DOI: 10.11992/tis.201912026

利用场景光照识别优化的双目活体检测方法

林峰[1], 杨忠程[2], 冯英[2], 颜水成[2], 魏子昆[2]
（1. 贵阳市信捷科技有限公司, 贵州 贵阳 550081; 2. 上海依图网络科技有限公司, 上海 200051）

摘　要: 人脸识别是生物特征识别技术中应用最广的技术之一。其中, 能判断人脸图像是否是真实人脸的活体检测模块, 是系统安全运行的重要保障。目前从安全度和经济性两方面综合考虑, 最常用的活体检测方法是双目活体检测。但由于不同场景下光线亮度和角度变化很大, 拍摄的人脸图片质量参差不齐, 严重影响了活体检测的质量。针对这一问题, 提出了通过对场景光照识别进行优化从而提升检测准确度的双目活体识别算法。算法通过串级 PID 算法对摄像头的感光度和补光灯进行控制, 并利用人脸识别算法定位优化测光区域, 从而对不同的光线强度和角度采取不同的策略。经过实验验证: 本方法将活体检测在复杂场景下的准确率提升约 30%, 保证了算法在室内外不同光照场景下的有效性。

关键词: 人脸活体检测; 人脸防伪; 展示攻击检测; 身份识别; 生物识别安全; 深度学习; 卷积神经网络; PID 控制
中图分类号: TP391　　**文献标志码:** A　　**文章编号:** 1673−4785(2020)01−0160−06

中文引用格式: 林峰, 杨忠程, 冯英, 等. 利用场景光照识别优化的双目活体检测方法 [J]. 智能系统学报, 2020, 15(1): 160–165.
英文引用格式: LIN Feng, YANG Zhongcheng, FENG Ying, et al. Binocular camera based face liveness detection with optimized scene illumination recognition[J]. CAAI transactions on intelligent systems, 2020, 15(1): 160–165.

Binocular camera based face liveness detection with optimized scene illumination recognition

LIN Feng[1], YANG Zhongcheng[2], FENG Ying[2], YAN Shuicheng[2], WEI Zikun[2]
(1. Guiyang Xinjie Technology Co., Ltd., Guiyang 550081, China; 2. YITU Tech, Shanghai 200051, China)

Abstract: Face recognition is one of the most widely applied biometric identification technologies, in which face liveness detection aiming to determine whether a face is genuine or fake, is used to help face recognition systems defend against replay and print attacks, and thus ensure system security. Considering safety and economy, binocular camera based face liveness detection is most commonly adopted at present. However, due to significant variations in lighting conditions of different scenes as well as face poses, the captured face images are often of low quality, which greatly harms the performance of face liveness detection. In this paper, we propose a binocular camera based face liveness detection algorithm, which improves detection performance through optimizing scene illumination recognition. In particular, the proposed algorithm uses the cascaded PID algorithm to adjust the light sensitivity and light supplement of the camera subject to specific lighting and pose angles. It also modifies the photometric range to be within the face area in the case of backlight to ensure effectiveness of the light exposure and supplement control strategy. Extensive experiments have been conducted and the results show that the proposed model outperforms other methods by around 30% in accuracy in complex scenes, with ensured generalizability to diverse application scenes.

Keywords: face liveness detection; face anti-counterfeiting; display attack detection; identity recognition; biometric security; deep learning; convolutional neural network; PID control

随着科技的进步和社会的发展, 生物识别技术被逐渐地应用到我们的日常生活中, 比如人脸

收稿日期: 2019−12−20.
通信作者: 杨忠程. E-mail: zhongcheng.yang@yitu-inc.com.

识别、指纹识别、声音识别等。其中人脸识别的应用最为广泛，如监控布控、人脸检索、门禁管理、身份验证等。在这些应用场景中，在使用人脸识别核实人的真实身份的同时，需要靠活体检测来判断被识别人是否为活体，从而使人脸识别系统抵御各种假冒攻击。常见的假冒攻击手段包括图片攻击、视频攻击、3D 人脸模型攻击等。其中图片攻击是一种最容易实现、代价最小的攻击方式，一般直接利用照片便可对系统进行攻击。视频攻击是利用合法用户的视频试图欺骗系统，视频中会包含用户的眨眼、张嘴等微表情，抵抗此种攻击方式的难度更高。而 3D 人脸模型攻击是通过合法用户的 3D 模型或者人皮面具等进行攻击，这种攻击方式可以模仿合法用户的各种微表情，是最难防的。

