计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2021,30(8):150−156 [doi: 10.15888/j.cnki.csa.008035]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

基于深度学习的计算机显示器电磁信息泄漏识别①

裴林聪[1], 张游杰[2], 马通边[2], 石　森[2]

[1](太原科技大学 计算机科学与技术学院, 太原 030024)
[2](中国电子科技集团公司第三十三研究所, 太原 030032)
通讯作者: 裴林聪, E-mail: MRDWXVIP@163.com

摘　要: 本文以计算机显示设备泄漏电磁信号为研究对象, 对于人工提取特征识别电磁泄漏信号存在的主观性强、特征冗余的问题, 区别于传统基于经验的人工特征提取模式, 利用人工智能深度学习方法, 使用处理图像的深度学习技术应用于电磁信息泄漏特征识别, 提出了一种基于卷积神经网络的识别方法. 该方法首先提取电磁泄漏信号的时频谱信息作为卷积神经网络模型的输入, 然后利用模型的自学习能力提取深层特征, 实现对不同分辨率来源电磁泄漏信号的识别, 识别准确率达到 98%, 单信号检测时间仅需 40 ms, 验证了卷积神经网络应用于电磁泄漏信号识别的有效性, 为电磁泄漏预警与防护提供了重要依据, 为电磁泄漏视频信号还原复现提供有力支撑.

关键词: 电磁泄漏; 特征提取; 卷积神经网络; 电磁防护; 电磁信号识别

引用格式: 裴林聪,张游杰,马通边,石森.基于深度学习的计算机显示器电磁信息泄漏识别.计算机系统应用,2021,30(8):150–156. http://www.c-s-a.org.cn/1003-3254/8035.html

Electromagnetic Information Leakage Recognition of Computer Display Based on Deep Learning

PEI Lin-Cong[1], ZHANG You-Jie[2], MA Tong-Bian[2], SHI Sen[2]

[1](College of Computer Science and Technology, Taiyuan University of Science and Technology, Taiyuan 030024, China)
[2](The 33rd Research Institute of China Electronics Technology Group Corporation, Taiyuan 030032, China)

Abstract: The electromagnetic leakage signals recognized by manually extracted features are strongly subjective with feature redundancy. For this reason, different from the traditional artificial feature extraction mode based on experience, this study proposes a recognition method based on a Convolutional Neural Network (CNN), with the electromagnetic leakage signals of computer displays as the research object. This method employs the artificial intelligence-based deep learning method and applies the deep learning technology of image processing to the leakage feature recognition of electromagnetic information. Firstly, the time-frequency spectrum information of electromagnetic leakage signals is extracted as the input of the CNN model. Then, the deep-seated features are extracted by the self-learning ability of the model to recognize electromagnetic leakage signals from sources with different resolutions. Finally, the recognition accuracy reaches 98%, and the detection of a single signal only takes 40 ms, which verifies the effectiveness of CNN in the recognition of electromagnetic leakage signals. The proposed method provides an important basis for the early warning and protection of electromagnetic leakage and offers strong support to the restoration and reproduction of electromagnetic leakage video signals.

Key words: electromagnetic leakage; feature extraction; Convolution Neural Network (CNN); electromagnetic protection; electromagnetic signal recognition

① 基金项目: 山西科技厅重点研发计划 (201903D111002)
Foundation item: Project of Research and Development Key Program of Science and Technology Bureau, Shanxi Province (201903D111002)
收稿时间: 2020-11-17; 修改时间: 2020-12-21; 采用时间: 2021-01-07; csa 在线出版时间: 2021-07-31

1 引言

信息安全是每个国家都需要去重视的安全问题, 在全世界范围内, 对于国家安全、社会稳定和经济发展的影响十分巨大. 电磁波是最常见的信息载体, 电磁发射与信息安全有着必然的联系[1]. 而随着网络信息安全技术飞速发展的同时, 物理空间信息安全技术也逐渐得到重视, 关键信息技术设施安全首当其冲, 成为物理空间信息安全于防护的首要关注目标, 其中电磁信息泄漏所带来的负面影响范围更广[2], 对于电磁防护, 电磁泄漏信号精准定位, 评估电磁泄漏风险以及威胁程度, 需要结合计算机领域深度学习与图像识别等技术来提供良好支持.

