

基于面部生理信号的人脸活体检测

隋雅茹¹, 姜磊², 饶治¹, 安梦雪¹, 嵇晓强¹

(1. 长春理工大学 生命科学技术学院, 长春 130022;

2. 中国科学院长春光学精密机械与物理研究所, 长春 130033)

摘要:针对现有人脸活体检测算法生理特征鲁棒性差的问题,提出一种新的基于面部生理信号的人脸活体检测算法。首先,利用远程光体积变化描记术从面部图像中提取由心脏跳动引起的面部生理信号;之后,对原始的面部信号使用带通滤波进行去噪,再进行快速傅里叶变换将信号转换至频域,提取新的频谱特征;最后,采用机器学习模型实现二分类,区分真实人脸和虚假人脸。结果表明,在Replay-Attack数据库上,应对打印、屏显两种欺诈攻击类型,最佳准确率达到99.15%。该算法在屏显攻击场景下展现出优越的性能,为进一步深化人脸反欺诈算法的研究奠定了坚实基础。

关键词:远程光电体积描记术;心率;梯度提升树;活体检测

中图分类号: TP391

文献标志码: A

文章编号: 1672-9870(2024)04-0094-07

Face Liveness Detection Base on Facial Signal

SUI Yaru¹, JIANG Lei², RAO Zhi¹, AN Mengxue¹, JI Xiaoqiang¹

(1. School of Life Science and Technology, Changchun University of Science and Technology, Changchun 130022;

2. Changchun Institute of Optics, Fine Mechanics and Physics, Chinese Academy of Sciences, Changchun 130033)

Abstract: In view of the poor robustness of existing face detection algorithms, a new face detection algorithm based on facial physiological signals is proposed in this paper. First, remote photoplethysmography is used to extract facial physiological signals caused by heart beats from facial images. After that, the original facial signal is denoised by band-pass filtering, and then the signal is converted to frequency domain by fast Fourier transform to extract new spectral features. Finally, machine learning model is used to realize binary classification and distinguish real faces from false faces. The results show that on Replay-Attack database, the best accuracy rate is 99.15% against two types of fraud attacks: print and screen display. The algorithm shows excellent performance in the screen attack scenario, which lays a solid foundation for further deepening the research of face anti-fraud algorithm.

Key words: remote photo plethysmography; heart rate; gradient boosting tree; liveness detection

人脸活体检测是确保人脸识别系统安全的关键环节,需要在复杂环境下识别各类欺诈攻击,确保对真实活体进行有效验证,又被称为人脸反欺诈(Face Anti-spoofing, FAS)^[1]。非交互式人脸活体检测方法主要利用彩色(RGB)相机、

深度(Depth)相机、红外(IR)相机、双目相机、光场相机、三维扫描仪和多光谱成像仪等各种传感器设备采集的视频图像中的纹理信息、图像质量、运动信息和深度信息等,以区分真实人脸和欺诈攻击^[2-13]。传统的人脸活体检测算法仅

收稿日期: 2024-03-07

基金项目: 吉林省科技发展计划项目(20240101339JC)

