

基于卷积神经网络的服务机器人 听觉隐私信息分类算法

王怀豹,杨观赐*,李 杨,林家丞

(贵州大学 现代制造技术教育部重点实验室,贵州 贵阳 550025)

摘 要:为获得机器人听觉行为隐私感知方法,解决语音监听设备存在的隐私泄露风险,本文提出了基于卷积神经网络的服务机器人听觉隐私信息分类算法(APICA)。首先,设计了基于卷积神经网络的服务机器人听觉隐私信息分类算法及其卷积神经网络模型;其次,给出了机器人的听觉隐私信息监听系统工作流程;最后,为评估该听觉隐私信息分类算法性能,构建了训练和测试数据集,并在服务机器人平台上部署和实现了该算法。测试结果表明:系统识别隐私信息的平均精确率 P 、召回率 R 和 $F1$ 值分别为 96.35%、93.20%和 94.53%,具有良好的识别和分类效果。

关键词:隐私感知方法;服务机器人;分类算法;听觉隐私信息

中图分类号:TP181

文献标识码:A

随着人口老龄化趋势加快,越来越多的独居老人需要被照顾,人们对助老机器人的需求也越来越明显^[1]。为辅助老年人日常生活,薛同来等^[2]研究了基于激光 SLAM 的助老机器人,其拥有自主构建室内地图以及自主导航的功能,可以定位目标物体和自主移动,并使用机械臂对物体进行抓取。为解决老年人心理健康问题,刘策等^[3]构建了具有语音识别、手势识别、人脸识别和远程控制功能的多模式友好交互系统,实现了注册与验证、移动控制、新闻点播、日程提醒及语音对话 5 种功能。与此同时,为给老年人提供科学合理的饮食建议,苏志东等^[4-5]提出了基于服务机器人听觉的个体膳食构成自主感知算法,实现了对用户膳食构成的智能感知,为用户医疗诊断、饮食干预和机器人的主动服务等提供决策依据。为了应对老年人记忆力衰退的情况,Ahn Ho 等^[6]提出了一种基于家庭服务机器人的大脑训练方法,将记忆训练部署到机器人上,以增强机器人功能性。为增强老年人的体质,降低老年人摔倒的风险,Foukarakis 等^[7]提出了一种利用机器人视觉系统来识别和跟踪用户行为的方法,

可以提供相关的练习和反馈来激励用户进行体育锻炼和康复训练。为满足老年人的远程护理需求,Zhou 等^[8]提出了一种基于服务机器人的远程医疗系统。该系统在家庭成员和医生之间建立连接,利用自动健康数据采集技术和目标检测算法,实现远程护理。然而,智能家居系统和服务机器人广泛使用语音监听设备,这存在用户隐私泄露的风险。

有研究表明,用户会因担忧语音监听设备泄露隐私而影响心理状态甚至引起心理障碍^[9]。如何构建对隐私内容符合人心理需求反应的系统,是值得深入研究的课题。为获得机器人听觉行为隐私感知方法,解决语音监听设备存在的隐私泄露的风险,本文提出了基于卷积神经网络的服务机器人听觉隐私信息分类算法。

1 基于卷积神经网络的服务机器人 听觉隐私信息分类算法

卷积神经网络是受生物学启发而提出形成的一种前馈神经网络,利用局部连接和权值共享特性,减少模型参数,并具有平移、尺度和视角不变

收稿日期:2020-01-08

基金项目:国家自然科学基金项目资助(61863005);贵州省科技计划项目资助(黔科合平台人才[2018]5702,黔科合平台人才[2018]5781,黔科合平台人才[2020]6007,黔科合支撑[2019]2814,黔科合支撑[2020]4Y056)

作者简介:王怀豹(1992-),男,在读硕士,研究方向:智能与自主机器人,Email:871398270@qq.com.

*通讯作者:杨观赐,Email:gcyang@gzu.edu.cn.

性^[10]。卷积神经网络不仅在图像分类领域贡献巨大,而且在自然语言方面也取得了引人注目的成果^[11-13]。针对机器人听觉行为隐私感知,本文提出了算法1所示的基于卷积神经网络的服务机器人听觉隐私信息分类算法(Social Robot Auditory Privacy Information Classification Algorithm based on Convolutional Neural Network, APICA)。图1是卷积神经网络模型。

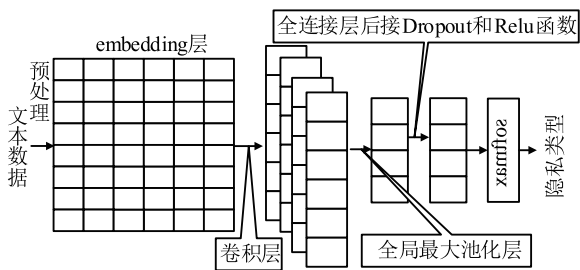


图1 卷积神经网络模型

Fig.1 Convolutional neural network model

算法1 基于卷积神经网络的服务机器人听觉隐私信息分类算法

输入:训练数据集 I ;

