



专题：智能通信技术的应用

人工智能在电信实名认证中的关键技术及应用

姚慧, 马思研

(中移在线服务有限公司, 河南 郑州 450001)

摘要: 应国务院及工业和信息化部的实名制要求, 结合运营商业务转型的需要, 提出了一种基于人工智能技术的在线身份认证解决方案。首先介绍了基于深度学习技术的实名认证系统架构, 分别对系统的 4 个模块和系统整体特点进行详细阐述。其次论述了应用在实名认证系统中的人证比对与识别、证件 OCR、静默活体和视频认证等关键技术, 介绍了身份认证解决方案的应用现状, 此外分别从安全性的角度介绍了实名认证业务场景中抵御攻击的手段, 从性能的角度分析了本方案在实际应用中取得的良好效果。最后, 分析了人工智能技术在运营商业务领域中应用问题, 并探讨了未来基于实名认证的产品研发方向。

关键词: 实名认证; 深度学习; 身份认证

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2019093

Key technologies and application of artificial intelligence in telecom real-name system

YAO Hui, MA Siyan

China Mobile Online Services Co., Ltd., Zhengzhou 450001, China

Abstract: According to the real-name system requirements of the State Council and the Ministry of Industry and Information Technology, combined with the needs of telecom operators' business transformation, an online identity authentication solution based on artificial intelligence technologies was proposed. Firstly, a real-name authentication system architecture which is based on artificial intelligence technologies was introduced. Then the key modules of the system were expounded in detail. Secondly, the key technologies applied in real-name authentication system were explained, such as human authentication and identification, OCR, face liveness detection. The present situations of applying identity authentication solution were presented. Besides, the means of real-name authentication business scenarios against attacks from the perspective of security were introduced and the effectiveness and efficiency of the proposed solution were demonstrated. Finally, the application problems of artificial intelligence technologies in the field of operator business were analyzed and the future works on real-name authentication products were discussed.

Key words: real-name system, deep learning, identity authentication



1 引言

移动互联网技术的发展促进了现代服务业的蓬勃发展,利用网络提供远程服务成为电信、银行、证券、基金、保险等金融行业的发展趋势。作为业务办理和风险控制的关键环节,验证客户身份是业务提供方发展线上业务需要解决的首要问题。

传统业态的客户认证多通过网点面签的方式实现,存在运营成本高、覆盖面不足、体验不佳、耗费成本巨大等问题。在互联网新业态下,很多公司对高效、准确地实现远程客户身份认证具有迫切需求。目前对客户认证的需求主要分布在金融、电信、政府等行业,这些行业各自独立,重复投入,集约化程度不高,信息没有共享,设计系统、全面、方便信息共享的远程客户认证系统存在巨大市场需求。

2012年全国人民代表大会常务委员会出台了《关于加强网络信息保护的决定》,规定了一些重要的制度安排,要采取措施保护网络信息。工业和信息化部(简称工信部)也随即出台了《电信和互联网用户个人信息保护规定》,就进一步强化安全防护措施、健全管理制度、落实安全责任,做了一些具体的规定,即《电话用户真实身份信息登记规定》,拉开了电信运营商实名制工作序幕。规定要求用户在办理电话入网手续的时候,需要向电信企业出示有效证件、提供真实的身份信息,配合做好相关信息登记工作。

人工智能、大数据与云计算、芯片等面向未来的核心技术,正在加速各行业发展与技术变革,高效的人工智能正在逐步取代传统的服务方式^[1],本文介绍了一种基于深度学习的图像视觉技术的整套实名制身份认证解决方案,阐述了实名认证系统架构和关键的深度学习技术,重点介绍了人工智能技术在电信多产品形态中实名认证环节的应用情况。

2 基于深度学习的实名认证系统

基于深度学习技术的实名认证系统,是在原有的实名认证系统中增加核心域的功能模块,系统架构示意图如图1所示。系统主要分为4个模块:客户端、接入域、能力域和存储域。整体采用前后台分离模式,后台采用云化部署方案,保证客户端快速通过网络接入系统,后端管理系统可通过网络随时随地登录管理。同时,所有内部接口及外部接口均统一设计风格,便于第三方对接开发。此外,整个系统系统采用模块化设计,可以根据需求选择不同模块进行自由组合,数据在平台中打通统一管理。

