基于上下文特征与单类支持向量机的人脸活体检测

闫 龙，胡晓鹏
（西南交通大学 信息科学技术学院，四川 成都 611756）

摘 要： 非法入侵者通过伪装人脸欺骗识别系统，给人脸识别应用带来严重威胁。现有人脸活体检测方法多为在同一数据集内进行训练和测试，当应用在跨数据集场景中时效果并不理想。针对这一问题，提出了利用 HOG 等算法对上下文环境中的线索信息进行提取，提取出来的特征送入单类支持向量机进行训练、分类。将分类结果与上下文环境中异常线索的探测结果相结合。算法在公开的数据集 NUAA 和 CASIA-FASD 上进行了验证，实验结果表明在跨数据集检测时该算法的泛化能力及检测准确率较已存在算法有所提高。

关键词： 人脸活体检测；上下文特征；单类支持向量机；跨数据集
中图分类号： TN919.8 **文献标识码：** A DOI：10.16157/j.issn.0258-7998.191346

中文引用格式： 闫龙，胡晓鹏. 基于上下文特征与单类支持向量机的人脸活体检测[J].电子技术应用，2020，46(6)：32-35.
英文引用格式： Yan Long，Hu Xiaopeng. Face anti-spoofing based on context and OCSVM[J]. Application of Electronic Technique，2020，46(6)：32-35.

Face anti-spoofing based on context and OCSVM

Yan Long，Hu Xiaopeng
(School of Information Science & Technology，Southwest Jiaotong University，Chengdu 611756，China)

Abstract： Spoofing face can be used to deceive face authentication system for illegal purposes，and thus it poses a serious threat to the face recognition system. Most of the existing methods are training and testing in the same dataset，and the effect is not ideal when they are used in cross dataset scenario. In order to solve this problem，this paper proposes to use histogram of oriented gradients (HOG) to extract the cue information in the context and then send the extracted features to the one-class support vector machine (OCSVM) for training and classification. The classification results are combined with the abnormal cues detected in the context. And the algorithm is verified on the public database NUAA and CASIA-FASD. The experimental results show that the generalization ability and detection accuracy of the proposed algorithm has improved over the existing method when used in cross dataset scenario.

Key words： face anti-spoofing；context；OCSVM；cross dataset

0 引言

随着生物特征识别技术的日臻完善，人脸识别(Facial Recognition)、指纹识别(Fingerprint Recognition)等生物特征识别将在身份验证中扮演着重要角色，作为主流技术的人脸识别，有着认证自然、可视化等优点。人脸识别已经在最近几年取得了飞速的发展，并且已经逐渐应用到各行各业中。但也伴随产生了一些问题：一些不法分子利用一些技术仿冒人脸去欺骗识别系统，给合法用户带来了经济财产损失，造成社会纷扰。为了更安全地进行身份认证和检测身份来源的真实性，活体检测技术必不可少。对认证系统进行欺骗的对象一般都是刚性的、僵硬的物体(例如：打印的照片、手机或平板电脑屏幕显示的照片等)，因此通过人脸活体检测技术(Face Anti-Spoofing)来预防欺骗是常常采取的措施。人脸识别系统主要容易受到以下手段的欺骗：(1)用照片或高清打印图像假冒真人；(2)用在公开场合录制的视频或网上公开的视频片段来冒充真人；(3)用蜡或塑料等材质构造的 3D 模型来假冒真人。其中，照片欺骗是最常见的欺骗方法。

从 2004 年开始，国内外的学者对人脸活体检测技术进行了大量的研究。这些研究主要分为 4 类方法。(1)添加辅助设备的方法：使用红外摄像头、热成像摄像头等辅助设备检测活体特征[1]。(2)基于运动信息的方法：PAN G 等人[2]使用条件随机场人眼模型对眨眼动作建模，获取了较高的眨眼检测率，并通过检测是否有眨眼动作来进行活体检测。(3)基于手工提取特征的方法：LI J[3]等人利用二维傅里叶频谱分析方法进行活体检测，但其对扭曲照片的检测准确率不太理想；MÄÄTTÄ J[4]、TIAGO D F P[5]等人分别提出了使用局部二值模式(Local Binary Patterns，LBP)特征以及结合了时间和空间信息的LBP-TOP(Local

