显示器电磁信息泄漏的机器学习检测方法研究

关天敏[1,4], 韩振中[2], 茅 剑[3,4*]

[1]集美大学信息工程学院 厦门 中国 361021
[2]国防科技大学电子对抗学院 合肥 中国 230000
[3]集美大学计算机工程学院 厦门 中国 361021
[4]厦门市涉密信息技术重点实验室 厦门 中国 361021

摘要 根据电磁学原理, 在操作电子信息设备的过程中会产生无意的电磁辐射。电磁辐射会引发信息泄漏, 给信息安全造成严重威胁。面向计算机显示器的电磁信息安全问题, 提出基于机器学习的电磁信息泄漏检测方法。针对电磁泄漏信号的特点, 设计了 MGCNN 卷积神经网络。利用其独特的卷积和池化处理能力, 提取显示器电磁频谱信号中图像信息的多层次特征, 克服了传统检测方法需要事前明确电磁信息特征和缺乏自适应能力的缺陷, 从而有效地解决电磁信号中的信息泄漏检测问题。通过实测对比, 证明了 MGCNN 对于显示器的电磁信息泄漏检测的有效性。

关键词 电磁信息泄漏; 电磁辐射; 信息安全; 机器学习; 卷积神经网络; 计算机显示器; TEMPEST
中图法分类号 TP 319 **DOI 号** 10.19363/J.cnki.cn10-1380/tn.2021.03.07

Research on the detection method of electromagnetic information leakage from display by machine learning

GUAN Tianmin[1,4], HAN Zhenzhong[2], MAO Jian[3,4*]

[1] School of Information Engineering, Jimei University, Xiamen 361021, China
[2] College of Electronic Engineering, National University of Defense Technology, Hefei 230000, China
[3] Computer Engineering College, Jimei University, Xiamen 361021, China
[4] Xiamen Key Laboratory of secret information technology, Xiamen 361021, China

Abstract According to the principles of electromagnetics, unintentional electromagnetic radiation is generated during the operation of electronic information equipment. Electromagnetic radiation can cause information leakage and pose a serious threat to information security. Faced with the problem of electromagnetic information security of computer monitors, a method of electromagnetic information leakage detection based on machine learning is proposed. According to the characteristics of electromagnetic leakage signal, MGCNN convolutional neural network is designed. Using its unique convolution and pooling processing capabilities, MGCNN extracts multi-level features of image information in the electromagnetic spectrum signal of the display. It overcomes the defects of traditional detection methods that need to make clear the characteristics of electromagnetic information in advance and lack of adaptive ability, so as to effectively solve the problem of information leakage detection in electromagnetic signals. The effectiveness of MGCNN in detecting the electromagnetic information leakage of the display is proved through the actual measurement and comparison.

Key words electromagnetic information leakage; electromagnetic radiation; Machine learning; Convolutional Neural Network; information safety; computer display; TEMPEST

1 引言

电子信息设备在工作过程中, 会产生无意的、非主观通信的电磁辐射。研究表明[1], 无意辐射泄漏的电磁信号可能包含设备相关的有用信息, 如果对泄漏信号进行截获分析, 将导致电子信息设备的信息泄漏, 从而对电磁信息安全构成严重威胁。关于电磁信息泄漏研究称为 TEMPEST, 美国是 TEMPEST 研究发展最早的国家之一, 已有几十年的技术发展史, 制定了从技术到管理的一系列标准。随后欧洲和日

通讯作者: 茅剑, 博士研究生, 副教授, maojian@jmu.edu.cn:。
本课题得到福建省自然科学基金资助项目(No. 2017J01762); 福建省科技厅重点项目(No. 2018H0025); 厦门市科技局资助项目(No. 3502Z20183037)资助。
收稿日期: 2020-03-24; 修改日期: 2020-07-08; 定稿日期: 2020-12-21

本也相继开展了 TEMPEST 研究。1985 年, Van Eck [2] 实现了低成本的攻击实验, 他用价值仅几百美元的器件对普通电视机进行改造, 然后将其安装在汽车里, 在街道上接收到了放置在八层楼上的计算机电磁辐射的信息, 并显示出计算机屏幕上显示的图像。这被认为是民用 TEMPEST 研究的里程碑事件。1998 年起, 英国剑桥大学的 Markus G. Kuhn, 针对计算机的 CRT[3-4]、LCD[5-7]显示器开展了电磁信息泄漏截获复现实验, 取得了一系列成果; 并且基于显示器的电磁信息泄漏原理提出了一种信息隐藏传输方法(Soft TEMPEST)[8]。2010 年, Hidenori Sekiguchi[9-10] 研究了触摸屏的电磁信息泄漏问题, 从截获重建后的显示图像中识别出触摸屏的按键操作图像。2011 年, Taishi Ikematsu 等[11]从定量的角度讨论了电磁场噪声抑制技术与信息泄漏抑制技术的区别, 在定量评价信号和噪声分量的基础上, 研究了信息泄漏及其有效对策。2013 年, Yuichi Hayashi 等[12]提出了一种基于电磁干扰理论的分析密码体制中电磁信息泄漏的方法, 能根据板尺寸、电源线长度等物理参数获取电磁辐射的频率特性。2016 年起, 徐艳云等研究了信息设备电磁信息泄漏的还原图像文本识别和检测距离估计方法[13-14]。

