(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 112861135 B
(45)授权公告日 2024.05.31

(21)申请号 202110390469.0
(22)申请日 2021.04.12
(65)同一申请的已公布的文献号
申请公布号 CN 112861135 A
(43)申请公布日 2021.05.28
(73)专利权人 中南大学
地址 410083 湖南省长沙市岳麓区麓山南路932号
(72)发明人 汪洁 殷雪峰
(74)专利代理机构 长沙永星专利商标事务所(普通合伙) 43001
专利代理师 周咏 米中业
(51)Int.Cl.
G06F 21/56(2013.01)
G06N 3/0464(2023.01)
G06N 3/08(2023.01)

(56)对比文件
CN 106096415 A,2016.11.09
CN 109165510 A,2019.01.08
CN 110458239 A,2019.11.15
CN 110704842 A,2020.01.17
CN 106951782 A,2017.07.14
CN 108021806 A,2018.05.11
CN 108416213 A,2018.08.17
CN 109241741 A,2019.01.18
CN 109271788 A,2019.01.25
CN 109829306 A,2019.05.31
EP 2182458 A1,2010.05.05
KR 20200071822 A,2020.06.22
US 10133865 B1,2018.11.20
US 2006037080 A1,2006.02.16
US 2018144130 A1,2018.05.24
US 2019163904 A1,2019.05.30
US 2021004472 A1,2021.01.07
US 2021067544 A1,2021.03.04 (续)

审查员 肖倩

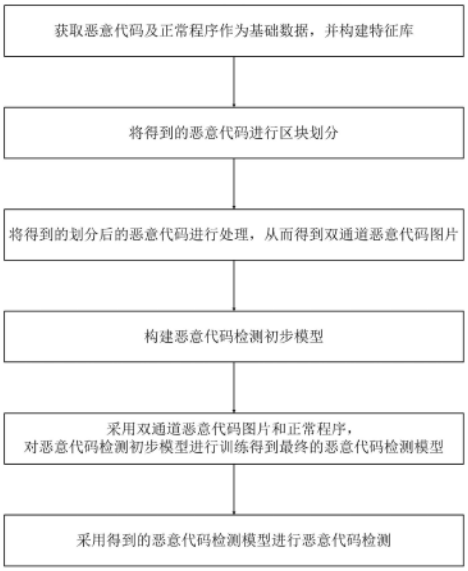
权利要求书2页 说明书6页 附图3页

(54)发明名称

基于注意力机制的恶意代码检测方法

(57)摘要

本发明公开了一种基于注意力机制的恶意代码检测方法,包括获取恶意代码及正常程序并构建特征库;将恶意代码进行区块划分和处理得到双通道恶意代码图片;构建恶意代码检测初步模型并训练得到最终的恶意代码检测模型;采用恶意代码检测模型进行恶意代码检测。本发明使用3-gram模型处理并构建3-gram特征库,再将操作码按照函数划分块,通过将块映射成图像中的不同行得到一个单通道图像;然后增加一个新的图像通道并根据3-gram特征库填入当前位置操作码的权重值,该通道可以有效的展现出恶意代码中关键的代码区域;最后针对该恶意代码图像,采用改进的识别模型进行恶意代码识别;因此,本发明方法可靠性高、实用性好且识别效率高。



CN 112861135 B

[转续页]

[接上页]

(56)对比文件

汪洁等.子图相似性的恶意程序检测方法.软件学报.2020,3436-3447.

杨宏宇等.一种Android恶意软件检测模型.西安电子科技大学学报.2019,45-51.

柳卓明.基于深度学习的恶意代码检测.中国优秀硕士学位论文全文数据库 (信息科技辑).2021,I139-58.

李玉等.基于抽象汇编指令的恶意软件家族分类方法.北京航空航天大学学报.2021,348-355.

王婷婷.基于操作码序列的恶意软件变体检测研究.中国优秀硕士学位论文全文数据库 (信息科技辑).2019,I139-124.

Hao, ZS等.A Novel Android Application Penetration Analysis Method.2nd Joint International Information Technology, Mechanical and Electronic Engineering Conference (JIMEC).2018,29-35.

Ren Zhuojun等.Pixel normalization method applied in malware visualization analysis.Computer Engineering and Applications.2016,121-125.

McLaughlin, N等.Deep Android Malware Detection.7th ACM Conference on Data and Application Security and Privacy (CODASPY).2017,301-308.

刘恒讯;艾中良.一种基于词向量的恶意代码分类模型.电子设计工程.2020,(第06期),16-22.

修扬;刘嘉勇.基于操作码序列频率向量和行为特征向量的恶意软件检测.信息安全与通信保密.2016,(第09期),97-101.