作者简介: 隋雅茹(1999-),女,硕士研究生, E-mail: suiyaru@mails.cust.edu.cn

通信作者: 嵇晓强(1982-),女,博士,教授,硕士生导师, E-mail: jixq2012@cust.edu.cn

依赖于单一模态的数据,难以有效地防范打印攻击、屏显攻击和面具攻击三种主要欺诈攻击类型。然而,在实际应用中,人脸识别系统的终端设备通常只配备了彩色视频功能。

利用远程光体积变化描记术(Remote Photoplethysmography, rPPG)技术使用普通RGB摄像机,能够远程检测面部感兴趣区域(Region of Interest, ROI)脉搏波信号。近年来,研究者通过分析面部生理信号实现了活体检测。2016年,Li等人^[14]首次提出利用rPPG信号来解决人脸活体检测问题。通过传统算法从人脸视频中提取rPPG信号,并计算频域信号的峰值和信噪比,作为识别欺诈攻击的依据。2017年,Nowara等人^[15]在文献[14]的算法基础上,在选取面部感兴趣区域时引入两个背景区域(面部的左右外侧),去除rPPG信号的背景噪声对活体检测的影响。2018年,Liu等人^[16]利用从面部不同感兴趣区域提取的rPPG信号之间相关性,识别真实人脸。Liu等人^[17]提出了一种CNN-RNN结构,提取人脸深度图和rPPG信号,区分真实人脸和欺诈攻击。2022年,Yu等人^[18]首先从输入人脸视频的背景区域和人脸区域分别提取rPPG信号,并对应转化为各自的多尺度时空图;然后采用自动化的视觉转换器代替手工特征提取的方式,从上述两个多尺度时空图中分别提取出rPPG特征,以充分捕捉时空图中的活体信息。殷超^[19]结合rPPG信号的功率谱密度特征和互相关谱特征作为判别虚假人脸的依据。

该方法仅需使用彩色视频数据,却能有效地对抗打印、屏显和面具等三种主要欺诈攻击。然而,由于屏显攻击所包含的微弱生理信息,导致对这类欺诈攻击的检测鲁棒性较差。为此,本文提出了一种新的基于面部信号的人脸活体检测算法,显著提高了对屏显攻击的准确检测率。

1 方法

面对人脸识别系统常见的照片、视频攻击,本文提出一种新的人脸反欺诈方法,流程如图1所示。首先对RGB视频进行人脸检测,再通过人脸关键点检测截取感兴趣区域,计算像素均值得到原始rPPG信号,对信号进行去噪之后转换至频域提取特征,最后在支持向量机、随机森林、决策树、梯度提升树四种机器学习模型上分类,寻找最佳分类器

1.1 检测原理

rPPG技术中,光反射起着关键作用。当环境光照射到皮肤表面时,部分光被皮肤中的色素和血液中的血红蛋白吸收,而另一部分光会被散射^[20],通过捕捉和分析反射回来的光信号,可以检测到由血液流动引起的微小光强度变化,从而提取心率等生理参数^[21]。rPPG技术通过计算图像像素均值的变化,获取与心跳频率同步的脉搏信号^[22]。然而,对于伪造的人造材料,由于其具有较低的透射率特性,无法有效地反映由心跳引起的肤色变化。因此,在虚假人脸上,rPPG技术无法探测到有效的信号^[23]。特别是,伪造材料的透射率越低,其与真实人脸的差异越显著,判别的特征也就越明显,rPPG技术在成为当前人脸活体检测领域中一种有效且可靠的手段。

1.2 面部信号的提取

1.2.1 图像预处理

对于人脸视频转帧后的图像,本文采用MTCNN算法,进行人脸检测。随后,使用Face Mesh算法实现关键点检测,获取包含468个详细的面部关键地标点信息。在有关提取人脸生理信号的研究中^[24-25],发现人脸脸颊、额头区域提取的

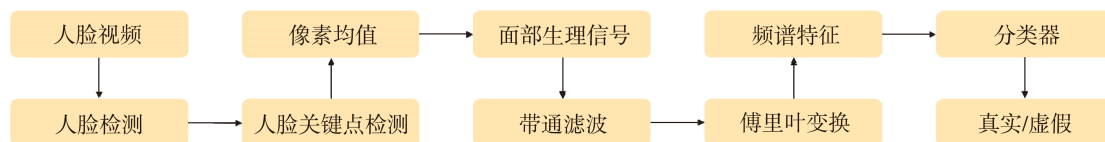


图1 基于面部信号的人脸活体检测流程

信号表现出比其他区域更强烈的生理活性。在选择感兴趣区域时,本研究专注于脸颊和额头,旨在更精准地捕捉面部的重要生理信息。通过沿着相关区域的关键点,分割出眼睛和嘴巴等易产生噪声的部分,最大化地保留脸颊和额头的部分,如图2所示。