为了使人脸识别系统可以抵御各种假冒攻击，活体检测技术也在不断地发展。Wild 等研究者提出了一种加强活体检测系统对欺骗的抵抗能力的方法，此方法基于中值滤波器来提高传统集成方法中的容差，再通过 bagging 的方法来联合多种特征进行活体检测[1]。Boulkenafet 等[2]提出一种基于颜色纹理分析的活体检测算法，通过 LBP 算子和纹理信息来提取图像的特征，用于判断图像是否为活体。Pinto 等[3]通过对图像进行傅里叶变换，然后提取 LBP、HOG 和 GCLM 3 种特征共同用于活体检测。但是这些传统的特征提取方法建模成本较高，当数据量增大的时候还会遭遇性能瓶颈。Atoum 等[4]提出一种将深度图输入卷积神经网络来判断是否为活体的方法，这种方法在拥有足量训练数据的情况下，可以有效鉴别待识别对象是否是真实人脸，是现在活体识别最常用的方法。Liu 等[5]提出了一种结合 CNN 和 RNN 的活体检测方法，使用深度图和 rPPG 信号作为输入，大大提高了活体检测的泛化性。Amine 等[6]针对活体检测中的假冒攻击，将攻击分为真人和攻击噪声进行研究，为活体检测问题提供了一种新的研究思路。Liu 等[7]针对活体检测中的未知攻击模型，提出一种基于卷积神经网络的活体检测方法，提升了对未知攻击方法的泛化性。对于图像仿冒攻击和视频仿冒攻击，常见的抵御方法是在活体检测中引入红外摄像头[8]，因为照片和视频等非真实人脸在红外摄像头中具有明显特征，和真实人脸在红外摄像头下区别较大，因此在活体检测问题上，红外摄像头可作为可见光摄像头的重要补充。

利用双目摄像头拍摄到的红外人脸图片和可见光人脸图片配合进行活体检测，可以使活体检测取得良好的性能。随着社会的发展，人脸识别系统应用场景也逐渐增多，比如室外的地铁闸机、室外门禁、银行的自动取款机等许多生活场景中，都可以见到人脸识别系统的身影。这给活体检测任务带来了新的挑战。部分场景的光线条件比较差，存在光线过暗或者过亮等亮度问题以及背光、侧光等角度问题，并且同一场景的光线条件也会发生变化，导致拍摄的照片质量参差不齐，对活体检测系统的性能造成了很大的影响。比如室外的地铁闸机，在白天有太阳直射的情况下拍摄的图片中，背光或者侧光的拍摄角度导致人脸部分较暗，而太阳直射的正面光照又会导致人脸部分较亮；在夜晚的时候，光线较暗，因而拍摄的图片中人脸部分一般也较暗。

一般活体识别算法只能适应有限的光照情况。而面对极端的光照情况（如画面过暗或者过亮造成画面过曝），由于图像损失信息过多，很难设计能够达到理想效果的算法。同时可见光和红外光的光照情况经常不同步，如室内光照强乃至过曝时，红外光不一定足够；而室外有时即便可见光是中等强度，红外光由于反射可能反而过曝。因此这时候就需要一个控制方法，通过控制摄像头光圈、曝光时间、可见光补光灯、红外补光灯等外部硬件，来同时获得最佳的可见光和红外光影像。使得活体识别算法能在室内外不同场景下使用。

1　研究方法

针对在多场景下活体检测面临的不同光线条件造成图片质量较差的问题，本文提出了一种通过优化场景光照识别从而提升双目活体识别性能的算法。不同光照条件主要有以下 6 种：图 1 给出了不同的光线强度和光线角度对摄像头拍摄图片的质量产生的影响。图 1(a) 为户外的正面光，摄像头过度曝光，导致拍摄的图片较亮；图 1(b) 为户外的侧面光，拍摄的人脸亮度不均匀，需要补光；图 1(c) 为背光，拍摄的照片中人脸比较暗，需要补光；图 1(d) 和图 1(e) 为晚上的黑暗场景，整个图片光线都很暗，摄像头欠曝，基本无法辨别人脸，都需要补光灯进行补光。