现有的研究主要集中在明确的环境条件下, 依据已知的电磁信息特征检测电磁信息泄漏, 而对未知的变化的环境条件下, 无法自适应地检测。传统的电磁图像检测方法主要基于图像重建后的人为识别, 存在局限性。检测设备必须具有足够的采样精度, 以保证能够捕获足够的像素信息。即使获得了足够的图像像素数据, 没有精确同步信号的指导, 图像也无法重建。此外, 识别结果容易受到操作人员经验的影响。因此, 本文探索了一种新的识别方法, 以减少人为干预对识别的影响, 并使识别过程尽量摆脱对先验知识的依赖。

卷积神经网络(Convolutional Neural Network, CNN)是深度学习的重要算法, 目前在图像识别[15-16], 降噪[17-18], 目标检测[19-21]和信号检测[22-25]等领域广泛应用并表现良好。2017年, Chen Sisi等[22]尝试使用卷积神经网络对太阳射电频谱进行分类。2018年, Pan Jun等[23]提出了一种深度学习网络, 可以在没有先验知识的情况下从原始机械振动信号中自适应地学习特征, 用于机械故障诊断。2019年, Jagiasi R. 等[25]利用密集卷积神经网络实现了一个不依赖文本、不依赖语言的语音信号识别系统。基于CNN在上述领域中的优异表现, 经过探索研究, 本文将CNN引入电磁信息泄漏检测, 并针对计算机显示器无意辐射的电磁信号特点, 设计基于卷积神经网络的电磁信息泄漏检测方法。实验证明该检测方法不仅克服传统方法无法自适应的缺陷, 而且在电磁信息泄漏检测领域具有良好性能。

2 计算机显示器的电磁信息泄漏原理

计算机显示器工作原理是通过逐行扫描, 以固定的时间间隔逐个刷新屏幕上的每个像素点, 以此显示数字图像。这个过程可视为将二维的图像矩阵展开成一维的像素时间序列。每个像素点刷新时的电流变化都会产生无意的电磁辐射, 辐射的电磁信号会反映图像中像素的变化情况, 如图 1 所示。因此计算机显示器在显示图像的过程中, 伴随着与图像信息有关的无意电磁辐射, 从而导致了电磁信息泄漏。

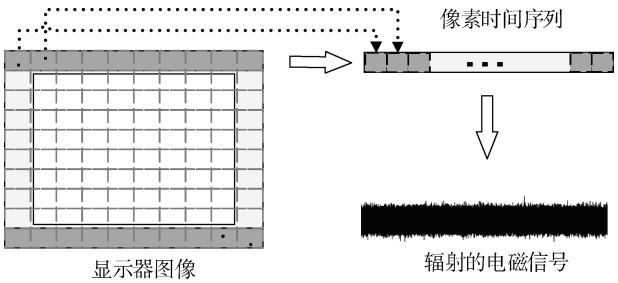


图 1 显示图像过程中的电磁辐射

Figure 1 Electromagnetic radiation during image display

通过上述分析, 可知计算机显示器泄漏的电磁信息为图像信息, 二维的图像信息被碎片化在一维的泄漏电磁信号中。因此对显示器电磁信息泄漏的检测本质是从泄漏的电磁信号中找出图像信息特征。传统的电磁图像检测方法的第一步所截获的电磁泄漏信号, 是在时域内采集的信号序列, 对应的是一维像素时间序列, 如图 1 所示。根据之前的分析, 一维时域信号中隐藏着二维图像信息。如果按照传统的方法, 需要同步信号的指导, 才能提取复现二维图像。本文提出的一种基于卷积神经网络的电磁图像检测方法, 在没有同步信号的先验知识指导, 完全依靠神经网络提取信号中的图像特征。

3 面向电磁信息泄漏的 CNN 算法设计

CNN 由于其特有的卷积运算, 对检测目标具有局部特征感知能力。经过探索研究, 面向计算机显示器的图像信息泄漏, 针对性地设计 CNN, 通过机器学习, 提取泄漏电磁信号中隐藏的图像信息特征。

3.1 显示器电磁信息泄漏特征提取

目前经典的CNN结构大多应用于图像处理领域, 还未见有针对电磁信息泄漏检测或识别所设计的CNN 架构。由于图像是以二维形式表示的, 基于图像识别的CNN都采用了二维卷积核进行特性提取。然而, 在电磁信息泄漏检测中, 数字化信号采集设备接收的电磁信号是一维形式的数字序。显然, 借助传统图像领域中的二维CNN来识别一维电磁泄漏信号是不合适的。因此, 本文提出一个适用于电磁图像信息识别的 CNN 结构, 命名为 MGCNN, 该结构特别地采用一维卷积核。利用 MGCNN 提取电磁信息泄漏特征的过程示意如图 2 所示。

