国家信息中心主办
中国科技核心期刊

第 8 卷 第 5 期 2022 年 5 月
Vol.8 No.5 May 2022

信息安全研究

Journal of Information Security Research

信息安全研究

第八卷 第五期

CN 10-1345/TP
ISSN 2096-1057
9 772096 105228 05>
邮发代号：2-41 定价：38.00 元

二〇二二年五月

Xinxi Anquan Yanjiu

信息安全研究

（月刊　2015 年创刊）

第 8 卷第 5 期（总第 80 期）2022 年 5 月

本刊是中国科技核心期刊，入选 CCF T3 优秀期刊目录，全文被《中国核心期刊（遴选）数据库》《中文科技期刊数据库》《CNKI 中国期刊全文数据库》《超星期刊域出版平台》《博看网》收录。

主管单位　国家发展和改革委员会
主办单位　国家信息中心

出版单位　《信息安全研究》杂志社
地址　北京市西城区三里河路 58 号
邮编　100045
电话　+86(10)68557385
网址　http://www.sicris.cn
电子信箱　ris@cei.cn

社长　李新友
主编　吕　欣
副主编　马修军
融媒体主编　崔传桢

出版日期　每月 5 日
国际标准连续出版物号　ISSN 2096-1057
国内统一连续出版物号　CN 10-1345/TP
广告经营许可证　京西市监广登字 20210016 号
印刷单位　北京博海升彩色印刷有限公司
国内发行　北京市报刊发行局
订购处　全国各地邮电局（所）
邮发代号　2-41
定价　38.00 元

协办单位　亚信安全　龙象之本
合作单位　360 集团　安恒信息
恒安嘉新　航天云网
绿盟科技　蚂蚁集团
明朝万达　奇安信集团
青藤云安全　数字认证
天融信集团　信安世纪

»区块链与可信交易专题

»技术应用

CONTENTS 目次

Issue on Blockchain and Trusted Transaction

Technical Applications

Journal of Information Security Research

Vol.8 No.5 May 2022

Publishing Period: Monthly

Date of Publication: 5th day of each month

International Standard Serial Number: ISSN 2096-1057

Issues of Domestic Unit: CN 10-1345/TP

Director: Li Xinyou

Editor-in-Chief: Lü Xin

Directed by: National Development and Reform Commission

Sponsored by: The State Information Center

Published by: Journal of Information Security Research

Address: No.58 Sanlihe Road, Xicheng District, Beijing

Zip Code: 100045

Website: http://www.sicris.cn

E-mail: ris@cei.cn

Distributor: Beijing Press and Publication Bureau

Domestic Issue Code: 2-41

Price: 38.00RMB

DOI:10.12379/j.issn.2096-1057.2022.05.13

基于多模态与多尺度融合的抗欺骗人脸检测算法研究

刘龙庚[1] 任 宇[2] 王 莉[1]

[1](中国软件评测中心 北京 100048)

[2](四川大学计算机学院 成都 610065)

(liulonggeng@cstc.org.cn)

Face Anti-spoofing Detection Algorithm Based on a Multi-modal and Multi-scale Fusion

Liu Longgeng[1], RenYu[2], and Wang Li[1]

[1](*China Software Testing Center*, *Beijing* 100048)

[2](*College of Computer Science*, *Sichuan University*, *Chengdu* 610065)

Abstract This paper studies the problem that multi-modal features are not fully utilized in facial liveness detection, and proposes a face anti-spoofing detection algorithm based on multi-modal and multi-scale fusions, which makes full use of the complementary characteristics of visible light, near-infrared light and depth to filter the forged samples step by step. For the samples to be tested, firstly the playback attacks are filtered by near-infrared face detection, and then plane attacks are filtered by deep discriminant network. Finally, the samples which were difficult to be classified are input into multi-modal fusion module for comprehensive discrimination to obtain the final classification. In this paper, a high resolution multi-modal data set of nearly 20 000 groups is constructed, and lightweight discriminant networks with multi-scale input are designed to further improve the adaptability of the algorithm. The experimental results show that the proposed algorithm has significantly higher detection accuracy than the single modal solution, and the total number of parameters and reasoning time are only 480 000 and 8.07 ms, which are far lower than other popular fusion methods.

Key words face detection; demonstration attack; multi-modal; weighted fusion; light-weight network

摘 要 就现今人脸活体检测尚未充分利用多模态特性的问题展开研究,提出了一种多模态与多尺度融合检测算法,充分利用可见光、近红外、深度 3 种模态数据的互补特性逐级过滤伪造样本.待测样本首先经近红外人脸检测过滤回放攻击,然后经过深度判别网络过滤平面攻击,最后将前 2 层难分类的样本输入多模态融合模块综合判别得到最终分类.构建了 1 个近 2 万组的高分辨率多模态数据集,设计了多尺度输入的轻量级判别网络,进一步提高算法的适应性.对比实验证明,提出的算法检测准确率比单模态方案显著提高,总参数量仅有 48 万个,推理时间为 8.07 ms,远低于其他常见融合方式.