随着科技进步, 计算机技术快速发展的同时, 神经网络作为深度学习一项重要技术和基础成为研究关注的热点, 学术界进行了多种研究方向的探索, 众多领域取得了很大的成就, 深度学习在更加广泛的领域上, 产生了深远的影响, 引起了社会各界的热切关注. 深度学习等技术应用于电磁信号[3]、雷达信号等信号处理[4]识别方法中成为一种趋势, 深度学习在电磁信号识别任务中具有独特优势, 相较于传统的信号特征识别分类, 卷积神经网络以简洁的优势、良好的效果、成为理想选择. 传统方法依赖于人工特征提取, 这些特征虽然有一定的普适性, 但针对复杂环境以及特定场景时, 通过人工经验方法去提取特征会有很大的挑战, 能提取出准确完成目标的人工特征也绝非易事. 而通过神经网络自主学习模拟大脑的视觉处理机制, 从训练中提取目标特征, 层次化的抽象、自动筛选特征, 实现了高度自动化的特征提取, 使得在应对信号处理, 特征提取识别等领域有了极大的用武之地, 也是未来发展的方向和趋势, 本文利用深度学习技术[5]代替传统人工的复杂操作, 提取电磁泄漏信号的模式特征, 提高电磁泄漏信号的识别能力[6]. 深度学习作为信号处理的一种新型应用技术, 已经展现出其独特的优势, 为解决信号处理的一些技术难题提供了新的思路[7], 本文的主要研究了基于时频分析和卷积神经网络的电磁泄漏信号识别方法, 首先将一维电磁信号通过短时傅里叶变换转化为含有时频谱信息的二维时频图像作为卷积神经网络的输入, 实现对于电磁泄漏信号的分类识别输出, 省去了特征提取相关的繁琐工作, 配合自主开发的实时监测识别系统验证算法的可行性和有效性.

2 相关研究工作

2.1 研究概述

本文通过设计训练卷积神经网络模型 CNN[8] 去实现监测识别计算机视频电磁信息泄漏信号, 具体的工作流程为: 首先, 对计算机显示器的分辨率以及传输线 VGA 时序分析了解相关机理, 为数据采集以及预处理提供理论支持, 使用高性能设备完成数据采集工作, 再通过时频分析短时傅里叶变换将一维信号转化为二维时频图像, 输入到卷积神经网络模型 CNN 训练出满意的识别效果模型; 然后, 利用该模型识别出计算机视频不同分辨率电磁信号, 将整个模型嵌入实时监测识别系统来验证算法的有效性和可行性, 整体流程如图 1 所示.

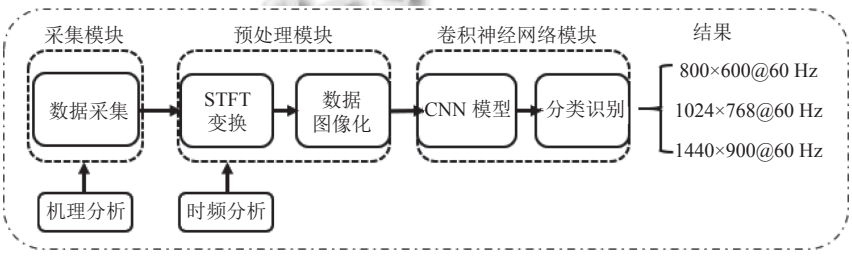

图 1 电磁泄漏信号识别示意图

2.2 视频分辨率及传输线 VGA 时序分析

基于常用显示器 LCD 分辨率 1024×768, 屏幕刷新率为 60 Hz, 屏幕刷新一帧所用的时间为 16.6 ms, 显示器屏幕分辨率设置为 1024×768 时根据视频电子标准协会 (Video Electronics Standards Association, VESA) 定义行时序和场时序都需要同步脉冲 a、显示后沿 b、显示时序段 c 和显示前沿 d 组成一个完整的时序如图 2、图 3 所示.