算法的主要流程如图 2 所示。算法分为待机态和工作态。在待机态下，红外摄像头通过一个基于串联 PID 的摄像头曝光模式和补光模式控制算法，以较低功耗的状态等待识别人脸。当红外摄像头捕捉到人脸后，即进入工作态。工作态下，算法首先基于红外捕捉到的人脸影像，重新设置测光点。可见光摄像头在新的测光点上采

样，并使用基于 PID 的曝光补光模式控制算法，调整到适合当前场景下光照情况的状态。在合理曝光下，采集高质量的双目摄像头影像，通过基于卷积神经网络的活体识别算法，获得活体识别的结果。获得结果后做出反馈，并回到待机态。


(a) 室外正面光　(b) 室外侧面光　(c) 室外背光　(d) 室外暗光　(e) 室内暗光　(f) 室内正面光

图 1　不同光线角度及强度示意图

Fig. 1　Different light angles and intensities

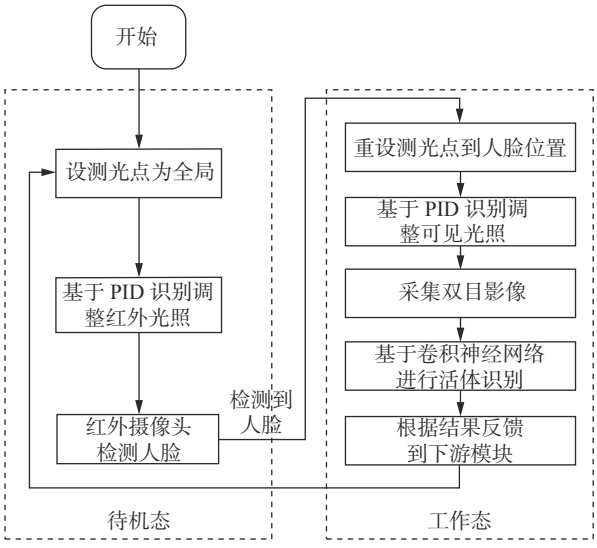


图 2　整体算法流程图

Fig. 2　Algorithm flowchart

1.1　基于卷积神经网络的活体检测

卷积神经网络在图像问题上已经被证明是最有效的方法之一。本文采用 Kaiming He 等[9] 提出的 Resnet 来进行活体检测。Resnet 在神经网络中引入了残差学习单元，在卷积层的输入和输出之间建立一条直接关联的通道，使得残差学习单元的输出为卷积输出与输入的和。残差学习单元可以让网络重点学习输入与输出之间的残差，提升了网络性能。在反向传播优化时，梯度可以直接向前传播，在一定程度上缓解了梯度消失，同时解决了卷积神经网络深度加深时出现的退化问题。

卷积神经网络在可见光图像和红外图像上进行活体检测的工作流程如图 3 所示。首先，利用卷积神经网络判断红外摄像头拍摄的红外图像中是否存在人脸。如果红外图像中不存在人脸，网络判定待识别对象为非活体；如果存在人脸，网络将进一步提取可见光图像和红外图像中的特征，判断图像是否存在活体特征。若不存在活体特征，判断待识别对象为非活体；若存在活体特征，分别确定待识别对象与红外摄像头和可见光摄像头之间的距离，并分别确定待识别对象与红外摄像头和可见光摄像头之间的角度，通过距离和角度来确定红外摄像头和可见光摄像头捕捉到的待识别对象是否为同一物体。若为同一物体，判定待识别对象为活体；否则判定待识别对象为非活体。