Binary Pattern histograms from Three Orthogonal Planes)特征进行活体检测；2015 年 KIM W 等人[6]首次提出基于 LSP(Local Speed Patterns)特征的检测方法，并取得了较好的检测结果。(4)基于深度学习的方法：Yang Jianwei[7]等人首次使用了卷积神经网络(Convolutional Neural Networks，CNN)的方法；李冰等人[8]提出将人脸的灰度图和局部定向模式分别作为两个不同结构的网络的输入，然后采用主成分分析对每个网络的全连接层的输出分别降维后级联，最后将级联的特征向量送入极限学习机(Extreme Learning Machine，ELM)进行活体检测；文献[9]通过将真实人脸和照片进行数据去中心化、ZCA 白化去噪声、随机旋转等处理，并使用卷积神经网络对照片的面部特征进行提取，提取出来的特征送入神经网络训练、分类，从而得到检测结果。

虽然上述研究方法已取得了一些成果，但仍然存在一些问题。例如，在某些现实应用场景中不具备采集动态影像进行活体检测的条件，而添加辅助设备也增加了应用的成本。另外，手工提取特征的方法具有主观性、不全面等缺陷，导致预测结果不理想，而基于深度学习的方法所获得的训练模型在跨数据集(即模型训练数据集与测试数据集不同)检测时表现不佳。

本文提出基于上下文特征与单类支持向量机(One Class Support Vector Machine，OCSVM)的人脸活体检测方法。首先通过方向梯度直方图(Histogram of Oriented Gradients，HOG)对欺骗行为中普遍存在的上下文特征(例如，非法入侵者为了通过手机呈现待识别对象的人脸照片而引入的规则矩形边框)进行提取，然后使用 OCSVM 对特征向量进行训练分类，接下来利用 TensorFlow 目标检测 API(应用程序接口)对图片中的特定欺骗特征(例如，握住手机等欺骗媒介的人手)进行检测，最后根据 OCSVM 的分类结果以及 TensorFlow 的目标检测结果进行真假判定。

1 基于上下文特征与 OCSVM 的人脸活体检测方案

当非法入侵者对人脸识别系统进行欺骗时，为了呈现待识别对象的人脸照片，在入侵过程中往往会引入欺骗媒介的上下文特征，例如，图 1 中的矩形手机边框及握住手机的人手。而真实的待检测人脸周围往往不会有这些成规律性的特征。当使用 HOG 对待检测人脸图像进行处理后，真实的待检测人脸与呈现在欺骗媒介里的待检测人脸的特征向量之间存在较大差异。基于这种差异，利用 OCSVM 分类器对所得到的特征向量进行训练，从而得到 OCSVM 分类器的分类模型。当对人手进行检测时，由于人手会呈现出多种不同的姿势，且当握住欺骗媒介时手掌部分会被遮住仅露出部分手指，其所呈现的特征具有一定的多样性。在处理含有多样性、复杂性特征的训练样本时，基于深度学习的目标检测方法具有较好的检测性能，因此本方案使用基于深度学习的目标检测框架 TensorFlow[10]对人手进行检测。

图 1 真实人脸及欺骗人脸(第一行)和对应图片的 HOG 特征可视化结果(第二行)

1.1 训练过程

1.1.1 矩形框特征训练

由于使用单类支持向量机作为分类器，本文仅使用训练数据集中含有欺骗人脸的照片来进行模型训练。首先，通过使用 OpenCV CascadeClassifier 分类器来识别输入图片中的人脸，然后将所得人脸识别区域的宽度及高度分别扩展至其原有长度的一倍及两倍。这样做的目的是去除图片中其他不需要的背景信息，但保留可能出现的上下文特征。将扩展后的区域截取出来并正则化为 80×70 大小的图片，用 HOG 算法处理正则化后的图片，从而生成 OCSVM 分类器的输入特征向量，再将特征向量送入分类器进行训练得到分类模型。

1.1.2 人手特征训练

在训练人手检测模型时，通过使用 TensorFlow 目标检测 API 训练 EgoHands 与 CoCoHand 数据集得到人手检测模型。EgoHands 与 CoCoHand 数据集包含了优质的像素级别标注，分别含有 4 800 张与 4 535 张包含人手的图像。在训练数据时本方案使用迁移学习来缩短训练模型所需的时间，即使用一个已经在相关领域(例如，图像分类)训练过的现有模型，并重新对它的最后一层或几层网络进行训练从而生成人手检测模型。