以 1024×768@60 Hz 时序参数为例, 其行时序参数与场时序参数如表 1 所示,

则一帧的 RGB 信号中包含消隐区的像素行数为 806, 一行的像素个数为 1344, 包含消隐区的屏幕分辨率为 1344×768, 总计 1032 192 个像素点.

根据 VESA 发布的计算机显示器时序指南[9] 如表 2 所示.

计算机的 RGB 信号是一个复合信号, 其中会包含行、场同步信号, 以及像素时钟信号, 在 1024×768、60 Hz 刷新率的情况下, 行同步信号频率为 60.004 Hz, 场同步信号频率为 48.363 kHz, 像素时钟频率为 65 MHz.

在此条件下, 数据采集参数设置为, 采样时间为 20 ms, 采样深度 5 M, 采样频率 250 MHz. 可以达到复现级别的采样精度, 以及满足采样信号内容不丢失.

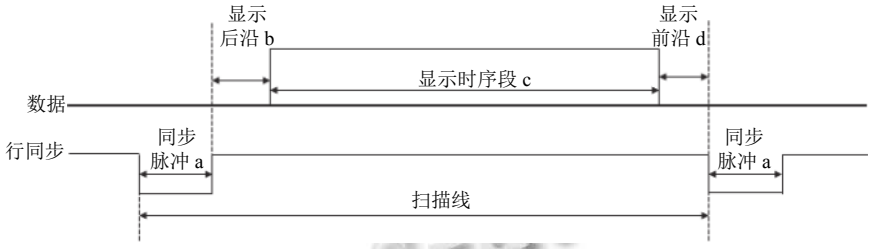

图 2　视频传输线 VGA 行时序

图 3　视频传输线 VGA 场时

表 1　1024×768@60 Hz 时序参数

视频显示模式	行时序参数(单位: 像素)					场时序参数(单位: 行)				
参数	a	b	c	d	消隐	a	b	c	d	消隐
1024×768@60 Hz	136	160	1024	24	1344	6	29	768	3	806

表 2　计算机视频显示时序标准参数

视频显示模式	场频 (Hz)	行频 (kHz)	像素时钟 (MHz)	消隐分辨率
800×600@60 Hz	60.317	37.879	40	1056×628
1024×768@60 Hz	60.004	48.363	65	1344×806
1440×900@60 Hz	59.887	55.935	106.5	1904×934
1440×900@60 Hz(RB)	59.901	55.469	106.5	1600×926

2.3　时频分析短时傅里叶变换

短时傅里叶变换是较为常用的一种方法, 一种易于理解的方法, 即在频域中的每一个特征信息都对应于一个时间段. 当我们使用窗的特性来分割信号表征某一个时刻的信号特征[10]. 窗口函数是整个短时傅里叶变换的核心, 窗口宽度对于短时傅里叶变换有着直接影响. 以窗口的宽度来截取电磁泄漏信号, 所以窗口的宽度与信号长度成正比例关系, 经过一个窗口的傅里叶变换之后, 宽口宽度大时, 频率分辨率也同时变高, 可以观测频谱的快变化. 当窗口的宽度小时, 相应的信号截取也较短, 频率分辨率也随着变低, 不可以观测到频谱的快变化. 时间分辨率与窗口宽度成反比例关系, 窗口宽度大、时间分辨率小, 窗口宽度小, 时间分辨率大. 随着窗口的滑动整个信号的瞬时特征相应被得到, 一系列的傅里叶变换最终被排列成二维的时频图像[11].

影响短时傅里叶变换效果的因素有两个: 窗函数的类型以及窗的宽度, 不同的窗函数会有不同的频谱泄漏和谱间干扰, 而时域和频域的相对分辨率则是受到窗的宽度影响, 窗体较宽则频域分辨率较高, 窗体较窄则时域分辨率较高. 根据上述短时傅里叶变换的公式可以表示为:

$$STFT_Z(\mathrm{t},f)=\int_{-\infty}^{\infty}[z(u)g(u-t)]e^{-j2\pi fu}\mathrm{d}u \qquad (1)$$

其中, $z(t)$ 为时域信号, $g(t)$ 是以 t 时刻为中心的时间窗口函数.