1.一种基于注意力机制的恶意代码检测方法,包括如下步骤:

S1.获取恶意代码及正常程序作为基础数据,并构建特征库;

S2.将步骤S1得到的恶意代码进行区块划分;

S3.将步骤S2得到的划分后的恶意代码进行处理,从而得到双通道恶意代码图片;具体为采用如下步骤得到双通道恶意代码图片:

a.计算每个函数内所包含的3-gram特征的信息增益总和,并删除信息增益总和为0的函数;

b.获取步骤a得到的每个函数的操作码;

c.将操作码映射到设定的整数区间,保证每一个整数代表一种操作码;

d.将每个函数中的操作码进行转换得到一维向量,将得到的一维向量进行拼接得到单通道恶意代码图片;

e.针对步骤d得到的单通道恶意代码图片,将图片中每一个像素与其之后的两个像素重新组成新的3-gram特征,并与步骤S1构建的特征库进行比较,从而得到像素所对应的新的信息增益值;

f.将步骤e得到的像素所对应的新的信息增益值与设定值yy相乘,得到像素权重值;$yy=\frac{65535}{xx}$,xx为特征库中信息增益的最大值;

g.在步骤d得到的单通道恶意代码图片上,添加一个新的图像通道,图像通道的值为对应像素的像素权重值,从而得到最终的双通道恶意代码图片;

S4.构建恶意代码检测初步模型;

S5.采用步骤S3得到的双通道恶意代码图片,以及步骤S1获取的正常程序,对步骤S4构建的恶意代码检测初步模型进行训练,从而得到最终的恶意代码检测模型;

S6.采用步骤S5得到的恶意代码检测模型进行恶意代码检测。

2.根据权利要求1所述的基于注意力机制的恶意代码检测方法,其特征在于步骤S1所述的获取恶意代码及正常程序作为基础数据,并构建特征库,具体为采用如下步骤构建特征库:

A.获取恶意代码数据集和正常程序数据集;

B.对获取的恶意代码进行反汇编,并按照函数进行区块划分;

C.采用3-gram模型对每个函数内的操作码进行切分,从而得到3-gram特征;

D.采用如下算式计算每个3-gram特征的频率$f_y(D^i)$:

$$f_y(D^i)=\frac{S(D^i,y)}{\sum_{i=1}^{n}S(D^i,y)}$$

式中D为3-gram特征集合;D^i为所有3-gram特征中的第i个特征;y为恶意代码样本;$S(D^i,y)$为样本y中特征D^i的总数;样本中每个3-gram特征的频率在区间[0,1]内;

E.对步骤D计算得到的每个3-gram特征的频率$f_y(D^i)$进行离散化处理;

F.采用如下算式计算每个3-gram特征的信息熵H(X):

$$H(X)=-\sum_{i=1}^{n}p(x_i)\log(p(x_i))$$

式中$p(x_i)$为3-gram特征X的取值属于x_i区间的概率;n为对连续3-gram特征X离散化后得到的取值区间的总数;log()为取底数为2的对数操作;

G.采用如下算式计算每个3-gram特征的条件熵H(Y|X):

$H(Y|X)=\sum_{x\in X}p(x)H(Y|X=x)$

式中Y为样本标签,用于表示代码是否为恶意代码;

H.计算3-gram特征X的信息增益G(X)为G(X)=H(X)-H(Y|X);

I.得到每个3-gram特征的信息增益后,保留信息增益值最大的前若干个3-gram特征和对应的信息增益值,并将剩余的3-gram特征的信息增益值直接设置为0,从而构成最终的特征库。

3.根据权利要求2所述的基于注意力机制的恶意代码检测方法,其特征在于步骤S2所述的将步骤S1得到的恶意代码进行区块划分,具体为将恶意代码按照函数划分为若干个区块,并根据特征库去掉无用函数。

4.根据权利要求3所述的基于注意力机制的恶意代码检测方法,其特征在于步骤S4所述的构建恶意代码检测初步模型,具体为采用如下步骤构建恶意代码检测初步模型:

恶意代码检测初步模型包括输入层、第一卷积层、第一池化层、第二卷积层、第二池化层、第三卷积层、第三池化层、压缩操作层、激励操作层、全连接层和softmax函数层;

输入层:用于接收双通道恶意代码图片;

第一卷积层:用于对输入层的数据进行二维卷积,并输出到第一池化层;

第一卷积层中卷积核的大小为1*3,步长为1;

第一池化层:用于对第一卷积层输出的数据进行池化处理,从而更好的捕获局部特征;

