文章编号：2095-4980(2023)09-1144-06

Jetson Nano神经网络物理电磁泄漏安全研究

吴晨曦，张洪欣，崔晓彤

(北京邮电大学 电子工程学院，北京 100876)

摘　要：如果采用旁路攻击方法对神经网络结构、框架进行攻击，恢复出结构、权重等信息，会产生敏感信息的泄漏，因此，需要警惕神经网络计算设备在旁路攻击领域产生敏感信息泄露的潜在风险。本文基于Jetson Nano平台，针对神经网络及神经网络框架推理时产生的旁路电磁泄漏信号进行采集，设计了基于深度学习方法的旁路攻击算法，对旁路进行分析研究，并对两个维度的安全进行评估。研究表明，良好的网络转换策略能够提升网络分类识别准确率5%~12%。两种评估任务中，针对同一框架下不同结构的典型神经网络推理时，电磁泄漏的分类准确率达到97.21%；针对不同神经网络框架下同一种网络推理时，电磁泄漏的分类准确率达到100%。说明旁路电磁攻击方法对此类嵌入式图像处理器(GPU)计算平台中的深度学习算法隐私产生了威胁。

关键词：旁路攻击；电磁泄漏；深度学习；一维卷积神经网络；Jetson Nano平台

中图分类号：O441.4　　**文献标志码：**A　　**doi：**10.11805/TKYDA2021211

Research on electromagnetic leakage safety of Jetson Nano neural network

WU Chenxi，ZHANG Hongxin，CUI Xiaotong

(School of Electronic Engineering，Beijing University of Posts and Telecommunications，Beijing 100876，China)

Abstract：If a side-channel attack can attack the structure and framework of the neural network to recover information such as structure and weight, sensitive information leakage will occur. Therefore, it is important to guard the neural network computing devices against disclosure of sensitive information in the field of side-channel attack. Based on the Jetson Nano platform, a method is designed for the side-channel electromagnetic leakage signal acquisition during the inference of the neural network. The side-channel analysis is conducted by using the deep learning method, and two aspects of security are assessed. Research shows that a good network conversion strategy can improve the classification and recognition accuracy of the network by 5%~12%. In the two evaluation tasks, the classification accuracy of electromagnetic leakage is 97.21% for typical neural network inferences with different structures under the same framework; it reaches 100% for the same kind of network reasoning under different frameworks of neural network. It indicates that the side-channel electromagnetic attack method poses a threat to the privacy of deep learning algorithms in such embedded Graphics Processing Unit(GPU) computing platforms.

Keywords：side-channel attack；electromagnetic leakage；deep learning；one-dimensional Convolutional Neural Network；Jetson Nano

针对神经网络结构的旁路攻击，最终目的是破译神经网络的结构、超参数及内部权重。在攻击方法的选择上，Weizhe Hua等使用访问片外内存信息的定时旁路攻击方式[1]，Sanghyun Hong等通过访问CPU缓存信息对神经网络体系结构进行破解[2]。出于安全和隐私方面的考虑，神经网络运行载体的供应商有时并不允许用户访问如内存或缓存结构，此时此类访问内部信息的旁路攻击方式无法生效。文献[3-4]中，研究人员使用基于电磁泄露的旁路攻击方式对神经网络的结构进行非入侵式的恢复攻击，其神经网络运行的载体分别为ARM芯片及现场可

收稿日期：2021-05-21；**修回日期：**2021-08-09

基金项目：国家自然科学基金资助项目(62071057)；中央高校基本科研业务费专项资金资助项目(2019XD17)

*通信作者：张洪欣　email:hongxinzhang@263.net

编程门阵列(Field Programmable Gate Array，FPGA)平台，但基于这两种体系运行的神经网络应用的广泛程度远不如基于GPU结构的神经网络。本文研究了基于GPU结构Jetson Nano设备的典型神经网络电磁泄漏信号分类识别方法，为进一步利用电磁泄漏破译Jetson平台神经网络的超参数及内部权重奠定基础。

