

恶意文件检测方法、装置、设备及计算机可读存储介质

本申请要求于 2018 年 5 月 23 日提交中国专利局、申请号为 201810503125.4、发明名称为“恶意文件检测方法、装置、设备及计算机可读存储介质”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本发明涉及恶意软件检测技术领域，更具体地说，涉及一种恶意文件检测方法、装置、设备及计算机可读存储介质。

10 背景技术

随着互联网的发展，网络中恶意软件的数量急剧增加，严重影响了互联网用户的正常生活和工作，并造成巨大损失。为了解决这一问题，恶意软件检测产品应运而生，用于检测客户系统中潜伏的恶意软件。然而，现在业界普遍使用的基于规则或特征码的检测方案的有效性正在变得越来越低。一方面，规则和特征码只能处理已知的恶意软件，而对于未知攻击，例如“Oday”漏洞，这些检测方案的效用通常很低。另一方面，随着攻击者技术的增长，新型态的恶意软件越来越多，这极大增加了通过安全专家来人工分析恶意样本以提取新规则或特征码的难度。目前，神经网络技术为恶意软件检测提供了新的方向：一方面，神经网络具有很强的泛化能力，通过使用少量样本进行训练就可以在未知样本集达到很好的性能。另一方面，神经网络技术不再需要使用者进行复杂的特征工程，降低了对安全专家的人工分析的依赖。

但现在的基于神经网络的检测技术通常使用文件的二进制内容直接作为网络单一输入，使用通用的网络结构进行检测。而一个PE文件通常可以被分成数十甚至是上百个不同的区域，每个区域表征的信息都是不同的，并且每个区域里面的二进制数值的语义也是不同的。因此，目前将文件中所有二进制数值混杂在一起考量，会导致检测效果低下。

发明内容

本发明的目的在于提供及一种恶意文件检测方法、装置、设备及计算机可读存储介质，以提高恶意文件的检测效果。

为实现上述目的，本发明实施例提供了如下技术方案：

5 一种恶意文件检测方法，包括：

获取待检测文件；

对所述待检测文件进行解析，确定与所述待检测文件对应的二进制值，以及与每个二进制值对应的高层含义；其中，所述高层含义为二进制值的附加属性；

10 将所述待检测文件对应的二进制值，以及与每个二进制值对应的高层含义输入神经网络，通过所述神经网络对所述待检测文件进行检测；其中，所述神经网络为预先通过恶意文件集合训练生成。

