基于 Ghost-DenseNet-SE 的恶意代码检测方法

李　怡，李　进
（空军工程大学防空反导学院，西安，710051）

摘要　针对现有恶意代码检测模型对恶意代码及其变种识别率不高，且参数量过大这一问题，将轻量化卷积 Ghost、密集连接网络 DenseNet 与通道域注意力机制 SE 相结合，提出一种基于 Ghost-DenseNet-SE 的恶意代码家族检测模型。该模型为压缩模型体积、提升识别速率，将 DenseNet 中的标准卷积层替换为轻量化 Ghost 模块；并引入通道域注意力机制，赋予特征通道不同权重，用以提取恶意代码的关键特征，提高模型检测精度。在 Malimg 数据集上的实验结果表明，该模型对恶意代码家族的识别准确率可以达到 99.14%，与 AlexNet、VGGNet 等模型相比分别提高了 1.34%和 2.98%，且模型参数量更低。该算法在提升分类准确率的同时，降低了模型复杂度，在恶意代码检测中具有重要的工程价值和实践意义。

关键词　恶意代码；轻量化卷积；密集连接网络；通道域注意力机制
DOI　10.3969/j.issn.1009-3516.2021.05.008
中图分类号　TP309　　**文献标志码**　A　　**文章编号**　1009-3516(2021)05-0049-07

A Malicious Code Detection Method Based on Ghost-DenseNet-SE

LI Yi, LI Jin
(Air and Missile Defense College, Air Force Engineering University, Xi'an 710051, China)

Abstract　Aimed at the problems that the existing malicious code detection model is iow in recognition rate of malicious code and its variants, and the amount of parameters is too large, a method of Malicious code family detection model is proposed based on Ghost-DenseNet-SE is proposed in combination with the lightweight convolutied Ghost, densely connected network DenseNet and the channel domain attention mechanism SE. This model serves as a type of compressing the model volume and improving the recognition rate. the standard convolutional layer in DenseNet is replaced with a lightweight Ghost module, and the channel domain attention mechanism is introduced to assign different weights to the feature channels to extract the key features of malicious code and improve model checking accuracy. The experimental results on the Malimg data set show that the model's recognition accuracy of malicious code families can reach 99.14%, Compared with AlexNet and VGGNet, the recognition accuracy increases by 1.34% and 2.98% respectively, and the amount of model parameters is lower. This algorithm not only improves the classification accuracy, but also reduces the complexity of the model. The algorithm has important engineering value and practical significance in malicious code detection.

收稿日期：2021-06-15
作者简介：李　怡(1995—)，女，山西运城人，硕士生，研究方向：防空反导网络信息防御、恶意代码检测。E-mail:15735104394@163.com
通信作者：李　进(1971—)，男，陕西西安人，副教授，研究方向：地空导弹武器系统总体和嵌入式系统。E-mail:ljlxls@163.com

引用格式：李怡，李进. 基于 Ghost-DenseNet-SE 的恶意代码检测方法[J]. 空军工程大学学报(自然科学版)，2021，22(5)：49-55. LI Yi，LI Jin. A Malicious Code Detection Method Based on Ghost-DenseNet-SE[J]. Journal of Air Force Engineering University (Natural Science Edition)，2021，22(5)：49-55.

Key words malicious code; lightweight convolutional; densely connected network; channel domain attention mechanism

近年来,互联网上的恶意代码数量呈井喷式增长,已成为互联网安全的主要威胁之一。《2020 年中国网络安全报告》[1] 显示:2020 年瑞星“云安全”系统共截获病毒样本总量 1.48 亿个,病毒感染次数 3.52 亿次,病毒总体数比 2019 年同期上涨 43.71%。与此同时,为了躲避杀毒软件的检测,攻击者采用各种混淆技术对恶意代码进行变种,使其隐蔽性大大增强,安全检测难度加大,因此对恶意代码及其变种进行高效检测是互联网安全目前面临的巨大挑战。