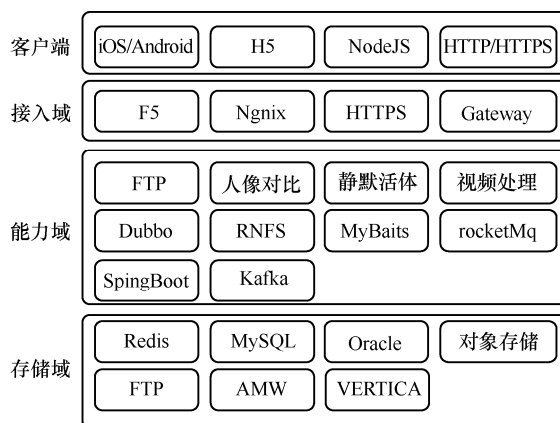


图1 实名认证系统架构示意图

客户端:主要面向用户,整合算法引擎输出结果和业务校验结果,向用户反馈业务审核消息;提供对外接口,支持与第三方系统进行基础数据的互通。

存储域:用于存储各类解析后的解码视频文件、音频文件、人像、业务流水信息及日志信息。

数据存储部分:针对业务中沉淀的海量图片,采取分布式存储方案,分别存放于多台物理主机硬盘中,在存入图片的同时将图片的相关基本信息存放于MySQL、Oracle等关系型数据库中,以便实名认证业务进行调用,同时为确保相关数据信息安全,图片数据和图片信息在存储时都进行

了脱敏加密, 存储模块示意图如图2所示。

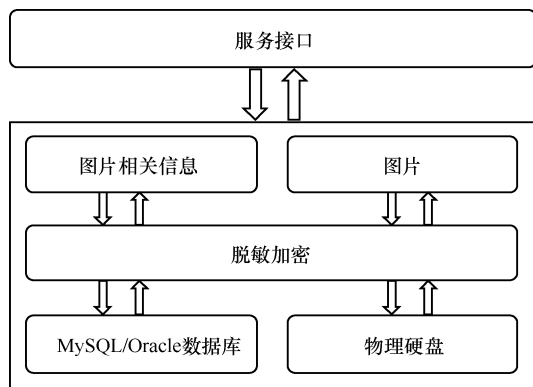


图2 数据存储部分示意图

接入域：用于实现请求源调度和搭建外网通信协议。

能力域：用于提供数据处理、解析服务和日志管理能力。服务解析能力包括人脸识别、OCR、静默活体、视频解析和语音识别；数据处理能力包括各种数据的存储管理、资源调度、对外数据访问服务、数据检索服务及大数据分析服务。

实名认证系统及能力建设，采取前后台分离模式，统一承担全网实名制人工智能技术的实施和部署，并扩展前后台分离模式应用领域，致力于建立“前端属地化、后端集中化”的低成本高效运营体系，将实现姓名、身份证号联网校验能力，并逐步发展迭代增加人像联网校验功能，形

成全套的信息采集及联网查验解决方案，提高了实名认证的精确度。实名认证系统具备以下特点。

(1) 前后台分离模式

基于前后分离模式的认证技术，采用“互联网+”模式，前端仅对客户信息进行采集，并将所有采集到的密文信息传到后台服务器进行全网集中解密识别和认证，其中，客户信息获取方式包括NFC方式读取有效证件信息、身份证件拍照上传、手动录入、客户现场抓拍照，通过上述渠道采集后的信息进行加密传输，回传至实名认证后台进行信息解密和人证一致性校验。前后台分离模式示意图如图3所示。

(2) 多元校验方式，严控信息安全

信息安全主要包括：信息的安全传递和信息的安全存储。本文介绍的系统通过运用IMEI、IMSI、随机码校验、错误操作次数控制、清除缓存及离线数据、信息传输加密等多种手段保障信息安全。