1.2 检测过程

本方案通过对图片中待检测人脸周围出现的规则矩形边框以及人手进行检测，从而来判断待测对象是否为真实人脸。

当对待识别对象进行检测时，首先提取输入图像的 HOG 特征向量，然后将提取到的特征向量送入训练好的 OCSVM 模型进行分类判定。如果分类结果为真(即在人脸周围检测到规则矩形边框)则判定为假人脸，否则将输入图像再送入 TensorFlow 人手检测模型。如果检测到人手则判定为假人脸，否则判定为真实人脸。整个检测方案如图 2 所示。

2 OCSVM 单类支持向量机

OCSVM 算法[11]是 Scholkopf 在传统 SVM 算法的基础上发展而来的，属于无监督学习算法。其原理是将所有输入样本作为目标样本，通过核函数将输入样本映射到高维空间中，使得存在一个最优超球体，能够尽可能地

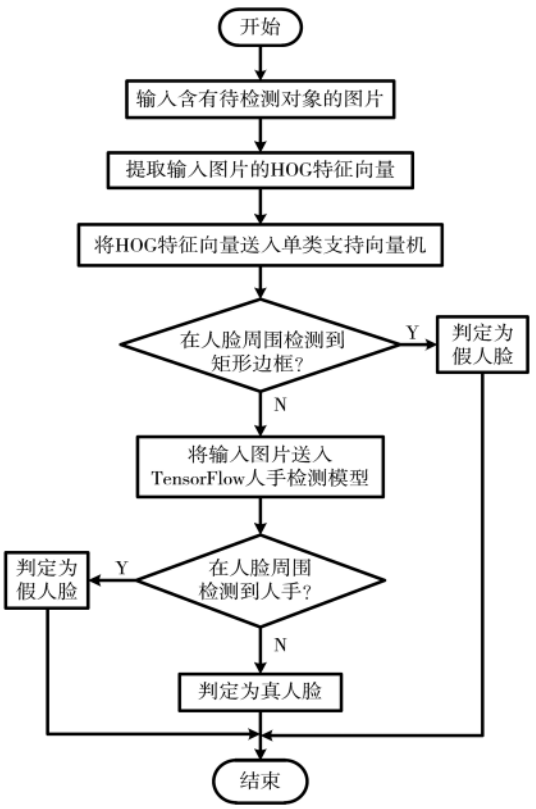

图 2 基于上下文环境与 OCSVM 的人脸活体检测方案

将目标样本包含在超球体中，而将非目标样本排除在超球体外，同时最小化该超球体的体积。由于 OCSVM 算法只需要单类样本，就可以通过对其训练得到二分类模型，而在某些人脸识别应用场景中真实人脸样本与假人脸样本分布不均匀，因此，OCSVM 算法很适合用来解决样本数量分布不均匀时训练活体检测分类器遇到的问题。OCSVM 原理如图 3 所示。

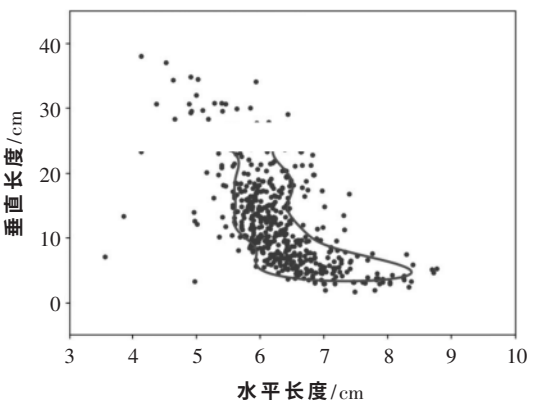

图 3 OCSVM 原理图

OCSVM 模型将样本集聚类，并通过改变参数调整模型的结构，得到最优模型解。欺骗攻击图片的选择就是一种聚类，每一张输入 OCSVM 分类器的图片即为一个样本，每个样本都是超维空间中的一个点，OCSVM 就是要选择一个超球体，使其尽量覆盖所有样本点的同时最小化超球体的体积。即 OCSVM 使用超球体来代替超平面对数据进行划分，其目标函数为：