本文针对NVIDIA公司推出的Jetson Nano设备，从以下两方面对电磁泄漏安全性进行评估：一，分类识别同一框架TensorRT下7种不同的神经网络的电磁泄漏，评估同一框架下不同结构的典型神经网络对电磁旁路攻击的防御性能；二，分类识别TensorRT、Tensorflow[5]、Pytorch[6]这3种框架下同一种网络ResNet−50[7]的电磁泄漏，评估在不同框架下的典型网络运行时的电磁旁路攻击的防御性能。

1　实验信号采集

Jetson电磁泄漏信号采集平台由示波器、电磁探头、探头夹具、计算机以及Jetson系列设备构成。Jetson设备为运行神经网络算法的载体，是产生电磁泄漏信号的主体，本文采用Jetson Nano开发者套件。电磁探头用于感应电磁泄漏信号，并将感应的电磁信号传输给示波器。探头夹具固定电磁探头，便于采集数据。示波器与电磁探头连接，采集、记录电磁信号并传输给计算机。在采集电磁泄漏信号的过程中，计算机储存示波器信道中采集到的电磁泄漏信号并进行预处理。图1为Jetson电磁泄漏信号采集平台的原理图。

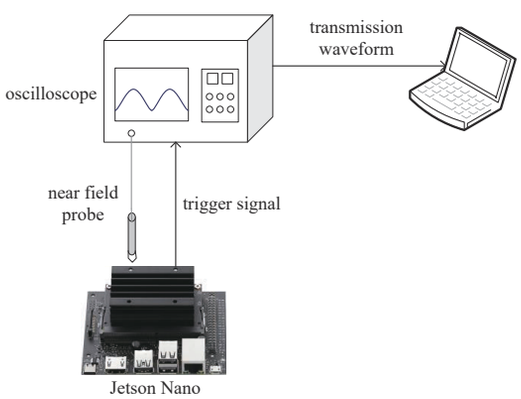

Fig.1 Acquisition platform of Jetson electromagnetic leakage signal
图1　Jetson电磁泄漏信号采集平台原理图

本文针对Jetson Nano设备在运行神经网络算法时所产生的电磁泄漏信号进行信息安全分析。设计中使用的卷积神经网络为图片分类神经网络，其功能是指示输入的图片属于现实世界中的哪一类别。在进行旁路攻击时，Jetson Nano运行神经网络所推理的图片内容对攻击者是完全未知的。为了更加符合真实情况，在图片选择上采用多个图像数据集融合的方式进行模拟。

在数据集选择上，首先使用ImageNet[8]数据集，选择ImageNet子集Tiny−ImageNet中的2 000张图像；然后在图像尺寸较小的CIFAR−10数据集中随机挑选2 000张图片，模拟实际情况下较小尺寸图片经过神经网络时的电磁泄漏；最后在图片检测任务中常用的COCO数据集[9]中挑选2 000张图片，最终获得共含6 000张图片的实验数据集。虽然本实验使用的是图像分类网络，但也能识别出图像检测数据集的图片中占据画面主体的物品类别。注意，图片数据集只用来产生卷积神经网络推理过程的电磁泄漏，与后续的针对电磁泄漏信号的分类实验无关。

任务一：使用7种不同卷积神经网络模型(AlexNet、GoogleNet、Inception−v4、ResNet−18、ResNet−50、ResNet−101、ResNet−152)，在同一框架TensorRT下推理此图片数据集中随机选择的单张图片，并记录下推理时产生的电磁泄漏信号，最终获得电磁泄漏数据集。7类卷积神经网络每种推理时产生700条，共4 900条电磁泄漏信号。