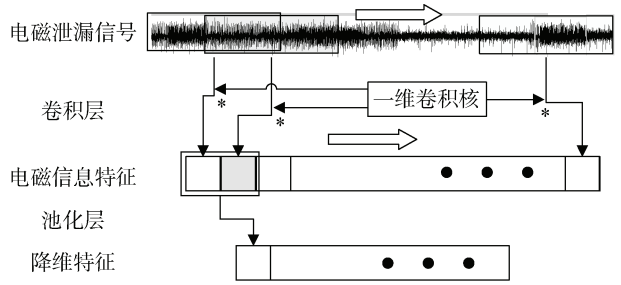


图 2 MGCNN 提取电磁信息泄漏特征示意图

Figure 2 Schematic diagram of electromagnetic information leakage feature extracted by MGCNN

卷积和池化是CNN方法的核心。在电磁信息泄漏检测过程中, 检测仪器接收到的电磁信号数值化后的形式为一维序列。为了直接从电磁信号序列中提取特征信息, MGCNN 的卷积层滑动一维卷积核, 使其与对应信号序列片段进行卷积运算, 从而提取显示器图像信息的局部特征, 并将其组合成特征向量。池化层通过降维操作进一步压缩特征向量。

3.2 MGCNN

本小节详细介绍本文提出的 MGCNN 结构。经过电磁信息泄漏检测实践, 针对电磁信号特点设计的 MGCNN 由两个卷积层、两个池化层和一个全连接层组成, 如图 3 所示。

MGCNN 每一层的网络结构参数如表 1 所示。网络的输入为预处理之后的一维信号, 长度为 8192。经过逐层的计算和特征提取之后, 到达全连接层之前的输出为 16 个通道的特征向量, 每个特征向量长度为 256。

以下介绍 MGCNN 中各层的计算过程和作用。

3.2.1 卷积层

卷积层的作用是提取一维电磁信号中泄漏的信息特征。

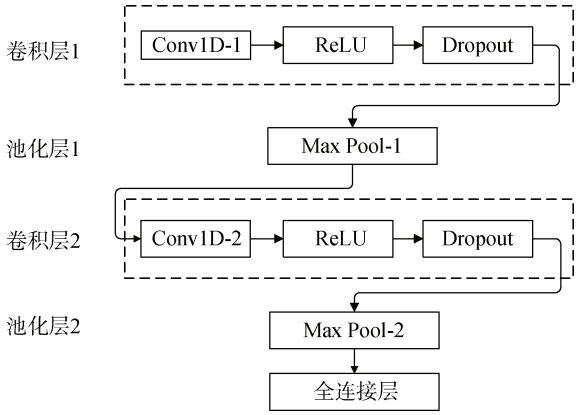


图 3 MGCNN 结构

Figure 3 Structure of MGCNN

表 1 MGCNN 结构参数

Table 1 MGCNN Structure parameter

神经网络层次	输入长度	输入通道	卷积核/滤波器	计算步长	输出通道	输出长度
Conv1D-1	8192	1	160	4	16	2048
Max pooling-1	2048	16	2	2	16	1024
Conv1D-2	1024	16	12	2	16	512
Max pooling-2	512	16	2	2	16	256
Fully Connected	256	16	-	-	-	2

(1) 一维卷积(Conv1D)

本文特别设计一维卷积核来提取电磁信号中的信息特性。一维卷积计算过程是以特定的步长, 滑动卷积滤波器的窗口, 有序地提取输入信号的局部特征。两个卷积层分别设置了相应的尺寸, 如表 1 所示, 逐层抽取并压缩电磁泄漏信息特征。

卷积计算的公式如下所示:

$$X^{(L+1)} = X^{(L)} \otimes W^{(L)} + B^{(L)} \tag{1}$$

其中 L 是神经网络中各层的索引号, $X^{(L)}$和$X^{(L+1)}$分别为计算过程中第 L 层的输入和输出特征向量, $W^{(L)}$是第 L 层神经网络的权值向量, $B^{(L)}$是第 L 层的偏置向量。

(2) ReLU

MGCNN 选择 ReLU 作为激活函数。与以往的Sigmoid和Tanh函数相比, ReLU激活函数可以缓解梯度消失问题, 有助于抑制深度学习的过拟合问题, 提高神经网络的学习速度。ReLU 的计算公式如下所示:

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

将 Conv1D 和 ReLU 的合并计算, 计算过程可以表示为下式:

$$X^{(L+1)} = \max(0, X^{(L)} \otimes W^{(L)} + B^{(L)}) \tag{3}$$

(3) Dropout

在 ReLU 函数之后, 网络中还加上了 Dropout 函

数, 其作用是缓解网络的过拟合。其原理是以一定概率减少网络中传递的特征数量, 使部分参数不更新。Dropout 函数的计算如下所示:

$$r_{i,j}^{(L)} \sim Bernoulli(p) \tag{4}$$

$r_{i,j}^{(L)}$是一个独立的伯努利随机变量, 它以 p 的概率取值为 1, 以 1-p 的概率取值为 0。神经网络中的数据传输受到 Dropout 函数影响之后, 如下式:

$$x*_{i,j}^{(L)} = x_{i,j}^{(L)} \times r_{i,j}^{(L)} / p \tag{5}$$

其中 $x_{i,j}^{(L)}$是第 L 层的特征值 $X^{(L)}$中的第 i 个通道的序列中第 j 个单元的数值; $x*_{i,j}^{(L)}$是 Dropout 之后的单元值。在本文的实验中, p 设为 0.5。