恶意代码检测主要分为静态检测和动态检测。静态检测[2] 指不实际运行样本,通过反编译工具将恶意代码反汇编为可读的二进制源代码,从中提取操作码和 API 等静态特征对其进行分析。动态检测[3] 指在安全可控的虚拟环境中运行样本,根据恶意代码对操作系统的资源调度行为进行分析。然而这些传统方法需要依赖大量人工特征工程,比较耗时,也无法有效检测恶意代码变体。近年来,研究人员在传统检测方法的基础上,将恶意代码二进制文件可视化为图像,然后结合深度学习对恶意代码家族进行分类。卷积神经网络[4] 是深度学习中最具代表性的技术之一,近年来在自然语言处理、文本处理和图像识别等领域发展迅速,它可以自动学习输入数据的特征而不需要人工参与。Cui 等人[5] 提出了一种基于 CNN 的恶意软件变体检测模型,将恶意代码转化为灰度图,并使用 BAT 算法解决了恶意代码样本家族数量不平衡的问题。王国栋等人[6] 提出基于 CNN-BiLSTM 的恶意代码家族检测模型,该模型可以从恶意代码灰度图中自动学习特征,大大降低了人工提取特征的成本,同时 BiLSTM 可以关注更多的局部和全局特征。但随着恶意代码变种越来越多样化,浅层卷积神经网络已不足以提取复杂的纹理特征,于是一些深层卷积神经网络被用于恶意代码家族检测中,如:Alexnet[7]、VGGNet[8]、GoogleNet[9] 和 ResNet[10] 等,这些网络结构通过不断加深网络深度和宽度,使其能够提取更深层次的特征。蒋考林等人[11] 提出一种基于多通道图像特征和 AlexNet 神经网络的恶意代码检测方法,多通道图像比二阶灰度图能体现更多的纹理特征。王博等人[12] 利用 VGGNet 生成恶意样本分类模型,对恶意代码 RGB 图像进行分类检测,识别准确率有一定提升。不断加深网络深度,一定程度上可以提高恶意代码识别效率,但同时也会引起模型梯度爆炸,参数量剧增等问题,需要耗费大量的计算开销。

针对上述现有恶意代码检测模型识别率不高且模型参数过大的问题,本文提出一种基于 Ghost-DenseNet-SE 的恶意代码家族检测方法。同时,为进一步提高对恶意代码家族准确分类的能力,在 DenseNet 中引入通道域注意力机制,得到特征更显著的特征图。通道注意力机制的加入也会增加模型参数量,并使用 Ghost 模块替换 Dense Block 的卷积层,以达到保证模型检测精度的前提下减少模型参数,最终实现恶意代码家族检测模型的轻量化,使其能更好地部署在资源有限的平台上。

1 基础理论

1.1 密集连接网络 DenseNet

DenseNet 是 Huang G[13] 等人提出的一种具有密集连接的卷积神经网络。该网络结构主要由稠密块(Dense Block)和过渡层(Transition Layer)组成,模型结构见图 1。DenseNet 网络结构中包含了多个 Dense Block 模块,其中每个 Dense Block 由 BN-Relu-Conv(3×3)组成;每两个相邻的 Dense block 之间的 Transition Layer 由 BN-Relu-Conv(1×1)(filternum:m)-doupout-Pooling(2×2)组成。

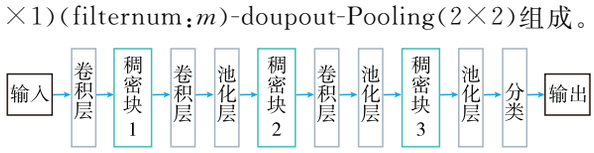


图 1 DenseNet 结构

1.1.1 稠密块(Dense Block)

在 Dense Block 模块中,任意两层之间有着密切的联系,其内部结构见图 2,将所有层的特征进行相互拼接,即对任意一层之前的所有层的输出结果进行叠加作为该层的输入,然后把该层的结果和之前层的输出结果作为下一层的输入传输下去。

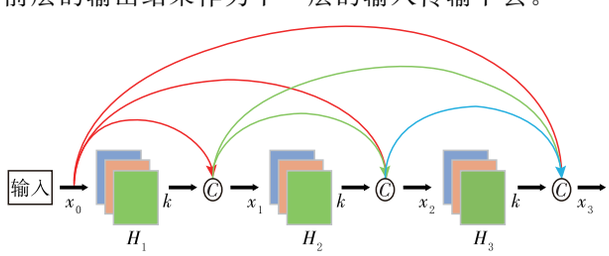


图 2 Dense Block 内部结构

对于 L 层网络而言,第 l 层的输入由式(1)得出:

$$x_l = H([x_0, x_1, \cdots, x_{l-1}]) \tag{1}$$

式中：$x_0, x_1, \cdots, x_{l-1}$ 分别表示第 0 层到第 $l-1$ 层所对应的特征图；

$[x_0, x_1, \cdots, x_{l-1}]$ 表示对第 0 层到第 $l-1$ 层的所对应的特征图进行级联；

$H_l(\cdot)$ 表示包含 BN，Relu 和 Conv 3 种操作的复合函数。

在 Dense Block 中每个复合函数 $H_l(\cdot)$可以输出 k 个特征图，则第 l 层会输入 $k_0+k(l-1)$特征图，其中 k_0 表示输入层的的通道数 channel。k 也称为网络的生长率(groeth rate)，它是一个超参数，用来避免网络增长过快。