任务二：采用同一个卷积神经网络ResNet−50，在3种不同的深度学习框架(TensorRT、Tensorflow、Pytorch)下推理此图片数据集中随机选择的单张图片，并记录下推理时产生的电磁泄漏信号，最终获得电磁泄漏数据集。3种不同框架每种推理时产生1 400条电磁泄漏信号，共4 200条信号。

任务一与任务二中用于产生电磁泄漏的卷积神经网络模型，均为使用ImageNet数据集训练的高精确度模型。

2　针对神经网络电磁泄漏的卷积神经网络设计

在设计任务一、任务二所使用的深度学习算法时，需将典型的二维卷积神经网络转化为适合于电磁泄漏攻击的一维卷积神经网络。二维卷积神经网络，如图片分类检测网络、语音Mel频谱图分类网络等，已经有非常多的成熟标准网络可以使用，但目前没有任何一个深度网络框架标准供一维神经网络调用。因此，本文借鉴二维神经网络的思路设计一维卷积神经网络。

BN层(批归一化层)、Dropout层、残差结构等超参数和网络的输入没有太大关联，在设计一维卷积网络时不需要专门考虑它们的超参数。但卷积层，其卷积核的大小、卷积核通道的数量、卷积的步长等要素，都和网络输入数据的实际物理意义相关，如图像任务中，卷积核的大小代表了动物神经中感受野的概念。本实验借鉴二

维卷积网络结构，如 LeNet、AlexNet、VGG 等，通过计算一维卷积核的超参数与原有网络卷积核的比例，将二维卷积网络结构修改为一维卷积网络结构。注意，此处提到的 AlexNet 等网络与任务一中用于推理时产生电磁泄漏的 7 种网络区别开，此处的网络结构是用于训练电磁泄漏数据的分类网络。

使用任务一中所采集的电磁泄漏数据集进行实验，此实验为一个 7 类的分类识别问题，探索如何根据二维网络结构设计适合一维电磁泄漏信号的网络结构。在完成任务一的一维卷积网络设计后，采用任务二的数据集验证设计的一维卷积神经网络的有效性。

2.1 全连接神经网络实验结果

首先使用非卷积网络，即全连接的多层感知器(Multilayer Perceptron，MLP)进行实验，主要研究 MLP 神经元个数和 Dropout 对于任务一的分类准确率的影响。

研究单隐层神经网络中神经元个数对实验结果的影响。网络配置中，固定输入层的维度为(128,10 000,1)，意义是每个 mini-batch 有 128 个神经网络电磁泄漏信号，电磁泄漏信号为 10 000 个特征点的一维信号。其中隐藏层中使用了 Relu 激活函数，分类输出层使用 Softmax 激活函数，并使用 Adam 作为优化器。固定以上参数后，以隐层的神经元个数作为变量，研究单隐层全连接网络中神经元数量对任务一模型分类准确率的影响，其实验结果如表 1 所示。

表1 隐层神经元数量对一维信号分类的影响

Table1 Effect of number of neurons in the hidden layer on the one-dimensional signal classification accuracy

number of neurons in the hidden layer	training accuracy/%	validation accuracy/%
500	98.93	16.12
1 000	99.39	18.37
5 000	99.77	20.41
10 000	99.73	20.82
20 000	99.09	21.22

从实验结果可以看出，在单隐层神经网络中，模型产生了严重的过拟合现象，由于模型的特征点个数很多，全连接网络无法获取到足够的特征去分类。实验结果中，在神经元个数增加时，验证准确率有所提升，这符合神经元数量增加、网络复杂度增加、表征能力增强、模型分类效果变好的基础理论。

2.2 标准二维卷积网络变换一维卷积网络

本文选取了具有代表性的 3 个网络，LeNet、AlexNet 以及 VGG，探究如何将其改造为适合一维信号的神经网络。为了更好地对比卷积核参数对网络结果的影响，同时为避免全连接层较强的拟合能力对实验结果造成影响，将原网络中的全连接层替换为全局最大池化(Global Max Pooling，GMP)层。