3.2.2 池化层

池化层, 即下采样层, 通过特征压缩, 减少神经网络中的数据和参数的数量, 从而抑制网络的过拟合, 简化计算复杂度。本文采用 Max pooling 的池化方法, 以固定的步长, 在特征序列上滑动取样窗口, 将窗口内所有单元的最大值保留至下一层。本文中的池化层步长和窗口均取值为 2, 经过池化层处理后, 特征向量的长度压缩为原先的一半。

3.2.3 全连接层

全连接层将前一层输出的特征向量以完全连接的方式进行加权计算后, 输出分类预测结果。在本文中, 全连接层之后紧接着采用 Softmax 函数获取同分布最高概率输出。Softmax 函数可以将全连接层之后的特征向量, 映射成同尺寸的向量, 使得向量中每一个元素的数值规范在 0~1 之间, 并且这些元素的和为 1。全连接加上 Softmax 的作用是将神经网络中各层计算提取的电磁信息特征映射成最终的分类识别得分, 最终根据得分值大小判断当前电磁信号中隐藏的信息。

在电磁信息泄漏检测工作中, 利用实测电磁泄漏信号, 对 MGCNN 网络进行基于反向传播机制的训练, 即深度学习过程, 可以得到具有电磁信息泄漏特征提取能力的 MGCNN 模型。MGCNN 模型中由卷积和池化构成的多层结构, 可以逐层提取电磁辐射信号中隐藏的信息泄漏特征向量; 多个卷积核的分别运算形成的多个特征通道, 可以同时从不同角度提取电磁信号中的信息泄漏特征分量, 解决电磁信号中的多元信息检测问题。

4 显示器电磁信息泄漏检测实验设计

基于 MGCNN 的显示器电磁信息泄漏检测方法, 包括电磁信号样本采集、数据预处理、生成训练数据、机器学习模型训练与获取。实验流程如图 4 所示。

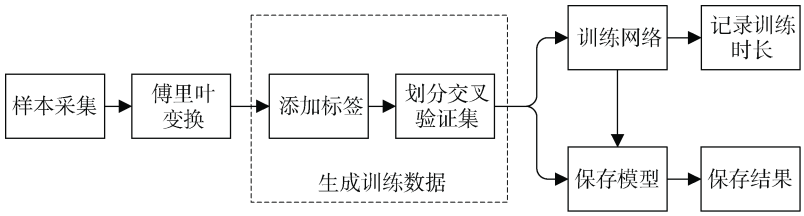


图 4 实验流程图

Figure 4 Flow diagram of experiment

4.1 样本采集

本文中的实验环境为正常的室内环境。不同于常见电磁检测所需的电磁屏蔽暗室, 实验未采取任何屏蔽措施, 以验证本文提出的方法在较复杂电磁环境下的有效性。

采集显示器的电磁辐射的装置如图 5 所示。检测对象是型号为 PHILIPS HWE9220F 的计算机显示器, 该显示器通过 VGA 视频线缆连接在台式计算机上。信号采集设备包括一个卡钳式电磁信号探头和一台信号接收机, 电磁信号探头的型号为 A.H.Systems BCP-620, 信号接收机的型号为 NI PXIe-5162。

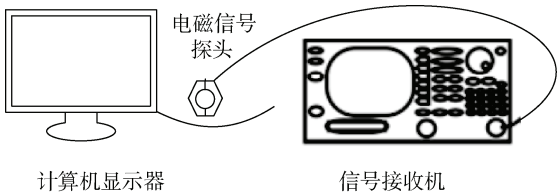
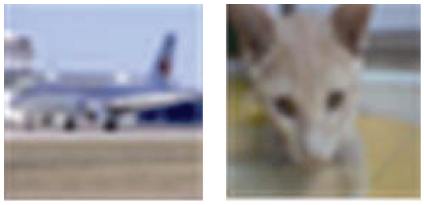


图 5 实验装置

Figure 5 Experimental device

电磁信号探头从连接工作显示器的 VGA 线缆上截获电磁辐射信号, 连接探头的信号接收机对电磁信号进行采样和存储。采集的信号样本为记录显示器线缆上电磁辐射幅值变化情况的时域序列。

本次实验选取了图像识别的公开数据集 CIFAR-10 中的 20 幅图像作为实验图像。这 20 幅图像均为实物照片, 分为飞机和猫共两类, 每类图像各 10 张。图像的内容示例如图 5 所示。飞机图像作为第一类; 猫图像作为第二类。