3 数据采集与处理

3.1 数据采集设计

通过 LabView 自主编写的采集系统利用 NI-Scope 控件, 连接到高精度高速数据采集卡 NI PXI-5152 采集视频泄漏信号的时域波形信号, 使用环形钳, 探测传输线缆上的电磁泄漏传导信号, 实时加载到 LabView 搭建的实时监测系统处理平台中进行后续数据操作与保存, 其整体流程如图 4 所示.

通过实时监测系统, 完成数据采集以及泄漏信号监测, 其时域、频域如图 5、图 6 所示.

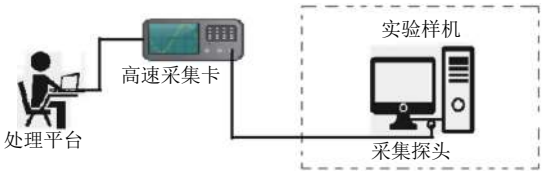

图 4 数据采集系统示意图

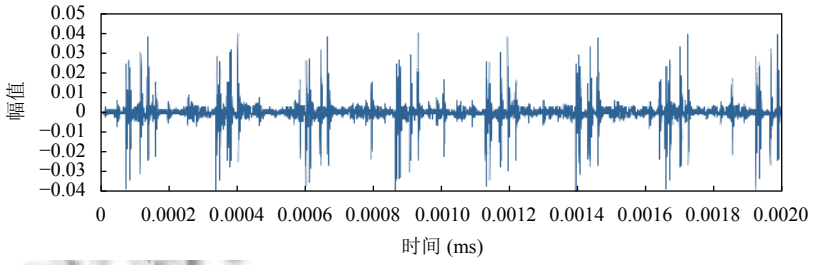

图 5 时域信号

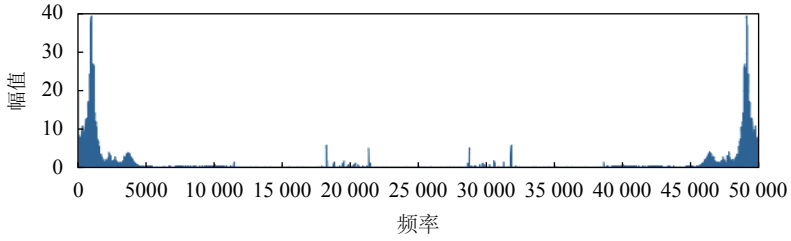

图 6 频域信号

3.2 数据预处理

按照采样时间为 20 ms, 采样深度 5 M, 采样频率 250 MHz 的采样规格, 连续采集三组数据, 同时将 3 组数据通过图像预处理平台, 进行时频分析, 采用短时傅里叶变换 (STFT), 将数据信号以时频图的方式展现出来如图 7 所示, X 轴代表时间, Y 轴代表频率, 图像颜色深度代表能量, 通过 3 个不同的维度, 更加直观精细的分析信号的变化情况, 以求提取深层次特征.

通过 LabView 与 Python 联合编程实现的系统中预处理功能, 批量处理, 产生数据, 并保存到本地. 将信号数据输入预处理系统, 分批处理, 制作 45 000 张时频图作为卷积神经网络的数据样本, 同时以 4:1 的比例抽取 36 000 张, 作为训练集, 抽取 9000 个数据作为验证集, 输入神经网络训练模型. 利用短时傅里叶变换 STFT 进行时频分析, 获得时频图像, 并对时频图像进行图像归一化预处理, 生成 224×224 大小的 RGB 图像集, 通过编写的 Python 脚本将预处理好的相应网络图片批量导入带有分类的标签文件夹, 来建立输入网络的图片标签, 并为每张图片修改名称及序号来达到标注效果.