$$\min_{R,\zeta,c} R^2+\frac{1}{vl}\sum_{i=1}^{l}\zeta_i$$

$$\text{Subject to} \quad \|\boldsymbol{x}_i-\boldsymbol{c}\|^2\leqslant R^2+\zeta_i$$

$$\zeta_i\geqslant 0, i=1,2,\cdots,l \tag{1}$$

式中：R 为模型半径；ζ 为松弛因子；l 为样本数量；c 为圆心值；v 为模型平衡参数，满足 $0<v\leqslant 1$。

通过设定参数，使超球体半径及超球体所包含的训练样本数目进行折中。

上述目标函数的拉格朗日函数为：

$$L=R^2+\frac{1}{vl}\sum_{i=1}^{l}\zeta_i-\sum_{i=1}^{l}\alpha_i(R^2+\zeta_i-\|\boldsymbol{x}_i-\boldsymbol{c}\|^2)-\sum_{i=1}^{l}\zeta_i\beta_i \tag{2}$$

式中：$\alpha_i\geqslant 0$ 和 $\beta_i\geqslant 0$ 为拉格朗日乘积因子。

对式(2)求偏导数得：

$$\frac{\partial L}{\partial R}=2R-\sum_{i=1}^{l}\alpha_i\cdot 2R=0 \tag{3}$$

$$\frac{\partial L}{\partial C}=\sum_{i=1}^{l}\alpha_i\cdot 2(\boldsymbol{x}_i-\boldsymbol{c})=0 \tag{4}$$

$$\frac{\partial L}{\partial \zeta_i}=\frac{1}{vl}-\alpha_i-\beta_i=0 \tag{5}$$

将式(3)~式(5)带入式(2)，得到式(1)的对偶问题为：

$$\min_{\alpha}\sum_{i,j}\alpha_i\alpha_j(\boldsymbol{x}_i\cdot\boldsymbol{x}_j)-\sum_{i}\alpha_i(\boldsymbol{x}_i\cdot\boldsymbol{x}_j)$$

$$\text{Subject to} \quad 0\leqslant\alpha_i\leqslant\frac{1}{vl}, i=1,2,\cdots,l$$

$$\sum_{i=1}^{l}\alpha_i=1 \tag{6}$$

通过最优化方法求得解 $\alpha_i(i=1,2,\cdots,l)$。带入式(3)与式(4)得到半径值和圆心值。

3 实验结果

对本文中的算法进行测试，应用南京航空航天大学公开的数据集 NUAA 以及中国科学院自动化研究所发布的 CASIA-FASD 数据集，将所提出的方法在 NUAA 数据集上进行模型训练以及参数调整，然后在 CASIA-FASD 数据集上进行测试。在 NUAA 数据集中欺骗样本为7 509 张照片，从其中随机选取 3 000 张照片作为训练集，采用 10-folder 交叉验证[12]方式对算法进行验证调参(其中测试集含有 2 700 张照片，验证集含有 300 张照片)。CASIA-FASD 数据集中包含了来自 50 个对象的 600 段视频，其中有 150 段合法请求及 450 段欺骗攻击。测试集中选择了 360 段视频，每段视频中随机截取 5 帧图片，得到1 800 张图片作为测试集。训练集和测试集的分配如表 1 所示。

为了验证改进算法的性能，本文将实验结果与基于

表 1 训练集与测试集样本分配表

训练集	验证集	测试集	总和
2 700	300	1 800	4 800

LBP 纹理特征以及使用卷积神经网络 CNN 的人脸活体检测方法进行对比，结果如表 2 所示。表中 FRR(False Reject Rate)为错误拒绝率，FAR(False Accept Rate)为错误接受率，HTRE(Half Total Error Rate)为半错误率。半错误率指的是错误接受率和错误拒绝率总和的一半。

表 2 跨数据集活体检测准确率对比

检测方法	FRR/%	FAR/%	HTRE/%
LBP	11.4	80.3	45.9
CNN	47.2	44.3	45.7
改进方法	0.5	10.02	5.26