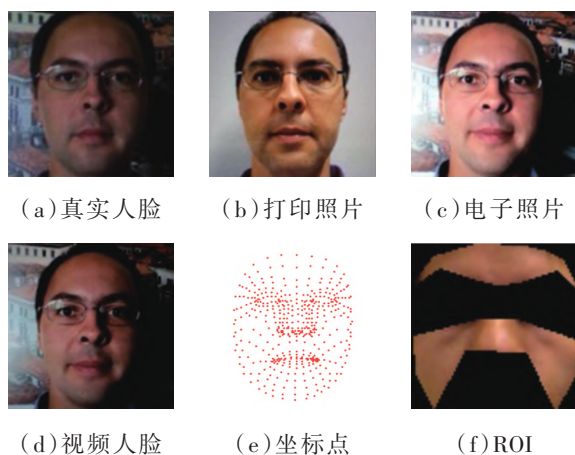


图2 图像预处理结果

MTCNN^[26]算法是基于深度学习的人脸检测方法,采用高效的级联策略,实现在多个尺度上的人脸检测。其优势不仅在于有效地处理遮挡、光照和姿态等问题,还同时保障了检测的高效性和准确性。此外,相较于传统人脸检测算法,MTCNN算法可以在同一视频帧上检测多个人脸,并且具备人脸识别的功能。Face Mesh^[27]算法能够在人脸上准确地检测大量的关键点,提供了更为详细和全面的面部信息,对于不同年龄、种族和面部特征差异也具有较好的适应性,能够应对多样性的面部形态。

1.2.2 rPPG信号提取

本文通过对R、G、B三个通道的感兴趣区域图像求取均值,得到各通道的rPPG信号,如图3所示。人体皮肤主要由血红蛋白和黑色素负责吸收入射光,其吸收波长主要集中在500~600 nm范围内,对应可见光谱中的黄绿色区域^[28]。由此,绿色通道的信号更能准确地反映心脏的周期性变化。

本文选择绿色通道的信号作为rPPG的原始信号,有助于捕捉由心脏跳动引起的生理信息,

从而增强从真实人脸视频与虚假人脸视频提取特征的区分性。

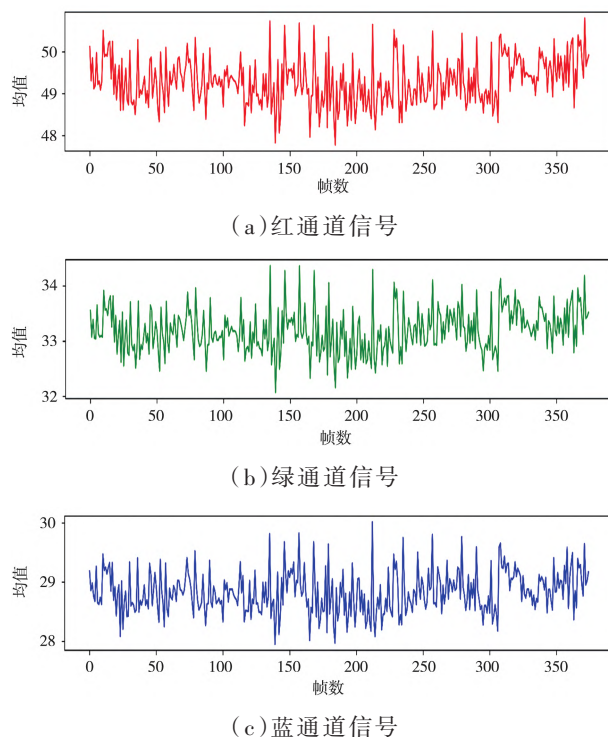


图3 原始rPPG信号

1.3 信号预处理

除了由眼部运动以及表情变化产生的运动伪影,人的头部或整个身体的微小运动,例如颤抖、摇晃或移动,会导致图像中的面部区域出现变化,从而产生噪声干扰提取的面部生理信号。此外,环境光的变化和视频录制设备产生的干扰,都会降低rPPG信号的信噪比。本文采用带通滤波去除原始rPPG信号中的低频、高频噪声和基线漂移,截止频率设置为0.6~4 Hz。