其中，所述与每个二进制值对应的高层含义包括以下高层含义中的至少一者：

15 用来表征二进制值来源的高层含义，用来表征指令中二进制值的具体含义的高层含义，用来表征指令中相关二进制值在执行流中的关系的高层含义。

其中，所述第二图层包括以下至少一种图层：

20 用来表征字节来源的图层，表征指令中字节的含义的图层，表征指令相关字节在执行流中的关系的图层，表征字节的读写权限图层。

其中，所述表征字节来源的图层包括：

指令图层，数据图层，PE 头结构体图层，资源节图层。

其中，所述表征指令中字节的含义的图层包括：

操作码图层，操作数图层，位移长度图层。

25 其中，所述表征指令相关字节在执行流中的关系的图层包括：

目标指令地址图层，函数范围图层，制流图的节点范围图层。

其中，所述对所述待检测文件进行解析，确定与所述待检测文件对应的二进制值，以及与每个二进制值对应的高层含义，包括：

-3-

对所述待检测文件进行解析，将与所述待检测文件对应的二进制值作为第一图层，将与所述二进制值对应的高层含义作为第二图层；

将所述第一图层和所述第二图层组合生成与所述待检测文件的多图层图像；其中，所述第二图层中包括至少一个图层，且每个图层与每种类型的高层含义相对应。

其中，所述将所述待检测文件对应的二进制值，以及与每个二进制值对应的高层含义输入神经网络，通过所述神经网络对所述待检测文件进行检测，包括：

对所述多图层图像进行降维处理，生成降维数据；

10 将所述降维数据输入神经网络，通过所述神经网络对所述待检测文件进行检测。

其中，所述对所述多图层图像进行降维处理，生成降维数据包括：

利用无监督学习网络和/或有监督学习网络对所述多图层图像进行降维，生成降维数据。

15 一种恶意文件检测装置，包括：

获取模块，用于获取待检测文件；

确定模块，用于对所述待检测文件进行解析，确定与所述待检测文件对应的二进制值，以及与每个二进制值对应的高层含义；其中，所述高层含义为二进制值的附加属性；

20 检测模块，用于将所述待检测文件对应的二进制值，以及与每个二进制值对应的高层含义输入神经网络，通过所述神经网络对所述待检测文件进行检测；其中，所述神经网络为预先通过恶意文件集合训练生成。

其中，所述高层含义包括以下高层含义中的至少一者：用来表征二进制值来源的高层含义，用来表征指令中二进制值的具体含义的高层含义，

25 用来表征指令中相关二进制值在执行流中的关系的高层含义

其中，所述确定模块包括：

图层确定单元，用于对所述待检测文件进行解析，将与所述待检测文件对应的二进制值作为第一图层，将与所述二进制值对应的高层含义作为

-4-

第二图层；其中，所述第二图层中包括至少一个图层，且每个图层与每种类型的高层含义相对应；

多图层图像确定单元，用于将所述第一图层和所述第二图层组合生成与所述待检测文件的多图层图像。

- 5 其中，所述第二图层包括以下至少一种图层：用来表征字节来源的图层，表征指令中字节的具體含义的图层，表征指令相关字节在执行流中的关系的图层，表征字节的读写权限图层。

其中，所述表征字节来源的图层包括：指令图层，数据图层，PE 头结构体图层，资源节图层。

- 10 其中，所述表征指令中字节的具體含义的图层包括：操作码图层，操作数图层，位移长度图层。

其中，所述表征指令相关字节在执行流中的关系的图层包括：目标指令地址图层，函数范围图层，制流图的节点范围图层。

其中，所述检测模块包括：

- 15 数据降维单元，用于对所述多图层图像进行降维处理，生成降维数据；
文件检测单元，用于将所述降维数据输入神经网络，通过所述神经网络对所述待检测文件进行检测。

其中，所述数据降维单元具体用于：利用无监督学习网络和/或有监督学习网络对所述多图层图像进行降维，生成降维数据。

- 20 一种恶意文件检测设备，包括：

存储器，用于存储计算机程序；处理器，用于执行所述计算机程序时实现上述恶意文件检测方法的步骤。

一种计算机可读存储介质，所述计算机可读存储介质上存储有计算机程序，所述计算机程序被处理器执行时实现上述恶意文件检测方法的步骤。

- 25 通过以上方案可知，本发明实施例提供的一种恶意文件检测方法，包括：获取待检测文件；对所述待检测文件进行解析，确定与所述待检测文件对应的二进制值，以及与每个二进制值对应的高层含义；其中，所述高层含义为二进制值的附加属性；将所述待检测文件对应的二进制值，以及与每个二进制值对应的高层含义输入神经网络，通过所述神经网络对所述

-5-

待检测文件进行检测；可见，在本方案中，在对待检测文件进行检测时，不仅仅利用文件的二进制值，还需要利用与二进制值对应的高层含义来进行综合判别，从而实现了多种角度对文件进行判别，提高了文件检测精度以及对恶意文件的检测效果；本发明还公开了一种恶意文件检测装置、设备