信息的安全存储：该系统涉及用户信息等敏感数据，因此采用了高可靠性的数据库管理系统与物理存储功能，对客户资料等敏感信息采用“软+硬”双重方式的加密存储，数据库采用严格的权限管理，具备备份与恢复功能；此外增加数字签名措施，采取控制台安全、机器物理隔离、

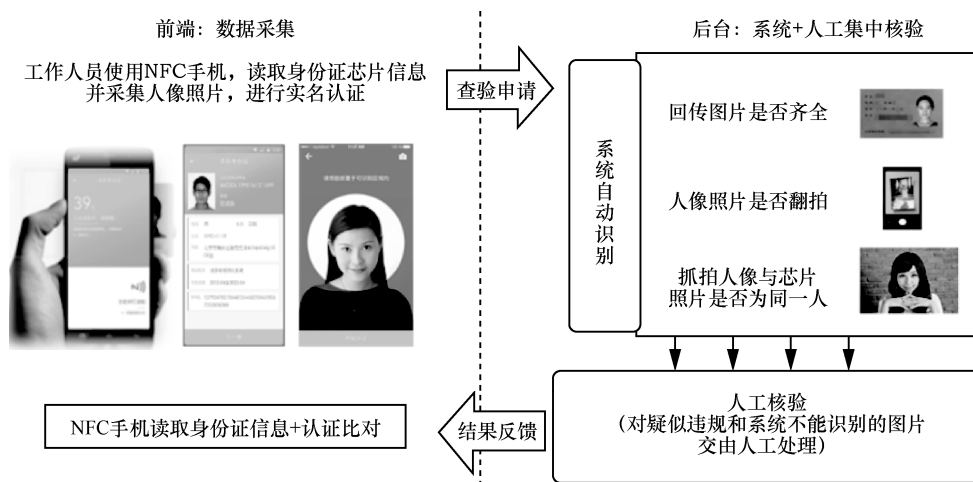


图3 前后台分离模式示意图



保护安装介质等多重手段，保证数据存放的可靠性、完整性、保密性。

信息的安全传递：在系统内部进行处理时，数据严格执行不允许出系统的系统安全限制要求，涉及外部系统的访问，必须采取安全性更高的 HTTPS 加密方式，信息传输采用“软+硬”的双重加密方式，双方根据唯一密钥进行传输数据的加解密，密钥获取采用系统接口级方式，确保双方数据传输的安全性、不可获取性。

3 实名认证系统的关键技术

实名认证系统中广泛使用了深度学习技术：利用先验知识搭建神经网络模型，不断地从线上获取各业务场景中的数据，自动学习并获取数据的特征表达。经过有限次的迭代后，模型可以根据提供的数据进行决策（分类或回归），算法模型训练流程如图 4 所示。首先通过对学习任务和具体业务场景的分析选取适合的网络结构搭建深度神经网络模型或直接选取开源的预训练模型，即初始模型架构。对历史数据（包括图片、视频和音频）进行数据清洗以及必要的预处理，获取可以用于训练和测试的样本数据。随后经过有限次的模型迭代（即模型的训练）和迁移学习后，获取具有较好效果的第一代模型。将第一代模型存储在 AI 算法模型仓库中，进入线上环节。服务上线后，

系统将自动获取、存储线上采集到的实际场景数据并将其发布为标注平台的任务，采用人工或半自动的标注方式进行数据标注，因此系统将不断地获取新的训练数据，从而不断优化本文的模型仓库中存储的模型。通过版本管理功能对模型版本进行管理，评估并选取更优的模型替换线上模型。通过这一闭环训练平台，可以自动地进行模型的迭代和优化，不断地提高系统的识别准确率。本文的实名认证系统中涉及的深度学习技术主要为人证比对与识别、身份证 OCR、身份证件信息读取与认证、视频活体检测和语音识别等。

3.1 人证比对与识别

人脸识别是基于人的脸部特征信息进行用户身份认证的一种生物识别技术^[2]。人证比对与识别是特定于身份证人脸图像与现场照进行比对识别的人脸识别任务。整个流程一般包含图像采集、人脸检测、人脸图像预处理、人脸特征提取和人脸识别 5 部分。