第二卷积层:用于对第一池化层的数据进行二维卷积,并输出到第二池化层;第二卷积层中卷积核的大小为3*3,步长为1;

第二池化层:用于对第二卷积层输出的数据进行池化处理,从而更好的捕获局部特征;

第三卷积层:用于对第二池化层的数据进行二维卷积,并输出到第三池化层;第一卷积层中卷积核的大小为3*3,步长为1;

第三池化层:用于对第三卷积层输出的数据进行池化处理,从而更好的捕获局部特征;

压缩操作层:对第三池化层输出的H*W*C特征进行压缩和global average pooling,从而得到1*1*C大小的特征向量;H为特征通道的高;W为特征通道的宽;C为特征通道的数量;

激励操作层:包括两个全连接层和两个激活函数,第一全连接层的神经元个数和两个激活函数均自行设定;第二全连接层的神经元个数为C;将权重值分别和原特征通道的二维矩阵相乘,从而得到加权后的大小为H*W*C的特征,并进行扁平化处理,并输出到全连接层;

全连接层:用于对上述步骤得到的特征进行拟合;

softmax函数层:用于完成对恶意代码的识别。

基于注意力机制的恶意代码检测方法

技术领域

[0001] 本发明属于信息技术领域,具体涉及一种基于注意力机制的恶意代码检测方法。

背景技术

[0002] 随着经济技术的发展和人们生活水平的提高,由恶意代码所引发的安全问题也越来越多。根据国家互联网应急中心的报告,近几年恶意代码的数量迅速增长,恶意代码带来的威胁也日益严重。如何快速有效的检测恶意代码,成为当前信息安全不可回避的挑战之一。

[0003] 早期的恶意代码检测方法,主要是根据这些特征信息生成特征签名或者启发式规则来判断恶意代码。然而,随着恶意代码的演化,早期的检测方法并不能有效的识别恶意代码。

[0004] 近年来,随着深度学习算法的兴起,研究人员提出了不少基于深度学习的恶意代码检测模型。尽管目前基于深度学习的检测方法在一定程度上提升了恶意代码的识别率,但是深度学习主要应用于图像识别和自然语言处理方面,因此无法直接将恶意代码输入至神经网络并进行训练,而是需要首先将恶意代码转换成特征向量或者图像的形式。目前,恶意代码转换为图像的方法,通常是将其中的操作码或者字节码映射成数字作为图像中的像素值;然而,这种方法生成的图像包含信息比较单一,而且容易受到混淆的干扰,从而导致神经网络的识别率下降。

发明内容

[0005] 本发明的目的在于提供一种可靠性高、实用性好且识别效率高的基于注意力机制的恶意代码检测方法。

[0006] 本发明提供的这种基于注意力机制的恶意代码检测方法,包括如下步骤:

[0007] S1.获取恶意代码及正常程序作为基础数据,并构建特征库;

[0008] S2.将步骤S1得到的恶意代码进行区块划分;

[0009] S3.将步骤S2得到的划分后的恶意代码进行处理,从而得到双通道恶意代码图片;

[0010] S4.构建恶意代码检测初步模型;

[0011] S5.采用步骤S3得到的双通道恶意代码图片,以及步骤S1获取的正常程序,对步骤S4构建的恶意代码检测初步模型进行训练,从而得到最终的恶意代码检测模型;

[0012] S6.采用步骤S5得到的恶意代码检测模型进行恶意代码检测。

[0013] 步骤S1所述的获取恶意代码及正常程序作为基础数据,并构建特征库,具体为从采用如下步骤构建特征库:

[0014] A.获取恶意代码数据集和正常程序数据集;

[0015] B.对获取的恶意代码进行反汇编,并按照函数进行分块;

[0016] C.采用3-gram模型对每个函数内的操作码进行切分,从而得到3-gram特征;

[0017] D.采用如下算式计算每个3-gram特征的频率$f_y(D^i)$:

[0018] $$f_y(D^i)=\frac{S(D^i,y)}{\sum_{i=1}^{n}S(D^i,y)}$$

[0019] 式中D为3-gram特征集合;D^i为所有3-gram特征中的第i个特征;y为恶意代码样本;$S(D^i,y)$为样本y中特征D^i的总数;样本中每个3-gram特征的频率在区间[0,1]内;

[0020] E.对步骤D计算得到的每个3-gram特征的频率$f_y(D^i)$进行离散化处理;

[0021] F.采用如下算式计算每个3-gram特征的信息熵H(X):

[0022] $$H(X)=-\sum_{i=1}^{n}p(x_i)\log(p(x_i))$$

[0023] 式中$p(x_i)$为3-gram特征X的取值属于x_i区间的概率;n为对连续3-gram特征X离散化后得到的取值区间的总数;log()为取底数为2的对数操作;