对于去噪后的rPPG信号,进行快速傅里叶变换(Fast Fourier Transform, FFT)将提取的面部信号从时域转换为频域,获得信号的频谱图,如图4所示。

1.4 特征提取

本文通过将多尺度长期频谱统计特征(Multi Scale Long Term Statistical Spectral, MS-LTSS)^[29]和心率(Heart Rate, HR)级联的方式进行融合,形成一个融合心率的频谱统计特征(Spectral Statistical Features with Heart Rate, SSF-HR)。其提取

信号中精细特征的同时,还能捕捉更为强健的活性信息,从而提高检测的准确性。

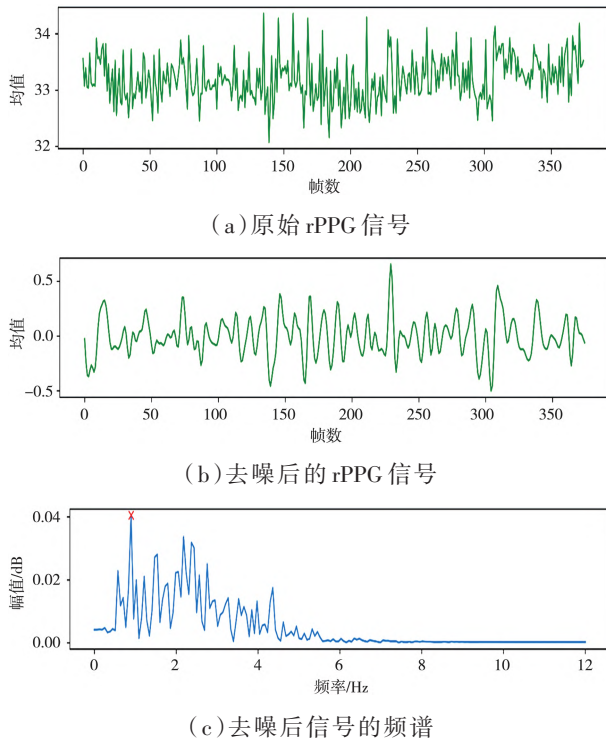


图4 信号预处理结果

对于估算心率,检测频谱的峰值 P ,如图4(c)中“x”所示。通过公式(1)得到时域心率所对应的频域频率信息。

$$f_{\max} = \frac{f_s}{N} \times P_{\max} \quad (1)$$

其中, N 为快速傅里叶变换的点数; f_s 为帧频; $f_{\max}$ 为时域心率所对应的频率。之后再通过公式(2)即可估算出心率值。

$$HR = f_{\max} \times 60 \quad (2)$$

MS-LTSS可结合不同长度和不同重叠尺寸的滑动窗口来统计频谱特征,从而可以获得更为精细的rPPG信息。对于一个滑动窗口 w 内的频域信号,得到一个向量 $[X_1(k), \dots, X_w(k)]$ 。如果 $|X_w(k)|$ 小于1,将其设置为1,使其取对数的值始终为正。系数向量的均值和方差如下所示:

$$\mu(k) = \frac{1}{w} \sum_{i=1}^w \log(|X_i(k)|) \quad (3)$$

$$\sigma^2(k) = \frac{1}{w} \sum_{i=1}^w \log(|X_i(k) - \mu(k)|) \quad (4)$$

通过设置不同的滑动窗口长度 w 和滑动窗口重叠大小 o ,计算rPPG频域信号中各自窗口内

系数的均值和方差,即由 w_1, o_1 计算 μ_1, σ^2_1 ,类似地,由 w_n, o_n 计算 μ_n, σ^2_n 。最后,将其依次作为MS-LTSS特征向量的元素,则:

$$\text{MS-LTSS} = [\mu_1, \sigma^2_1, \dots, \mu_n, \sigma^2_n] \quad (5)$$

最后,以矩阵级联的形式融合HR和MS-LTSS特征,得到SSF-HR特征。

$$\text{SSF-HR} = [\text{HR}, \text{MS-LTSS}] \quad (6)$$

2 结果与分析

2.1 数据集

本文采用公开数据集Replay-Attack^[30],检验算法应对打印攻击和屏显攻击的能力。这个数据集收录了来自50名测试者使用MacBook摄制的视频,涵盖了不同光照条件下的录像。视频分辨率为320×240,总计包含1 300个时长为10 s的人脸视频,其中真实人脸视频为300个,欺骗人脸视频为1 000个。在Replay-Attack数据集中,欺骗人脸视频的采集采用手持或固定的方式。其中,手持欺骗媒介可能导致视频出现抖动,从而增加了对欺骗性眨眼检测器的挑战。这种多样性的欺骗手段使得眨眼检测模型需要更好地适应不同的录制条件,提高了对眨眼真实性的准确性要求。

2.2 评价指标

人脸活体检测方法的性能评估指标主要包括:攻击表示分类错误率(Attack Presentation Classification Error Rate, APCER)、真实表示分类错误率(Bonafide Presentation Classification Error Rate, BPCER)、平均分类错误率(Average Classification Error Rate, ACER)^[31]。此外,还包括错误拒绝率(False Rejection Rate, FRR)、错误接受率(False Acceptance Rate, FAR)、半错误率(Half Total Error Rate, HTER)、等错误率(Equal Error Rate, EER)^[31]。等错误率为错误拒绝率与错误接受率相等时的值。其他评价指标根据混淆矩阵参数真正类(TP)、真负类(TN)、假正类(FP)、假负类(FN)进行计算,公式如下:

表 1 分类模型最优参数

分类器	参数名称	参数含义	最优解	准确率/%
随机森林	n_estimators	表示决策树的数量	50	94.71
决策树	criterion	代表决策树的类型	gini	96.41
支持向量机	Kernel	核函数	RBF	99.15
	Gamma	表示支持向量的个数	1	
	C	惩罚因子,控制对错误样本的惩罚程度	10	
梯度提升树	n_estimators	表示决策树的数量	230	99.15
	learning_rate	表示模型的学习率	0.2	
	max_depth	树的最大深度	2	

$$APCER = \frac{FP}{TN + FN} \tag{7}$$

$$BPCER = \frac{FN}{TP + FP} \tag{8}$$

$$ACER = \frac{APCER + BPCER}{2} \tag{9}$$

$$FRR = \frac{FN}{TN + FN} \tag{10}$$

$$FAR = \frac{FP}{TP + FP} \tag{11}$$

$$HTER = \frac{FRR + FAR}{2} \tag{12}$$

2.3 实验结果

在 Replay-Attack 训练集上,使用支持向量机 (Support Vector Machine, SVM)、随机森林(Random Forest, RF)、决策树 (Decision Tree, DT)、梯度提升树 (Gradient Boosting Tree, GBT) 四种机器学习模型进行训练,各分类器模型的参数采用网格搜索和交叉验证的方法确定最优解,如表 1 所示。表 1 中决策树的类型“gini”表示分类回归树 (Classification and Regression Trees, CART) 算法,梯度提升树和随机森林都采用该决策树作为基础学习器。

在 Replay-Attack 测试集上,评估各机器学习最优模型的性能,结果如表 2 所示。

表 2 模型评估

分类器	APCER/%	BPCER/%	ACER/%
RF	0.250	30.000	15.125
DT	1.530	13.750	7.650
SVM	0.760	1.250	1.005
GBT	0.760	1.250	1.005

梯度提升树模型和支持向量机模型在测试集上都取得了显著的成效。在面对人脸活体检测的图像分类任务时,需要有效地处理大量具有复杂非线性关系的数据。梯度提升树和支持向量机都能有效处理非线性关系,适用于各种复杂的数据。但在大规模数据和高维数据集上,梯度提升树的计算相对更为高效。因此,本文采用梯度提升树作为分类器,区分真实人脸和虚假人脸。