收稿日期:2021-12-28

引用格式:刘龙庚, 任宇, 王莉. 基于多模态与多尺度融合的抗欺骗人脸检测算法研究[J]. 信息安全研究, 2022, 8(5): 513-520

关键词　人脸检测；演示攻击；多模态；加权融合；轻量级网络

中图法分类号　TP391.41

近年来，人脸识别技术由于简单、无接触和高判别性等特点成为智能设备解锁、安全支付、考勤和安检等身份认证应用的主要手段之一[1]．由于人脸识别技术被广泛应用于各个领域，高识别精度的人脸识别技术在恶意伪造身份攻击下存在明显安全漏洞[2]．人脸识别系统一旦被演示攻击攻破，将会造成不必要的损失[3]．人脸活体检测技术可通过检测并过滤伪造的攻击图像，以达到抵御攻击的目的．然而，现有的人脸活体检测技术还存在数据模态单一化、图像分辨率不高、采集方式和攻击方式单一化等诸多问题．

现有的公开数据集不能兼顾多模态、多姿态、多攻击方式等条件．在人脸活体检测任务中，多模态数据通常包括可见光（visible light，VIS）图像、近红外（near-infred，NIR）图像和深度（depth）图像．VIS图像拥有其他模态数据不具备的颜色与纹理信息，但难以抵御数码设备回放；NIR图像对回放攻击有极高的辨别能力；depth图像对各种平面类的攻击方式都有良好的防御能力，并且对光照和环境变化不敏感，能有效提高泛化性能．CASIA-SURF数据集[4]是首个包含3种模态数据的人脸活体检测数据集，其不足之处有3点：一是分辨率较低；二是其近红外摄像头没有配备滤光片；三是数据集中不包含回放攻击样本．

近年来，多模态融合方法逐渐成为提升人脸识别检测准确率的新思路[5-6]；文献[4]在提出CASIA-SURF数据集的同时，也提出一种基于ResNet18网络的多模态融合的方式；文献[7]在CASIA-SURF的基础上提出了一种轻量级的人脸活体检测网络和一种决策层融合方法；文献[8]提出一种基于ResNext[9]的多模态融合方法，该方法提出的MFE（modal feature erasing）模块可以有效降低网络过拟合风险；文献[10]提出了一种多层级数据融合的方法，该方法使用ResNet34作为基础网络并将各个模态res1，res2，res3部分输出进行合并．现有的多模态融合方法大致分为2种：早融合（early fusion）方法和晚融合（late fusion）方法．早融合方法需要使用多分支输入分别提取多模态特征；晚融合方法的最终决策结果可以根据实际需求调整，相比早融合方法更加灵活．

在实际应用场景中，算法通常依附于人脸识别应用部署在嵌入式或者移动设备中，这就要求算法需要足够轻量化，而现有多模态融合算法对算法复杂度和参数量等问题还鲜有研究．在现有的晚融合基础上，本文提出了一种基于多模态与多尺度融合的人脸活体检测算法．在可见光人脸检测后，首先经近红外人脸第1层检测以过滤回放攻击，然后经过深度判别网络第2层检测过滤平面攻击，对于前2层检测难分类的样本进行3种模态融合加权判断得到最终分类．为了兼顾实时性能，本文对其中的判别网络进行了轻量级设计，利用多尺度图像的信息互补性进行多尺度特征提取与融合，并使用全局深度卷积代替全局平均池化提高了网络对于人脸特征的表征能力，选择Focal Loss[11]替代交叉熵损失函数解决了样本不均衡问题．在构建的多模态高分辨率人脸数据集上的对比实验证明，多模态方法在准确率指标上明显优于单模态算法，推理时间远低于其他常见融合方式．

1　多模态人脸活体检测数据集构建

本文在现有数据集采集方案的基础上，构建了一种多模态人脸活体检测（multi-modal face anti-spoofing，MMFAS）数据集．

1.1　数据集采集系统

MMFAS数据集采集系统由上下堆叠的双目摄像机和RealSense D415构成，如图1所示．其中RealSense D415由2个红外摄像头、1个可见光摄像头和1个红外结构光发射器组成，负责depth图像的获取．双目摄像机由1个可见光摄像头、1个加装850 nm窄带滤光片的红外摄像头和1个红外发射器组成，负责VIS图像和NIR图像的获取．摄像头与目标之间相距0.3～1 m，被采集目标如果是人物，需要按指示进行头部旋转操作；如果被采集目标是伪造介质，操作者需要持伪造介质按指示进行相应攻击操作．