由于卷积核的尺寸与原有输入数据的尺寸强相关，因此定义了 4 种一维卷积核的计算公式。首先给出变量定义，原有二维网络的输入为 $D_{in}\times D_{in}\times C_{in}$($C_{in}$ 为图像的通道数，D_{in} 为输入的尺寸)，若为灰度图，则为 1；若为 RGB，则为 3。原卷积核的大小为 $D_K\times D_K\times C$，D_K 为卷积核的宽度，C 为卷积核的通道数，原步长为 S。

策略一：主要关注一维信号的局部相关性。使用原卷积核宽度作为一维卷积核大小，即一维卷积核为 $D_O\times C_O$，其中 D_O 为卷积核大小，C_O 为卷积核的通道数，策略一中 $D_O=D_K$，$C_O=C$，步长使用原步长 S。

策略二：为了增加参数量以匹配原二维网络，将 D_O 定义为式(1)，其余参数与策略一保持一致。

$$D_O=D_K\times D_K \tag{1}$$

策略三：为了继续延续局部的相关性，不同于策略二中增加 D_O，而是通过增加一维卷积核的通道数，获取更多的特征映射来增加参数量。策略三中的 C_O 如式(2)所示，其余参数与策略一保持一致。

$$C_O=C\times\sqrt{D_K} \tag{2}$$

策略四：假设关心的是网络中原始输入数据和卷积核之间的相对比例，设一维信号维度为 $D_{O,in}\times 1$，可以将一维卷积核的 D_O 定义为式(3)。若计算后 $D_O<D_K$，则还是使用原有 D_K。

$$D_O=\frac{D_{O,in}\times D_K\times D_K}{D_{in}\times D_{in}} \tag{3}$$

2.3 LeNet 实验结果

首先利用卷积神经网络 LeNet[10]进行手写数字识别。输入数据为 32×32 的灰度图片，网络结构中只有两层卷

积层，称之为Conv1与Conv2，通过2.2节中的4种假设，将一维卷积网络的卷积核定义如表2所示，其中第1个维度为一维的占位符，第2个维度为卷积核的大小，第3个维度为滤波器的数量。由于策略四的计算中涉及到原本二维网络输入的大小，而32×32的输入很小，导致策略四中的卷积核维度非常大，感受野相应增加。

表2 LeNet网络一维化的卷积模型参数

Table2 The one-dimensional convolution kernel dimension of LeNet

convolution layer	strategy 1	strategy 2	strategy 3	strategy 4
Conv1	1×14×6	1×196×6	1×14×24	1×2 500×6
Conv2	1×10×16	1×100×16	1×10×48	1×1 275×16

表3展示了在利用电磁泄漏信号分类7种不同网络时，LeNet转换一维网络的验证准确率以及参数量，可以看到，策略一中仅使用了1 000多个参数达到了62.31%的验证准确率，远远高于全连接网络，说明了卷积结构对一维任务的有效性。而策略一到策略四中，验证准确率随着参数量的提高而提高，其中策略二到策略三提升了约10%的准确率，其原因在于策略三大幅度提升了滤波器的数量，让网络学习到更多的特征映射，提高了模型表现。从策略四可以看出，虽然策略四使用了非常不符合常规的2 500维、1 275维的卷积核，但准确率依旧提升了，说明LeNet网络对于本任务，参数量太小，表征能力不足，可以通过增加参数量来改善模型的表现。

表3 LeNet一维网络的验证准确率以及参数量

Table3 LeNet one-dimensional network validation accuracy and parameter amount

experimental strategy	accuracy/%	parameter
strategy 1	62.31	1 185
strategy 2	63.33	10 917
strategy 3	73.20	12 271
strategy 4	77.35	137 541

2.4 AlexNet实验结果

AlexNet[11]的卷积层有5层，将其定义为Conv1~5，原AlexNet网络的输入为224×224×3。将AlexNet一维卷积网络的卷积核定义如表4所示，其中策略四中Conv2~5由于计算后$D_O < D_K$，则还是使用原有D_K。