[0024] G.采用如下算式计算每个3-gram特征的条件熵H(Y|X):

[0025] $H(Y|X)=\sum_{x\in X}p(x)H(Y|X=x)$

[0026] 式中Y为样本标签,用于表示代码是否为恶意代码;

[0027] H.计算3-gram特征X的信息增益G(X)为$G(X)=H(X)-H(Y|X)$;

[0028] I.得到每个3-gram特征的信息增益后,保留信息增益值最大的前若干个3-gram特征和对应的信息增益值,并将剩余的3-gram特征的信息增益值直接设置为0,从而构成最终的特征库。

[0029] 步骤S2所述的将步骤S1得到的恶意代码进行区块划分,具体为将恶意代码按照函数划分为若干个区块,并根据特征库去掉无用函数。

[0030] 步骤S3所述的将步骤S2得到的划分后的恶意代码进行处理,从而得到双通道恶意代码图片,具体为采用如下步骤得到双通道恶意代码图片:

[0031] a.计算每个函数内所包含的3-gram特征的信息增益总和,并删除信息增益总和为0的函数;

[0032] b.获取步骤a得到的每个函数的操作码;

[0033] c.将操作码映射到设定的整数区间,保证每一个整数代表一种操作码;

[0034] d.将每个函数中的操作码进行转换得到一维向量,将得到的一维向量进行拼接得到单通道恶意代码图片;

[0035] e.针对步骤d得到的单通道恶意代码图片,将图片中每一个像素与其之后的两个像素重新组成新的3-gram特征,并与步骤S1构建的特征库进行比较,从而得到像素所对应的新的信息增益值;

[0036] f.将步骤e得到的像素所对应的新的信息增益值与设定值yy相乘,得到像素权重值;$yy=\frac{65535}{xx}$,xx为特征库中信息增益的最大值;

[0037] g.在步骤d得到的单通道恶意代码图片上,添加一个新的图像通道,图像通道的值为对应像素的像素权重值,从而得到最终的双通道恶意代码图片。

[0038] 步骤S4所述的构建恶意代码检测初步模型,具体为采用如下步骤构建恶意代码检测初步模型:

[0039] 恶意代码检测初步模型包括输入层、第一卷积层、第一池化层、第二卷积层、第二池化层、第三卷积层、第三池化层、压缩操作层、激励操作层、全连接层和softmax函数层;

[0040] 输入层:用于接收双通道恶意代码图片;

[0041] 第一卷积层:用于对输入层的数据进行二维卷积,并输出到第一池化层;第一卷积层中卷积核的大小为1*3,步长为1;

[0042] 第一池化层:用于对第一卷积层输出的数据进行池化处理,从而更好的捕获局部特征;

[0043] 第二卷积层:用于对第一池化层的数据进行二维卷积,并输出到第二池化层;第二卷积层中卷积核的大小为3*3,步长为1;

[0044] 第二池化层:用于对第二卷积层输出的数据进行池化处理,从而更好的捕获局部特征;

[0045] 第三卷积层:用于对第二池化层的数据进行二维卷积,并输出到第三池化层;第一卷积层中卷积核的大小为3*3,步长为1;

[0046] 第三池化层:用于对第三卷积层输出的数据进行池化处理,从而更好的捕获局部特征;

[0047] 压缩操作层:对第三池化层输出的H*W*C特征进行压缩和global average pooling,从而得到1*1*C大小的特征向量;H为特征通道的高;W为特征通道的宽;C为特征通道的数量;

[0048] 激励操作层:包括两个全连接层和两个激活函数,第一全连接层的神经元个数和两个激活函数均自行设定;第二全连接层的神经元个数为C;将权重值分别和原特征通道的二维矩阵相乘,从而得到加权后的大小为H*W*C的特征,并进行扁平化处理,并输出到全连接层;

[0049] 全连接层:用于对上述步骤得到的特征进行拟合;

[0050] softmax函数层:用于完成对恶意代码的识别。

[0051] 本发明提供的这种基于注意力机制的恶意代码检测方法,使用3-gram模型处理操作码并通过计算其信息增益构建3-gram特征库,再将操作码按照函数划分成多个块,通过将这些块映射成图像中的不同行得到一个单通道图像;然后提出增加一个新的图像通道并根据3-gram特征库填入当前位置操作码的权重值,该通道可以有效的展现出恶意代码中关键的代码区域;最后针对该恶意代码图像,采用改进的识别模型进行恶意代码识别;因此,本发明方法可靠性高、实用性好且识别效率高。