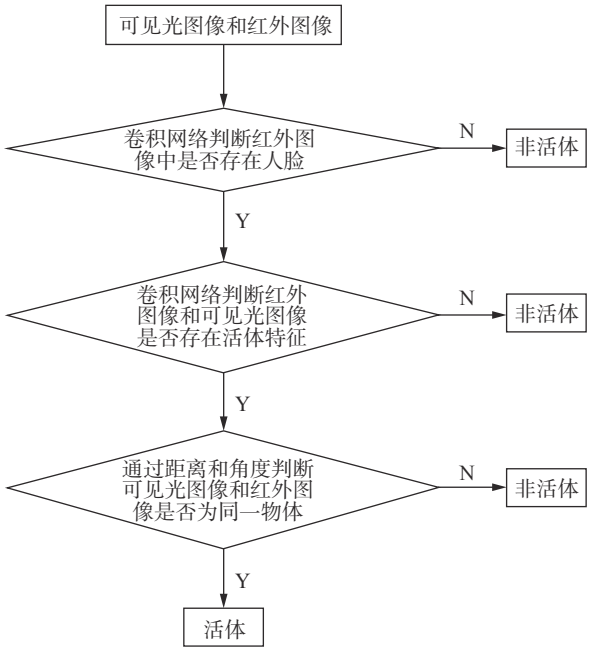


图 3　基于卷积神经网络的活体判别算法

Fig. 3　Face liveness detection algorithm based on convolutional neural network

用于判断待识别对象是否为活体的卷积神经网络的结构如图 4 所示。输入的单通道的红外摄

像头图像和三通道的可见光摄像头图像, 在通道层拼接为一个四通道的图片。将得到的四通道的图片输入 5 个卷积块 18 层卷积的 Resnet18, 输出是活体或者非活体的概率。

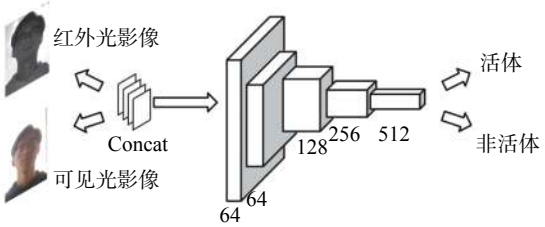


图 4　卷积神经网络结构示意图

Fig. 4　Convolutional neural network structure

1.2　基于串级 PID 的摄像头曝光和补光控制算法

为了使摄像头能够拍摄高质量的人脸图片, 考虑对摄像头的测光点进行监测, 来调整到合适的曝光程度。当测光点感知的光线较暗或者较亮的时候, 调节摄像头的曝光程度和补光灯的状态, 使得光线质量维持在稳定的范围内。为此, 选择利用串级 PID 算法对摄像头的曝光和补光灯进行控制。

1.2.1　比例积分微分 (PID) 算法

比例积分微分 (PID) 控制, 其算法简洁且具有很好的鲁棒性[10], 被广泛应用到各种控制算法中, 其公式为

$$u(t)=K_{\mathrm{p}}e(t)+K_{\mathrm{i}}\int_0^t e(t)\mathrm{d}t+K_{\mathrm{d}}\frac{\mathrm{d}e(t)}{\mathrm{d}t} \tag{1}$$

此算法包涵的思想比较简单, 根据给定值和实际值得到差值, 然后将差值按照比例、积分和微分来构成控制量, 对被控对象进行控制。其中比例控制环节为有差调节, 即当有误差产生时就会进行调节。积分环节能对误差进行记忆, 可以消除静态误差, 提高系统的性能。微分环节可以反映误差信号的变化快慢和变化趋势, 通过趋势信息, 使系统尽快做出调整, 缩短控制调整时间。

1.2.2　串级 PID 算法

单纯的 PID 只能解决单一控制变量的情况。实际应用中存在需要通过多个控制变量控制系统的情况, 并需要保证其中部分变量稳定。这种情况需要一些其他方法, 或者对 PID 算法进行一些变形。串级 PID 算法是进行多变量控制的有效方法之一。其主要思想为将两个 PID 控制器进行串联工作, 其中外环控制器的输出作为内环控制器的输入, 而内环控制器的输出会影响外环控制器的输出, 从而达到对外环的被控变量更好的控制效果。

根据串级控制的思想, 本文设计了一套摄像头的曝光补光控制算法, 如图 5 所示。

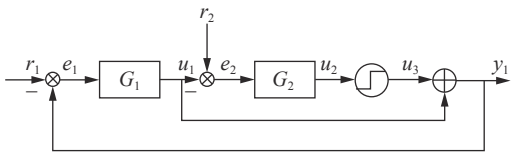


图 5　基于串联 PID 的场景光照识别优化方法

Fig. 5　Scene lighting recognition optimization method based on cascaded PID

摄像头的曝光补光算法具体公式如下:

$$\begin{aligned}
e_1(t)&=r_1-y_1(t)\\
u_1(t)&=G_1(e(t))\\
e_2(t)&=r_2-u_1(t)\\
u_2(t)&=G_2(e_2(t))\\
u_3(t)&=\sum_{i=1}^{m}J[u_2(t)-L_i]\\
y_1(t)&=u_1(t)+u_2(t)
\end{aligned} \tag{2}$$