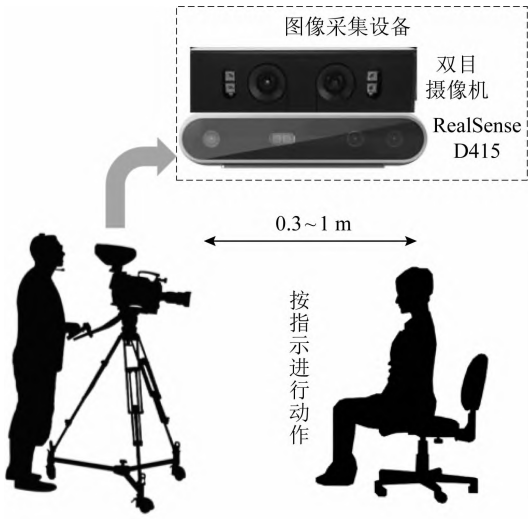
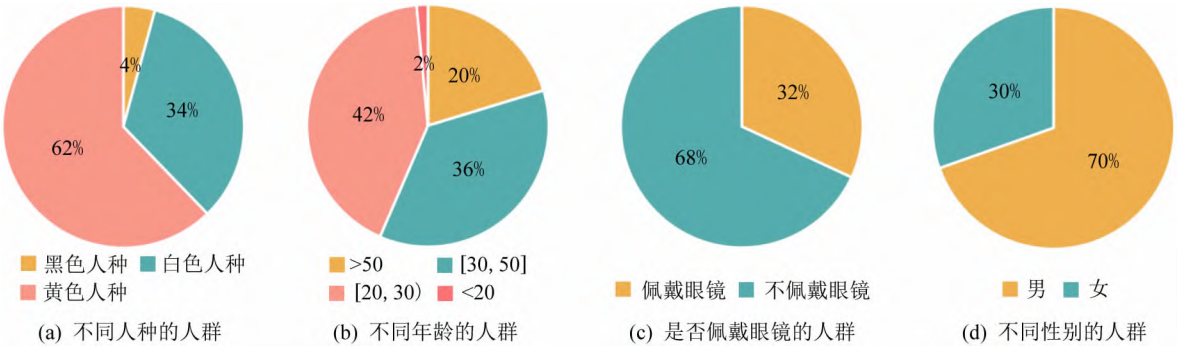


图 1　MMFAS 数据集图像采集设备及拍摄对象示意图

1.2　MMFAS 数据集统计信息

MMFAS 数据集共包含 19 938 组图片，每组图片又包含 3 个模态数据，共计 59 814 张图片，其中训练数据、验证数据和测试数据的样本数量比约为 7∶1∶2.MMFAS 数据集包含 69 个目标人脸，其中 31 个目标为实际采集目标，包含真实数据与攻击数据，剩余 38 个为来自 SiW 数据集[12]和网络的扩展目标，由于其真实数据源不同于 MMFAS，所以只包含攻击数据.MMFAS 数据集中涵盖了各个年龄段、不同人种、不同性别、是/否佩戴眼镜的人群，包括 6 种打印攻击子类、3 种回放攻击子类以及 5 种面部姿态子类，MMFAS 数据集的详细数据分布情况如图 2 所示.

表 1 综合统计了本文构建的 MMFAS 数据集和公开数据集多种属性差异.



(a) 不同人种的人群　(b) 不同年龄的人群　(c) 是否佩戴眼镜的人群　(d) 不同性别的人群

图 2　MMFAS 数据集的数据分布情况

表 1　MMFAS 数据集与公开数据集的对比

数据集	年份	目标人脸	样本/个		表情	姿态	光照	数据模态	分辨率	攻击手段
			真实样本	欺骗样本						
NUAA[1]	2010	15	5 105	7 509*	无	正面	有	VIS	低	打印
CASIA-MFSD[13]	2012	50	150	450	无	正面	无	VIS	低到高	打印、回放
Replay-Attack[14]	2012	50	200	1 000	无	正面	有	VIS	低到中	打印、回放
3DMAD[15]	2013	17	170	85	无	正面	无	VIS /depth	低/低	面具
MSU-MFSD[16]	2015	35	110	330	无	正面	无	VIS	低到高	打印、回放
Msspoof[17]	2016	21	1 680	3 024*	无	正面	有	VIS /NIR	中/中	打印
OULU-NPU[18]	2017	55	1 980	3 960	无	正面	有	VIS	高	打印、回放
SiW[12]	2018	165	1 320	3 300	有	±90°	有	VIS	高	打印、回放
CASIA-SURF[4]	2018	1 000	3 000	18 000	无	±30°	无	VIS /NIR/depth	中/低/低	打印、裁剪
CelebA-Spoof[19]	2020	10 177	150 129	475 408*	有	—	有	VIS	低到高	打印、回放
MMFAS(本文)	2020	69	20 496	39 318*	有	±30°	有	VIS /NIR/depth	高/高/中	打印、裁剪、回放

* 表示该数据集只含图片不含视频；高：1 920×1 080 分辨率；中：1 280×720 或 1 024×768 分辨率；低：640×480 及以下分辨率.