附图说明

[0052] 图1为本发明方法的方法流程示意图。

[0053] 图2为本发明方法的恶意代码图片的生成过程示意图。

[0054] 图3为本发明方法的检测模型的结构示意图。

具体实施方式

[0055] 如图1所示为本发明方法的方法流程示意图:本发明提供的这种基于注意力机制的恶意代码检测方法,包括如下步骤:

[0056] S1.获取恶意代码及正常程序作为基础数据,并构建特征库;具体为从采用如下步骤构建特征库:数据来自VXHeaven等网站下载的恶意代码数据集与从portableapps等网站下载的正常程序。通过工具IDA pro对这些程序进行反汇编并按照函数将其分块,然后使用3-gram模型对每个函数内的操作码进行切分,并计算这些3-gram特征的信息增益;

[0057] A.获取恶意代码数据集和正常程序数据集;

[0058] B.对获取的恶意代码进行反汇编,并按照函数进行分块;

[0059] C.采用3-gram模型对每个函数内的操作码进行切分,从而得到3-gram特征;

[0060] D.采用如下算式计算每个3-gram特征的频率$f_y(D^i)$:

[0061] $$f_y(D^i)=\frac{S(D^i,y)}{\sum_{i=1}^{n}S(D^i,y)}$$

[0062] 式中D为3-gram特征集合;D^i为所有3-gram特征中的第i个特征;y为恶意代码样本;$S(D^i,y)$为样本y中特征D^i的总数;样本中每个3-gram特征的频率在区间[0,1]内;

[0063] E.对步骤D计算得到的每个3-gram特征的频率$f_y(D^i)$进行离散化处理(比如,采用CART算法);

[0064] F.采用如下算式计算每个3-gram特征的信息熵H(X):

[0065] $$H(X)=-\sum_{i=1}^{n}p(x_i)\log(p(x_i))$$

[0066] 式中$p(x_i)$为3-gram特征X的取值属于x_i区间的概率;n为对连续3-gram特征X离散化后得到的取值区间的总数;log()为取底数为2的对数操作;

[0067] G.采用如下算式计算每个3-gram特征的条件熵H(Y|X):

[0068] $H(Y|X)=\sum_{x\in X}p(x)H(Y|X=x)$

[0069] 式中Y为样本标签,用于表示代码是否为恶意代码;

[0070] H.计算3-gram特征X的信息增益G(X)为$G(X)=H(X)-H(Y|X)$;

[0071] I.得到每个3-gram特征的信息增益后,保留信息增益值最大的前若干个(比如800个)3-gram特征和对应的信息增益值,并将剩余的3-gram特征的信息增益值直接设置为0,从而构成最终的特征库;该步骤的目的在于使得后续模型在训练时更加关注关键的3-gram特征,信息增益值较低的3-gram特征部分来自一些常用的函数内部,它们对提升模型的准确率并没有帮助;

[0072] S2.将步骤S1得到的恶意代码进行区块划分;具体为将恶意代码按照函数划分为若干个区块,并根据特征库去掉无用函数;

[0073] S3.将步骤S2得到的划分后的恶意代码进行处理,从而得到双通道恶意代码图片(如图2所示);具体为采用如下步骤得到双通道恶意代码图片:

[0074] a.计算每个函数内所包含的3-gram特征的信息增益总和,并删除信息增益总和为0的函数;从而去掉非关键函数,减少生成图片的大小;

[0075] b.获取步骤a得到的每个函数的操作码;

[0076] c.将操作码映射到设定的整数区间(比如0～255区间),保证每一个整数代表一种操作码;

[0077] d.将每个函数中的操作码进行转换得到一维向量,将得到的一维向量进行拼接得

到单通道恶意代码图片；

[0078] e.针对步骤d得到的单通道恶意代码图片，将图片中每一个像素与其之后的两个像素重新组成新的3-gram特征，并与步骤S1构建的特征库进行比较，从而得到像素所对应的新的信息增益值；

[0079] f.将步骤e得到的像素所对应的新的信息增益值与设定值yy相乘，得到像素权重值；$yy=\frac{65535}{xx}$，xx为特征库中信息增益的最大值；

[0080] g.在步骤d得到的单通道恶意代码图片上，添加一个新的图像通道，图像通道的值为对应像素的像素权重值，从而得到最终的双通道恶意代码图片；

[0081] S4.构建恶意代码检测初步模型；具体为采用如下步骤构建恶意代码检测初步模型(如图3所示)：

[0082] 恶意代码检测初步模型包括输入层、第一卷积层、第一池化层、第二卷积层、第二池化层、第三卷积层、第三池化层、压缩操作层、激励操作层、全连接层和softmax函数层；

