

面向 VTM 的交互式活体检测算法

马钰锡, 谭 励, 董 旭, 于重重

(北京工商大学 计算机与信息工程学院 食品安全大数据技术北京市重点实验室, 北京 100048)

摘 要: 为提升远程视频柜员机人脸识别登录系统的识别率和安全性, 将改进的眨眼检测、背景检测和随机组合动作指令相结合, 提出一种交互式活体检测算法。基于 OpenCV 级联分类器人脸检测和局部二值特征人脸对齐算法, 结合坐标比例和眼球色素变化改进眨眼检测。利用背景检测和随机组合动作指令抵御动态视频攻击, 加入图像质量检测与校正功能, 使系统在弱光、歪斜等环境影响下对活体人脸检测有较好的检测效果。在活体人脸数据库 CASIA-FASD 和自建样本库上进行实验, 结果表明, 该算法识别率达到 97.67%, 与多光谱、卷积神经网络等检测算法相比性能有明显的提升。

关键词: 活体检测; 人脸识别; 眨眼检测; 背景检测; 局部二值特征

中文引用格式: 马钰锡, 谭励, 董旭, 等. 面向 VTM 的交互式活体检测算法[J]. 计算机工程, 2019, 45(3): 256-261.

英文引用格式: MA Yuxi, TAN Li, DONG Xu, et al. Interactive liveness detection algorithm for VTM[J]. Computer Engineering, 2019, 45(3): 256-261.

Interactive Liveness Detection Algorithm for VTM

MA Yuxi, TAN Li, DONG Xu, YU Chongchong

(Beijing Key Laboratory of Big Data Technology for Food Safety, School of Computer and Information Engineering, Beijing Technology and Business University, Beijing 100048, China)

[Abstract] In order to improve the recognition rate and security of the Video Teller Machine (VTM) face recognition login system, an interactive liveness detection algorithm that combines improved blink detection, background detection and random combined action instructions is proposed. Based on the OpenCV cascade classifier face detection and Local Binary Feature (LBF) face alignment algorithm, combining the coordinate proportion and the eye pigment change, the detection method is improved. Uses the background detection and the random combination action instruction to resist the dynamic video attack. Making use of the image quality detection and correction function, the system in weak light, skew and the other environmental condition has a good performance as well. Experiments are carried out on liveness face database CASIA-FASD and self-built sample library, the result shows that the recognition rate reaches 97.67%, which is obviously improved than multispectral, convolutional neural network, and the other existing detection algorithms.

[Key words] liveness detection; face recognition; blink detection; background detection; Local Binary Feature (LBF)

DOI: 10.19678/j.issn.1000-3428.0050353

0 概述

随着人脸识别技术日趋成熟, 其商业化应用愈加广泛。然而, 人脸极易通过照片、视频、人脸模型等方式进行复制, 假冒合法用户欺骗系统, 从而对远程视频柜员机 (Video Teller Machine, VTM) 人脸识别与认证系统的安全构成严重威胁^[1-3]。因此, 设计一种面向 VTM 的活体检测算法, 在 VTM 的人脸识别身份认证中加入活体检测技术非常必要。

活体检测是一项判断提交的生物特征是否来自有生命个体的技术, 主要包括基于图像微纹理的方

法^[4-5]、基于多光谱技术的方法^[6-7]和基于交互式面部动作检测的方法^[8]。基于图像微纹理的方法提取的特征维数大, 计算复杂度较高^[9]。基于多光谱技术的方法需要特殊的采集设备, 用户体验较差^[10]。因此, 目前投入市场应用的活体检测技术大多是基于交互式面部动作指令的判别, 例如支付宝、滴滴出行、百度文库等“刷脸登录”的方法, 都是以用户配合完成眨眼、摇头等动作实现活体检测。

文献[11]通过视频流捕捉 2 个顺序且独立的脸部帧, 使用隐马尔可夫模型生成特征, 分析两帧中的眨眼变化来抵御攻击。文献[12]提出一种基于纹理

基金项目: 国家自然科学基金 (61702020); 北京市自然科学基金 (4172013)。

作者简介: 马钰锡 (1995—), 男, 硕士研究生, 主研方向为计算机视觉、人工智能; 谭 励, 教授、博士; 董 旭, 硕士; 于重重, 教授、博士。

收稿日期: 2018-01-30 **修回日期:** 2018-03-01 **E-mail:** tanli@th.btbu.edu.cn

分析和运动检测的框架,利用堆叠的自动编码器和 softmax 分类器相连,检测脸部的活跃度来验证活体。文献[13]通过 haar 分类器检测脸部宏观特征,并分割出眼睛和嘴巴的区域,利用主成分分析 (Principal Component Analysis, PCA) 方法对眼睛和嘴巴的变化进行活体检测。