1.1.2　过渡层

过渡层用来连接两个相邻的密集块，通过池化来降低特征图的大小，让模型变得更紧凑。为了进一步压缩模型尺寸，引入压缩因子 θ，取值范围为 $(0,1]$。当密集块输出 m 个特征图时，过渡层通过卷积可以产生 θm 个特征。$\theta<1$ 时，特征图数目压缩为原来的 θ 倍；$\theta=1$ 时，不压缩。

1.2　通道域注意力机制(SeNet)

通道域注意力机制常被用于卷积神经网络中，对图像中的重要信息部分进行可视化[14]。该机制的核心架构单元为 Squeeze-and-Excitation(SE) Block[15]，内部结构如图 3 所示。首先使用 Squeeze(挤压)操作作用于经过卷积池化操作的特征图，使其在通道上得到特征图的全局信息；然后使用 Excitation(激励)操作来获得通道之间的依懒性，得到不同通道的权重，该操作采用 Sigmoid(门函数)；最后对最终特征图进行 Scale 操作。

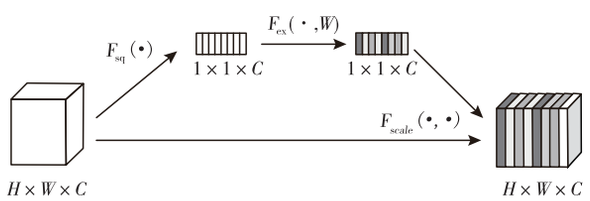


图 3　Squeeze-and-Excitation Block 内部结构

Squeeze 操作是对图像进行全局平均池化操作，即对得到的每个特征图进行空间维度上的压缩，结果得到该层 C 个特征图的全局信息。见式(2)：

$$Z_C = F_{sq}(u_C) = \frac{1}{W\times H}\sum_{i=1}^{W}\sum_{j=1}^{H}u_C(i,j) \quad (2)$$

Excitation 操作是对 Squeeze 得到的 $1\times1\times C$ 征图先进行全连接层操作，在全连接层操作中引入缩放因子(reduction ratio)来减少通道数量从而减少计算量；再将其结果经过 Sigmoid(门函数)得到 C 个特征图的权重，通过权重来表示通道之间的依赖程度，最终使得神经网络能够自主学习到不同通道的关键信息，见式(3)：

$$x=F_{ex}(z,W)=\sigma(g(z,W))=\sigma(W_2\delta(W_1z)) \quad (3)$$

式中：δ 为 ReLU 激活函数；σ 为 igmoid 激活函数；$W_1\in R^{\frac{C\times C}{r}}$，$W_2\in R^{\frac{C\times C}{r}}$；$r$ 为降维参数(reduction ratio)。

Scale 操作是将原特征通道值与 Excitation 相乘得到的不同权重，从而加强对原特征图的关键通道域的注意，得到新特征图并输入到下一层，如式(4)所示：

$$X_C = F_{scale}(u_C, s_C) = s_C \cdot u_C \quad (4)$$

1.3　Ghost 模块

Ghost 模块是 Han 等人从特征图的冗余问题出发，提出的一种轻量化卷积模块[16]。该卷积模块通过一系列线性操作来生成更多的特征映射，在不改变输出特征图大小的情况下，既保证了模型的精度，又减少了模型参数，达到了网络模型轻量化的效果。

Ghost 模块分两步进行，内部结构如图 4 所示。第 1 步先通过普通卷积生成少量真实的冗余特征图 Y；第 2 步对第 1 步生成的少量真实冗余特征图进行线性变换，获得另一部分冗余特征图 Y'；最后将两部分冗余特征图拼接在一起，组成完整的冗余特征图。