表4 AlexNet网络一维化的卷积模型参数

Table4 The one-dimensional convolution kernel model parameters of AlexNet

convolution layer	strategy 1	strategy 2	strategy 3	strategy 4
Conv1	1×11×96	1×121×96	1×11×288	1×23×96
Conv2	1×5×256	1×25×256	1×5×512	1×5×256
Conv3	1×3×384	1×9×384	1×3×768	1×3×384
Conv4	1×3×384	1×9×384	1×3×768	1×3×384
Conv5	1×3×256	1×9×256	1×3×512	1×3×256

表5展示了在分类7种不同网络时，AlexNet转换的一维网络的验证准确率以及参数量。与LeNet相比，即使参数量最小的策略一也比LeNet的策略四大很多，其准确率也比LeNet高。但在AlexNet结构中，并不是参数越多准确率越高，策略三的参数多于策略二，但是策略二的准确率更高，说明原本的滤波器数量即通道数[96,256,384,384,256]已经足够，并不需要盲目增加滤波器数量，而是可以通过提升卷积核的大小来提升准确率。

表5 AlexNet一维网络的验证准确率以及参数量

Table5 AlexNet one-dimensional network validation accuracy and parameter amount

experimental strategy	accuracy/%	parameter amount
strategy 1	79.18	1 159 303
strategy 2	84.29	3 725 767
strategy 3	82.11	4 875 655
strategy 4	76.33	1 160 455

2.5 VGG16实验结果

VGG网络[12]选择型号为VGG16，网络结构分为5个Block，其中每个Block包含多个卷积层和一个用于降维的池化层，其卷积核定义如表6所示。由于网络中的卷积核均为3×3，且原始二维网络的输入为224×224×3，其中策略四由于计算后$D_O < D_K$，则还是使用VGG16原有D_K。策略一与策略四的参数完全相同，此处表6中不列出策略四。

从表7中准确率上看，更多卷积层的堆叠，的确加强了模型的表征能力。3种策略的准确率均超过了90%，其中感受野最大的策略二效果最好，而参数量为策略一4倍的策略三仅比策略一高出约2%。从AlexNet和

VGG16可以看出，更多的通道数并不能大幅度提升一维卷积网络的性能，而从原始网络中通过增加卷积核长度，从而增加了感受野，往往能获得更好的效果。

表6 VGG16一维化的卷积模型参数

Table6 The one-dimensional convolution kernel model parameters of VGG16

block	strategy 1	strategy 2	strategy 3
ConvBlock1	$\begin{bmatrix}1\times3\times64\\1\times3\times64\end{bmatrix}$	$\begin{bmatrix}1\times9\times64\\1\times9\times64\end{bmatrix}$	$\begin{bmatrix}1\times3\times128\\1\times3\times128\end{bmatrix}$
ConvBlock2	$\begin{bmatrix}1\times3\times128\\1\times3\times128\end{bmatrix}$	$\begin{bmatrix}1\times9\times128\\1\times9\times128\end{bmatrix}$	$\begin{bmatrix}1\times3\times256\\1\times3\times256\end{bmatrix}$
ConvBlock3	$\begin{bmatrix}1\times3\times256\\1\times3\times256\\1\times3\times256\end{bmatrix}$	$\begin{bmatrix}1\times9\times256\\1\times9\times256\\1\times9\times256\end{bmatrix}$	$\begin{bmatrix}1\times3\times512\\1\times3\times512\\1\times3\times512\end{bmatrix}$
ConvBlock4	$\begin{bmatrix}1\times3\times512\\1\times3\times512\\1\times3\times512\end{bmatrix}$	$\begin{bmatrix}1\times9\times512\\1\times9\times512\\1\times9\times512\end{bmatrix}$	$\begin{bmatrix}1\times3\times1\,024\\1\times3\times1\,024\\1\times3\times1\,024\end{bmatrix}$
ConvBlock5	$\begin{bmatrix}1\times3\times512\\1\times3\times512\\1\times3\times512\end{bmatrix}$	$\begin{bmatrix}1\times9\times512\\1\times9\times512\\1\times9\times512\end{bmatrix}$	$\begin{bmatrix}1\times3\times1\,024\\1\times3\times1\,024\\1\times3\times1\,024\end{bmatrix}$