本文对比了近年来国内外的基于面部生理信号实现活体检测的方法在 Replay-Attack 数据集上的性能,如表 3 所示。

表 3 方法对比

方法	EER/%	HTER/%
Li ^[14]	31.00	30.30±13.40
Liu ^[23]	19.40	19.30±11.20
Nowara ^[15]	-	25.50
Li CVPR ^[32] +LTSS ^[33]	-	13.00
SSR ^[34] +LTSS ^[33]	-	5.90
rPPG ^[19]	7.90	5.60±3.10
rPPG+CNN ^[19]	5.65	2.03
本文	0.38	1.96

3 结论

本文提出了一种基于面部信号的人脸活体检测方法,只需通过普通的彩色视频就能识别欺诈攻击。通过在 Replay-Attack 数据集的测试,本文验证了该方法在面对打印攻击、照片屏显和视频屏显欺诈攻击时表现出卓越的性能,准确率达到了 99.15%。为提高人脸活体检测的实

用性和安全性带来了良好的效果。

然而,尽管本文所提方法在活体检测领域取得了显著的成果,仍然存在一些挑战和改进的空间。未来的研究可以集中在:(1)采用深度学习算法代替传统算法提取rPPG信号;(2)改善从面部信号提取的特征;(3)进一步拓展数据集规模以应对更广泛的场景。综合而言,本研究为人脸活体检测领域的发展提供了有益的启示,为构建更安全可靠生物特征认证系统奠定了坚实基础。

参考文献

- [1] AKHTAR Z, MICHELONI C, FORESTI G L. Biometric liveness detection: Challenges and research opportunities[J]. IEEE Security & Privacy, 2015, 13(5): 63-72.
- [2] YU Z, LI X, NIU X, et al. Face anti-spoofing with human material perception[C]. Computer Vision - ECCV 2020: 16th European Conference, 2020: 557-575.
- [3] WEN D, HAN H, JAIN A K. Face spoof detection with image distortion analysis[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(4): 746-761.
- [4] BOULKENAFET Z, KOMULAINEN J, HADID A. Face spoofing detection using colour texture analysis[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(8): 1818-1830.
- [5] YU Z, LI X, SHI J, et al. Revisiting pixel-wise supervision for face anti-spoofing[J]. IEEE Transactions on Biometrics, Behavior, and Identity Science, 2021, 3(3): 285-295.
- [6] ZHANG K Y, YAO T, ZHANG J, et al. Face anti-spoofing via disentangled representation learning[C]. Computer Vision - ECCV 2020: 16th European Conference, 2020: 641-657.
- [7] ZHANG S, LIU A, WAN J, et al. Casia-surf: A large-scale multi-modal benchmark for face anti-spoofing[J]. IEEE Transactions on Biometrics, Behavior, and Identity Science, 2020, 2(2): 182-193.
- [8] LIU Y, STEHOUWER J, JOURABLOO A, et al. Deep tree learning for zero-shot face anti-spoofing[C]. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2019: 4680-4689.
- [9] YANG X, LUO W, BAO L, et al. Face anti-spoofing: Model matters, so does data[C]. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2019: 3507-3516.
- [10] YU Z, ZHAO C, WANG Z, et al. Searching central difference convolutional networks for face anti-spoofing[C]. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2020: 5295-5305.
- [11] WANG Z, WANG Z, YU Z, et al. Domain generalization via shuffled style assembly for face anti-spoofing[C]. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2022: 4123-4133.
- [12] NIKITIN M Y, KONUSHIN V S, KONUSHIN A S. Face anti-spoofing with joint spoofing medium detection and eye blinking analysis[J]. Компьютерная оптика, 2019, 43(4): 618-626.
- [13] YU Z, ZHAO C, WANG Z, et al. Searching central difference convolutional networks for face anti-spoofing[C]. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2020: 5295-5305.
- [14] LI X, KOMULAINEN J, ZHAO G, et al. Generalized face anti-spoofing by detecting pulse from face videos[C]. 2016 23rd International Conference on Pattern Recognition (ICPR), IEEE, 2016: 4244-4249.
- [15] NOWARA E M, SABHARWAL A, VEERARAGHAVAN A. Ppgsecure: Biometric presentation attack detection using photoplethysmograms[C]. 2017 12th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2017), IEEE, 2017: 56-62.
- [16] LIU S Q, LAN X, YUEN P C. Remote photoplethysmography correspondence feature for 3D mask face presentation attack detection[C]. Proceedings of the European Conference on Computer Vision (ECCV), 2018: 558-573.
- [17] LIU Y, JOURABLOO A, LIU X. Learning deep models for face anti-spoofing: Binary or auxiliary supervi-