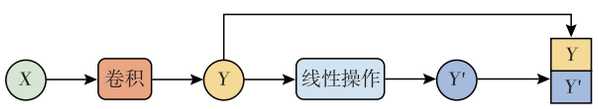


图 4　Ghost 模块内部结构

假如输入特征为 $h\times w\times m$，输出特征为 $h'\times w'\times n$。其中 h、w 分别为输入数据的长和宽，m 为输入的通道数；h'、w' 分别为输出数据的长和宽，n 为输出的通道数，k 为卷积核的尺寸大小。当输入数据经过标准卷积后，参数量为 $n\times k\times k\times m$；当输入数据经过 Ghost 卷积模块之后，参数量为 $\frac{n}{s}\times k\times k\times m+(s-1)\times\frac{n}{s}\times k\times k$。则 Ghost 模块的参数量压缩比 $s\times m/(m+s-1)\approx s$。本文参数设置 $s=2$，当 $s=2$ 时，在网络中嵌入 Ghost 模块使得网络性能最好。

2　基于 Ghost-Densenet-SE 的恶意代码家族检测模型

2.1　恶意代码可视化

恶意代码二进制位字符串可以分为多个长度为 8 bit 的子字符串，这些子字符串中的每一位都可以被视为一个像素，因为这 8 bit 可以解释为 0～255

范围内的无符号整数,其中 0 为黑色,255 为白色。选取连续的 3 个子字符串,分别对应于彩色图像中的 R、G、B 3 个通道,即第 1 个 8 bit 字符串转化为 R 通道的值,第 2 个 8 bit 字符串转化为 G 通道的值,第 3 个 8 bit 字符串转化为 B 通道的值;重复这一操作使得所有数据都被选完(最末段端数据量不足 3 字符串的,用 0 补足)。利用该原理,二进制恶意代码便转化为十进制数字的一维向量,固定 256 为行宽向量,高度根据文件大小变化。最终,恶意代码被解释为 RGB 图像,具体流程如图 5 所示。

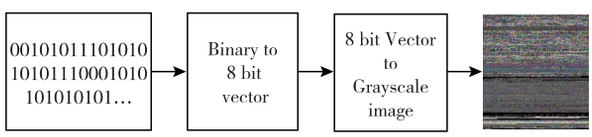


图 5 恶意代码可视化过程

2.2 模型构建

本文提出的基于 Ghost-Densenet-SeNet 的恶意代码家族检测模型,首先利用恶意代码可视化技术将恶意代码转化为 RGB 图像,然后用提出的模型对图像数据集进行训练,最终实现对恶意代码家族的分类识别。本文使用密集连接网络 DenseNet 作为主干网络,既缓解了传统卷积神经网络因不断加深网络深度和宽度而带来的梯度消失和参数量剧增问题;同时鼓励特征复用,能够提取恶意代码图像更丰富的特征。然后在 DenseNet 中引入通道域注意力机制,得到特征更显著的特征图,进一步提高对恶意代码家族准确分类的能力。最后使用 Ghost 模块去重构 Dense Block 的卷积层以减少模型参数,使得模型能更好地部署在资源有限的移动端。

在将图像数据集输入到模型中时,先做一次卷积操作,然后进入第 1 个 Dense Block,一共使用了 3 个 Dense Block。每 2 个 Dense Block 之间连接 1 个 Transition Layer,共 2 个 Transition Layer。在最后一个 Dense Block 之后引入 SE,得到特征更显著的特征图,SE 中共两个全连接层,在第 1 个全连接层中引入缩放因子 ratio 来减少通道数,具体数值通过实验调优来设置。为减少因引入 SE 而增加的模型参数,使用由 1 个点卷积和 1 个 5×5 的通道卷积组成的 Ghost 模块替换除第 1 层卷积之外,所有 Dense Block 中的 3×3 标准卷积。最后在 SE 后连接 1 个全局平均弛化和 1 个有 25 个神经元的全连接层,以实现对恶意代码家族的分类。

本文的恶意代码家族检测模型训练与检测过程相关算法如表 1 所示。

表 1 恶意代码家族检测模型训练与检测过程相关算法

算法:基于 Ghost-DenseNet-SE 的检测模型训练与检测过程

输入:$G=\{M_i\}$,$i=\{1,2,\cdots,n\}$,i 表示输入的序号,M_i 表示恶意代码可视化后的 RGB 图像,G 表示 RGB 图像集合。

输出:$R=\{r_i\}$,R 表示检测结果集合,r_i 表示第 i 个恶意代码的检测结果。

步骤 1:构建 Ghost-DenseNet-SE 恶意代码家族检测模型

1)增加 1 个卷积核为 3 的卷积层,填充为 Same;

2)增加 1 个包含 12 个 1×1 和 Ghost 轻量化卷积的 Dense Block,Ghost 模块由 1 个点卷积和 1 个 5×5 的通道卷积组成;

3)增加 1 个包含 1×1 卷积操作,1 个平均池化层和批量归一化层(BN)的 Transition Layer;