2 算法描述

2.1 算法总体流程设计

本文所提出的基于多模态融合的抗欺骗人脸检测(face anti-spoofing based on multi-modal fusion，FAS-MMF)算法充分利用可见光、近红外、深度模态的互补特性进行逐级过滤，避免了全部样本都经过多个网络判别.主要包含3个步骤，其总体流程图如图3所示：

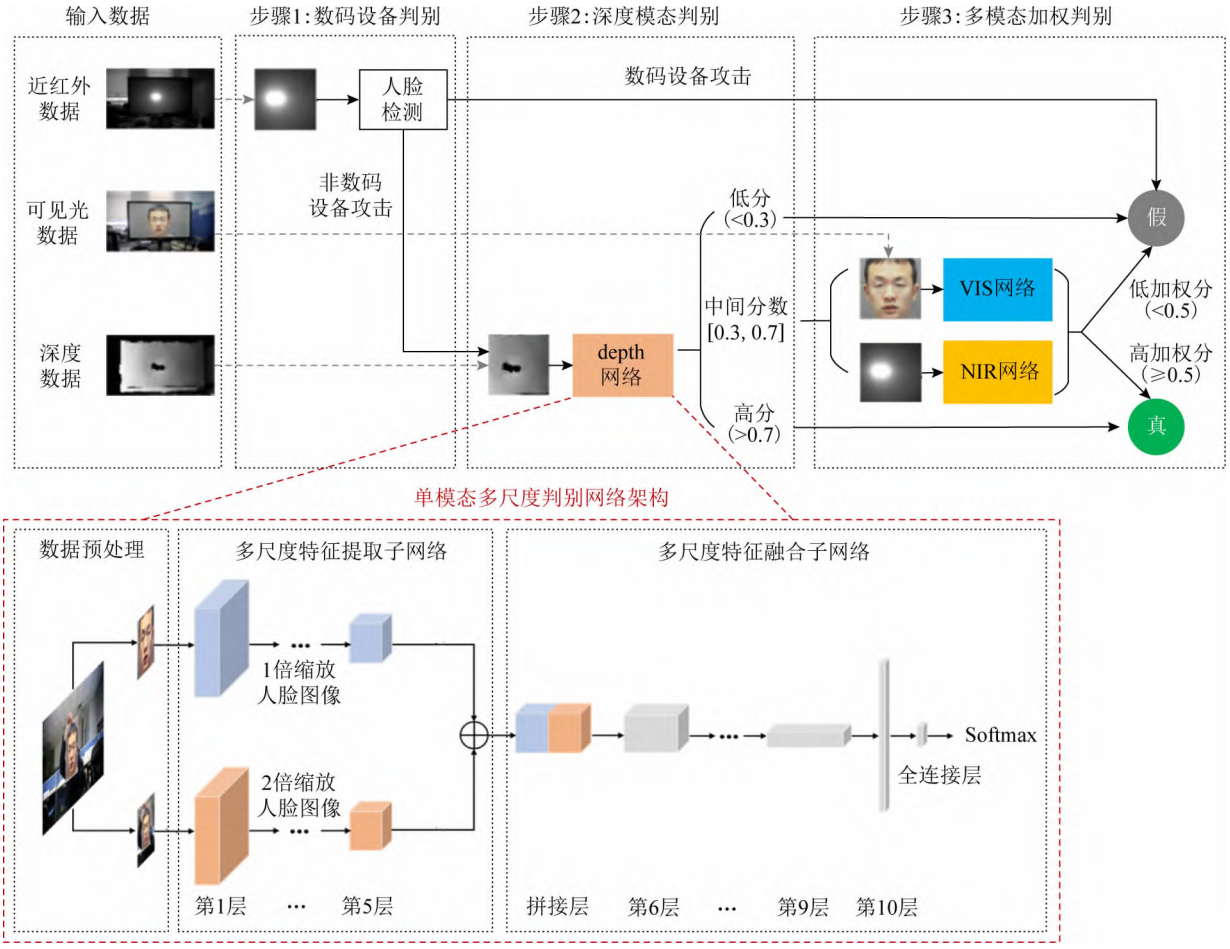


图3 基于多模态与多尺度融合的人脸活体检测算法框架

步骤1. 数码设备判别(NIRD).

分辨并过滤数码设备攻击(回放攻击).由于数码设备屏幕在NIR模态下不会成像，因此在NIR裁剪图中没有检测到人脸可以直接判断该样本为回放攻击样本，否则该样本为非回放攻击样本，可能是真实样本或打印攻击样本，需要进入步骤3进一步进行判断.