第一类 第二类

图 6 飞机和猫图像示例

Figure 6 Examples of airplane and cat images

实验中, 显示器的工作分辨率设为 640×480@60Hz, 将 20 幅图像分别显示在计算机显示器上。然后以 1MS/s 的采样率对每幅图像产生的电磁辐射进行信号采集, 每幅图像分别采集了 1220 个信号样本, 如表 2 所示。

表 2 采集内容

Table 2 Collection Content

图像类别	图像数量	信号采样率	电磁信号样本数量
第一类	10	1MS/s	1220×10
第二类	10	1MS/s	1220×10
合计	20		24400

4.2 样本预处理

图像信息识别流程的第一步所截获的电磁泄漏信号, 是在时域内采集的信号序列, 对应的是一维像素时间序列。根据之前的分析, 一维时域信号中隐藏着二维图像信息。如果按照传统的方法, 需要同步信号的指导, 才能提取复现二维图像。本文提出的新方法没有同步信号的先验知识指导, 完全依靠神经网络提取信号中的图像特征。而原始的二维图像特征分散到一维序列中之后, 难以提取出二维图像的特征。

因此, 预处理过程将采集到的时域信号转换为频谱信号。这是因为频谱可以增强信号的周期和频率特性。图像的电磁辐射信号含有丰富的周期和频率特征: 同步信号是明显的周期信号, 图像的空间特征也可以映射到频域。这些特征以及其他未知的电磁信息特征被 CNN 提取和学习, 成为识别图像内容的基础。

采集原始数据之后, 要对这些原始数据进行处理。原始数据内包括很多参数描述, 需要将其处理成标准的数组格式。处理后的样本由 24400 个长度为 16384 的时域信号。图 7 是第一类和第二类图像的电磁信号时域图示例。

在时域处理的基础上, 对其进行傅里叶变换, 会将原本的长度为 16384 的样本转换成长度为 8192 的样本。图 8 是第一类和第二类图像的电磁信号频域图示例。

4.3 训练数据生成

本实验为针对电磁泄漏信号中图像信息的二分类实验。实验采用五折交叉验证, 将数据集中来自 20 幅图像的 24400 个电磁信号样本平均分为五份, 每份中包含 4 幅图像的样本共 4880 个。每一次交叉验证, 选取五份样本其中的一份作为测试样本, 其余的四份样本作为训练样本, 即每次使用 16 幅已知图像的电磁泄漏信号数据执行 MGCNN 模型训练, 然后利用训练好的模型对剩余 4 幅未知图像的电磁泄漏信号进行识别, 以检测电磁信号中隐藏的图像信息泄漏。