5 设备及计算机可读存储介质，同样能实现上述技术效果。

附图说明

为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，

10 下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

图 1 为本发明实施例公开的一种恶意文件检测方法流程示意图；

图 2 为本发明实施例公开的一种具体的恶意文件检测方法流程示意图；

15 图；

图 3 为本发明实施例公开的具体的恶意文件检测流程图；

图 4 为本发明实施例公开的一种恶意文件检测装置结构示意图。

具体实施方式

20 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

25 本发明实施例公开了一种恶意文件检测方法、装置、设备及计算机可读存储介质，以提高恶意文件的检测效果。

参见图 1，本发明实施例提供的一种恶意文件检测方法，包括：

S101、获取待检测文件；

具体的，本方案中的待检测文件为需要判别是否是恶意文件的文件，目前现有的对待检测文件进行恶意文件判断时，仅仅根据文件的本身进行判别，也就是说，将待检测文件的二进制内容直接作为网络单一输入，并
5 使用通用的网络结构进行检测，但是这种方式没有考虑到待检测文件的高层含义，本实施例中的高层含义为每个二进制值的附加属性，例如：与二进制值对应的指令的位移、执行权限、函数范围等；因此，本方案获取待检测文件时，不仅仅获取与待检测文件对应的二进制值，还包括与每个二进制值对应的高层含义，从而能更精确的对文件进行检测。

10 S102、对所述待检测文件进行解析，确定与所述待检测文件对应的二进制值，以及与每个二进制值对应的高层含义；其中，所述高层含义为二进制值的附加属性；

在该步骤中，需要通过已知的恶意文件的结构知识，对待检测文件进行解析，提取待检测文件的特征；因为恶意文件为了实现其恶意功能，其
15 必然具有与正常文件不同的指令序列，数据以及资源等，因此他们的二进制字节序列是有差异的，因此将待检测文件的二进制值作为一个检测特征以辅助分类。进而，在本方案中还需要提取与每个二进制对应的高层含义，作为另一个检测特征以辅助分类。

具体的，二进制的高层含义可以理解为与每个字节对应的语义含义，
20 也可以称作与每个字节对应的附加属性，将待检测文件的附加属性提取出来，作为识别恶意文件的另一个标准，可以从多种角度更细致化的对文件进行检测分类；例如：如果该字节实际上对应的是指令的操作数中的位移，那么该位移变量描述了数据间的引用关系，或者指令跳转关系。相似的，指令的对应的执行权限，对应的函数范围等其他高层属性也可以提取出来。
25 需要说明的是，高层含义有很多种类型，因此本方案在选取高层含义时，并不限制其选取的数量及类型，具体的选取标准可根据实际情况进行调整。

S103、将所述待检测文件对应的二进制值，以及与每个二进制值对应的高层含义输入神经网络，通过所述神经网络对所述待检测文件进行检测；其中，所述神经网络为预先通过恶意文件集合训练生成。

-7-

最终的，确定待检测文件的特征后，即确定待检测文件的二进制值以及
与二进制值对应的高层含义之后，需要将上述特征输入至已经训练好的
神经网络，进行分类检测；该训练好的神经网络，是预先通过恶意文件训
练生成；在训练神经网络时，同样是利用恶意文件的原始二进制值及对应
5 的高层含义进行训练，训练结束后，并可使用训练好的神经网络进行恶
意文件检测。

具体来说，在该步骤中，本方案可使用 CNN 神经网络进行分类，以
识别对应的原始二进制文件是否为恶意文件。且本方案中的 CNN 神经网
络主要由卷积层，最大池化层，非线性层，全连接层等组合而成，同样的，
10 这一步也可以使用业界成熟的网络结构作为判别 CNN，例如：
Inception-Net，Google-Net，Residual-Net 等，在此并不具体限定。

可见，在本方案中，在对待检测文件进行检测时，不仅仅利用文件的
二进制值，还需要利用与二进制值对应的高层含义来进行综合判别，从而
实现了多种角度多层次的对文件进行判别，提高了文件检测精度以及对恶
15 意文件的检测效果。