[0083] 输入层：用于接收双通道恶意代码图片；

[0084] 其中$W^{channel1}$表示操作码通道，$W^{channel2}$为操作码权重值通道；用如下两式表示两个通道的矩阵(其中Vec_1_i和Vec_2_i分别表示操作码通道与操作码权重通道中的每一行像素)

[0085] $W^{channel1}=[Vec\_1_1,Vec\_1_2,...,Vec\_1_n]$

[0086] $W^{channel2}=[Vec\_2_1,Vec\_2_2,...,Vec\_2_n]$

[0087] 第一卷积层：用于对输入层的数据进行二维卷积，并输出到第一池化层；第一卷积层中卷积核的大小为1*3，步长为1；

[0088] 第一池化层：用于对第一卷积层输出的数据进行池化处理，从而更好的捕获局部特征；

[0089] 第二卷积层：用于对第一池化层的数据进行二维卷积，并输出到第二池化层；第二卷积层中卷积核的大小为3*3，步长为1；

[0090] 第二池化层：用于对第二卷积层输出的数据进行池化处理，从而更好的捕获局部特征；

[0091] 第三卷积层：用于对第二池化层的数据进行二维卷积，并输出到第三池化层；第一卷积层中卷积核的大小为3*3，步长为1；

[0092] 第三池化层：用于对第三卷积层输出的数据进行池化处理，从而更好的捕获局部特征；

[0093] 间距后的向量采用如下两式进行表示：

[0094] $W_{conv}^{channel1}=[Vec\_conv1_1,Vec\_conv1_2,...,Vec\_conv1_n]$

[0095] $W_{conv}^{channel1}=[Vec\_conv2_1,Vec\_conv2_2,...,Vec\_conv2_n]$

[0096] 池化层的具体池化方法可以自行设定，比如max-pooling、K-Max Pooling、average-pooling等；移动步长和窗口大小均可自行确定；

[0097] 压缩操作层：对第三池化层输出的H*W*C特征进行压缩和global average pooling，从而得到1*1*C大小的特征向量；H为特征通道的高；W为特征通道的宽；C为特征通道的数量；

[0098] 激励操作层:包括两个全连接层和两个激活函数,第一全连接层的神经元个数和两个激活函数均自行设定;第二全连接层的神经元个数为C;将权重值分别和原特征通道的二维矩阵相乘,从而得到加权后的大小为H*W*C的特征,并进行扁平化处理,并输出到全连接层;

[0099] 全连接层:用于对上述步骤得到的特征进行拟合;

[0100] softmax函数层:用于完成对恶意代码的识别;

[0101] S5.采用步骤S3得到的双通道恶意代码图片,以及步骤S1获取的正常程序,对步骤S4构建的恶意代码检测初步模型进行训练,从而得到最终的恶意代码检测模型;