目前,人脸识别系统在现实应用场景中主要面临二次翻拍照片人脸攻击、二次翻拍视频人脸攻击和三维人脸模型攻击 3 种攻击类型^[14]。现有的交互式活体检测方法并不能完全抵御这 3 种攻击。例如,可以通过照片折叠、翻转等角度变化模拟指定动作,或提前录制相应的视频进行认证,达到欺骗系统、成功登录的目的。此外,检测过程容易受到检测环境的限制,例如,光照强度、拍摄角度等,均会给检测结果和系统性能带来一定的影响^[15-16]。

针对上述方案存在的缺陷,本文提出一种面向 VTM 改进的交互式活体检测算法,通过眼球色素差与眼部特征点变化相结合的认证方法改进眨眼检测,抵御静态照片的模拟攻击。采用随机组合动作指令和背景检测的方法,抵御视频和 3D 模具的模拟攻击。加入图像质量检测与校正过程,消除检测环境对结果的影响。在实现 OpenCV 级联分类器人脸检测^[17]和基于局部二值特征 (Local Binary Feature, LBF) 人脸对齐^[18]的基础上,提高活体检测的健壮性。在公开活体人脸数据库 CASIA-FASD^[19]和自建样本库上进行实验,以验证该算法的准确性和有效性。

1 检测算法具体步骤

改进的交互式活体检测算法包括图像质量检测与校正、眨眼检测、唇部动作检测、背景检测等环节,整体流程如图 1 所示。打开摄像头开始活体检测,首先采用 OpenCV 内置的 haar 级联分类器对视频流进行人脸检测^[17],然后采用基于 LBF 的机器学习算法进行人脸对齐^[18],对采集到的人脸图片进行图像质量检测与校正,调整亮度、角度等使其满足后续的检测过程,最后按照随机组合动作指令进行改进的眨眼检测和唇部动作检测,并执行背景检测。客户按照指令完成相应的动作,如果背景检测合格,则通过活体检测。

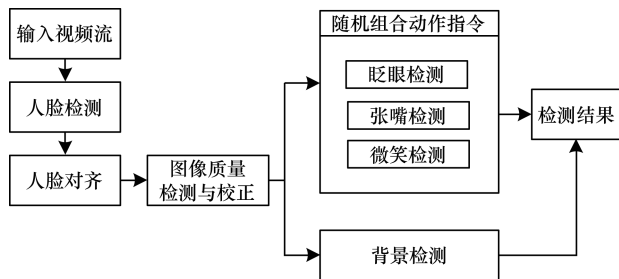


图 1 活体检测整体流程

1.1 图像质量检测与校正

对视频流中的每一帧图像进行人脸检测和对齐

后,首先要对采集到的人脸图像进行质量检测及校正。调整和优化人脸角度、区域亮度和对比度,包括将人脸角度调整到正脸角度,根据检测环境的光照强度把图像对比度和亮度调整到设定标准,排除眼睑、眉毛等区域对后续眨眼检测的干扰等。图像质量检测与校正的步骤如下:

步骤 1 采取仿射变换对人脸角度进行校正,目标为人脸对齐后的 68 个关键点。通过式(1)进行仿射变换,将原坐标 (x, y) 转换为校正后的新坐标 (x', y') ,然后根据新的坐标点得到校正后的图像。

$$\begin{bmatrix} x' \\ y' \\ 1 \end{bmatrix} = \begin{bmatrix} m00 & m01 & m02 \\ m10 & m11 & m12 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ 1 \end{bmatrix} = \begin{bmatrix} m00 \cdot x + m01 \cdot y + m02 \\ m10 \cdot x + m11 \cdot y + m12 \\ 1 \end{bmatrix} \quad (1)$$

具体过程如下:

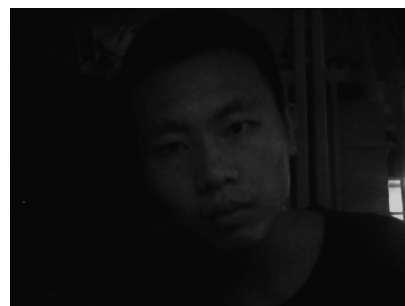
1) 根据人脸对齐后的人眼位置坐标计算两眼中心点,并按照此中心点进行旋转。

2) 计算旋转角度。当人脸摆正时,双眼连线水平,以此为基准计算当前两眼纵坐标差值与横坐标差值的比值,再利用三角函数求出旋转角度。

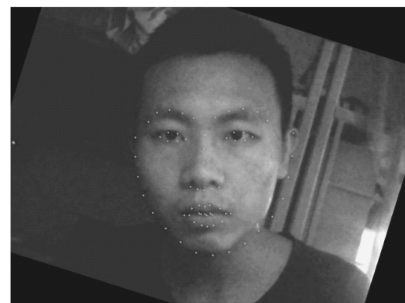
步骤 2 采取基于像素点算子的方法增强图片的对比度和亮度。其基本思想是像素的逐点处理,即输入图片像素值后进行某些全局信息或参数的处理,再输出相应的像素值。线性点运算公式如下:

$$g(x) = \alpha f(x) + \beta \quad (2)$$

其中,参数 α 和 β 分别称作增益参数和偏置参数, α 控制图像的对比度, β 控制图像的亮度, $f(x)$ 表示源图像像素, $g(x)$ 表示输出图像像素。最终调整效果如图 2 所示。



(a) 在环境较差处拍摄的图像



(b) 调整角度和对比度后的图像

图 2 图像质量检测与校正效果

1.2 改进的眨眼检测

1.2.1 基于坐标比例变化的眨眼检测

对输入视频流进行人脸检测和人脸对齐后,分割出如图3所示的人眼区域特征点位置。

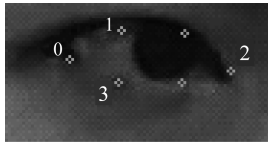


图3 人脸对齐后检测出的眼部区域

根据各个特征点位置的变化可以估计人眼的状态。由于人的双眼对称,以右眼为例,将上下眼皮的特征点位置标号为1和3,左右眼角特征点位置标号为0和2,如图3所示。通过式(3)计算眼睛的宽高比例,判断当前帧中右眼的状态:

$$R(P) = \frac{\|P_0(x) - P_2(x)\|}{P_1(y) - P_3(y)} \quad (3)$$

其中, $R(P)$ 为右眼的宽高比例, $P_i(x)$ 和 $P_i(y)$ 分别为特征点 i 的 x 和 y 坐标值。根据眼睛宽高比的变化,能够判断当前帧中眼睛的睁闭状态,同理可以判断左眼的状态。

1.2.2 基于眼部区域色素差的眨眼检测

检测到眼部区域后,对眼部图像进行灰度化、二值化和中值滤波等形态学操作,统计眼部图像中黑色像素的总和,分析眼部状态变化。首先对眼部区域图像灰度化后做二值化处理,得到黑白图像。由于人眼的眼珠像素比较深沉,并且呈圆形,因此选取一定尺寸的椭圆形结构元素对二值化后的图像进行闭运算,可以消除图像中的小型黑洞和低亮度值的孤立点,排除非眼珠区域对结果的干扰。其数学表达式如下:

$$dst = close(src, element) = erode(dilate(src, element)) \quad (4)$$

其中, dst 代表输出图像, src 代表输入图像, $element$ 代表结构元素。

根据VTM摄像头等硬件设备以及检测距离,调整二值化函数中阈值 $threshold$ 和闭运算中 $kernel$ 值的大小,尽可能地排除眼睑、眼角等干扰因素,得到最佳的眼球二值化图像,如图4(c)只含有眼珠的图像。不同阈值下滤波后的图像如图4所示。

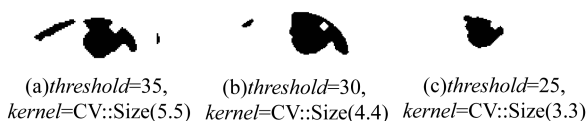


图4 不同阈值下滤波后的眼部图像

计算滤波后眼部图像的像素值,统计每帧图像中眼球像素的总和,分析其动态变化,进而判断是否

发生眨眼动作。基于眼部区域色素差变化的眨眼检测算法如下:

算法1 基于眼部区域色素差的眨眼检测

输入 当前用户眼部图像 P_k

输出 眨眼检测结果

初始化眨眼次数 $i=0$

眨眼检测过程:

1. Loop for n iterations
2. 统计 P_k 中的黑色像素值 V_k
3. If $V_{k-1} \neq 0$ and $V_k = 0$
4. 视为眨眼一次, $i++$
5. If $i \geq 3$
6. 结束循环,活体检测成功
7. End Loop for n iterations

基于坐标比例变化的眨眼检测可预防静态照片的晃动、翻转等攻击,而基于眼部区域色素差的眨眼检测可预防静态照片的极限角度、折叠等模拟眨眼动作的攻击。活体认证时2种检测作为独立的线程并行检测,结果进行“与”运算,在不失速度与准确率的前提下能有效提高对静态照片攻击的防御性。

1.3 唇部动作检测

唇部动作检测分为微笑检测和张嘴检测,均是对唇部区域的动作识别与判断。由于这2种动作所取距离比例值变化非常明显,其原理跟眨眼检测算法类似,因此这里不再赘述。在下文的随机指令中,可配合眨眼检测,组成动作序列实现活体认证。唇部动作检测效果如图5所示。

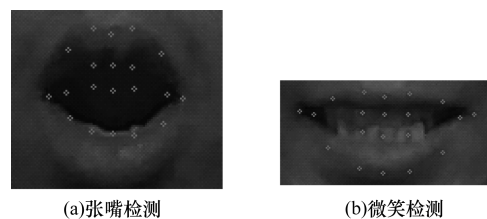


图5 唇部动作检测效果

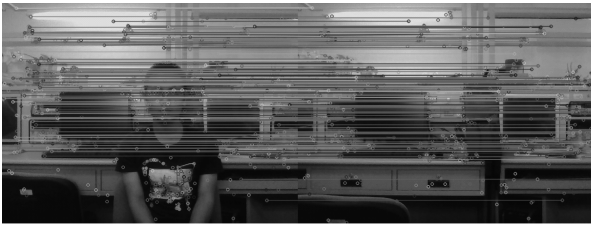
1.4 背景检测和随机组合动作指令

改进后的眨眼检测、微笑检测以及张嘴检测,可有效抵御静态照片的各种角度、动作对VTM活体认证的攻击。针对视频和3D模具的攻击,本文提出一种背景检测与随机动作指令相结合的方案。

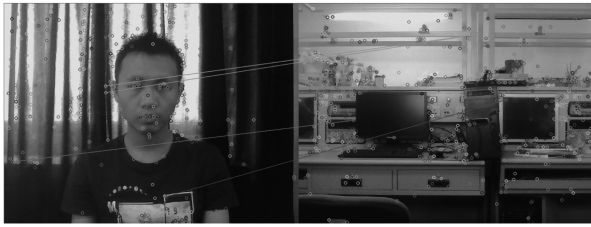
1.4.1 背景检测

在实际应用场景中,由于VTM机的位置和摄像头角度固定,检测的环境不变,因此可提前采集检测环境的背景照片存入本地,提取背景照片中的若干个关键点与当前视频中提取的背景图片的关键点做匹配算法,根据检测环境复杂度设置匹配关键点个数的阈值,以此预防用户在其他地方提前录制视频进行攻击。为了防止攻击视频的背景与实际检测背

景有相似角点的匹配,采用 OpenCV 中的 Surf 角点特征提取和 Brute Force 匹配。背景检测效果如图 6 所示。



(a)相同背景下关键点匹配



(b)不同背景下关键点匹配

图 6 背景检测效果

1.4.2 随机组合动作指令

在传统的活体检测中,系统发出的动作指令仅有摇头、眨眼等,且顺序和过程固定。为防止用户已知动作顺序,提前录制对应视频攻击系统,在上述已实现的眨眼检测、微笑检测与张嘴检测的前提下,设计 3 种动作的随机顺序组成随机组合动作指令,具体步骤如下:

1) 设定一个时间范围,在此范围内,完成系统随机组合的动作,例如左眼睁开,右眼闭合→微笑;微笑→张嘴;张嘴→左右眼同时睁开等。每登录一次,进行一次随机组合的动作指令。

2) 根据实际业务流程的复杂程度,制定复杂程度不同的组合指令,例如 3 个动作或者 4 个及以上。在此认证过程中,VTM 对人脸持续跟踪,防止切换视频,攻击系统。如果系统跟踪中断,即检测不到人脸,则认证失败,检测中止。随机组合动作系统指示界面如图 7 所示。



图 7 随机组合动作系统指示界面

在 VTM 实际使用过程中,系统会限制人脸识别登录次数。如果多次出现异常的检测结果,会引起系统预警、人工防范等。上述背景检测和随机组合动作指令的协同审核,可有效防止用户通过预先录制视频通过认证。

2 实验结果与分析

本文实验平台为 VTM,型号:易时代 ET-R100,OS: Windows 7,CPU: Intel(R) Core i3 3220,内存:64 GB, GPU:NVIDIA Tesla K40 m×2,显存:12 GB×2。

2.1 样本库建立与参数设置

实验收集和建立了自建样本库和公开的活体人脸数据库 CASIA-FASD 这 2 个样本库,每个样本库中都包含活体人脸照片和翻拍人脸照片。在自建样本库中采集 200 张活体人脸照片作为正样本库,再利用罗技 C920 型号的摄像头进行翻拍操作,包含对纸质照片的拍摄和视频录制两部分。在仿真过程中,分别采用静态图片和动态视频模拟实际 VTM 场景进行活体认证攻击。制作样本库时保留人脸的朝向角度、光照强度、表情等不同状态,从而真实地仿真出活体检测系统的现场环境状况,最终的样本库包含 400 张人脸图像。样本库部分人脸图像如图 8、图 9 所示。



图 8 自建样本库部分实验人脸展示



(a)真实人脸 (b)弯曲人脸 (c)裁剪人脸 (d)视频人脸

图 9 CASIA-FASD 真实人脸和伪装人脸样例

实验中VTM摄像头与检测区域的距离为1 m,将眨眼检测中二值化函数的阈值 $threshold$ 设为25,闭运算中 $kernel$ 值设为 $CV::Size(3,3)$,坐标比例 $R(P)$ 变化大于0.7视为睁眼或闭眼,背景检测中匹配点个数大于检测点总数的90%视为检测通过。

2.2 结果分析

为验证算法在数据库中的准确性和优越性,将本文算法与多光谱^[8]、局部二值模式(Local Binary Patterns, LBP)^[20]、普通交互式检测^[18]、卷积神经网络(Convolutional Neural Network, CNN)^[21]等其他活体人脸检测方法进行比较,对比各算法的识别率和检测时间。本文算法对定义内各个动作检测的准确率、不同算法的roc特征曲线如图10、图11所示。

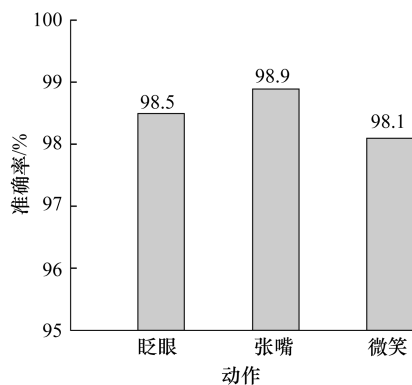


图10 本文算法各种动作检测的准确率

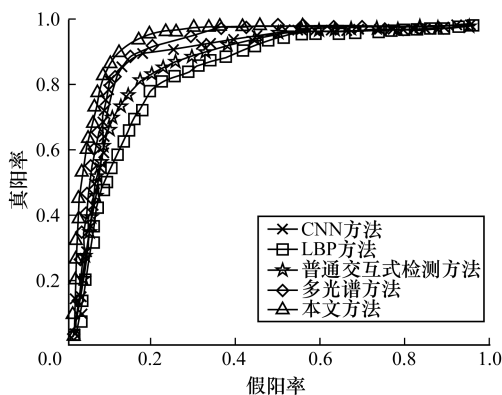


图11 不同方法 roc 特征曲线对比

从图10可以看出,本文算法对定义内的3种面部动作识别准确率均在98%以上,说明算法对定义的面部动作均能做出有效识别。从图11可以看出,相比于其他算法,本文算法具有较好的性能,其线下面积AUC最大,达到96.72%,对数据库中的人脸样本有较好的鉴别效果。