输出:特征模型 M_i 。

步骤1 对训练数据集 I 进行数据预处理,生成批量不同类别隐私的训练数据集 $I_i, I = \{I_1, I_2, \dots, I_i\}$;

步骤2 输入批量数据集 I_i , 经过 Embedding 层, 利用 word2vec 生成相同维度的字向量, 使每条文本数据的尺寸为 $(600, 64)$;

步骤3 经过卷积层, 进行一维卷积, 通过256个尺寸为 5×1 的卷积核, 获得256个 596×1 的特征向量;

步骤4 经过全局最大池化层, 得到256个最大特征向量值;

步骤5 经过第一个全连接层, 后面接 Dropout 及 Relu 激活函数, 防止过拟合, 同时增加神经网络模型的非线性;

步骤6 经过第二个全连接层, 通过 softmax 函数计算出文本数据包含隐私信息的预测概率分布及其相应的损失值;

步骤7 执行误差反向传播操作, 用 Adam 算法优化更新特征模型 M_i , 满足设置条件后输出隐私特征模型 M_i 。

步骤1中, 进行数据预处理时, 首先考虑到程

序在 python2 环境下运行的编码问题。在打开文本数据集时, 把文本的格式编码成 UTF-8 格式, 在处理文本时解码为 Unicode 格式, 然后按以下步骤进行: ①读取训练数据集 I_i , 构建列表 contents, 列表中的每个元素即为一条文本数据中的字和符号; 同时构建列表 labels, 列表中的每个元素即为对应文本数据的隐私类别; 并构建字列表 words, 列表中的元素即为训练集中的字和符号; ②读取字列表 words, 由此构建 |字: 数字 id| 的字典 D_1 ; ③读取分类目录, 构建 |隐私类别: 数字 id| 的字典 D_2 ; ④根据字典 D_1 , 将列表 contents 中每个元素包含的字与符号进行数字编码, 即为列表 date_id; 根据字典 D_2 , 将列表 labels 中的每个元素进行数字编码, 即为 label_id; ⑤经过 padding, 把列表 date_id 中的每一个元素填充为固定长度 600, 同时对标签进行 one-hot 编码; ⑥生成批量训练数据集 $I = \{I_1, I_2, \dots, I_i\}$ 。

在运用算法1获得特征模型 M_i 后, 可得如下所示的机器人的听觉隐私信息监听系统工作流程:

(1) 获取听觉设备监听的语音数据 S ;

(2) 加载隐私特征模型 M_i ;

(3) 利用科大讯飞语音模块将语音数据 S 转化为文本数据 T ;

(4) 利用隐私特征模型 M_i , 对文本数据 T 进行鉴定, 从而判断所监听的语音信息中是否具有所关注的隐私信息, 并输出隐私类别;

(5) 如果监听结束, 则卸载模型; 否则转步骤(1)循环监听。

2 机器平台

图2所示为课题组搭建的服务机器人平台 MAT^[5,14], 主要包括 Intel NUC mini 主机、EAI Dash-goB1 移动底盘、iPad 显示屏、科大讯飞六麦环形麦克风阵列板、Microsoft Kinect V2 深度摄像头、辅助传感器和数据处理器等。听觉系统采用的六麦环形麦克风阵列板具有声源定位、回声消除、噪声过滤等功能, 用于实现对音频信号的采集; 视觉采用的 Microsoft Kinect V2 深度摄像头用于采集 RGB 彩色图像; 机器人上配备的 GSM 通信模块可以在紧急状况下与监护人进行通话。为减少机器人平台运算负荷, 训练数据和数据分析由数据处理工作站完成。服务机器人主机安装了 Ubuntu16.04 操作系统、Kinect 版本 ROS (Robot Operation System)

系统、TensorFlow CPU 版本深度学习框架和机器视觉工具包 Opencv3.3.0。课题组运用 Python 语言实现了 APICA 算法,并将其部署在 MAT 机器人上。



图 2 服务机器人平台 MAT
Fig.2 Used MAT robot

3 测试与分析

3.1 训练数据集、测试数据集和性能指标

使用 MAT 服务机器人的六麦环形麦克风阵列收集训练语音数据。与此同时,考虑到法律、文化习俗、认知心理学等与隐私信息形成有关的因素,调研相关文献资料,收集、整理、归纳出家庭生活中涉及语音隐私信息的特殊场景,研究确定不同场景下所涉及的语音隐私内容特征,设计了以下 6 种场景:(1)对话内容涉及家庭人员出行计划的场景;(2)对话内容涉及家庭人员联系方式的场景;(3)对话内容涉及支付密码的场景;(4)对话内容涉及宗教的场景;(5)对话内容涉及贵重物存放处的聊天场景;(6)对话内容涉及言语批评朋友或者攻击双方父母的场景。