式中: r_1 为测光点的期望值; r_2 为摄像头曝光系数的期望值; y_1 为测光点的实际值; u_1 为摄像头的曝光调整系数; u_2 为补光的期望调整量; u_3 为补光灯的控制系数; G_1 和 G_2 为式 (1) 中的 PID 函数。L_i 为补光的期望调整量与补光灯档位的映射函数, J 为阶跃函数。

式 (2) 中, 通过补光的期望调整量与补光灯档位之间的映射函数, 来确定补光灯的档位。即在调整曝光系数无法满足当前测光点期望值的情况下, 通过调整补光灯的档位来进行光线的补偿。

1.3　测光点优化

当待识别对象处于背光的角度时, 由于光线从人的背后射过来, 会造成背景光线亮度较高而人脸亮度较低的现象, 如图 6 所示。在这种情况下, 如果全局均匀选取或者随机选取测光点, 当选在背景时, 由于背景较亮, 摄像头的曝光补光算法会调整感光度, 降低补光灯档位甚至关闭补光灯, 使得采集到的人脸可见光图像较暗, 影响活体检测的性能。

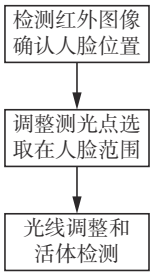


图 6　基于人脸位置的测光点选取

Fig. 6　Metering point selection process based on face position information

为了解决上述问题，本文提出对测光点的选取方式进行优化。由于红外摄像头对光线条件不敏感，所以先通过红外摄像头采集到的红外图像确定人脸所在的范围，然后动态地将测光点选取在人脸的范围内。这样可以保证测光点始终在人脸的范围内，保证摄像头曝光补光控制算法的有效性。

2　实验验证

由于测试时获得的影像和曝光补光策略相关，难以通过离线采集数据后建立测试集的方法来比较评估各个算法的性能。因此在本文中，我们邀请若干名测试人员，在多个地点不同时间段对算法进行测试。同一测试人员在同一时段同一地点，分别使用多个攻击手段 (照片、视频回放、面具) 和真实人脸来检测各个活体算法的性能。通过比较不同算法在不同场景下的活体测试的准确率，来验证它们在不同场景下的有效性和泛化性。

我们收集测试数据的实验场景包括室外正面光、室外侧面光、室外背面光、室外昏暗、室内正面光、室内昏暗等。其中双目摄像头所拍摄到的影像都包括两张影像：一张可见光摄像头拍摄的彩色图像，和一张红外摄像头拍摄的灰度影像。采集实验数据的人员有 23 名，收集的测试用例分布基本均匀，具体数据见表 1。

表 1　测试用例采集分布表

Table 1　Test case distribution table

场景	采集方式				总计
	正常人脸	人脸伪造方式			
		打印照片	平板视频	面具	
室外正面光	69	23	23	23	138
室外侧面光	69	23	23	23	138
室外背面光	69	23	23	23	138
室外昏暗	69	23	23	23	138
室内正面光	69	23	23	23	138
室内昏暗	69	23	23	23	138

测试的算法包括 3 个：1) 单纯的卷积神经网络，作为基准线算法；2) 卷积神经网络+场景光照优化：使用串行 PID 算法来优化调整补光曝光策略的算法；3) 卷积神经网络+场景光照优化+测光点优化：在前述补光曝光策略优化算法的基础上，通过人脸识别算法调整测光区域的方法。具体测试结果见表 2。如表 2 所示，没有场景光照识别优化的基准线算法在室内正面光下表现不错，但一旦到户外复杂光照场景，尤其是侧面光和背面光的情况，其性能开始锐降，在昏暗场景下甚至几乎无法正常工作。使用了补光曝光调整策略的算法，性能得到了明显提升，昏暗场景下性能基本达到和有光条件下一样，同时户外场景性能也有明显提升，但在侧面光和背光场景下仍然有些问题。在加上基于人脸区域调整测光区域的方法后，在之前方法的良好性能基础上，对侧面光场景和背面光场景下的检测性能有所增益，性能基本和其他场景持平。