（1）图像采集

通过摄像机或手机摄像头等前端设备获取包含人脸的视频或图像。

（2）人脸检测

人脸检测即从图像中检测得到人脸位置的技术。传统的人脸检测方法使用人工设计的特征如直方图特征、颜色特征、模板特征、结构特征及

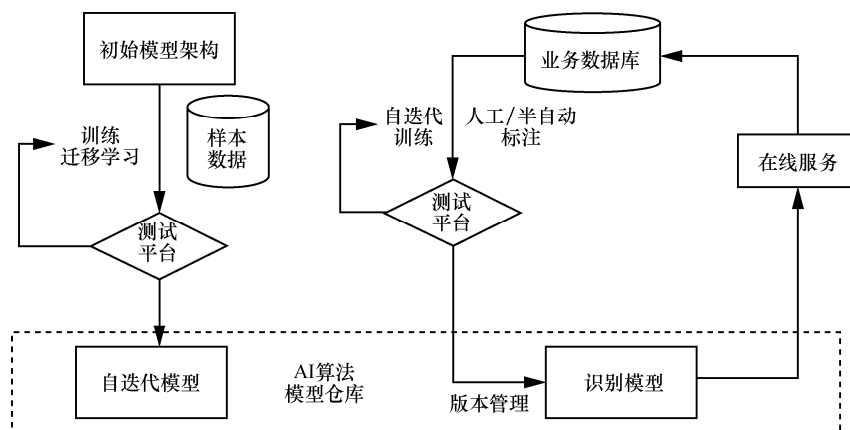


图 4 深度学习算法训练流程

Haar 特征等,训练得到一个多尺度分类器,对人脸区域和背景区域进行分类,进而定位出人脸区域;深度学习方法则使用深度神经网络从数据中学习适合人脸检测使用的深度特征。通过学习得到的特征往往比传统人工设计的特征要更优,基于深度学习的人脸检测方法在精度方面要优于传统方法。

(3) 人脸图像预处理

在得到人脸检测框位置之后,人脸图像需要经过对齐操作,将人脸大小归一化到统一尺度,并消除人脸姿态对于后续人脸识别的影响。通常的做法是定位出人脸面部若干个关键点,并根据这些关键点进行尺度归一和人脸姿态矫正,最终得到一张便于做人脸识别的人脸图像。

(4) 人脸特征提取

目前主流的人脸特征提取方法是采用深度学习算法搭建深度网络模型,使用海量数据训练,获取最能表征人脸身份信息的特征的提取方式。根据损失函数,可以分为基于度量学习的方法和基于分类的方法。基于度量学习的方法核心出发点是让同一个人的人脸图像经过特征变换以后尽量靠近,不同人的脸图像尽量拉远,典型的方法包括 Contrastive Loss^[3] 和 Triplet Loss^[4]。基于分类的方法即使用 Softmax Loss 对训练集中所有人进行分类学习。为了使类内收缩更紧,类间拉到更开,在传统 Softmax Loss 基础上引入 Margin 变量,通过引入该变量提升人脸识别特征的判别能力,典型的方法包括 Large-Margin Softmax Loss^[5]、SphereFace^[6]、CosFace^[7]和 ArcFace^[8]。此外,随着人脸数据的不断增加,如何基于上千万人的脸图像进行高效大规模训练成为学术界和工业界研究的热点问题。

(5) 人脸识别

人脸识别是指通过计算前端设备获取的人脸图像的特征与数据库中存储的人脸特征的相似度来判断是否为同一人的过程。在实名认证系统中,

主要为两个应用方向:一是确认,即前端设备采集到的人脸图像特征与数据库中存储的人脸特征进行一对一的比对,通过设定的阈值来判断是否为同一人;另一类是辨认,是前端获取的人脸图像的特征与数据库中多个人脸特征的一对多的比对过程。1:1 的人脸识别技术可以用于登录验证、身份识别等应用场景。通过人脸识别技术可以帮助用户快速判定两张照片是否为同一个人、判定视频中的人脸是否为目标人脸并支持实时识别认证,还可以实现身份和人脸绑定等功能。1:N 人脸识别技术可以将目标人脸图片与人脸库自动识别,返回识别信息来判断目标人脸身份。