步骤2. 深度模态判别.

对步骤1数码设备判别模块判别为非数码设备的样本进行判断.将其对应的depth图像输入depth判别网络进行人脸活体检测，并根据深度图的输出分数高低将样本分为真人、攻击和不易辨别3个类别.深度判别模块设置高分阈值0.7和低分阈值0.3，当分数大于0.7时直接判断该样本为真实样本，如果分数小于0.3则直接判断该样本为攻击样本，当分数在0.3～0.7之间时，则认为该样本的类别不确定，需要进入步骤3继续进行多模态加权判别.

步骤3. 多模态加权判别.

对步骤1和步骤2难辨别的样本进行融合加权获得最终分类.首先将VIS图像和NIR图像分别输入对应的判别网络，得到VIS分数和NIR分数，然后再与depth分数加权求和得到最终分数，加权公式见式(1)，根据各模态数据对人脸活体检

测任务的重要程度进行分析，将 depth 图像、NIR 图像和 VIS 图像的权重 α，β，γ 分别设置为 0.5，0.3，0.2，最后加权分数大于等于 0.5 的划分为真，小于 0.5 的划分为假.加权求和公式如式(1)：

$$score=\alpha\times score_{depth}+\beta\times score_{NIR}+\gamma\times score_{VIS}, \tag{1}$$

其中 α 为 depth 模态权重；$score_{depth}$ 为 depth 模态分数；β 为 NIR 模态权重；$score_{NIR}$ 为 NIR 模态分数；γ 为 VIS 模态权重；$score_{VIS}$ 为 VIS 模态分数.

2.2 单模态多尺度判别网络设计

为了进一步降低算法复杂度，图 3 中 depth 网络、NIR 网络、VIS 网络均采用多尺度轻量级判别网络(light-weight networks based on multi-scale fusion，LWDN-MS)作为主干网络，其网络架构如图 3 中虚线框内所示.主要包括如下 3 个步骤：

1) 数据预处理.

对原始图像进行预处理得到多尺度人脸样本.首先使用 RetinaFace[20] 对 VIS 图像进行人脸检测得到人脸框坐标，接着根据人脸框坐标位置裁剪出包含面部细节的 1 倍缩放图和包含人脸主体、背景信息或攻击介质边框的 2 倍缩放人脸图.将经过增强的图像在通道维度上进行拼接，得到 6×224×224 的特征图并送入特征提取子网络.

2) 多尺度特征提取子网络.

对多尺度输入进行特征提取.首先将步骤 1)输出的特征图在通道维度拆分为 2 个 3×224×224 的张量，分别输入各自的特征提取网络，2 路分别对应 1 倍和 2 倍缩放人脸图像.特征提取网络对应 MobieNetV2[21] 的前 5 层，第 1 层是图像下采样和通道扩张的标准卷积层，第 2～5 层依次为重复 1 次、2 次、3 次、4 次的堆叠的倒置残差块，从第 3 层开始逐层下采样操作，即特征图尺寸依次减半.第 5 层输出 2 个 8×14×14 的特征图，作为多尺度特征融合子网络的输入.

3) 多尺度特征融合子网络.

将步骤 2)输出的特征图进行融合并得到精确分类.第 6 层首先将步骤 2)中 2 个 8×14×14 的特征图在通道维度进行特征连接，得到 16×14×14 的堆叠特征图.网络的第 7 层和第 8 层为倒置残差块，第 9 层使用 1×1 卷积进行通道融合，第 10 层用全局深度卷积(GDC)替换全局平均池化层以获得自适应的权重.网络最后一层将逐点卷积替换为全连接层进行最终分类，得到通道数为 2 的输出，最后经过 Softmax 计算得到正负样本概率.

3 实验及结果分析

为了进一步验证本文算法的检测性能和鲁棒性，设置了如下 2 组实验：

1) 检测精度对比实验.3.3 节对不同的融合方式、不同的模态组合方式进行对比.

2) 单模态算法与多模态算法对比实验.3.4 节从检测性能和算法轻量化程度进行算法对比.

网络的深度学习框架使用 Pytorch 1.7.0，python3.7 进行编码.算法在 Intel Core i7-8700 CPU @ 3.2 GHz，16 G-RAM，NVIDIA GeForce GTX 1080Ti 的 Ubuntu18.04 的环境下运行.