基于上述 6 种场景构建了包括 7 种类别的训练数据集:

- (1)第 1 类数据 对话内容涉及家庭人员出行计划的场景,其对话内容中包含:①未来出行计划的时间名词;②未来出行计划的地理名词。
- (2)第 2 类数据 对话内容涉及家庭人员联

系方式的场景,其对话内容中包含:①联系方式的相关表达;②有关联系方式的数字。

(3)第 3 类数据 对话内容涉及支付密码的场景,其对话内容中包含:①支付密码的相关表达;②有关支付密码的数字和字母。

(4)第 4 类数据 对话内容涉及宗教的场景,其对话内容中包含:①某人是某宗教成员;②某人表达愿意加入某宗教;③某人喜欢、尊崇、信仰某宗教。

(5)第 5 类数据 对话内容涉及贵重物存放处的场景,其对话内容中包含:①贵重物品的名称;②对应贵重物品的存放地点。

(6)第 6 类数据 对话内容涉及言语批评朋友或者言语攻击双方父母的场景,其对话内容中包含批评或谩骂朋友或父母的词汇。

(7)第 7 类数据 不属于上述 6 种场景的对话,属于不包含隐私信息的数据。

测试数据集构建方面,对话内容通过网上收集和课题组成员构思获得。训练数据集和测试数据规模见表 1。

表 1 训练数据与测试数据规模
Tab.1 Detailed information about the training and test datasets

数据类别	数据规模/条	
	训练数据	测试数据
1	1 146	75
2	345	72
3	457	76
4	116	58
5	130	48
6	96	58
7(不涉及隐私)	3 781	238

采用精确率 P 、召回率 R 与综合评价指标 $F1$ 值度量算法的性能。

3.2 测试结果与分析

在已搭建的服务机器人平台上部署设计的算法,将超参数设置为:迭代次数为 3 000,卷积核数目为 256,批处理参数为 64,初始学习率为 0.001,Dropout 保留比例为 0.5。测试数据识别结果的混淆矩阵如表 2 所示。精确率 P 、召回率 R 和综合评价指标 $F1$ 值统计结果如表 3 所示。

表 2 识别结果的混淆矩阵

Tab.2 Confusion matrix of recognition accuracy

数据类别	识别数/条						
	1	2	3	4	5	6	7
1	68	0	0	0	0	0	7
2	0	72	0	0	0	0	0
3	0	0	76	0	0	0	0
4	0	0	0	54	0	0	4
5	0	0	0	0	48	0	0
6	0	0	0	0	0	42	16
7	5	0	0	2	0	2	229

表 3 *P*、*R* 和 *F1* 值统计结果

Tab.3 Statistical results of *P*, *R* and *F1* %

测试数据类别	<i>P</i>	<i>R</i>	<i>F1</i>
1	93.15	90.67	91.89
2	100	100	100
3	100	100	100
4	96.43	93.10	94.75
5	100	100	100
6	95.45	72.41	82.35
7	89.45	96.22	92.71

观察表 2 和表 3 可知:

(1)第 1 类测试数据共 75 条,其中正确识别数为 68 条,错误识别的有 7 条,系统的精确率和召回率分别为 93.15% 和 90.67%。核查识别错误的数 据,发现识别错误的原因 为:①对话未出现具体的 地理名词,而是通过其中 一般名词和方向名词可 以推理出地理名词;②对 话出现多个地理名词,且 对话双方经过反复谈论 出行计划但最终又否定 出行计划。

(2)第 2 类、第 3 类和第 5 类测试数据分别有 72 条、76 条和 48 条,系 统的精确率和召回率均 为 100%。

(3)第 4 类测试数据共 58 条,其中正确识别数 为 54 条,错误识别为类 别 7 的有 4 条,系统的精 确率和召回率分别为 96.43% 和 93.10%。核查识别 错误的数 据,发现识别错误的原因为:对话内容中 存在否定是某个宗教人 员的话语,如“我不是佛 教成员,我是基督教成 员。”

(4)第 6 类测试数据共 58 条,其中正确识别数 为 42 条,错误识别为类 别 7 的有 16 条,其精确率

和召回率分别为 95.45% 和 72.41%。核查识别错 误的数 据,发现识别错误的原因为:①言语批评的 对象为影视剧或历史人 物;②一些词语在不同的 语句中含义不同,例:“我 身体不舒服,有点想吐” 与 “我每次看到我们领导 都想吐”,这两句话中的 “吐”字,用在不同的地 方具有不同的语义;③语 气导致的语义改变而导 致识别错误。