表1为本文算法与其他算法在数据库中的检测效果对比。从表1可以看出,针对照片攻击情况,本文方法的检测正确率达97.67%,比LBP、多光谱、CNN和普通交互式检测正确率分别提高16.14%、0.81%、3.77%、7.15%。针对视频攻击情况,本文

方法的检测正确率达到97.78%,比LBP、多光谱、CNN和普通交互式检测的正确率分别提高20.09%、2.32%、5.18%、8.43%。通过对比可以看出,在照片攻击时,无论是相对传统的普通交互式检测方法,还是目前流行的活体检测方法,本文方法都具有更高的检测正确率。在视频攻击时,LBP、多光谱、CNN和普通交互式相对于照片攻击时正确率都有所下降,其中LBP效果最差,检测正确率下降18.84%,而本文方法仍保持很高的检测正确率,对照片攻击和视频攻击的抵御效果相当。在时效性上,本文方法相比于普通交互式检测算法,检测时间没有明显增大,满足VTM应用环境高精度和实时性的要求。

表1 不同方法的检测效果对比

方法	正确率/%		检测时间 /ms
	照片攻击	视频攻击	
LBP方法	81.53	77.69	238
多光谱方法	96.86	95.46	428
CNN方法	93.90	92.60	367
普通交互式检测方法	90.52	89.35	424
本文方法	97.67	97.78	436

3 结束语

根据当前VTM人脸识别系统面临的问题及现有活体检测算法存在的缺陷,本文提出一种面向VTM改进的交互式活体检测算法。该算法基于OpenCV级联分类器人脸检测和LBF人脸对齐算法,有效结合了改进的眨眼检测、背景检测、随机组合动作指令等。模拟图片攻击和视频攻击实验,结果表明,本文方法的检测正确率与LBP、多光谱、CNN等方法相比均有所提升。尤其是对比普通交互式检测算法,检测正确率提升8%左右,表明该方法可有效抵抗静态照片和动态视频的模拟攻击,能够满足VTM高精度和高安全性的要求。下一步将根据VTM用户的使用反馈来设计交互动作,优化本文算法,提高识别效率并改善交互体验。

参考文献

- [1] XU Y, LI Z, YANG J, et al. A survey of dictionary learning algorithms for face recognition [J]. IEEE Access, 2017, 5: 8502-8514.
- [2] WU L, XU Y, XU X, et al. A face liveness detection scheme to combining static and dynamic features [M]. Berlin, Germany: Springer, 2016: 628-636.
- [3] MOHAN K, CHANDRASEKHAR P, JILANI S A K. A combined HOG-LPQ with Fuz-SVM classifier for object face liveness detection [C] // Proceedings of International Conference on IoT in Social, Mobile, Analytics and Cloud. Washington D. C., USA: IEEE Press, 2017: 531-537.