4)重复步骤 2)和步骤 3),共添加 3 个 Dense Block 和 2 个 Transition Layer;

5)增加注意力层,得到 C 个特征图的全局信息 u_C 及对应的特征权重 s_C;

6)将上一个卷积层得到的原特征通道 u_C 与注意力层得到的权重 s_C 相乘,即执行 $s_C u_C$ 操作;

7)增加 1 个包含全局平均池化的全连接层,激活函数为 ReLu;

8)增加 1 个包含 25 个神经单元的全连接层,激活函数为 Softmax;

步骤 2:Ghost-DenseNet-SE 模型训练与测试

9)模型参数初始化;

10)while 满足训练条件 do:

11)while 训练集数据剩余非空 do:

12)模型训练输入 1 组小批量数据样本;

13)使用 Softmax 函数对恶意代码样本分类;

14)使用 Adam 梯度下降优化算法更新权重值;

15)end while

16)使用测试集数据验证模型性能;

17)end while

3 实验结果与分析

3.1 数据集

本文选取公开数据集 Malimg,此数据集包括 25 个不同家族的恶意样本,共 9 339 个,具体样本种类和数量分布如图 6 所示。

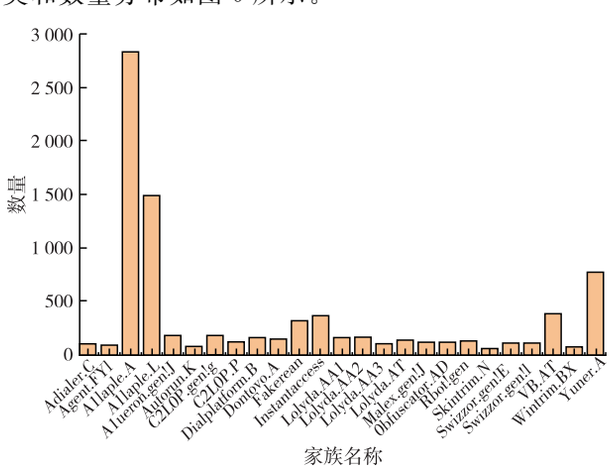
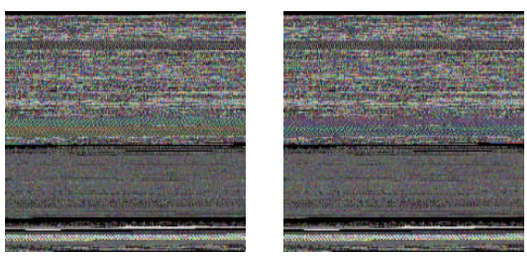


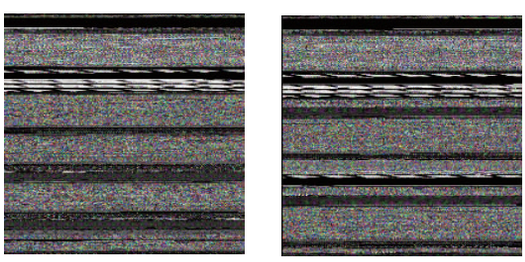
图 6 Malimg 恶意代码样本种类和数量分布

3.2　数据预处理

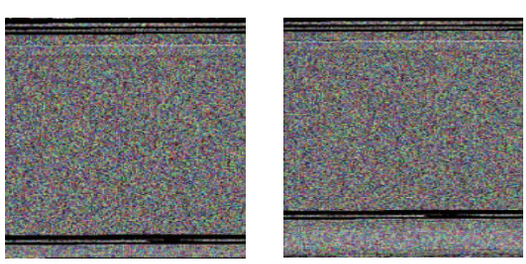
卷积神经网络要求输入的图像大小要相同，而不同大小的恶意代码二进制可执行文件转化成的RGB图像尺寸不同，因此在输入神经网络之前需要先将图像处理为大小一致的图片。本文所使用的模型要求输入的 RGB 图像尺寸为 224×224，为了确保图像纹理信息的完整性，本文先对图像的边界部分使用 0 byte 填充使其成为正方形，然后等比例缩放至 224×224 大小。图 7 显示了部分恶意代码家族二进制文件预处理后的图像示例，由上到下依次是：Adialer.C 家族，VB.AT 家族和 Skintrim.N 家族。从这些图像示例中可以看出，同一家族的恶意代码在图像纹理性上具有相似性，而不同家族的恶意代码在图像纹理性上具有差异性。