表7 VGG16一维网络的验证准确率以及参数量

Table7 VGG16 one-dimensional network validation accuracy and parameter amount

experimental strategy	accuracy/%	parameter
strategy 1	90.75	4 910 919
strategy 2	95.58	14 717 127
strategy 3	92.78	19 627 655

3 一维卷积网络结构电磁泄漏旁路分析

通过实验发现VGG16的策略二在任务一中的效果最佳，在进行对比实验时，为了避免全连接层较强的拟合能力对卷积的实验结果造成影响，将原本网络的全连接层替换为GMP层。最终的网络结构设计为：将VGG16策略二的分类头前增加一个丢弃率为0.5的Dropout层和一个包含384个神经元的全连接层。

从表8可以看出，当使用最终网络结构时，准确率达到了最高97.21%，但策略二加上全连接层，准确率并没有提高，反而降低了；且单独增加Dropout层，准确率也有提升，说明Dropout层+全连接层是有效的。

表8 任务一中最终VGG网络与对比实验的参数量及准确率对比

Table8 Comparison of the parameter amount and accuracy of the final VGG network with the comparison experiment in task one

experimental strategy	accuracy/%	parameter amount
VGG strategy 2+Dropout+fully connected layer(final network structure)	97.21	14 911 683
VGG strategy 2+ fully connected layer	95.37	14 913 223
VGG strategy 2+Dropout	96.19	14 717 127
VGG strategy 2	95.58	14 717 127

在实验中同样对比如表8中所列举的4种网络结构，对任务二进行评估，结果如表9所示。由表9可知，使用最终网络结构及其他对比网络结构在任务二上的准确率均达到100%，证明了最终网络结构在不同神经网络电磁泄漏任务上的泛用性。

表9 任务二中最终VGG网络与对比实验的参数量及准确率对比

Table 9 Comparison of the parameter amount and accuracy of the final VGG network with the comparison experiment in task two

experimental strategy	accuracy/%	parameter amount
VGG strategy 2+Dropout+fully connected layer(final network structure)	100	14 911 683
VGG strategy 2+ fully connected layer	100	14 913 223
VGG strategy 2+Dropout	100	14 717 075
VGG strategy 2	100	14 717 075

图2为使用最终网络结构训练任务一与任务二中前10个EPOCH的验证准确率。从图中可以看出，相比任务一，任务二中的3种框架产生的电磁泄漏更容易区分。

4 结论

本文利用Jetson Nano电磁泄漏信号采集平台，对神经网络运行时电磁泄漏信号的分类识别准确率进行分析，构建了适合分类一维神经网络泄漏信号的网络结构。在使用最终网络结构的情况下，任务一，即同一框架7种不

同网络产生的电磁泄漏分类识别准确率达到了97.21%，任务二，即不同框架中同一网络产生的电磁泄漏分类识别准确率达到了100%。说明在Jetson Nano这种一体化嵌入式AI计算平台上，不同的典型卷积神经网络的电磁泄漏信号通过深度学习算法进行分类攻击成功率极高，旁路电磁攻击方法对此类嵌入式GPU计算平台中的深度学习算法隐私产生了威胁。