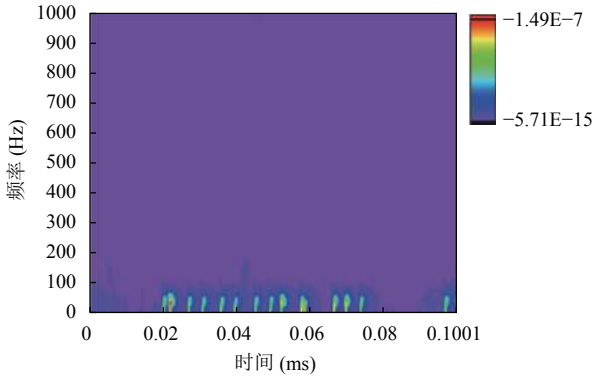

图 7 STFT 一维信号转化为二维时频图

4 构建卷积神经网络模型

4.1 卷积神经网络概况

近年来深度学习神经网络应用于信号处理等领域应用广泛[12],本文通过将深度学习卷积神经网络应用于电磁泄漏信号识别, 利用神经网络自动提取电磁信号的特征[13], 避免基于经验的人工特征提取的复杂条件, 通过二维图像对电磁信号进行表征, 利用卷积神经网络层次化地理解和识别电磁信号.

神经网络的研究与人类视觉的研究密切相关, 为了进一步提高神经网络的性能, 通过借鉴人脑视觉系统的最新研究成果为卷积神经网络的研究寻找下一个突破口, 已成为越来越受到学术界关注的研究方向[14]. 卷积神经网络 (Convolutional Neural Network, CNN) 是一种特殊的深层前馈网络, 在前馈神经网络基础上进行升级改造的深层神经网络, 每个神经元都只与邻近的局部神经元相互作用[15].

4.2 算法实现步骤

CNN 模型主要包含输入层 (input layer)、卷积层 (CONV layer)、池化层 (pooling layer) 以及全连接层 (FC layer) 等.

通过测试, 本文设计的卷积神经网络结构图如图 8 所示, 其中, 卷积神经网络由 8 层组成, 分别为 4 个卷积层、2 个池化层和 1 个全连接层, 最后一层选择采用 Softmax 分类器, 在建立卷积神经网络模型中选择 4 个卷积层都使用 3×3 的卷积核是为了通过卷积核去压缩卷积神经网络模型中参数个数, 而且在每次下采样的操作之后可以将特征通道的数量成倍增加, 这样可以尽量保持特征的完整性, 整个网络都使用了同样大小的卷积核尺寸 3×3 和最大池化尺寸 2×2, 较小的卷积核和池化采样域, 使得卷积神经网络模型在卷积和下采样操作过程中能够在获得更多图像特征信息还可以节制参数的个数, 避免因为大量的计算和过于复杂的模型结构导致模型冗余, 只使用一个全连接层来减少模型参数, 达到更好效果. 因此建立的 8 层卷积神经网络模型具有简洁的结构和较少参数等优点, 并在此基础上达到不错的效果.

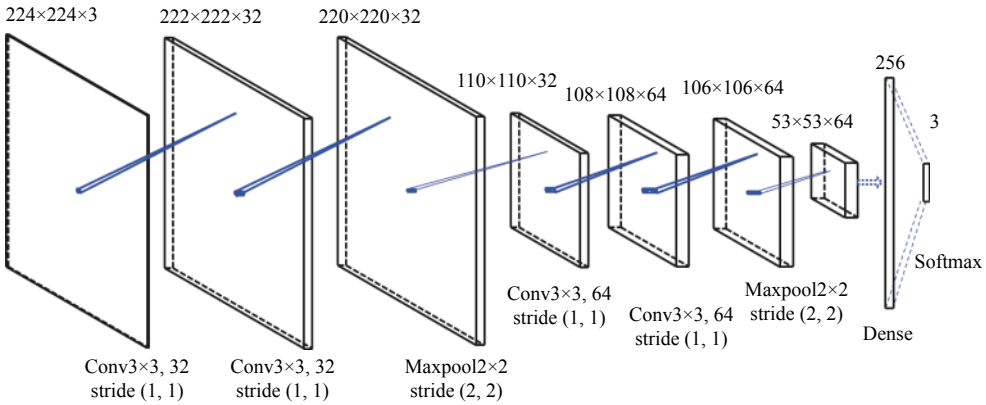

图 8 卷积神经网络结构图

每层使用 ReLU 作为激活函数. 与传统的 Sigmoid 函数和 tanh 函数相比, ReLU 作为优化的网络结构参数在深层的卷积神经网络训练过程中表现出明显的优势[16], 其定义为:

$$f(x) = \max(0, x) \tag{2}$$

ReLU 函数和导数都不包含复杂数学运算, 使得网络的收敛速度更加快速, 解决了梯度消失问题, 显著提升了深度神经网络的性能[17]. 模型损失函数使用 categorical-crossentropy, 优化器使用的是 SGD. 为了防止梯度弥散, 型中在卷积层加入 50%的 dropout 处理.

将 224×224 大小的时频图像输入到卷积神经网络模型中, 卷积层 Conv1、Conv2 的卷积核大小为 3×3, 深度为 32, 使用 ReLU (Rectified Linear Unit 修正线性单元) 作为激活函数, Padding 选择不填充 (Valid), 步长 Stride 为 1. 最大池化层 MaxPool1 大小为 2×2, 步长 Stride 为 2, 使用 25% 的 dropout 防止梯度弥散.

卷积层 Conv3、Conv4 的卷积核大小为 3×3, 深度为 64, 使用 ReLU 作为激活函数, Padding 选择不填充 (Valid), 步长 Stride 为 1. 最大池化层 MaxPool2 大小为 2×2, 步长 Stride 为 2, 使用 25% 的 dropout 防止梯

度弥散. 全连接层 FC 为 256, 使用 50% 的 dropout 避免过度拟合, 最后使用 Softmax[18] 分类器输出 800×600@60 Hz、1024×768@60 Hz、1440×900@60 Hz 分类识别结果. 其网络模型参数见表 3.

表 3 卷积神经网络模型参数

网络模型	输入维度	卷积核个数	卷积核大小	步长	输出维度
Input	224×224×3	—	—	—	—
Conv1	224×224×3	32	3×3	1	222×222×32
Conv2	222×222×32	32	3×3	1	220×220×32
MaxPool1	220×220×32	—	2×2	2	110×110×32
Conv3	110×110×32	64	3×3	1	108×108×64
Conv4	108×108×64	64	3×3	1	106×106×64
MaxPool2	106×106×64	—	2×2	2	53×53×64
Fc	53×53×64	—	—	—	1×1×256
Softmax	1×1×256	—	—	—	1×1×3

5 实验结果分析

在训练过程中, 每次迭代后数据被打乱再重新开始下一轮迭代. 加入早停法 (EarlyStopping) 组件, 使得模型在每次迭代结束后会检查验证损失值 (Validation loss), 如果验证损失值连续多次不再发生变化, 则表明模型参数训练充分, 则终止训练过程, 并输出训练结果.如图 9、图 10 所示,训练效果通过识别准确率和损失率来衡量.

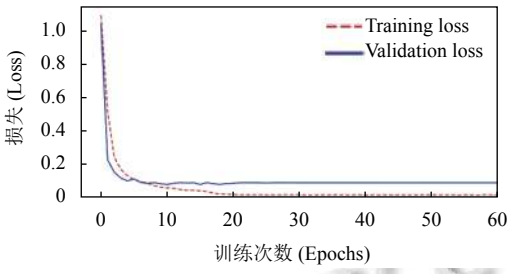

图 9 损失函数曲线

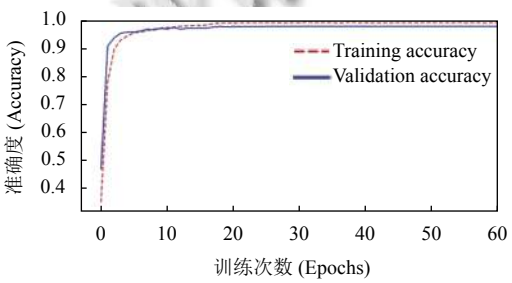

图 10 准确率曲线

从图 9 中可以看出, 随着训练迭代数的不断增加, 训练集损失值 (training loss) 和验证集损失值 (validation loss) 均逐渐减小, 在第 50 代以后, 曲线趋于平缓, 当验证集损失值下降到 0.05～0.2 时, 验证集损失值几乎不再发生变化, 最终触发早停法停止训练, 网络模型参数训练充分, 训练结束, 整个训练花费时间约为 4 个小时, 训练过程中每一轮耗时约为 225 s.