3.1 算法评估方法

3.1.1 人脸活体检测性能指标

本文采用 TPR@FPR[4,19] 指标对人脸活体检测算法进行性能评估，将真实人脸定义为正类，攻击人脸定义为负类.TPR@FPR 表示在当前 FPR 取值情况下 TPR 的值，该指标能在一定程度上反映分类器对正负样本的划分质量.其中 TPR 表示 TP 占总正样本数的比例，FPR 表示 FP 占总负样本数的比例.同时，依据生物活体检测标准文件[22]，本文采用攻击样本分类错误率(attack presentation classification error rate，APCER)计算攻击样本的分类错误率，采用真实样本分类错误率(bona fide presentation classification error rate，BPCER)计算真实样本的分类错误率，采用平均分类错误率(average classification error rate，ACER)计算攻击样本与真实样本的整体分类错误率，作为最终的评价指标.

3.1.2 网络轻量级指标

本文采用网络的参数量(params)表示网络模型的参数总量，采用浮点运算数(floating point operations，FLOPs)衡量网络的总体计算规模.

3.2 训练测试过程及参数

在深度学习训练过程中涉及到的参数设置如下：批处理尺寸(batch size)统一设置为 128，部分网络模型显存占用较大，1 次读取无法容纳所有数据，此时批处理尺寸依次减半；初始学习率为 0.01；权重衰减设置为 0.000 1；优化算法采用随机

梯度下降算法；网络输入设置图片大小为 224×224；最大训练次数(epoch)为 200 轮.

采用 Focal Loss[11] 作为损失函数解决样本不均衡问题，α 设为 0.2，γ 设为 2；深度判别网络和近红外网络的输入为单通道，可见光判别网络的输入为 3 通道.

3.3 算法检测性能分析

本节设置了 2 个实验，表 2 列出了不同融合算法与本文的融合算法之间的对比效果，表 3 列出了单模态、双模态不同组合、3 模态不同组合以及本文算法的检测效果对比.值得注意的是，在 VIS 和 NIR 模态融合时，由于没有 depth 分数，所以权重参数 α，β，γ 分别设置为 0，0.6，0.4.由于 TPR@FPR 指标的计算需要使用分类器输出的分数，而 NIRD 模块不会输出分数，所以对 NIRD 模块的输出进行修改，将所有被 NIRD 模块判断为回放攻击的样本记为 0 分，其余样本由后续判别网络输出分数.

表 2 不同融合方式的对比

融合方式	TPR/%			FP/个	FN/个	APCER/%	BPCER/%	ACER/%
	FPR=0.005	FPR=0.001	FPR=0.0005					
Halfway fusion[9]	100	100	100	1	0	4	0	2
SEfusion[9]	100	100	100	0	0	0	0	0
FAS-MMF(本文多模态算法)	100	100	100	0	0	0	0	0

APCER：攻击样本的分类错误率；BPCER：真实样本的分类错误率；ACER：攻击样本与真实样本的整体分类错误率.TPR 表示 TP 占总正样本数的比例；FPR 表示 FP 占总负样本数的比例；TPR@FPR 表示在当前 FPR 取值情况下 TPR 的值.FP 表示攻击样本中被预测为真的数量；FN 表示真实样本中被预测为真的数量.

表 3 不同模态组合方式的对比

模态组合方式	TPR/%			FP/个	FN/个	APCER/%	BPCER/%	ACER/%
	FPR=0.005	FPR=0.001	FPR=0.0005					
VIS	98.09	92.64	64.58	93	0	344	0	172
NIR	97.82	94.46	91.28	16	12	59	109	84
depth	100	99.73	89.1	5	0	18	0	9
NIRD	0	0	0	2188	0	8095	0	4047
NIRD+depth	100	99.73	99.73	4	0	15	0	7
VIS+NIR	100	99.73	99.18	3	3	11	27	19
NIRD+VIS+NIR	100	99.73	99.18	2	3	7	27	17
depth+VIS+NIR	100	100	89.1	1	0	4	0	2
FAS-MMF(本文多模态算法)	100	100	100	0	0	0	0	0

APCER：攻击样本的分类错误率；BPCER：真实样本的分类错误率；ACER：攻击样本与真实样本的整体分类错误率.TPR 表示 TP 占总正样本数的比例；FPR 表示 FP 占总负样本数的比例；TPR@FPR 表示在当前 FPR 取值情况下 TPR 的值.FP 表示攻击样本中被预测为真的数量；FN 表示真实样本中被预测为真的数量.

表 2 的结果表明，本文提出的融合算法与另外 2 种融合算法的性能相当，其平均分类错误率都非常低，其中 SE fusion 算法与本文算法对所有样本都能正确分类.各种算法在检测性能方面都取得较好结果的原因可能在于多种模态数据具有较强的互补性，同时采集的数据能充分发挥各自模态的优势[23-26]，具有较强的判别性.