3.2 证件 OCR

OCR (optical character recognition, 光学字符识别)是指将图片中的文字内容转换为可编辑文本的过程^[9]。一般来说,实名认证系统中证件 OCR 技术主要包括 3 个步骤:证件检测、文本检测和文字识别。

(1) 证件检测:在图片中定位证件的角点信息或边缘信息。通过证件检测可以去除证件区域外的干扰信息,提高特定场景下 OCR 准确率。

(2) 文字检测:首先使用透视变换等图像处理手段将上一步中得到的证件区域矫正为矩形区域,然后在该区域内定位出需要识别的文本所在区域。传统的文字检测算法包括 MSER^[10]、SWT^[11]、Multi-Oriented^[12]等,随着深度学习算法的不断发展,各种基于深度学习的文字检测算法也层出不穷,如 PhotoOCR^[13]、YOLO^[14]、EAST^[15]等。在实名认证系统中,采用 EAST 算法准确定位需要识别的关键字段,同时屏蔽无关信息字段,提高了整套 OCR 算法的识别准确率。

(3) 文字识别:将检测到的文本区域切片识别成文本。早期的文字识别算法需要对文本行进行字符切割,然后对单个的字符进行分类,从而达到文本行识别的目的。本文采用 CNN^[16]、RNN^[16]以及 CTC LOSS^[16]结合的方法,根据文字



上下文直接识别整行文字，识别流程更加简化，效率更高，并具有更高的识别准确率。

3.3 静默活体检测

静默活体检测技术是针对配合式的活体检测技术提出的一种活体检测技术。配合式的活体检测技术通常需要用户根据设备的提示做出指定动作来帮助算法确认用户是否为真人，但是这种检测技术存在用户体验较差和有攻破风险等弊端^[17-18]。

通过大量的数据分析，可以知道真人拍摄样本和非真人直接拍摄的样本（播放设备翻拍、照片或面具等）存在着特征区别，如边框、反光、摩尔纹、分辨率和对比度等。基于这样的原理，本文采用深度学习算法，设计了一个深度卷积网络来学习区分这些正负样本，实现了仅需一张静态照片即可判别是否为真人的静默活体检测技术。用户仅需在前端图像采集设备前停留较短的时间，算法通过分析视频流中的一帧或多帧图像即可判断是否为真人用户办理业务，通过融合多帧检测的结果，可以进一步提升静默活体检测的精度，配合人脸识别技术，保证业务办理的高度安全。

3.4 身份证件信息读取和认证能力

公安部认证身份信息能力，主要指通过对公民身份证号码及姓名的真实性、一致性进行验证，返回验证通过与否的结果。其中获取公民身份信息的方式有如下两种。

（1）通过 OCR 识别获取用户身份信息，实时公安部数据库联网比对，验证身份信息真伪。

（2）通过在 NFC 手机上安装 App，实现 NFC 读取身份证芯片信息，并与后端认证系统连接进行后端解码，同公安部数据库进行联网比对，查验证件信息真实性，核验证件真实性。

3.5 语音识别

自动语音识别（automatic speech recognition, ASR）技术是将用户录制朗读随机码视频中的语音转为文字，并进行随机码一致性比对。此技术

基于电信行业数千万小时的标注语音数据，应用业界先进的端到端的深度学习模型进行训练，得到更加贴近实际业务场景的核心引擎，全面满足电话录音质检、视频认证等多种场景下的语音转文字需求。目前基于深度学习的语音识别模型主要包括两种：一种是将深度学习模型替换 GMM 部分，得到 DNN-HMM 模型；另外一种是从端到端的深度学习模型。其中基于端到端的模型主要包括基于 CTC 解码模型、基于 Attention 解码模型以及混合 CTC 与 Attention 共同解码模型^[19]，可以支持多语言体系和多方言的训练，例如 26 个英文字符，数字、中文等语言，此外在实时预测部分耗时更短，更有利于业务应用。

3.6 云存储技术

云存储^[20]是在云计算的概念上延伸和发展出来的一个新概念，是指通过集群应用、网格技术或分布式文件系统等功能，应用存储虚拟化技术将网络中大量各种不同类型的存储设备通过应用软件集合起来协同工作，共同对外提供数据存储和业务访问功能的一个系统，也可将云存储理解为配置了大容量存储设备的一个云计算系统。