基于上述方法实施例，在本实施例中，S101 中对待检测文件进行解析，
确定与待检测文件对应的二进制值，以及与每个二进制值对应的高层含义，
具体包括：

20 对所述待检测文件进行解析，将与所述待检测文件对应的二进制值作
为第一图层，将与所述二进制值对应的高层含义作为第二图层；

将所述第一图层和所述第二图层组合生成与所述待检测文件的多图层
图像；其中，所述第二图层中包括至少一个图层，且每个图层与每种类型
的高层含义相对应。

25 具体的，在本实施例中，在确定待检测文件对应的二进制值，以及与
每个二进制值对应的高层含义时，具体可以将每种类型的特征作为一个单
独的图层，也就是构建一个多图层的图像，图像中的每一层来表征了二进
制文件中每个字节的属性，进而通过丰富的属性图层来辅助分类。

首先，将每个字节的原始的二进制值作为单独一个图层，也就是本方案中的第一图层，因为恶意文件为了实现恶意功能，其必然具有与正常文件不同的指令序列，数据以及资源等，彼此的二进制字节序列是有差异的，因此可以作为一个图层特征辅助分类。进而，每种类型的高层含义也提取出来进行编码作为单独的图层。

需要说明的是，本方案中的与每个二进制值对应的高层含义包括以下高层含义中的至少一者：用来表征二进制值来源的高层含义，用来表征指令中二进制值的具体含义的高层含义，用来表征指令中相关二进制值在执行流中的关系的高层含义。因此，本方案中的第二图层包括与以上高层含义对应的至少一种图层，具体来说，本方案中的第二图层包括以下至少一种图层，且每个图层中的每个高层含义均与二进制图层的二进制值相对应：

1、用来表征字节来源的图层，具体包括以下图层：

1) 指令图层：表示对应字节是否为指令；2) 数据图层：表示对应字节是否为数据；3) PE 头结构体图层：表示对应字节是否为 PE 头结构；4) 资源节图层：表示对应字节是否为资源数据。

2、表征指令中字节的含义的图层，具体包括以下图层：

1) 操作码图层：表示对应字节是否为指令操作码，以及是什么操作；2) 操作数图层：表示对应字节是否为指令操作数，以及值是什么；3) 位移长度图层：表示对应字节是否表征跳转位移，以及位移长度是多少。

3、表征指令相关字节在执行流中的关系的图层，具体包括以下图层：

1) 目标指令地址图层：表示对应字节是否属于分支指令，以及目标指令的位置；2) 函数范围图层：表示哪些指令相关字节属于同一个函数；3) 制流图的节点范围图层：表示哪些字节属于同一个控制流图中的节点。

4、表征字节的其他特征的图层，例如：字节的读写权限图层：表示每个字节的读写权限。

可以理解的是，本实施例中的第一图层，是待检测文件的原始二进制值的图层，第二图层是与原始二进制值对应的高级含义的图层，但是第二图层的层数是根据选取高级含义的类型数量决定的；例如：选取高级含义

的类型共三种，那么第二图层则包括第一种类型的图层、第二种类型的图层以及第三种类型的图层。

参见图 2，本发明实施例提供的一种具体的恶意文件检测方法，在本
5 实施例中的 S201-S203 已在上述实施例中进行解释说明，在此便不具体赘述，仅对 S204-S205 进行解释；该恶意文件检测方法具体包括：