[0102] S6.采用步骤S5得到的恶意代码检测模型进行恶意代码检测。

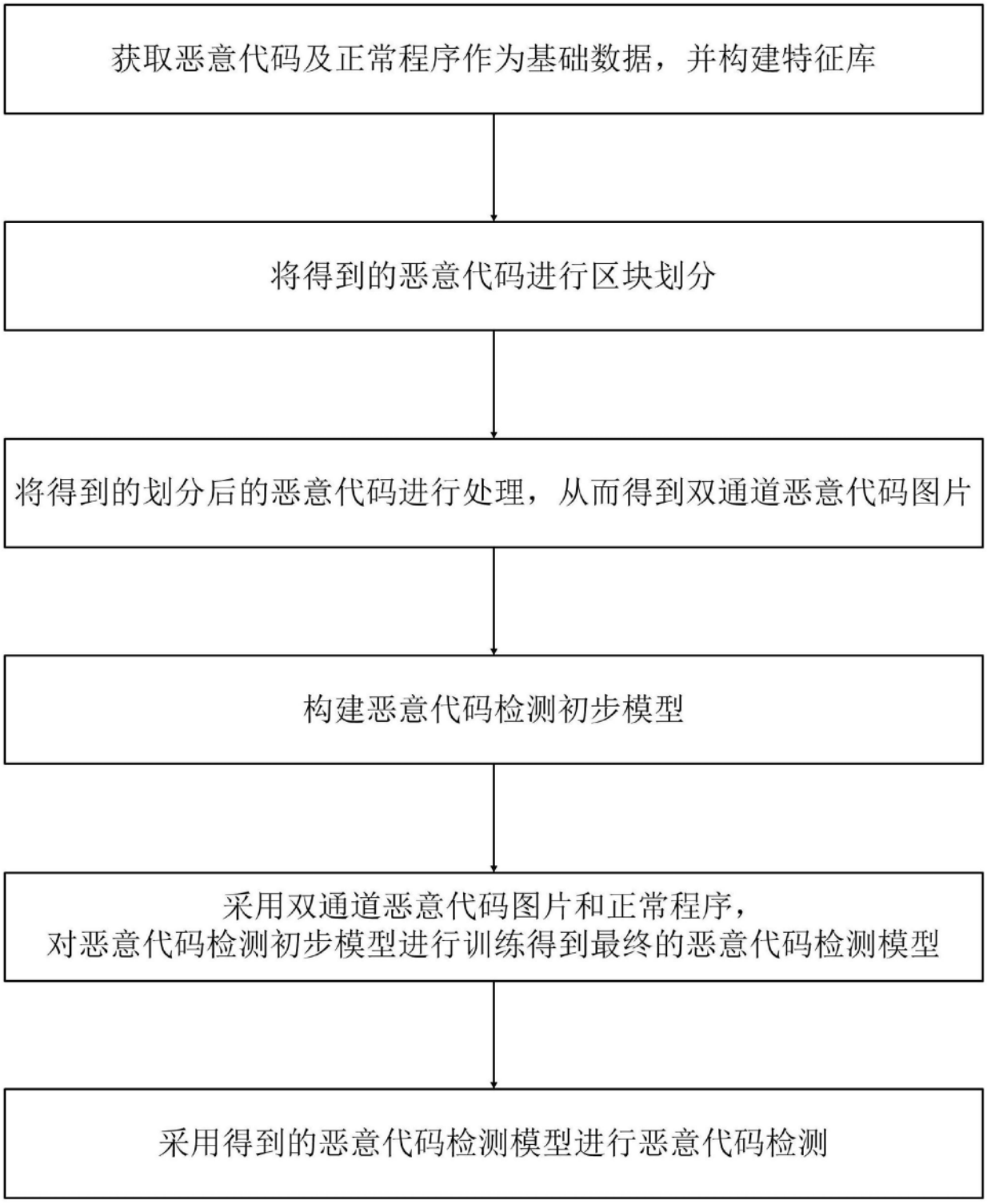

获取恶意代码及正常程序作为基础数据，并构建特征库
将得到的恶意代码进行区块划分
将得到的划分后的恶意代码进行处理，从而得到双通道恶意代码图片
构建恶意代码检测初步模型
采用双通道恶意代码图片和正常程序，
对恶意代码检测初步模型进行训练得到最终的恶意代码检测模型
采用得到的恶意代码检测模型进行恶意代码检测

图1

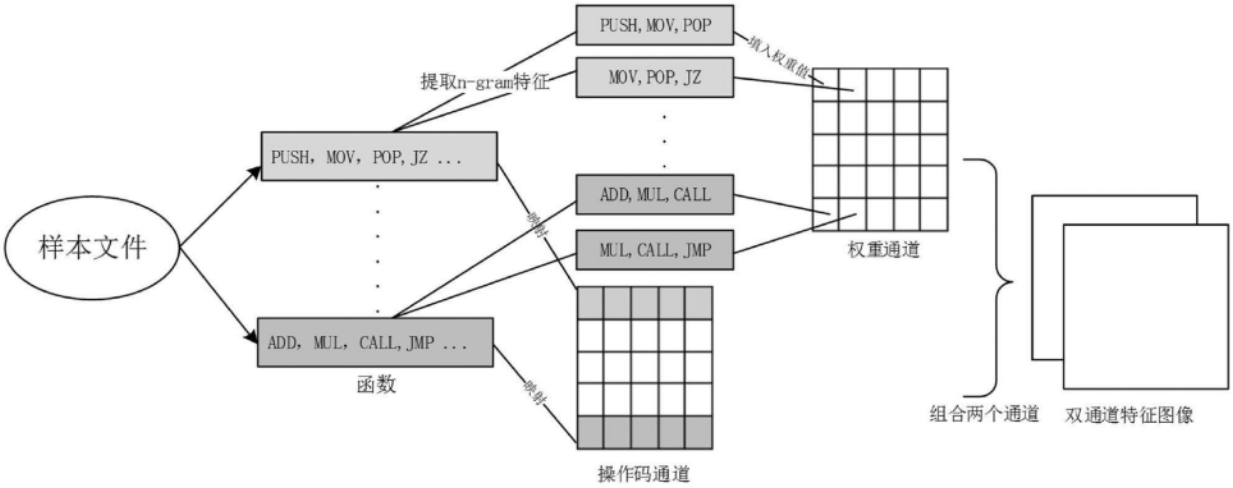

样本文件
PUSH，MOV，POP，JZ ...
ADD，MUL，CALL，JMP ...
函数
提取n-gram特征
映射
映射
PUSH, MOV, POP
MOV, POP, JZ
ADD, MUL, CALL
MUL, CALL, JMP
填入权重值
权重通道
操作码通道
组合两个通道
双通道特征图像