表 2　各算法活体检测准确率

Table 2　Accuracy of each algorithm

场景	测试量	算法性能		
		卷积神经网络	卷积神经网络+场景光照优化	卷积神经网络+场景光照优化+测光点优化
室外正面光	138	0.77	0.91	0.96
室外侧面光	138	0.63	0.80	0.93
室外背面光	138	0.62	0.78	0.88
室外昏暗	138	不能识别人脸	0.91	0.96
室内正面光	138	0.92	0.95	0.97
室内昏暗	138	不能识别人脸	0.91	0.97

通过分析错误例子，我们发现其中较难解决的问题是背面光情况下，当太阳角度较低并与摄像头成一定角度时，会有较强的镜头炫光。如图 7，图像中的炫光会对算法的活体判断准确度造成影响，事实上炫光区域不仅干扰算法正确规划曝光补光方案，也会直接破坏人脸区域影像，使下游活体识别神经网络得到不正常的输入。理论上讲，通过使用更大的光圈，或者更好素质的光学镜头，可以有效减少炫光的程度和发生概率。但是这些方案成本较高，不太实用。

图 7　背光出现炫光的情况
Fig. 7　Glare picture

3　结束语

本文研究了在复杂光照条件下部署双目活体识别系统，通过基于串行 PID 的场景光照识别优化算法来提高人脸活体识别准确度的问题。本算法根据场景内的光照情况自动调整对应的曝光方案和补光方案，并针对活体识别的特殊性，有侧重地实施只关注人脸区域的优化方式，将双目活体识别从只能在良好光照条件下的室内场景，成功迁移到复杂光照条件下的室外场景，解锁了更多活体检测场景和可能性，使人脸识别认证可以得到更广泛的部署和使用。但是本算法在特别复杂的光照场景下，如背光产生镜头炫光的情况，性能还需进一步提高。这部分有待以后的研究和探索。

参考文献：

[1] WILD P, RADU P, CHEN Lulu, et al. Robust multimodal face and fingerprint fusion in the presence of spoofing attacks[J]. Pattern recognition, 2016, 50: 17–25.

[2] BOULKENAFET Z, KOMULAINEN J, HADID A. Face anti-spoofing based on color texture analysis[C]//Proceedings of 2015 IEEE International Conference on Image Processing. Quebec City, Canada, 2015: 2636–2640.

[3] PINTO A, SCHWARTZ W R, PEDRINI H, et al. Using visual rhythms for detecting video-based facial spoof attacks[J]. IEEE transactions on information forensics and security, 2015, 10(5): 1025–1038.

[4] ATOUM Y, LIU Yaojie, JOURABLOO A, et al. Face anti-spoofing using patch and depth-based CNNs[C]//Proceedings of 2017 IEEE International Joint Conference on Biometrics. Denver, USA, 2017.

[5] LIU Yaojie, JOURABLOO A, LIU Xiaoming. Learning deep models for face anti-spoofing: binary or auxiliary supervision[J]. arXiv: 1803.11097, 2018.

[6] JOURABLOO A, LIU Yaojie, LIU Xiaoming. Face de-spoofing: anti-spoofing via noise modeling[J]. arXiv: 1807.09968, 2018.

[7] LIU Yaojie, STEHOUWER J, JOURABLOO A, et al. Deep tree learning for zero-shot face anti-spoofing[J]. arXiv: 1904.02860, 2019.

[8] 陈远浩. 一种基于红外可见双目图像的活体检测方法及装置 [P]. 中国: CN106372601A, 2017-02-01.

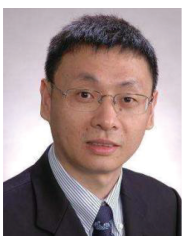
[9] HE Kaiming, ZHANG Xiangyu, REN Shaoqing. Deep residual learning for image recognition[C]//Proceedings of 2016 IEEE Conference on Computer Vision and Pattern Recognition. Las Vegas, USA, 2016.

[10] SKOGESTAD S. Simple analytic rules for model reduction and PID controller tuning[J]. Journal of process control, 2003, 13(4): 291–309.

作者简介：

林峰，工程师，主要研究方向为大数据产业。

杨忠程，高级研究员，主要研究方向为机器视觉。



颜水成，新加坡工程院院士，IEEE Fellow，IAPR Fellow，主要研究方向是计算机视觉、机器学习与多媒体分析。曾任 360 集团副总裁、首席科学家、人工智能研究院创始院长，现任依图科技 CTO。