S201、获取待检测文件；

S202、对所述待检测文件进行解析，将与所述待检测文件对应的二进制值作为第一图层，将与所述二进制值对应的高层含义作为第二图层；

10 S203、将所述第一图层和所述第二图层组合生成与所述待检测文件的多图层图像；其中，每个类型的高层含义单独作为一个第二图层；

S204、对所述多图层图像进行降维处理，生成降维数据；

S205、将所述降维数据输入神经网络，通过所述神经网络对所述待检测文件进行检测；其中，所述神经网络为预先通过恶意文件集合训练生成。

15 参见图 3，为本实施例提供的一具体的恶意文件检测流程图，通过图 3 可以看出，本方案需要通过构建多图层图像、降采样神经网络以及判别 CNN (Convolutional Neural Network, 卷积神经网络) 这三个步骤对恶意文件进行检测。在本实施例中，主要对降采样神经网络进行介绍。需要说明的是，由于二进制文件过大的尺寸，会导致其不适合直接用作分类网络的输入；因此在本实施例中，为了解决处理大文件时计算效率低下的问题，
20 在得到多图层图像之后，需要利用降采样神经网络对图像进行降维，以降低后续分类网络的输入尺寸，从而提高计算效率。具体来说，本方案使用两种降维方式来对多层图像进行降维，也就是说，本方案对多图层图像进行降维处理，生成降维数据时，具体包括：利用无监督学习网络和/或有监督学习网络对所述多图层图像进行降维，生成降维数据。
25

具体的，无监督网络不需要对数据进行标记，对于给定的输入集合，能够直接学习到一种有效的编码格式，例如 autoencoder 及其变种。我们通过卷积层，池化层及全连接层等几类结层结构为基础设计了我们的无监督网络。通过训练无监督网络，他们的输出直接提供降维后的编码。同时，

- 10 -

本方案还可以使用有监督学习网络对数据进行降维。因为神经网络的高层特征尺寸远小于输入的尺寸，所以我们利用高层特征作为降维后的结果。

为此，我们训练了一个结构简单，能够接受大尺寸输入的 CNN

（Convolutional Neural Network，卷积神经网络）。由于该 CNN 的主要目的是降维，我们使用卷积层，以及多种池化层组合成了我们的降维 CNN。

可以理解的是，如果本方案需要通过无监督学习网络和/或有监督学习网络对多图层图像进行降维处理，则需要预先通过恶意文件对无监督学习网络和/或有监督学习网络进行训练，以备后续使用。可以看出，本方案通过将得到的多图层图像进行降维处理后，再输入至 CNN 神经网络进行识别检测，可以更加高效的识别完整的二进制文件。

下面对本发明实施例提供的恶意文件检测装置进行介绍，下文描述的恶意文件检测装置与上文描述的恶意文件检测方法可以相互参照。

参见图 4，本发明实施例提供一种恶意文件检测装置，包括：

15 获取模块 100，用于获取待检测文件；

确定模块 200，用于对所述待检测文件进行解析，确定与所述待检测文件对应的二进制值，以及与每个二进制值对应的高层含义；其中，所述高层含义为二进制值的附加属性；

20 检测模块 300，用于将所述待检测文件对应的二进制值，以及与每个二进制值对应的高层含义输入神经网络，通过所述神经网络对所述待检测文件进行检测；其中，所述神经网络为预先通过恶意文件集合训练生成。

其中，所述高层含义包括以下高层含义中的至少一者：用来表征二进制值来源的高层含义，用来表征指令中二进制值的具体含义的高层含义，用来表征指令中相关二进制值在执行流中的关系的高层含义。

25 其中，所述确定模块包括：

图层确定单元，用于对所述待检测文件进行解析，将与所述待检测文件对应的二进制值作为第一图层，将与所述二进制值对应的高层含义作为第二图层；其中，所述第二图层中包括至少一个图层，且每个图层与每种类型的高层含义相对应；

多图层图像确定单元，用于将所述第一图层和所述第二图层组合生成与
所述待检测文件的多图层图像。

其中，所述第二图层包括以下至少一种图层：用来表征字节来源的图
层，表征指令中字节的含义的图层，表征指令相关字节在执行流中的
5 关系的图层，表征字节的读写权限图层。