图2

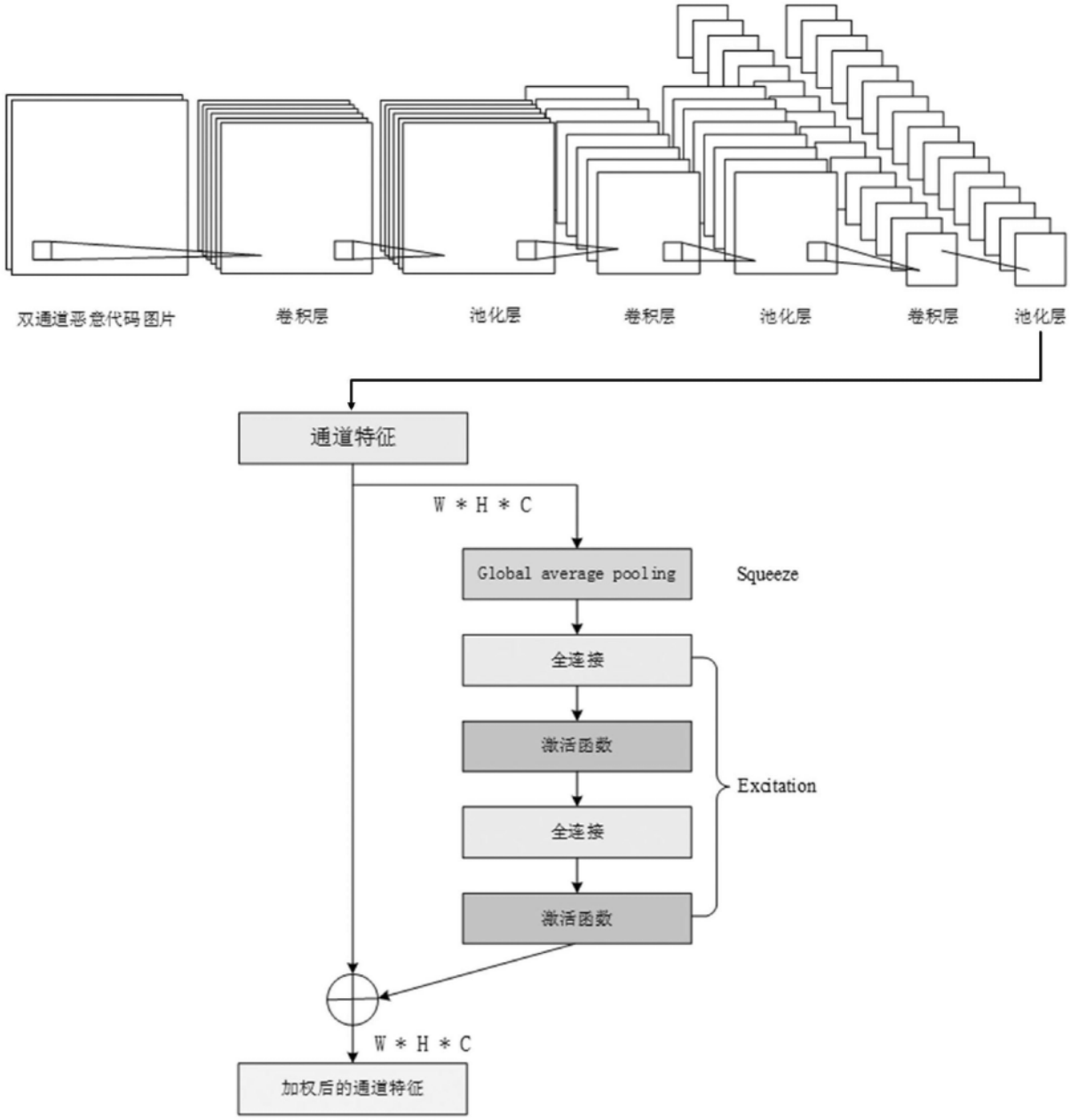

双通道恶意代码图片
卷积层
池化层
卷积层
池化层
卷积层
池化层
通道特征
W * H * C
Global average pooling
Squeeze
全连接
激活函数
全连接
激活函数
Excitation
W * H * C
加权后的通道特征

图3