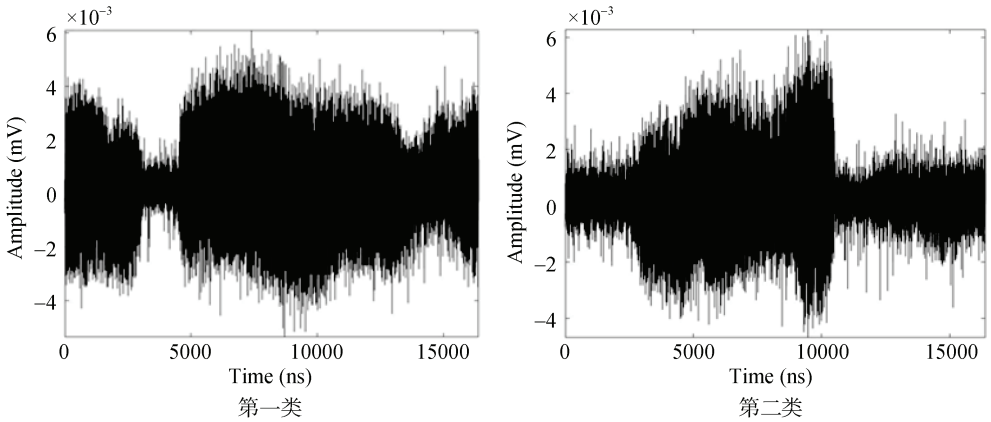


图 7 电磁信号时域图

Figure 7 Time domain diagram of electromagnetic signals

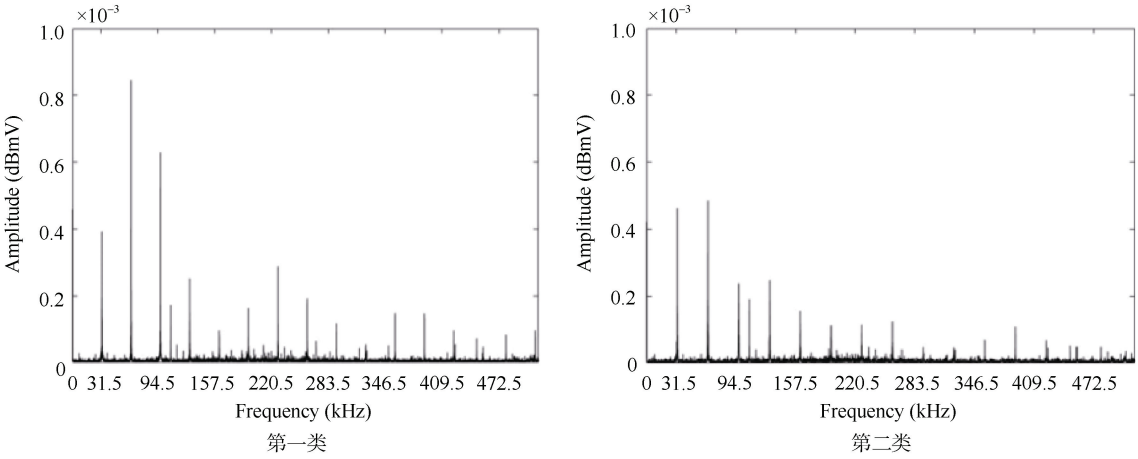


图 8　电磁信号频域图

Figure 8　Frequency domain diagram of electromagnetic signal

4.4　MGCNN 模型训练与获取

实验使用 TensorFlow 框架实现本文设计的 MGCNN 模型, 利用梯度下法训练模型, 并获得分类检测模型, 实现电磁泄漏信息样本分类检测。在算法的训练过程中, 优化器为自适应矩估计(Adaptive moment estimation, Adam), 批处理大小设置为 100, 学习率为 0.001, 数据一共训练 50 轮。通过五折交叉验证进行实验, 取 5 次测试的平均值作为实验的结果。

5　实验结果与分析

为了比较传统的电磁图像检测方法, 设计了传统检测方法流程: 检测仪器采集电磁辐射信号, 根据采样率、分辨率和刷新率, 对一维电磁信号进行二维重排, 形成可视化图像, 然后通过肉眼识别检测。为了实现检测性能的量化对比, 在对比实验中, 改造了传统检测方法, 即在传统图像重建基础上, 把肉眼识别检测改成利用机器学习方法进行识别检测, 如图 9 所示。其中机器学习分类算法选取 AlexNet、GoogleNet 和 VGGNET 三个经典的图像分类算法: 分别标记为 AlexNet_Tra、GoogleNet_Tra 和 VGGNet_Tra。

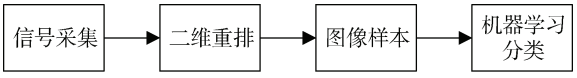


图 9　传统检测方法流程

Figure 9　Traditional detection method flow

此外, 为了比较本文提出的 MGCNN 算法的性能, 在缺乏电磁图像信息识别的同类一维卷积算法的情况下, 本文设计了面向时频信号的二维 CNN 检测方法, 选取了三个经典的图像识别 CNN 结构进行对比实验: AlexNet、GoogLeNet 和 VGGNet。它们都是在图像识别大赛中获得优胜的经典算法。由于上述三个算法均是采用二维卷积运算, 在使用它们进行对比实验时, 将电磁信号样本进行短时傅里叶变换转换成二维的时频信号图, 输入样本尺寸为 227×227。对于 MGCNN, 本实验还特别增加了时域信号的对比实验, 即对采集到的时域信号不做傅里叶变换处理, 直接输入 MGCNN。在本实验中, 为了以示区分, 基于时域信号的 MGCNN 被标记为 MGCNN_T, 基于频域信号的 MGCNN 被标记为 MGCNN_F。

本实验中, 算法性能的评价选取了准确率、精确率、召回率和 F1 四项指标。上述算法经过五折交叉验证后, 将五次实验的平均值记录在表 3 中。为了直观对比, 又将实验结果可视化为图 10。

对比实验结果可以看出, 传统检测方法是在二维时域信号上进行分类识别, 其性能低于面向时频信号的二维 CNN 检测方法的识别性能。同时, 一维频域信号的 MGCNN_F 检测方法明显优于一维时域信号的 MGCNN_T 检测方法, 也优于传统检测方法和面向时频信号的二维 CNN 检测方法。这证明了 MGCNN 相比与传检测方法和面向时频信号的二维 CNN 检测方法, 更能适应电磁图像信息识别。其原因在于, 本文以显示器上二维图像的无意辐射产生的一维电磁信号作为检测对象, 目的是从一维电磁信号中检测识别出图像信息。然而, 传统检测方法和面向时频信号的二维检测方法都是对二维数据进行检测, 在检测之前分别对一维时域和一维频域样本进行了升维处理, 然后使用二维 CNN 进行检测。由于升维处理过程缺乏有效图像信息的指导, 在不同程度上破坏了一维电磁信号中隐藏的图像特征, 从而导致图像检测质量的下降。

表 3 1MS/s 采样率下各算法性能对比

Table 3 Comparison of performance of each algorithm at 1MS/s sampling rate

比较算法	准确率(%)	精确率(%)	召回率(%)	F1(%)
MGCNN_F	87.21	98.63	74.74	83.67
MGCNN_T	64.95	76.60	60.00	64.64
AlexNet	79.32	84.24	65.01	69.16
GoogleNet	75.99	78.95	76.38	70.43
VGGNet	50.00	40.00	80.00	53.33
AlexNet_Tra	50.95	32.05	39.16	32.70
GoogleNet_Tra	72.93	73.42	80.90	72.91
VGGNet_Tra	61.00	63.53	66.38	59.70