(5)第 7 类测试数据共 238 条,系统正确识别 229 条,错误识别为类别 1、4、6 的数据分别有 5 条、 2 条和 2 条,系统的精确 率和召回率分别为 89.45% 和 96.22%。

综上,测试数据集共 625 条数据,系统正确识 别数为 589 条,总体识别 准确率为 94.24%,平均精 确率为 96.35%,平均召 回率为 93.20%,综合评 价指标为 94.53%,系统 具有很好的识别和分类 效果。

4 结语

研究服务机器人听觉隐私信息的感知和保护 技术,有助于服务机器人 的推广与普及。本文正 是针对机器人所听到的 语音数据,提出和实现了 基于卷积神经网络的服务 机器人听觉隐私信息分 类算法,来判定语音数据 的隐私类别,为隐私数据 的保护奠定基础。下一 步将继续补充和完善训 练数据集,使监听系统 具有更好的鲁棒性;此外, 听觉隐私数据的保护机 制与方法也是值得深入 研究的方向。

参考文献:

[1] ZHAO J M, LI X Y. The status quo of and development strategies for healthcare towns against the background of aging population[J]. Journal of Landscape Research, 2018, 10(4): 41-44.

[2] 薛同来,赵冬晖,韩菲,等. 基于激光 SLAM 的助老机器人[J]. 工业控制计算机, 2019, 32(6): 35-36.

[3] 刘策,刘小峰. 助老服务机器人多模式友好交互系统设计与实现[J]. 电子测量与仪器学报, 2019, 33(1): 177-182.

[4] 苏志东,杨观赐,李杨,等. 基于服务机器人听觉的个人膳食构成自主感知算法[J]. 贵州大学学报(自然科学版), 2019, 36(4): 80-86.

[5] SU Z D, LI Y, YANG G C. Dietary composition perception algorithm using social robot audition for mandarin Chinese[J]. IEEE Access, 2020, 8: 8768-8782.

[6] AHN H S, SANTOS M P G, WADHWA C, et al. Development of brain training games for a healthcare service robot for older people [C]//6th International Conference on Social Robotics (ICSR 2014). Sydney, NSW, Australia: Springer Verlag, 2014 :1-10.

[7] FOUKARAKIS M, ADAMI I, IOANNIDI D, et al. A Robot-based

application for physical exercise training[C]//Proceedings of the International Conference on Information and Communication Technologies for Ageing Well and e-Health. Rome, Italy: SciTePress, 2016: 45-52.

[8] ZHOU B, WU K, LV P, et al. A new remote health-care system based on moving robot intended for the elderly at home[J]. Journal of Healthcare Engineering, 2018, 2018:4949863.

[9] KALPANA S, JEAN C, KAY C, et al. Aging, privacy, and home-based computing: development of a framework for design[J]. IEEE Pervasive Computing, 2012, 11(4): 46-54.

[10] 籍祥. 卷积神经网络在中文问题分类中的应用[J]. 软件导刊, 2018, 17(9): 25-27.

[11] 赵力, 将春辉, 邹采荣, 等. 语音信号中的情感特征分析和识别的研究[J]. 电子学报, 2004, 32(4): 606-609.

[12] 韩文静, 李海峰, 阮华斌, 等. 语音情感识别研究进展综述[J]. 软件学报, 2014, 25(1): 37-50.

[13] 徐济仁, 陈家松, 徐屹. 语音信号预处理技术综述[J]. 电子工程师, 2001, 27(6): 26-27.

[14] 杨观赐, 杨静, 苏志东, 等. 改进的 YOLO 特征提取算法及其在服务机器人隐私情境检测中的应用[J]. 自动化学报, 2018, 44(12): 2238-2249.

(责任编辑: 曾 晶)

Social Robot Auditory Privacy Information Classification Algorithm Based on Convolutional Neural Network

WANG Huaibao, YANG Guanci*, LI Yang, LIN Jiacheng

(Key Laboratory of Advanced Manufacturing Technology of Ministry of Education, Guizhou University, Guiyang 550025, China)

Abstract: In order to obtain the robot auditory behavior privacy perception method and solve the risk of privacy leakage in speech monitoring equipment, APICA, a social robot auditory privacy information classification algorithm based on Convolutional Neural Network was proposed. Firstly, the algorithm and convolutional neural network structure of the proposed APICA were presented, and then the work flow of the social robot auditory privacy information monitoring system was put forward. Finally, to evaluate the performance of APICA, training dataset and test dataset were established, and the proposed method was implemented in a social robot platform. The test results show that APICA is capable of recognizing privacy information with an average accuracy rate, recall rate and *F1* score of 96.35%, 93.20% and 94.53%, respectively.

Key words: privacy perception; social robot; classification algorithm; auditory privacy information