通过对比发现，LBP 和 CNN 检测方法都取得了较高的半错误率，表明在进行跨数据集活体检测时这两种方法的泛化性能较差。而改进方法的 HTER 值为 5.26%，表明其检测准确率高于前两种方法。

4 结论

本文针对现有活体检测方法在跨数据集时泛化能力较差从而导致检测准确率低的问题，提出了基于检测环境中的上下文信息并使用单类支持向量机对检测对象进行分类的活体检测方法。通过实验发现，改进方法的泛化能力优于 LBP 和 CNN 方法。但在某些活体检测场景中可能没有可以利用的上下文信息，此时如何实现准确率较高的跨数据集活体检测将是后续研究的方向。

参考文献

[1] 孙霖.人脸识别中的活体检测技术研究[D].杭州：浙江大学，2010.

[2] PAN G，SUN L，WU Z，et al.Eyeblink-based anti-spoofing in face recognition from a generic webcamera[C].IEEE 11th International Conference on Computer Vision，IEEE，2007：1-8.

[3] LI J，YU W，KUANG G Y，et al.A compound face recognition system design[J].Journal of National University of Defense Technology(China)，2003，25(3)：45-48.

[4] MÄÄTTÄ J，HADID A，PIETIKÄINEN M.Face spoofing detection from single images using micro-texture analysis[C].2011 International Joint Conference on Biometrics(IJCB).IEEE，2011：1-7.

[5] TIAGO D F P，ANDRÉ A，JOSÉ MARIO D M，et al.LBP-TOP based countermeasure against face spoofing attacks[M].Computer Vision-ACCV 2012 Workshops.Springer Berlin Heidelberg，2013.

[6] KIM W，SUH S，HAN J J.Face liveness detection from a single image via diffusion speed model[J].IEEE Transactions on Image Processing，2015，24(8)：2456-2465.

[7] Yang Jianwei，Lei Zhen，LI S Z.Learn convolutional neural network for face anti-spoofing[J].Computer Science，2014，9218：373-384.

[8] 李冰，王宝亮，由磊，等.应用并联卷积神经网络的人脸防欺骗方法[J].小型微型计算机系统，2017，38(10)：2187-2191.

[9] 黄海新，张东.基于深度学习的人脸活体检测算法[J].电子技术应用，2019，45(8)：44-47.

[10] 黄睿，陆许明，邬依林.基于 TensorFlow 深度学习手写体数字识别及应用[J].电子技术应用，2018，44(10)：12-16.

[11] 尹传环，牟少敏，田盛丰，等.单类支持向量机的研究进展[J].计算机工程与应用，2012，48(12)：1-5.

[12] 刘学艺，李平，郜传厚.极限学习机的快速留一交叉验证算法[J].上海交通大学学报，2011，45(8)：1140-1145.

(收稿日期：2019-12-09)

作者简介：

闫龙(1989-)，男，硕士研究生，主要研究方向：人脸活体检测、机器学习、软件架构。

胡晓鹏(1972-)，男，博士，副教授，主要研究方向：软件架构、机器学习。

(上接第 31 页)

993-1022.

[9] 王振振，何明，杜永萍.基于 LDA 主题模型的文本相似度计算[J].计算机科学，2013，4(12)：229-232.

[10] 曾祥坤，张俊辉，石拓，等.基于主题提取模型的交通违法行为文本数据的挖掘[J].电子技术应用，2019，45(6)：41-45.

[11] 徐佳俊，杨飏，姚天昉，等.基于 LDA 模型的论坛热点话题识别和追踪[J].中文信息学报，2016，30(1)：43-49.

[12] 唐明，朱磊，邹显春.基于 Word2vec 的一种文档向量表示[J].计算机科学，2016，43(6)：214-217.

[13] BROWN P F，DESOUZA P V，MERCER R L.Class-based n-gram models of natural language[J].Journal Computational Linguistics，1992，18(4)：467-479.

(收稿日期：2019-11-20)

作者简介：

肖晗(1994-)，男，硕士研究生，主要研究方向：自然语言处理。

毛雪松(1975-)，男，博士，教授，主要研究方向：智能驾驶路径规划、环境信息感知和智能光设备。

朱泽德(1985-)，男，博士，副研究员，主要研究方向：自然语言处理。

版权声明