（a）Adialer.C家族



（b）VB.AT家族



（c）Skintrim.N家族

图 7　部分恶意代码家族图像

3.3　评价指标

在实验过程中，本文使用以下 5 个评价指标对本文提出的恶意代码检测模型进行评估：A 为准确率(Accuracy)，P 为精确率(Precision)，R 为召回率(Recall)，F_1 为 F1-score，L 为损失率(Loss)。

TP 为正类样本被模型预测为正类的比例；TN 为负类样本被模型预测为负类的比例；FP 为负类样本被模型预测为正类的比例；FN 为正类样本被模型预测为负类的比例。

$$A=\frac{TP+TN}{TP+FP+TN+FN} \tag{5}$$

$$P=\frac{TP}{TP+FP} \tag{6}$$

$$R=\frac{TP}{TP+FN} \tag{7}$$

$$F_1=\frac{2\times P\times R}{P+R} \tag{8}$$

$$L=-\sum_{i=1}^{i=q} y_{i1}\log\hat{y}_{i1}+y_{i2}\log\hat{y}_{i2}+\cdots+y_{id}\log\hat{y}_{id} \tag{9}$$

式中：q 为样本个数；d 为样本类别数；y_{id} 为 one-hot 编码值（0 或 1）；$\hat{y}_{id}$ 为 Softmax 函数输出值（$\sum_{d=1}^{d=25}\hat{y}_{id}$）。

3.4　对比分析

本次实验在 Centos7 系统环境下进行，硬件配置：Intel(R) Xeon(R) Silver 4110 CPU @ 2.10 GH，GPU 型号为 Quadro RTX 5000/Pcle/SSE2，CUDA 11.0。软件平台为 PyCharm，使用 Phthon3.8 编程，训练与测试框架为深度学习开源框架 Keras2.4.3 和 TensorFlow2.4.1。

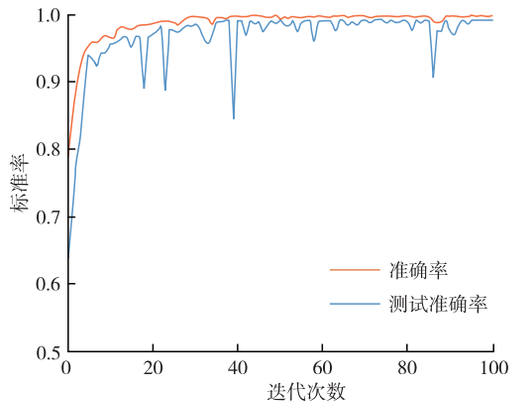
3.4.1　压缩比影响实验

本实验将恶意代码图像数据集按照 8∶1∶1 的比例随机划分为训练集、验证集和测试集。Epoch 设置为 100，Batch Size 设置为 32。实验模型采用加入通道域注意力机制的密集连接网络 DenseNet，其学习率、压缩比、损失函数等参数的设置都会影响恶意代码检测的精度。模型采取交叉熵损失函数来衡量真实值与预测值之间的差异，采用 Adam 优化器对网络进行优化，学习率选用经验值 0.001，最终通过 softmax 函数进行分类。通道域注意力机制中的超参数 ratio 通过实验获取最合适的值。压缩比 ratio 对恶意代码检测性能的影响如表 2 所示：

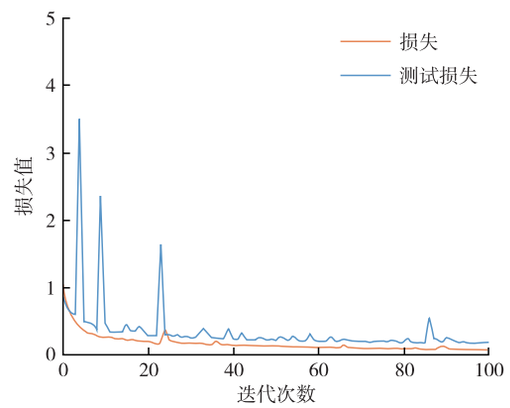
表 2　压缩比 r 对检测结果的影响

r	准确率/%	参数量
2	98.99	714 111
4	99.14	654 989
6	99.11	633 259
8	99.06	622 804

经上述实验，通过权衡模型的准确率和参数量，最终将超参数 ratio 设置为 4。本文提出的方法实验结果如图 8 所示，随着测试次数的增加，精确度和交叉熵损失值会收敛到一定值，模型逐渐收敛、平稳。在这 100 次迭代过程中，选取测试集中准确率最高的值为模型的准确率，相应的损失值即为该模型的损失值，本模型的准确率可达到 99.14%。