其中，所述表征字节来源的图层包括：指令图层，数据图层，PE 头结
构体图层，资源节图层。

其中，所述表征指令中字节的含义的图层包括：操作码图层，操
作数图层，位移长度图层。

10 其中，所述表征指令相关字节在执行流中的关系的图层包括：目标指
令地址图层，函数范围图层，制流图的节点范围图层。

其中，所述检测模块包括：

数据降维单元，用于对所述多图层图像进行降维处理，生成降维数据；

文件检测单元，用于将所述降维数据输入神经网络，通过所述神经网
15 络对所述待检测文件进行检测。

其中，所述数据降维单元具体用于：利用无监督学习网络和/或有监督
学习网络对所述多图层图像进行降维，生成降维数据。

本发明实施例还提供一种恶意文件检测设备，包括：存储器，用于存
储计算机程序；处理器，用于执行所述计算机程序时实现如上述恶意文件
20 检测方法的步骤。

本发明实施例还提供一种计算机可读存储介质，所述计算机可读存储
介质上存储有计算机程序，所述计算机程序被处理器执行时实现如上述恶
意文件检测方法的步骤。

具体的，该存储介质可以包括：U 盘、移动硬盘、只读存储器（Read-Only
25 Memory，ROM）、随机存取存储器（Random Access Memory，RAM）、
磁碟或者光盘等各种可以存储程序代码的介质。

综上所述，在本方案公开了一种恶意文件检测方法、装置、设备及计
算机可读存储介质中，在对待检测文件进行检测时，不仅仅利用文件的二
进制值，还需要利用与二进制值对应的高层含义来进行综合判别，从而实

— 12 —

现了多种角度对文件进行判别，提高了文件检测精度以及对恶意文件的检测效果；并且，在得到包括二进制值以及对应的高层含义的多图层图像之后，通过神经网络对其进行降维处理，可以提高检测效率。

本说明书中各个实施例采用递进的方式描述，每个实施例重点说明的
5 都是与其他实施例的不同之处，各个实施例之间相同相似部分互相参见即可。

对所公开的实施例的上述说明，使本领域专业技术人员能够实现或使用
10 本发明。对这些实施例的多种修改对本领域的专业技术人员来说将是显而易见的，本文中所定义的一般原理可以在不脱离本发明的精神或范围的情况下，在其它实施例中实现。因此，本发明将不会被限制于本文所示的这些实施例，而是要符合与本文所公开的原理和新颖特点相一致的最宽的范围。

权 利 要 求

- 1、一种恶意文件检测方法，其特征在于，包括：
获取待检测文件；
对所述待检测文件进行解析，确定与所述待检测文件对应的二进制值，
5 以及与每个二进制值对应的高层含义；其中，所述高层含义为二进制值的附加属性；
将所述待检测文件对应的二进制值，以及与每个二进制值对应的高层含义输入神经网络，通过所述神经网络对所述待检测文件进行检测；其中，所述神经网络为预先通过恶意文件集合训练生成。
- 10 2、根据权利要求 1 所述的恶意文件检测方法，其特征在于，所述与每个二进制值对应的高层含义包括以下高层含义中的至少一者：
用来表征二进制值来源的高层含义，用来表征指令中二进制值的具体含义的高层含义，用来表征指令中相关二进制值在执行流中的关系的高层含义。
- 15 3、根据权利要求 1 所述的恶意文件检测方法，其特征在于，所述对所述待检测文件进行解析，确定与所述待检测文件对应的二进制值，以及与每个二进制值对应的高层含义，包括：
对所述待检测文件进行解析，将与所述待检测文件对应的二进制值作为第一图层，将与所述二进制值对应的高层含义作为第二图层；
20 将所述第一图层和所述第二图层组合生成与所述待检测文件的多图层图像；其中，所述第二图层中包括至少一个图层，且每个图层与每种类型的高层含义相对应。
- 4、根据权利要求 3 所述的恶意文件检测方法，其特征在于，所述第二图层包括以下至少一种图层：
25 用来表征字节来源的图层，表征指令中字节的具体含义的图层，表征指令相关字节在执行流中的关系的图层，表征字节的读写权限图层。
- 5、根据权利要求 4 所述的恶意文件检测方法，其特征在于，所述表征字节来源的图层包括：
指令图层，数据图层，PE 头结构体图层，资源节图层。