分析实验结果可知, 随着训练次数不断提升, 训练准确率和验证准确率也不断提升并趋于稳定, 经过测试, 对于 800×600@60Hz、1024×768@60Hz、1440×900@60Hz 分辨率下信号分类识别率达到 98.7%. 混淆矩阵 (confusion matrix) 是评价多分类问题的主要手段, 是一种通过特制矩阵来展现算法性能的手段, 其数据可视化的效果让观测者能够更加直观的了解算法优劣, 包含实际分类和预测分类的信息, 混淆矩阵的对角线上所展示的值越高, 代表预测的效果越好, 准确度越高[19], 实验使用混淆矩阵来进一步评估算法的性能, 如图 11 所示, 混淆矩阵横轴为电磁信号模式的预测值, 纵轴为电磁信号模式的真实值, 右侧色彩条的颜色深浅来表示从 0 至 1 的准确程度.

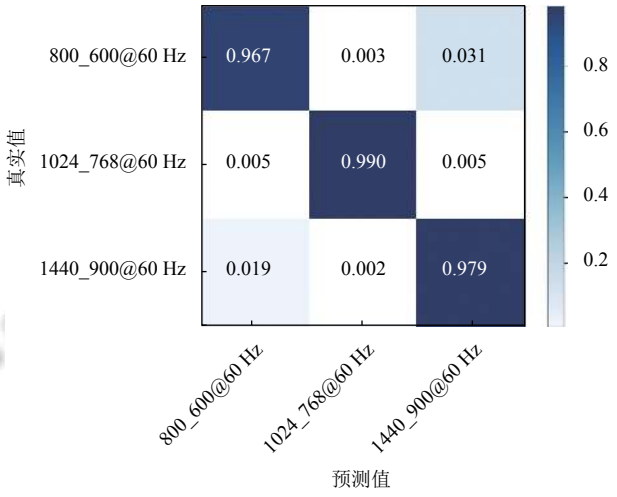

图 11 归一化混淆矩阵

在常规的识别方法中由专业人员通过对信号样本进行监测分析, 在时域, 频域, 空间以及能量等条件下挑选信号关键特征, 如相位脉冲个数, 包络峭度等, 最后计算特征参数值来基于固定方法分类, 此方法对工作人员专业技术经验要求极高, 而在数据较多时, 人工先验的传统模式分析效率和准确率也会大打折扣. 而本文的方法基于深度学习实现端到端的识别模型, 自动从样本图像中学习图像特征通过深层次的网络结构提取到更加准确, 更加高维, 更加抽象的特征, 这些特

征最后输入网络模型的分类器中从而达到不错的分类识别效果以及更高的准确度, 提高了计算机电磁泄漏信号的识别能力.

6 结论与展望

文章提出了一种基于深度学习卷积神经网络的视频电磁信息泄漏信号在不同分辨率下的识别新方法, 通过时频分析等预处理方式将一维信号转变为二维时频图像来对电磁信号表示, 使得能够利用图像识别等领域的手段来处理问题, 为视频电磁信息泄漏信号的识别提供了新的思路, 相较于传统特征提取过程深度学习技术实现自动化的去学习目标的抽象特征, 避免了传统人工带来的繁琐与利用率低等问题, 实验表明利用卷积神经网络能够实现端到端的视频电磁泄漏信号识别的可行性. 为了验证本文算法的实用性能, 基于 LabView 和 Python 开发了一套实时采集监测识别系统,实验结果表明算法能有效识别电磁信号.

所提出的方法应用于视频电磁泄漏信号识别还是初步尝试, 对于时频分析方法的选择, 以及相关电磁泄漏信号类别的提升, 网络模型优化还值得进一步研究.