(a) 准确率



(b) 损失值

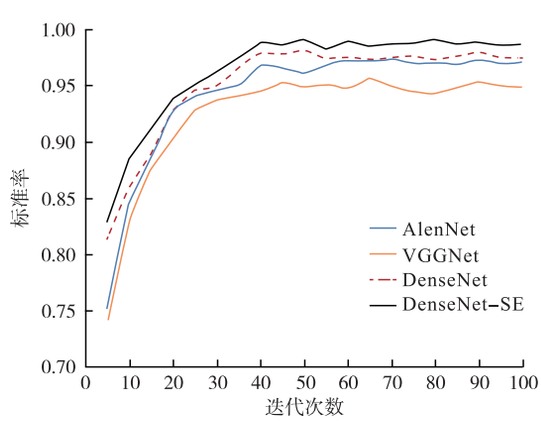
图 8 Ghost-DenseNet-SE 检测模型实验结果

3.4.2 模型性能对比

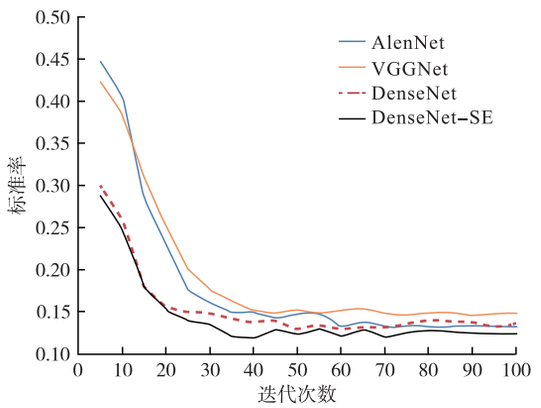
为了进一步验证本文所提的加入通道域注意力机制的 DenseNet 模型对恶意代码家族有更高的识别准确率,将其与文献[11]中的 AlexNet 检测模型与文献[12]中的 VGGNet 检测模型进行比较。采用准确率、召回率、F1-score 和损失值等作为评价指标,实验结果如表 3、图 9 所示。

表 3 各模型实验结果对比

模型	准确率/%	精确率/%	召回率/%	F1-score	损失值
AlexNet	97.80	97.85	97.50	96.56	0.132
VGGNet	96.16	96.10	96.53	96.36	0.148
DenseNet	98.20	98.33	96.72	97.52	0.128
DenseNet-SE	99.17	99.10	98.80	98.95	0.119



(a) 各模型准确率



(b) 各模型损失值

图 9 各模型实验结果对比

从上述表和图可以看出,在实验数据不变的情况下,结合通道域注意力机制和密集连接网络 DenseNet 的恶意代码家族检测模型效果最好,准确率高达 99.17%,对比文献[11]中的 AlexNet 和文献[12]中的 VGGNet 分别提高了 1.37% 和 3.01%,召回率和 F1-score 也均高于文献中的两种模型,模型收敛速度也更加迅速;同时 DenseNet-SE 的损失值也最低,表明该模型的检测结果与真实值更接近。在没有加入注意力机制之前,仅采用 DenseNet,准确率也高于其余两种模型,这是由于 Dense Block 采用密集连接方式,使所有层之间的特征都相互联系,加强了特征传播,因此 DenseNet 网络对恶意代码图像特征的提取能力更强。在 DenseNet 中加入注意力机制后,准确率提高了 0.97%,说明该机制为通道分配不同的权重,能够得到信息更显著的特征通道。因此 DenseNet-SE 模型在恶意代码家族识别准确率和收敛速度上有更优越的性能。

实验除对各模型准确率进行对比外,还对各模型参数进行对比。在提高恶意代码检测精度的前提下,减小模型体积也是优化模型的目标之一,模型参数对比结果如表 4 所示。

表 4 各模型参数量对比

模型	准确率/%	参数量
AlexNet	97.80	21.00×10^7
VGGNet	96.16	14.00×10^7
DenseNet	98.20	0.89×10^7
DenseNet-SE	99.17	1.08×10^7
Ghost-DenseNet-SE	99.14	0.66×10^7

由上表可以清晰地看出,DenseNet 网络对于 AlexNet 准确率虽只提高了 0.4%,但是模型参数却大大减少,对比 VGGNet 模型参数量也明显减少。这还是由于 DenseNet 各层间密集连接的方