从表 3 可以看出，只使用单模块进行检测，效果远差于多种模块组合的方法，和 depth 模块进行组合能取得更好的效果，比如 NIRD+depth 组合、VIS+NIR 与 depth 组合的效果要优于其他 2 种组合方式；值得注意的是，VIS+NIR 与 depth 组合时存在 FP 样本，在加上 NIRD 模块之后，FP 样本被正确检测，说明 NIRD 模块和 depth 模态具有互补作用.本文提出的融合方法融合了 depth 模态、VIS 模态、NIR 模态和 NIRD 输出信息，在各

项指标上都取得了最优结果，是所有模态组合方式中最好的.

3.4 单模态与多模态算法的检测效率对比

本实验从网络轻量化程度和准确率2方面对2.2节描述的单模态多尺度判别网络(LWDN-MS)和多种多模态算法进行对比，本节实验的推理时间的计算在i7 8700上进行，并且不使用推理框架，FAS-MMF的参数量为depth判别网络、NIR判别网络和VIS判别网络参数量的总和.

从表4可知，相比于其他常见网络，本文提出的判决网络结构具有最少的参数数量，只包含19万个网络参数和8.07 s的推理时间.多模态融合准确率指标上明显优于单模态算法.但是单模态算法在参数量和推理时间上更具优势.本文提出的FAS-MMF方法在现阶段适合在不限制成本并且对精度要求非常高的场景下使用.

表4 单模态算法与多模态算法的检测效率对比

融合方法	总参数量/个	推理时间/ms	APCER/%	BPCER/%	ACER/%
LWDN-MS(本文2.2节单模态判别网络)	**0.19×10^6**	14.96	37	82	59
Halfway fusion[4]	13.33×10^6	37.74	4	**0**	2
SE fusion[4]	13.34×10^6	39.39	**0**	**0**	**0**
FAS-MMF(本文多模态算法)	0.48×10^6	**8.07**	**0**	**0**	**0**

APCER：攻击样本的分类错误率；BPCER：真实样本的分类错误率；ACER：攻击样本与真实样本的整体分类错误率.

4 结 论

针对现有的人脸活体检测模态单一、攻击方式单一、数据集质量不高等问题，本文利用多模态数据之间的互补特性，设计了基于多模态融合的人脸活体检测算法，大多数攻击样本仅需前2步判别就能被正确分类，避免了全部样本都经多个网络判别.本文对各判别网络进行了轻量级设计，进一步降低了算法的复杂度.在构建的多模态高分辨率人脸活体数据集上进行的对比实验证明了本文算法在检测性能和推理时间2方面的优越性.本文构建的数据集均为二分类样本，后续研究可丰富样本采集环境如人脸属性、攻击子类型、攻击设备、光照、姿态等，进一步提高算法的泛化性和鲁棒性.

参 考 文 献

[1] Tan X, Li Y, Liu J, et al. Face liveness detection from a single image with sparse low rank bilinear discriminative model [C/OL] //Proc of the European Conf on Computer Vision. 2010 [2022-01-01]. https://link.springer.com/Content/pdf/10.1007%2F978-3-642-15567-3_37.pdf

[2] 梁嘉骏. 基于深度学习的人脸安全认证：现状与挑战[J]. 信息安全研究，2019，5(11)：1008—1012

[3] 苗杰. 人脸识别"易破解"面临的风险挑战及监管研究[J]. 信息安全研究，2021，7(10)：984—988

[4] Zhang S, Wang X, Liu A, et al. A dataset and benchmark for large-scale multi-modal face anti-spoofing [C/OL] //Proc of the IEEE/CVF Conf on Computer Vision and Pattern Recognition. 2019[2022-01-01]. https://ieeexplore.ieee.org/document/8953793

[5] Xu Z, Li S, Deng W. Learning temporal features using LSTM-CNN architecture for face anti-spoofing [C/OL] //Proc of the 3rd IAPR Asian Conf on Pattern Recognition (ACPR). 2015 [2022-01-01]. https://ieeexplore.ieee.org/document/7486482

[6] 邓茜文，冯子亮，邱晨鹏. 基于近红外与可见光双目视觉的活体人脸检测方法[J]. 计算机应用，2020，40(7)：2096—2103

[7] Zhang P, Zou F, Wu Z, et al. Feathernets: Convolutional neural networks as light as feather for face anti-spoofing [C/OL] //Proc of the IEEE/CVF Conf on Computer Vision and Pattern Recognition Workshops. 2019 [2022-01-01]. https://ieeexplore.ieee.org/document/9025672

[8] Shen T, Huang Y, Tong Z. Facebagnet: Bag-of-local-features model for multi-modalfaceanti-spoofing [C/OL] //Proc of the IEEE/CVF Conf on Computer Vision and Pattern Recognition workshops. 2019 [2022-01-01]. https://ieeexplore.ieee.org/document/9025418

[9] Xie S, Girshick R, Dollár P, et al. Aggregated residual transformations for deep neural networks [C/OL] //Proc of the IEEE Conf on Computer Vision and Pattern Recognition. 2017 [2022-01-01]. https://ieeexplore.ieee.org/document/8100117