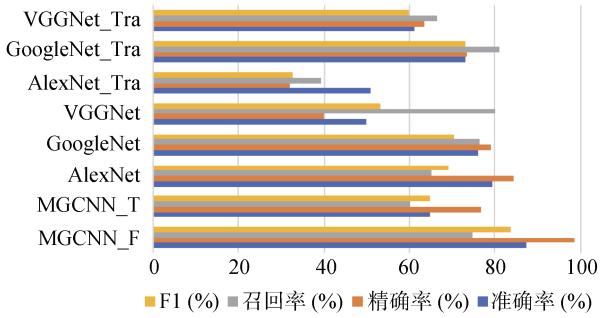


图 10 各算法的性能对比

Figure 10 Performance comparison of each algorithm

MGCNN 不仅识别性能更好，算法的执行效率也大大优于其他结构。由于 MGCNN 采用了一维卷积，网络层次结构也较为简单，在相同样本量的训练时长上，MGCNN 仅为 AlexNet 的 1/3、GoogLeNet 的 1/5、VGGNet 的 1/15。因此，MGCNN 在算法的性能和效率两方面均占优。

此外，同为MGCNN结构，对于频域信号的分类识别性能也优于时域信号，这是因为频谱可以增强信号的周期和频率特性。图像的电磁辐射信号含有丰富的周期和频率特征：同步信号是明显的周期信号，图像的空间特征也存在周期特性，可以映射到频域。这些特征以及其它未知特征被 MGCNN 提取和学习，成为识别图像内容的基础。需要说明的是，预处理的过程并没有定义和提取信号特征。预处理只是将信号转换到不同的分析域，便于后续的识别计算。有别于传统方法，基于 MGCNN 算法的检测方法不需事先明确待测信息的特征。这说明频域信号能够更好地表示电磁信号中的图像信息，证明了本文识别方法中信号预处理能够提升识别性能。

传统检测方法必须要已知图像信息特征，如显示器图像的分辨率和刷新率。本实验在未知图像信息特征情况下，通过神经网络的学习，自适应地提取图像信息特征，从而实现显示器电磁信息泄漏检测。因此相对于传统检测方法，基于 MGCNN 的机器学习检测方法，对于未知特征的电磁信息泄漏检测具有更好的适应性。

6 结论

本文针对计算机显示器的无意电磁信息泄漏问题，分析显示器的电磁信息泄漏机理，结合卷积神经网络的特点，阐释卷积神经网络模型提取电磁泄漏信息特征的原理，提出了一个基于 MGCNN 的电磁图像信息自适应的识别方法。通过大量采集显示器无意发射的电磁信号，建立了电磁图像信息泄漏样本数据集。在建立数据集的基础上，经过对比实验证明，提出的方法在识别性能和算法效率上优于传统检测方法和经典的 CNN 方法，同时克服了传统电磁图像检测方法需要预先明确电磁信息特征的缺陷。基于 MGCNN 的检测方法在电磁图像信息识别上得到了验证，但并不意味着该方法只能局限于检测显示器的电磁图像信息泄漏。在电磁信息安全的应用领域中，其最终目的是为目前以计算机为代表的电子信息设备及其部件的电磁信息泄漏问题提供智能化的检测新手段。

参考文献

[1] Liu T K, Li Y M, Liu J M, et al. Electromagnetic information leakage and protection technology[M]. National Defense Industry Press, 2015.
(刘泰康，李咏梅，刘晋明，等. 电磁信息泄漏及防护技术[M]. 国防工业出版社, 2015.)

[2] van Eck W. Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk[J]. *Computers & Security*, 1985, 4(4): 269-286.

[3] M. G. Kuhn. Eavesdropping attacks on computer displays[C]. *Information Security Summit*, 2006: 1-10.

[4] M. G. Kuhn. Optical time-domain eavesdropping risks of CRT displays[C]. *IEEE Symposium on Security & Privacy*, 2002: 3-18.

[5] Kuhn M G. Electromagnetic Eavesdropping Risks of Flat-Panel Displays[M]. Privacy Enhancing Technologies. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005: 88-107.

[6] Kuhn M G. Security Limits for Compromising Emanations[M]. Cryptographic Hardware and Embedded Systems – CHES 2005. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005: 265-279.

[7] Kuhn M G. Compromising Emanations of LCD TV Sets[J]. *IEEE Transactions on Electromagnetic Compatibility*, 2013, 55(3):

564-570.

[8] Kuhn M G, Anderson R J. Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations[M]. Information Hiding. Berlin, Heidelberg: Springer Berlin Heidelberg, 1998: 124-142.

[9] H. Sekiguchi. Information leakage of input operation on touch screen monitors caused by electromagnetic noise[C]. *IEEE International Symposium on Electromagnetic Compatibility*, 2010: 127-131.

[10] Sekiguchi H, Seto S. Measurement System of Information Signal in Display Image Leaking from Conducted Emission on Power Leads of a Personal Computer[J]. *Information Security*, 2009: 5-8.