6、根据权利要求4所述的恶意文件检测方法，其特征在于，所述表征指令中字节的具体含义的图层包括：

操作码图层，操作数图层，位移长度图层。

7、根据权利要求4所述的恶意文件检测方法，其特征在于，所述表征指令相关字节在执行流中的关系的图层包括：

目标指令地址图层，函数范围图层，制流图的节点范围图层。

8、根据权利要求3所述的恶意文件检测方法，其特征在于，所述将所述待检测文件对应的二进制值，以及与每个二进制值对应的高层含义输入神经网络，通过所述神经网络对所述待检测文件进行检测，包括：

10 对所述多图层图像进行降维处理，生成降维数据；

将所述降维数据输入神经网络，通过所述神经网络对所述待检测文件进行检测。

9、根据权利要求8所述的恶意文件检测方法，其特征在于，所述对所述多图层图像进行降维处理，生成降维数据包括：

15 利用无监督学习网络和/或有监督学习网络对所述多图层图像进行降维，生成降维数据。

10、一种恶意文件检测装置，其特征在于，包括：

获取模块，用于获取待检测文件；

20 确定模块，用于对所述待检测文件进行解析，确定与所述待检测文件对应的二进制值，以及与每个二进制值对应的高层含义；其中，所述高层含义为二进制值的附加属性；

检测模块，用于将所述待检测文件对应的二进制值，以及与每个二进制值对应的高层含义输入神经网络，通过所述神经网络对所述待检测文件进行检测；其中，所述神经网络为预先通过恶意文件集合训练生成。

25 11、根据权利要求10所述的恶意文件检测装置，其特征在于，

所述高层含义包括以下高层含义中的至少一者：用来表征二进制值来源的高层含义，用来表征指令中二进制值的具体含义的高层含义，用来表征指令中相关二进制值在执行流中的关系的高层含义。

12、根据权利要求 10 所述的恶意文件检测装置，其特征在于，所述确定模块包括：

5 图层确定单元，用于对所述待检测文件进行解析，将与所述待检测文件对应的二进制值作为第一图层，将与所述二进制值对应的高层含义作为第二图层；其中，所述第二图层中包括至少一个图层，且每个图层与每种类型的高层含义相对应；

多图层图像确定单元，用于将所述第一图层和所述第二图层组合生成与所述待检测文件的多图层图像。

10 13、根据权利要求 12 所述的恶意文件检测装置，其特征在于，所述第二图层包括以下至少一种图层：用来表征字节来源的图层，表征指令中字节的具体含义的图层，表征指令相关字节在执行流中的关系的图层，表征字节的读写权限图层。

14、根据权利要求 13 所述的恶意文件检测装置，其特征在于，所述表征字节来源的图层包括：指令图层，数据图层，PE 头结构体图层，资源节
15 图层。

15、根据权利要求 13 所述的恶意文件检测装置，其特征在于，所述表征指令中字节的具体含义的图层包括：操作码图层，操作数图层，位移长度图层。

16、根据权利要求 13 所述的恶意文件检测装置，其特征在于，所述表征指令相关字节在执行流中的关系的图层包括：目标指令地址图层，函数范围图层，制流图的节点范围图层。
20

17、根据权利要求 12 所述的恶意文件检测装置，其特征在于，所述检测模块包括：

25 数据降维单元，用于对所述多图层图像进行降维处理，生成降维数据；
文件检测单元，用于将所述降维数据输入神经网络，通过所述神经网络对所述待检测文件进行检测。

18、根据权利要求 17 所述的恶意文件检测装置，其特征在于，所述数据降维单元具体用于：利用无监督学习网络和/或有监督学习网络对所述多图层图像进行降维，生成降维数据。

- 16 -

19、一种恶意文件检测设备，其特征在于，包括：

存储器，用于存储计算机程序；

处理器，用于执行所述计算机程序时实现如权利要求 1 至 9 任一项所述恶意文件检测方法的步骤。

- 5 20、一种计算机可读存储介质，其特征在于，所述计算机可读存储介质上存储有计算机程序，所述计算机程序被处理器执行时实现如权利要求 1 至 9 任一项所述恶意文件检测方法的步骤。