参考文献

1 Hayashi YI. State-of-the-art research on electromagnetic information security. Radio Science, 2016, 51(7): 1213–1219. [doi: 10.1002/2016RS006034]

2 王文学, 赵晔. 计算机电磁波信息安全防泄漏技术研究. 信息技术, 2003, 27(8): 63–66. [doi: 10.3969/j.issn.1009-2552.2003.08.023]

3 方成, 薛质. 基于全双谱和卷积神经网络的信号分类方法. 计算机应用研究, 2018, 35(12): 3766–3769. [doi: 10.3969/j.issn.1001-3695.2018.12.054]

4 Gao SP, Guo YK, Aung ZT, *et al*. Analysis of information leakage from MCU using neural network. Proceedings of the 12th International Workshop on the Electromagnetic Compatibility of Integrated Circuits. Hangzhou, China. 2019. 171–173.

5 Arel I, Rose DC, Karnowski TP. Deep machine learning—A new frontier in artificial intelligence research [Research Frontier]. IEEE Computational Intelligence Magazine, 2010, 5(4): 13–18. [doi: 10.1109/MCI.2010.938364]

6 周飞燕, 金林鹏, 董军. 卷积神经网络研究综述. 计算机学报, 2017, 40(6): 1229–1251. [doi: 10.11897/SP.J.1016.2017.01229]

7 Alaskar H. Deep learning-based model architecture for time-frequency images analysis. International Journal of Advanced Computer Science and Applications, 2018, 9(12). [doi: 10.14569/IJACSA.2018.091268]

8 Krizhevsky A, Sutskever I, Hinton GE. ImageNet classification with deep convolutional neural networks. Communications of the ACM, 2017, 60(6): 84–90. [doi: 10.1145/3065386]

9 Proposed VESA and Industry Standards and Guidelines for Computer Display Monitor Timing (DMT). Video Electronics Standards Association, 2008.

10 Daldal N, Cömert Z, Polat K. Automatic determination of digital modulation types with different noises using Convolutional Neural Network based on time –frequency information. Applied Soft Computing, 2020, 86: 105834. [doi: 10.1016/j.asoc.2019.105834]

11 邹红星, 周小波, 李衍达. 时频分析: 回溯与前瞻. 电子学报, 2000, 28(9): 78–84, 4. [doi: 10.3321/j.issn:0372-2112.2000.09.022]

12 Bashar A. Survey on evolving deep learning neural network architectures. Journal of Artificial Intelligence and Capsule Networks, 2019, 1(2): 73–82. [doi: 10.36548/jaicn.2019.2.003]

13 Al-Saffar AAM, Tao H, Talab MA. Review of deep convolution neural network in image classification. Proceedings of 2017 International Conference on Radar, Antenna, Microwave, Electronics, and Telecommunications. Jakarta, Indonesia. 2017. 26–31.

14 张顺, 龚怡宏, 王进军. 深度卷积神经网络的发展及其在计算机视觉领域的应用. 计算机学报, 2019, 42(3): 453–482. [doi: 10.11897/SP.J.1016.2019.00453]

15 王功鹏, 段萌, 牛常勇. 基于卷积神经网络的随机梯度下降算法. 计算机工程与设计, 2018, 39(2): 441–445, 462. [doi: 10.16208/j.issn1000-7024.2018.02.026]

16 孔维宇. 基于时频图像的雷达信号调制识别技术研究 [硕士学位论文]. 哈尔滨: 哈尔滨工程大学, 2018.

17 蒋昂波, 王维维. ReLU 激活函数优化研究. 传感器与微系统, 2018, 37(2): 50–52.

18 Xin MY, Wang Y. Research on image classification model based on deep convolution neural network. EURASIP Journal on Image and Video Processing, 2019, 2019(1): 40. [doi: 10.1186/s13640-019-0417-8]

19 Deng XY, Liu Q, Deng Y, *et al*. An improved method to construct basic probability assignment based on the confusion matrix for classification problem. Information Sciences, 2016, 340-341: 250–261. [doi: 10.1016/j.ins.2016.01.033]