[11] T. Ikematsu, Y. Hayashi, T. Mizuki, et al. Suppression of information leakage from electronic devices based on SNR[C]. *IEEE International Symposium on Electromagnetic Compatibility*, 2011: 920-924.

[12] Hayashi Y I, Homma N, Mizuki T, et al. Analysis of Electromagnetic Information Leakage from Cryptographic Devices with Different Physical Structures[J]. *IEEE Transactions on Electromagnetic Compatibility*, 2013, 55(3): 571-580.

[13] Xu Y Y, Guo J, Li Y W, et al. Research on Character Recognition of Reconstructed Image from Electromagnetic Emanation of Information Equipment[J]. *Journal of Information Security Research*, 2016, 2(2): 137-142.
(徐艳云, 郭佳, 李怡伟, 等. 信息设备电磁泄漏还原图像的文本识别研究[J]. 信息安全研究, 2016, 2(2): 137-142.)

[14] Xu Y Y, Zhang M, Huang W Q. Study on Detectable Distance for Electromagnetic Information Leakage of Information Equipment[J]. *Journal of Cyber Security*, 2020, 5(1): 44-56.
(徐艳云, 张萌, 黄伟庆. 信息设备电磁辐射信息泄漏的可检测距离估计方法研究[J]. *信息安全学报*, 2020, 5(1): 44-56.)

[15] Shu G S, Liu W Q, Zheng X J, et al. IF-CNN: Image-Aware Inference Framework for CNN with the Collaboration of Mobile Devices and Cloud[J]. *IEEE Access*, 2018, 6: 68621-68633.

[16] A. Krizhevsky, I. Sutskever and G. Hinton. ImageNet Classification with Deep Convolutional Neural Networks[C]. *Advances in neural information processing systems*, 2012: 1097-1105.

[17] Isogawa K, Ida T, Shiodera T, et al. Deep Shrinkage Convolutional Neural Network for Adaptive Noise Reduction[J]. *IEEE Signal Processing Letters*, 2018, 25(2): 224-228.

[18] Cho S I, Kang S J. Gradient Prior-Aided CNN Denoiser with Separable Convolution-Based Optimization of Feature Dimension[J]. *IEEE Transactions on Multimedia*, 2019, 21(2): 484-493.

[19] Deng Z P, Sun H, Zhou S L, et al. Multi-scale Object Detection in Remote Sensing Imagery with Convolutional Neural Networks[J]. *ISPRS Journal of Photogrammetry and Remote Sensing*, 2018, 145: 3-22.

[20] Ren Y, Zhu C R, Xiao S P. Object Detection Based on Fast/Faster RCNN Employing Fully Convolutional Architectures[J]. *Mathematical Problems in Engineering*, 2018, 2018: 1-7.

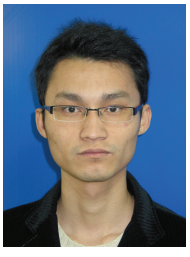
[21] Soon F C, Khaw H Y, Chuah J H, et al. PCANet-Based Convolutional Neural Network Architecture for a Vehicle Model Recognition System[J]. *IEEE Transactions on Intelligent Transportation Systems*, 2019, 20(2): 749-759.

[22] S. Chen, L. Xu, L. Ma, et al. Convolutional neural network for classification of solar radio spectrum[C] *2017 IEEE International Conference on Multimedia and Expo Workshops*, 2017: 198-201.

[23] Pan J, Zi Y Y, Chen J L, et al. LiftingNet: A Novel Deep Learning Network with Layerwise Feature Learning from Noisy Mechanical Data for Fault Classification[J]. *IEEE Transactions on Industrial Electronics*, 2018, 65(6): 4973-4982.

[24] X. Zhang, T. Lin, J. Xu, et al. DeepSpectra: An end-to-end deep learning approach for quantitative spectral analysis[J]. *Analytica Chimica Acta*, 2019, 1058: 48-57.

[25] R. Jagiasi, S. Ghosalkar, P. Kulal, et al. CNN based speaker recognition in language and text-independent small scale system[C]. *The 3rd International Conference on I-SMAC IoT in Social, Mobile, Analytics and Cloud, I-SMAC,* 2019: 176-179.



关天敏 于 2004 年在广东海洋大学计算机科学与技术专业获得学士学位。现任集美大学信息化中心实验师。研究领域为信息安全和人工智能。研究兴趣包括: 电磁信息安全。Email: gtm@jmu.edu.cn

韩振中 于 2015 年在北京交通大学电路与系统专业获得博士学位。现任国防科技大学电子可抗学院讲师。研究领域为信号处理、雷达信号处理。研究兴趣包括: 图像处理、电磁信息泄漏检测。Email: taylor_han87@163.com

茅剑 2019 年于国防科技大学电子科学学院博士毕业。现任集美大学计算机工程学院副教授。研究领域为信息安全和人工智能。研究兴趣包括: 电磁信息安全。
Email: maojian@jmu.edu.cn