vision and Pattern Recognition. 2018:389-398.
[36] BHARADWAJ S,DHAMECHA T I,VATSA M,et al. Computationally efficient face spoofingdetection with motion magnification[C]// Proceedings of Conference on Computer Vision and Pattern Recognition Workshops. USA:IEEE,2013:5-110.
[37] GHCHANDANA P. Image quality assessment for fake biometric detection[J]. International Journal scientific Research & Development,2014,2(3):1417-1419.
[38] TIRUNAGARI S,POH N,WINDRIDGE D,et al. Detection of face spoofing using visual dynamics[J]. Transactions on Information Forensics and Security,2015,10(4):762-777.
[39] KOMULAINEN J,HADID A,MATTI P. Face spoofing detection using dynamic texture[C]// Asian Conference on Computer Vision. Berlin:Springer,2012:5-6.
[40] 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[J]. IEEE Transactions on Multimedia,2018,20(3):552-566.
[41] BENLAMOUDI A,AIADIK E,OUAFI A,et al. Face anti-spoofing based on frame difference and multilevel representation[J]. Journal of Electronic Imaging,2017,26(4).
[42] BOULKENAFET Z,KOMULAINEN J,HADID A. Face anti-spoofing using speeded-up robust features and fisher vector encoding[J]. IEEE Signal Processing Letters,2017,24(2):141-145.
[43] TU X K,FANG Y C. Ultra-deep neural network for face anti-spoofing[C]// Proceedings of International Conference on Neural In-formation Processing. Guangzhou,China:Springer,2017: 686-695.
[44] LAKSHMINARAYANA N N,NARAYAN N,NAPP N,et al. A discriminative spatiotemporal mapping of face for liveness detectionn [C]// Proceedings of IEEE International Conference on Identity, Security and Behavior Analysis. New Delhi, India: IEEE,2017:1-7.
[45] REHMAN Y A U,PO L M,LIU M Y. LiveNet:Improving features generalization for face liveness detection using convolution neural networks[C]// Expert Systems with Applications. 2018, 108:159-169.
[46] NING X,LI W,WEI M,et al. Face anti-spoofing based on deep stackgeneralization networks[C]// 7th International Conference on Pattern Recognition Applications and Methods. 2018:317-323.
[47] LI L,FENG X Y,JIANG X Y,et al. Face anti-spoofing via deep local binary patterns[C]// Proceedings of IEEE International Conference on Image Processing. Beijing, China: IEEE, 2017: 101-105.
[48] LI H,HE P,WANG S,et al. Learning generalized deep feature representation for face anti-spoofing[J]. IEEE Transactions on Information Forensics & Security,2018,13(99):2639-2652.
[49] MENOTTI D,CHIACHIA G,PINTO A,et al. Deep representation-ns for iris,face,and fingerprint spoofing detection[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(4):864-879.
[50] MATTA J. Face spoofing detection from single images using texture and local shape analysis[J]. Iet Biometrics,2012,1(1): 3-10.
[51] KOSE N,DUGELAY J L. Classification of captured and recaptured images to detect photograph spoofing[C]// Proceedings of International Conference on Informatics,Electronics and Vision. Dhaka,Bangladesh:IEEE,2012:1027-1032.
[52] YANG J,LEI Z,LIAO S,et al. Face liveness detection with component dependent descriptor[C]// International Conference on Biometrics. IEEE,2013:1-6.
[53] ARASHLOO S R,KITTLER J,CHRISTMAS W. Face spoofing detection based on multiple descriptor fusion using multiscale dynamic binarized statistical image features[J]. IEEE Transactions on Information Forensics & Security,2017,10(11):2396-2407.
[54] DE FREITAS PEREIRA T,ANJOS A,DEMARTINO J M, et al. Can face anti-spoofing countermeasures work in a real world scenario? [C]// Proceedings of International Conference on Biometrics. Madrid,Spain:IEEE,2013:1-8.
[55] PATEL K,HAN H,JAIN A K. Cross-databasef-ace anti-spoofing with robust feature representation[C]// Proceedings of Chinese Conference on Biometric Recognition. Chengdu, China: Springer,2016:611-619.
[56] LI H L,LI W,CAO H,et al. Un-supervised domain adaptation for face anti-spoofing[J]. IEEE Transactions on Information Forensics and Security,2018,13(7):1794-1809.

LUAN Xiao, born in 1983, Ph.D, associate professor, is a member of China Computer Federation. His main research interests include face recognition, medical image processing and machine learning.