- [4] YE H C, CHANG H H. Face liveness detection with feature discrimination between sharpness and blurriness [C]// Proceedings of the 15th IAPR International Conference on Machine Vision Applications. Washington D. C., USA: IEEE Press, 2017: 398-401.
- [5] SINGH M, ARORA A S. A robust anti-spoofing technique for face liveness detection with morphological operations[J]. Optik-International Journal for Light and Electron Optics, 2017, 139(4): 347-354.
- [6] LAKSHMINARAYANA N N, NARAYAN N, NAPP N, et al. A discriminative spatio-temporal mapping of face for liveness detection [C]// Proceedings of IEEE International Conference on Identity, Security and Behavior Analysis. Washington D. C., USA: IEEE Press, 2017: 1-7.
- [7] 任玉强, 田国栋, 周祥东, 等. 高安全性人脸识别系统中的唇语识别算法研究[J]. 计算机应用研究, 2017, 34(4): 1221-1225.
- [8] WANG Y, HAO X, HOU Y, et al. A new multispectral method for face liveness detection [C]// Proceedings of IAPR Asian Conference on Pattern Recognition. Washington D. C., USA: IEEE Press, 2013: 922-926.
- [9] 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.
- [10] RAGHAVENDRA R, RAJA K B, VENKATESH S, et al. On the vulnerability of extended multispectral face recognition systems towards presentation attacks [C]// Proceedings of IEEE International Conference on Identity, Security and Behavior Analysis. Washington D. C., USA: IEEE Press, 2017: 1-8.
- [11] PAN G, SUN L, WU Z, et al. Eyeblink-based anti-spoofing in face recognition from a generic webcam [C]// Proceedings of International Conference on Computer Vision. Washington D. C., USA: IEEE Press, 2007: 1-8.
- [12] FENG L, PO L M, LI Y, et al. Face liveness detection using shearlet-based feature descriptors [EB/OL]. [2018-01-05]. http://www.ee.cityu.edu.hk/~lmpo/publications/2017_JEI_face_liveness.pdf.
- [13] SINGH A K, JOSHI P, NANDI G C. Face recognition with liveness detection using eye and mouth movement [C]// Proceedings of International Conference on Signal Propagation and Computer Technology. Washington D. C., USA: IEEE Press, 2014: 592-597.
- [14] 曹瑜, 涂玲, 毋立芳. 身份认证中灰度共生矩阵和小波分析的活体人脸检测算法 [J]. 信号处理, 2014, 30(7): 830-835.
- [15] MEI L, YANG D, FENG Z, et al. WLD-TOP based algorithm against face spoofing attacks [M]. Berlin, Germany: Springer, 2015: 6.
- [16] WILD P, RADU P, CHEN L, et al. Robust multimodal face and fingerprint fusion in the presence of spoofing attacks [J]. Pattern Recognition, 2016, 50(C): 17-25.
- [17] NOBLE F K. Comparison of OpenCV's feature detectors and feature matchers [C]// Proceedings of International Conference on Mechatronics and Machine Vision in Practice. Washington D. C., USA: IEEE Press, 2016: 1-6.
- [18] REN S, CAO X, WEI Y, et al. Face alignment at 3 000 FPS via regressing local binary features [C]// Proceedings of International Conference on Computer Vision and Pattern Recognition. Washington D. C., USA: IEEE Press, 2014: 1685-1692.
- [19] ZHANG Z, YAN J, LIU S, et al. A face anti-spoofing database with diverse attacks [C]// Proceedings of the 5th IAPR International Conference on Biometrics. Washington D. C., USA: IEEE Press, 2012: 26-31.
- [20] LIAO S, JAIN A K, LI S Z. A fast and accurate unconstrained face detector [J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2016, 38(2): 211-223.
- [21] AKBULUT Y, SENGUR A, BUDAK U, et al. Deep learning based face liveness detection in videos [C]// Proceedings of International Artificial Intelligence and Data Processing Symposium. Washington D. C., USA: IEEE Press, 2017: 1-4.

编辑 樊丽娜

(上接第255页)

- [9] 周燕, 曾凡智, 赵慧民. 基于压缩感知的视频双水印算法研究 [J]. 计算机科学, 2016, 43(5): 132-139.
- [10] 姚涛, 阙大顺, 王刚. 基于 Contourlet 变换的双重视频水印方案 [J]. 计算机工程, 2011, 37(8): 143-145.
- [11] 熊祥光. 空域强鲁棒零水印方案 [J]. 自动化学报, 2018, 44(1): 160-175.
- [12] 赵春晖, 刘巍. 基于分块压缩感知的图像半脆弱零水印算法 [J]. 自动化学报, 2012, 38(4): 609-617.
- [13] 李雪景, 李江隐, 康宝生, 等. 基于图像插值和直方图平移的可逆水印算法 [J]. 计算机应用研究, 2016, 33(4): 1159-1163.
- [14] LING H, WANG L, ZOU F. Low-complexity video watermarking scheme resisting geometric distortions [C]// Proceedings of IEEE International Conference on Signal Processing. Washington D. C., USA: IEEE Press, 2010: 1861-1864.
- [15] 叶天语, 钮心忻, 杨义先. 多功能双水印算法 [J]. 电子与信息学报, 2009, 31(3): 546-551.
- [16] 李智, 陈孝威. 基于熵模型的高透明性自适应视频水印算法 [J]. 软件学报, 2010, 21(7): 1692-1703.

编辑 樊丽娜