[10] Parkin A, Grinchuk O. Recognizing multi-modal face spoofing with face recognition networks [C/OL] //Proc of the IEEE/CVF Conf on Computer Vision and Pattern Recognition Workshops. 2019 [2022-01-01]. https://ieeexplore.ieee.org/document/9025477

[11] Lin T-Y, GoYal P, Girshick R, et al. Focal loss for dense object detection [C/OL] //Proc of the IEEE IntI Conf on Computer Vision. 2017 [2022-01-01]. https://ieeexplore.ieee.org/document/8417976

[12] Liu Y, Jourabloo A, Liu X. Learning deep models for face anti-spoofing: Binary or auxiliary supervision [C/OL] //Proc of the IEEE Conf on Computer Vision and Pattern Recognition. 2018 [2022-01-01]. https://ieeexplore. ieee.org/document/8578146

[13] Zhang Z, Yan J, Liu S, et al. A face antispoofing database with diverse attacks [C/OL] //Proc of the 5th IAPR Int Confon Biometrics (ICB). 2012 [2022-01-01]. https://ieeexplore.ieee.org /abstract/document/6199754

[14] Chingovska I, Anjos A, Marcel S. On the effectiveness of local binary patterns in face anti-spoofing [C/OL] //Proc of the Int Conf of Biometrics Special Interest Group (BIOSIG). 2012 [2022-01-01]. https://ieeexplore.ieee.org/abstract/document/6313548

[15] Nesli E, Marcel S. Spoofing in 2D face recognition with 3d masks and anti-spoofing with kinect [C/OL] //Proc of the 6th IEEE Int Conf on Biometrics: Theory, Applications and Systems (BTAS'13). 2013 [2022-01-01]. https://ieeexplore.ieee.org/abstract/document/6712688

[16] Wen D, Han H, Jain A K, et al. Face spoof detection with image distortion analysis [J]. IEEE Trans on Information Forensics and Security, 2015, 10(4): 746—61

[17] Chinggovska I, Erdogmus N, Anjos A, et al. Face recognition systems under spoofing attacks [M] //Face Recognition Across the Imaging Spectrum. Berlin: Springer, 2016: 165—194

[18] Boulkenafet Z, Komulainen J, Li L, et al. OULU-NPU: A mobile face presentation attack database with real-world variations [C/OL] //Proc of the 12th IEEE Int Conf on Automatic Face & Gesture Recognition (FG 2017). 2017 [2022-01-01]. https://ieeexplore.ieee.org/document/7961798

[19] Zhang Y, Yin Z, Li Y, et al. Celeba-spoof: Large-scale face anti-spoofing dataset with rich annotations [C/OL] //Proc of the European Conf on Computer Vision. 2020 [2022-01-01]. https://link. springer. com/chapter/10. 1007/978-3-030-58610-2_5

[20] Deng J, Guo J, Ververas E, et al. Retinaface: Single-shot multi-level face localisation in the wild [C/OL] //Proc of the IEEE/CVF Conf on Computer Vision and Pattern Recognition. 2020 [2022-01-01]. https://ieeexplore. ieee.org/document/9157330

[21] Sandler M, Howard A, Zhu M, et al. Mobilenetv2: Inverted residuals and linear bottlenecks [C/OL] //Proc of the IEEE Conf on Computer Vision and Pattern Recognition. 2018 [2022-01-01]. https://ieeexplore. ieee. org/document/8578572

[22] International Organization for Standardization. ISO/IEC 30107-3-2017 Information Technology-Biometric Presentation Attack Detection-Part 3: Testing and Reporting [S/OL]. (2017-09-01) [2022-04-21]. https://www. iso. org/standard/67381.html

[23] **刘龙庚. 大数据环境下无线传感器网络关键技术研究**[D]. **成都：电子科技大学**, 2017

[24] Liu L, Luo G. Routing optimization in networks based on traffic gravitational field model [J]. International Journal of Modern Physics B, 2017, 31(11): 1750074

[25] Liu L, Luo G, Qin K, et al. An algorithm based on logistic regression with data fusion in wireless sensor networks [J]. Eurasip Journal on Wireless Communications & Networking, 2017, 2017(1): 1—9

[26] Liu L, Luo G, Qin K, et al. An on-demand global time synchronization based on data analysis for wireless sensor networks [J]. Procedia Computer Science, 2018 (129): 503—510

刘龙庚

博士，高级工程师.主要研究方向为产业规划、信创规划、信息安全、架构设计与测试评估.

liulonggeng@cstc.org.cn

任　宇

硕士研究生.主要研究方向为计算机视觉、图像处理.

renyu@stu.scu.edu.cn

王　莉

硕士.主要研究方向为技术发展趋势、企业能力建设、产业发展分析.

wangli@cstc.org.cn