式，传统 CNN 有 L 个连接，而 DenseNet 只有 $L(L+1)/2$ 个连接。通道域注意力机制的引入，会导致模型参数量增加，在此基础上用轻量化 Ghost 模块重构 Dense Block 的卷积层，参数量减少了 39%，模型体积得到了有效的压缩，同时准确率只下降了 0.03%，几乎无损精度。结合轻量化 Ghost 卷积，密集连接网络 DenseNet 和通道域注意力机制 SE 的恶意代码家族检测模型最终综合性能优于其它检测模型，证明了本文所提方法的有效性。

4　结语

本文针对现有恶意代码家族检测模型存在识别准确率不高，且模型参数太大，难以在实际环境中运行等问题，提出一种基于 Ghost-DenseNet-SE 的恶意代码家族检测方法。将 DenseNet 作为主干网络，该网络对各层使用密集连接的方法，解决了由于加深网络带来的模型退化问题，减少了模型参数，又加强了特征传递。在提高模型准确率方面，同时探索了计算机视觉中的通道域注意力机制，发现该机制通过为特征通道分配不同的权重，能够对恶意代码 RGB 图像纹理特征的关键信息进行增强，进而提高原有模型的检测效果。在减少模型复杂度方面，使用轻量化 Ghost 模块对 Dense Block 的卷积层进行重构，减少了参数量，压缩了模型体积。实验结果表明，本文提出的方法在提高恶意代码家族检测精度的同时，又能减少参数量，降低模型复杂度，一定程度上解决了大批量恶意代码检测过程中的资源浪费问题。但本文方法还存在一定不足，模型训练时内存开销太大，后续工作将进一步研究保证模型检测精度与计算参数的同时，较少的模型内存开销使其能更好地部署在资源有限的移动端上。

参考文献

[1] 北京瑞星网安技术股份有限公司. 瑞星 2020 年中国网络安全报告[J]. 信息安全研究，2021，7(2)：102-109.

[2] AHMAD F，BADRUL A N，AHMAD K，et al. Discovering Optimal Features Using Static Analysis and a Genetic Search Based Method for Android Malware Detection[J]. Frontiers of Information Technology & Electronic Engineering，2018，19(6)：712-736.

[3] YAN P，YAN Z. A Survey on Dynamic Mobile Malware Detection[J]. Software Quality Journal，2018，26(3)：891-919.

[4] GU J，WANG Z，KUEN J，et al. Recent Advances in Convolutional Neural Networks[J]. Pattern Recognition，2018，77(C)：354-377.

[5] CUI Z，XUE F，CAI X，et al. Detection of Malicious Code Variants Based on Deep Learning[J]. IEEE Transactions on Industrial Informatics，2018，14(70)：3187-3196.

[6] 王国栋，芦天亮，尹浩然，等. 基于 CNN-BiLSTM 的恶意代码家族检测技术[J]. 计算机工程与应用，2020，56(24)：78-83.

[7] KRIZHEVSKY A，SUTSKEVER I，HINTON G. ImageNet Classification with Deep Convolutional Neural Networks[J]. Communications of the ACM，2012，60(6)：84-90.

[8] SIMONYAN K，ZISSERMAN A. Very Deep Convolutional Networks for Large-Scale Image Recognition[J]. Computer Science，2014(7)：21-34.

[9] SZEGEDY C，LIU W，JIA Y，et al. Going Deeper with Convolutions[C]// 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR). Boston，MA，USA：IEEE，2014：1-9.

[10] HE K，ZHANG X Y，REN S Q，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.

[11] 蒋考林，白玮，张磊，等. 基于多通道图像深度学习的恶意代码检测[J]. 计算机应用，2021，41(4)：1142-1147.

[12] 王博，蔡弘昊，苏旸. 基于 VGGNet 的恶意代码变种分类[J]. 计算机应用，2020，40(1)：162-167.

[13] HUANG G，LIU Z，LAURENS V D M，et al. Densely Connected Convolutional Networks[C]//2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR). Honolulu，HI，USA：IEEE，2017：2261-2269.

[14] WANG F，JIANG M，QIAN C，et al. Residual Attention Network for Image Classification[C]//2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR). Honolulu，HI，USA：IEEE，2017：2261-2269.

[15] HU J，SHEN L，SUN G，et al. Squeeze-and-Excitation Networks[C]// 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition. Salt Lake City，UT，USA：IEEE，2018：2011-2023.

[16] HAN K，WANG Y，TIAN Q，et al. GhostNet：More Features from Cheap Operations[C]// 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). Seattle，WA，USA：IEEE，2020：1577-1586.

（编辑：徐楠楠）