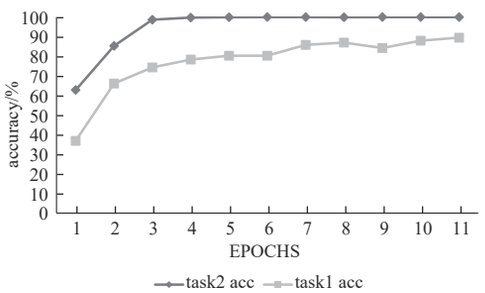

Fig.2 Validation accuracy of 10 EPOCHs from the beginning for task 1 and task 2

图2 任务一与任务二前10个EPOCH的验证准确率

参考文献：

[1] HUA Weizhe, ZHANG Zhiru, SUH G E. Reverse engineering convolutional neural networks through side-channel information leaks [C]// 2018 the 55th ACM/ESDA/IEEE Design Automation Conference (DAC). San Francisco,CA,USA:IEEE, 2018:1-6.

[2] HONG S,DAVINROY M,KAYA Y,et al. Security analysis of deep neural networks operating in the presence of cache side-channel attacks[EB/OL]. (2018-10-08)[2021-05-21]. https://doi.org/10.48550/arXiv.1810.03487.

[3] BATINA L,BHASIN S,JAP D,et al. CSI NN:reverse engineering of neural network architectures through electromagnetic side channel[C]// Proceedings of the 28th USENIX Conference on Security Symposium. Santa Clara,CA,USA:USENIX Association, 2019:515-532.

[4] YU Honggang,MA Haocheng,YANG Kaichen,et al. DeepEM:deep neural networks model recovery through EM side-channel information leakage[C]// 2020 IEEE International Symposium on Hardware Oriented Security and Trust(HOST). San Jose,CA, USA:IEEE, 2020:209-218.

[5] ABADI M,BARHAM P,CHEN Jianmin,et al. TensorFlow:a system for large-scale machine learning[C]// Proceedings of the 12th USENIX Conference on Operating Systems Design and Implementation. Savannah, GA, USA: USENIX Association, 2016: 265-283.

[6] PASZKE A,GROSS S,CHINTALA S,et al. Automatic differentiation in PyTorch[C]// The 31st Conference on Neural Information Processing Systems(NIPS 2017). Long Beach,CA,USA:[s.n.], 2017:1-4.

[7] HE Kaiming,ZHANG Xiangyu,REN Shaoqing,et al. Deep residual learning for image recognition[C]// 2016 IEEE Conference on Computer Vision and Pattern Recognition(CVPR). Las Vegas,NV,USA:IEEE, 2016:770-778.

[8] DENG Jia,DONG Wei,SOCHER R,et al. ImageNet:a large-scale hierarchical image database[C]// 2009 IEEE Conference on Computer Vision and Pattern Recognition. Miami,FL,USA:IEEE, 2009:248-255.

[9] LIN T Y,MAIRE M,BELONGIE S,et al. Microsoft COCO:common objects in context[C]// Computer Vision-ECCV 2014. Cham: Springer, 2014:740-755.

[10] LECUN Y,BOTTOU L,BENGIO Y,et al. Gradient-based learning applied to document recognition[J]. Proceedings of the IEEE, 1998,86(11):2278-2324.

[11] KRIZHEVSKY A, SUTSKEVER I, HINTON G E. ImageNet classification with deep convolutional neural networks[J]. Communications of the ACM, 2017,60(6):84-90.

[12] SIMONYAN K,ZISSERMAN A. Very deep convolutional networks for large-scale image recognition[EB/OL]. (2014-09-04). https://doi.org/10.48550/arXiv.1409.1556.

作者简介：

吴晨曦(1996-)，男，在读硕士研究生，主要研究方向为旁路攻击及机器学习.email:wuchenxi118@126.com.

张洪欣(1969-)，男，博士，教授，博士生导师，主要研究方向为无线通信与电磁兼容、通信信号处理、电磁辐射、信息安全、生物医学工程等.

崔晓彤(1995-)，女，在读博士研究生，主要研究方向为旁路攻击和深度学习.