- sion [C]. Proceedings of the IEEE conference on computer vision and pattern recognition, 2018: 389–398.
- [18] YU Z, SHEN Y, SHI J, et al. Physformer: Facial video-based physiological measurement with temporal difference transformer [C]. Proceedings of the IEEE/CVF conference on computer vision and pattern recognition, 2022: 4186–4196.
- [19] 殷超. 基于生理信号和深度学习的人脸活体检测方法研究[D]. 南充: 西华师范大学, 2021.
- [20] SUN Y, THAKOR N. Photoplethysmography revisited: from contact to noncontact, from point to imaging [J]. IEEE transactions on biomedical engineering, 2015, 63(3): 463–477.
- [21] 饶治, 李炳霖, 隋雅茹, 等. 成像式光体积描记术精神压力检测[J]. 中国光学(中英文), 2022, 15(6): 1350–1359.
- [22] DEHAAN G, JEANNE V. Robust pulse rate from chrominance-based rPPG [J]. IEEE Transactions on Biomedical Engineering, 2013, 60(10): 2878–2886.
- [23] LIU S, YUEN P C, ZHANG S, et al. 3D mask face anti-spoofing with remote photoplethysmography [C]. Computer Vision – ECCV 2016: 14th European Conference, 2016: 85–100.
- [24] 嵇晓强, 刘振瑶, 李炳霖, 等. 面部视频非接触式生理参数感知[J]. 中国光学, 2022, 15(2): 276–285.
- [25] 刘振瑶. 基于IPPG的人体生命体征感知研究[D]. 长春: 长春理工大学, 2022.
- [26] YIN X, LIU X. Multi-task convolutional neural network for pose-invariant face recognition [J]. IEEE Transactions on Image Processing, 2017, 27(2): 964–975.
- [27] WOOD E, BALTRUŠAITIS T, HEWITT C, et al. 3d face reconstruction with dense landmarks [C]. European Conference on Computer Vision. Cham: Springer Nature Switzerland, 2022: 160–177.
- [28] 栗立威, 陶雪, 饶治, 等. 基于IPPG技术的情绪识别算法[J]. 长春理工大学学报(自然科学版), 2023, 46(5): 115–121.
- [29] LIN B, LI X, YU Z, et al. Face liveness detection by rppg features and contextual patch-based cnn [C]. Proceedings of the 2019 3rd international conference on biometric engineering and applications, 2019: 61–68.
- [30] CHINGOVSKA I, ANJOS A, MARCEL S. On the effectiveness of local binary patterns in face anti-spoofing [C]. 2012 BIOSIG—proceedings of the international conference of biometrics special interest group (BIOSIG), IEEE, 2012: 1–7.
- [31] 谢晓华, 卞锦堂, 赖剑煌. 人脸活体检测综述[J]. 中国图象图形学报, 2022, 27(1): 63–87.
- [32] LI X, CHEN J, ZHAO G, et al. Remote heart rate measurement from face videos under realistic situations [C]. Proceedings of the IEEE conference on computer vision and pattern recognition, 2014: 4264–4271.
- [33] HEUSCH G, MARCEL S. Pulse-based features for face presentation attack detection [C]. 2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS), IEEE, 2018: 1–8.
- [34] WANG W, STUIJK S, DEHAAN G. A novel algorithm for remote photoplethysmography: Spatial subspace rotation [J]. IEEE transactions on biomedical engineering, 2015, 63(9): 1974–1984.