4 实名认证系统应用形态

在全网推广的过程中，基于人工智能技术的实名认证系统不仅要关注技术在复杂场景下的准确率，更要关注人工智能技术与运营商业务的紧耦合性。鉴于目前人工智能技术还有待进一步优化，在应用场景中仍有误识别情况存在，造成用户体验较差。针对该问题，本文介绍了两种解决方法，提升认证的安全性和准确性。

（1）核心能力的保障与提升

后台人工审核环节作为实名认证重要组成部分，在审核高风险业务、及时发现作假手段上作用显著。面向后台审核人员打造界面优化、操作便捷的专业化审核系统至关重要。通过引入抢单模式，将工单数据导入内存，快速推向审核人员，

极大缩短前端信息采集到后台审核时间,后台工单审核效率明显提升。审核界面引入快捷键操作,工单审核完成后进行快速页面切换,审核照片支持缩放和旋转,便捷支持后台工单审核。人工审核服务功能的加入,可以在系统识别校验基础上,增加后台渠道集中化稽核,由人工进行二次确认,提升审核结果的准确率。

(2) 适应多场景的全流程实名认证解决方案

身份信息认证环节,线下创新性开发 NFC+App 实名认证方式,通过二代证读卡器解耦,将 SAM 核心解码模块部署在云端统一解码;同时开发 App,引入 NFC 的技术,通过手机或者读头的 NFC 功能读取身份证芯片信息(密文),将密文发向云端进行解码,解码信息通过 App 在前端手机显示,实现低成本、便捷支撑实体渠道实名认证。线上通过接入公安部身份信息查验中心,打造支持高并发、低时延实时验证能力。

人证一致性验证环节,通过自主研发国内领先人脸比对与识别技术和活体检测技术,在保证身份信息真实基础上,通过活体检测保证验证人为现场操作,通过实时抓取人脸照片与公安部照片进行人脸比对,保证认证一致性。线上利用人像比对技术,提供电渠售卡的认证服务;利用网页和 H5 的形式在不改变省端流程的情况下灵活嵌入,通过 OCR、公安联网查验及人像比对+人工审核的方式,实现线上售卡的自助激活工作,为客户提供了便捷的认证方式。

以上实名认证能力支持通过 App、H5、Web 等多模式进行接入,同时支持线上线下身份信息认证、人脸比对与识别、身份信息证件 OCR、活体检测等多模块灵活配置适应实际业务场景。

5 结束语

本文介绍了基于人工智能技术的在线身份认证场景下的解决方案,首先描述了实名认证系统架构以及系统子模块功能,重点讲解了应用到该

系统中的人脸比对与识别、证件 OCR、静默活体检测以及语音识别技术的主流实现方法。其次,从业务的安全性和性能角度考虑,本文介绍了系统在实际业务场景中的应用现状和产品形态。从实践情况来看,该系统不仅节约了时间和人力成本,简化了认证流程,提高了身份认证的精确度,也有利于未来提高移动支付等功能的安全性,增强接入其他互联网应用的便利性,并能够有效打击通信诈骗犯罪,为移动用户提供一个安全的移动互联网使用环境。

参考文献:

- [1] 王志宏,杨震. 人工智能技术的哲学集系统性思考[J]. 电信科学, 2018, 34(4): 12-21.
WANG Z H, YANG Z. Philosophy and systematic thinking of artificial intelligence technology[J]. Telecommunications Science, 2018, 34(4): 12-21.
- [2] 山世光. 人脸识别中若干关键问题的研究[D]. 北京: 中国科学院计算技术研究所, 2004.
SHAN S G. Study on some key issues in face recognition[D]. Beijing: Institute of Computing Technology, Chinese Academy of Sciences, 2004.
- [3] MANG Z B, LIU P, CAI J, et al. Identity-aware convolutional neural networks for facial expression recognition[J]. Journal of Systems Engineering and Electronics, 2017, 28(4): 784-792.
- [4] HERMANS A, BEYER L, LEIBE B. In defense of the triplet loss for person re-identification[J]. arXiv:1703.07737, 2017.
- [5] LIU W Y, WEN Y D, YU Z D, et al. Large-margin softmax loss for convolution neural network[J]. arXiv:1612.02295, 2016.
- [6] LIU W Y, WEN Y D, YU Z D, et al. SphereFace: deep hypersphere embedding for face recognition[J]. arXiv: 1704.08063, 2017.
- [7] WANG H, WANG Y T, ZHOU Z, et al. CosFace: large margin cosine loss for deep face recognition[J]. arXiv:1801.09414, 2018.
- [8] DENG J K, GUO J, XUE N N, et al. ArcFace: additive angular margin loss for deep face recognition[J]. arXiv:1801.07698, 2018.
- [9] 汪一文. 深度卷积神经网络在 OCR 问题中的应用研究[D]. 成都: 电子科技大学, 2018.
WANG Y W. The research and application of deep convolution neural network in OCR problem[D]. Chengdu: University of Electronic Science and Technology of China, 2018.
- [10] NEUMANN L, MATAS J. A method for text localization and recognition in real-world images[C]//Asian Conference on



- Computer Vision(ACCV 2010), Nov 8-12, 2010, Queenstown, New Zealand. Heidelberg: Springer, 2010: 70-783.
- [11] EPSSTEIN B, OFEK E, WEXLER Y. Detecting text in natural scenes with stroke width transform[C]//IEEE Conference on Computer Vision and Pattern Recognition(CVPR 2010), June 13-18, 2010, San Francisco, USA. Piscataway: IEEE Press, 2010: 2963-2970.
- [12] YAO C, BAI X, LIU W Y. Detection texts of arbitrary orientations in natural images[C]//IEEE Conference on Computer Vision and Pattern Recognition(CVPR 2012), June 16-21, 2012, Providence, USA. Piscataway: IEEE Press, 2012: 1083-1090.
- [13] BISSACCO A, CUMMINS M, NETZER Y, et al. Photo OCR: reading text in uncontrolled conditions[C]//IEEE International Conference on Computer Vision, Dec 1-8, 2013, Sydney, Australia. Piscataway: IEEE Press, 2013: 785-792.
- [14] REDMON J, DIVVALA S, GIRSHICK R. You only look once: unified, real-time object detection[J]. arXiv: 1506. 02640, 2015.
- [15] ZHOU X Y, YAO C, WEN H. EAST: an efficient and accurate scene text detector[J]. arXiv: 1704.03155, 2017.
- [16] SHI B G, BAI X, YAO C. A end-to-end trainable neural network for image-based sequence recognition and its application to scene text recognition[J]. arXiv:1507.05717v1, 2015.
- [17] CHAKRABORTY, DAS S, DHRUBAJYOTI. An overview of face liveness detection[J]. International Journal on Information Theory (IJIT), 2014, 3(2).
- [18] KAHM O, DAMER N. 2D face liveness detection: an overview[C]//International Conference of Biometrics Special Interest Group, Sept 6-7, 2012, Darmstadt, Germany. Piscataway: IEEE Press, 2012: 1-12.
- [19] YUAN Z, LYU Z R, LI J W, et al. An improved hybrid CTC-ATTENTION model for speech recognition[J]. arXiv:1810.12020, 2018.
- [20] 陆小铭, 曹维华, 余勇昌. 电信运营商发展云存储业务的网络问题探讨[J]. 电信科学, 2010, 26(6): 71-75.
- LU X M, CAO W H, YU Y C. Analysis of network problems in development of cloud storage service by telecom operator[J]. Telecommunications Science, 2010, 26(6): 71-75.

[作者简介]



姚慧 (1991-), 女, 中移在线服务有限公司工程师, 主要从事图像处理相关算法引擎的研究与开发工作, 主要研究方向包括人脸识别、物体检测与识别、图像检索和通用 OCR 等。

马思研 (1989-), 女, 中移在线服务有限公司工程师, 主要从事图像领域内深度学习算法的研究与开发工作, 主要研究方向包括人脸识别、OCR 等。