

一种网页篡改检测方法及相关装置

本申请要求于 2019 年 1 月 25 日提交中国专利局、申请号为 201910075454.8、发明名称为“一种网页篡改检测方法及相关装置”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。

5 技术领域

本申请涉及网路安全技术领域，更具体地说，涉及一种网页篡改检测方法、系统、装置及计算机可读存储介质。

背景技术

- 10 随着网络的发展，人们已习惯通过上网浏览各个网站提供的网页来获取信息。网站都会在搜索引擎中有排名，黑客为了提高恶意网站的排名，会通过黑帽搜索引擎优化的方式来实现，黑帽搜索引擎优化是指使用作弊手段欺骗搜索引擎，从而非法提升恶意网站在搜索引擎中的排名。而网页篡改时黑帽搜索引擎优化的常见手段，黑客入侵一批高权重的合法网站，
- 15 篡改其网页内容，插入恶意文本，如博彩广告等，或者插入恶意链接指向恶意网站。网页篡改可以增加恶意网站在搜索引擎中的排名，为恶意网站获取更多的流量。但是，这会降低合法网站在搜索引擎的排名，给其造成巨大的经济损失，同时也会影响企业的形象。

- 20 目前主流安全厂商都提供了对网页篡改的检测，其检测技术主要是基于关键词匹配。即预先确定恶意关键词，然后检测网页中是否有恶意关键词，并结合恶意关键词的统计特征和联合概率分布来判定网页是否被篡改。

但是这种检测手段比较单一，无法应对未收录恶意关键词，对新型篡改网页的检测能力差。

- 25 因此，如何提高网页篡改检测能力，是本领域技术人员需要解决的问题。

发明内容

有鉴于此，本申请的目的在于提供一种网页篡改检测方法、系统、装置及计算机可读存储介质，以解决如何提高网页篡改检测能力的问题。

为实现上述目的，本申请实施例提供了一种网页篡改检测方法，包括：
解析待检测网页得到对应待检测网页的标签信息，将所述标签信息作

5 为待检测信息；

在所述待检测信息中提取篡改特征信息；

利用深度学习模型对所述篡改特征信息进行计算，得到所述待检测网页的篡改检测结果；其中，所述深度学习模型为预先利用与所述篡改特征信息对应的训练样本进行训练得到的深度学习模型。

10 可选地，所述在所述待检测信息中提取篡改特征信息之前，还包括：
判断所述标签信息的文本信息中是否包括预设敏感词；

若是，则执行所述在所述待检测信息中提取篡改特征信息的步骤；

若否，则确定所述待检测网页的篡改检测结果为未被篡改。

15 可选地，所述判断所述标签信息的文本信息中是否包括预设敏感词，
包括：

利用预设规则对所述标签信息的文本信息进行匹配，判断所述标签信息中是否包括满足所述预设规则的词；其中所述预设规则对应预设敏感词，每条所述预设规则中包括预设敏感词的核心敏感词与所述核心敏感词之间的关系。

20 可选地，所述利用预设规则对所述标签信息的文本信息进行匹配，判断所述标签信息中是否包括满足所述预设规则的词之前，还包括：

判断所述标签信息是否包括所述核心敏感词；

若是，则执行所述利用预设规则对所述标签信息的文本信息进行匹配，判断所述标签信息中是否包括满足所述预设规则的词；

25 若否，则确定所述待检测网页的篡改检测结果为未被篡改。

可选地，所述篡改特征信息包括：

对所述标签信息的文本信息进行情感分析的结果和/或对所述标签信息的文本信息进行语义分析的结果和/或对所述标签信息的链接信息的可疑性检测结果和/或专家预设篡改特征。

可选地, 所述利用深度学习模型对所述篡改特征信息进行计算, 得到所述待检测网页的篡改检测结果, 包括:

将至少两个深度学习模型作为弱分类器对所述篡改特征信息进行计算, 得到对应每个弱分类器的计算结果;

5 集成学习每个所述计算结果得到所述待检测网页的篡改结果。

可选地, 当所述篡改特征信息包括至少两种时, 所述至少两个深度学习模型包括:

分别利用一种所述篡改特征信息的训练样本进行训练, 得到的对应每种篡改特征信息的深度学习模型;

10 对应的, 所述将至少两个深度学习模型作为弱分类器对所述篡改特征信息进行计算, 得到对应每个弱分类器的计算结果, 包括:

将至少两个所述深度学习模型作为弱分类器分别对与每种所述深度学习模型对应的所述篡改特征信息进行计算, 得到计算结果。

15 可选地, 当所述篡改特征信息包括一种篡改特征信息时, 所述至少两个深度学习模型包括:

利用至少两种训练算法对所述篡改特征信息的训练样本进行训练得到的对应每种训练算法的深度学习模型;

对应的, 所述将至少两个深度学习模型作为弱分类器对所述篡改特征信息进行计算, 得到对应每个弱分类器的计算结果, 包括:

20 将至少两个深度学习模型作为弱分类器对同一种所述篡改特征信息进行计算, 得到对应每个弱分类器的计算结果。

可选地, 所述在所述待检测信息中提取篡改特征信息之前, 还包括:

获取所述待检测网页中的图片;

25 识别所述图片中的文本信息, 将所述图片中的文本信息作为待检测信息。

可选地, 所述在所述待检测信息中提取篡改特征信息之前, 还包括:

解析执行所述待检测网页中的JavaScript代码, 以跳转到所述JavaScript代码对应的目标页面;

解析所述目标页面得到对应所述目标页面的目标标签信息, 将所述目

标标签信息作为待检测信息。

为实现上述目的，本申请还提供了一种网页篡改检测系统，包括：

待检测网页解析模块，用于解析待检测网页得到对应待检测网页的标签信息，将所述标签信息作为待检测信息；

- 5 待检测信息特征提取模块，用于在所述待检测信息中提取篡改特征信息；

计算模块，用于利用深度学习模型对所述篡改特征信息进行计算，得到所述待检测网页的篡改检测结果；其中，所述深度学习模型为预先利用与所述篡改特征信息对应的训练样本进行训练得到的深度学习模型。

- 10 可选地，该系统还包括：

预设敏感词检测模块，用于判断所述标签信息的文本信息中是否包括预设敏感词；若是，则启动所述待检测信息特征提取模块对应的工作流程；若否，则确定所述待检测网页的篡改检测结果为未被篡改。

- 15 可选地，所述预设敏感词检测模块具体为用于利用预设规则对所述标签信息的文本信息进行匹配，判断所述标签信息中是否包括满足所述预设规则的词的模块；

其中，所述预设规则对应预设敏感词，每条所述预设规则中包括预设敏感词的核心敏感词与所述核心敏感词之间的关系。

可选地，该系统还包括：

- 20 核心敏感词检测模块，用于判断所述标签信息是否包括所述核心敏感词；若是，则启动所述预设敏感词检测模块对应的工作流程；若否，则确定所述待检测网页的篡改检测结果为未被篡改。

可选地，所述计算模块包括：

- 25 计算单元，用于将至少两个深度学习模型作为弱分类器对所述篡改特征信息进行计算，得到对应每个所述弱分类器的计算结果；

集成学习单元，用于集成学习每个所述计算结果得到所述待检测网页的篡改结果。

可选地，当所述篡改特征信息包括至少两种时，所述至少两个深度学习模型包括：

分别利用一种所述篡改特征信息的训练样本进行训练，得到的对应每种篡改特征信息的深度学习模型；

对应的，所述计算单元具体用于将至少两个所述深度学习模型作为弱分类器分别对与每种所述深度学习模型对应的所述篡改特征信息进行计算，得到计算结果。

可选地，当所述篡改特征信息包括至少两种时，所述至少两个深度学习模型包括：

利用至少两种训练算法对所述篡改特征信息的训练样本进行训练得到的对应每种训练算法的深度学习模型；

10 对应的，所述计算单元具体用于将至少两个深度学习模型作为弱分类器对同一种所述篡改特征信息进行计算，得到对应每个所述弱分类器的计算结果。

可选地，该系统还包括：

图片获取模块，用于获取所述待检测网页中的图片；

15 图片文本信息识别模块，用于识别所述图片中的文本信息，将所述图片中的文本信息作为待检测信息。

为实现上述目的，本申请还提供了一种网页篡改检测装置，包括：

存储器，用于存储计算机程序；

20 处理器，用于执行所述计算机程序时实现如任一项所述网页篡改检测方法步骤。

为实现上述目的，本申请还提供了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任一项所述网页篡改检测方法的步骤。

25 通过以上方案可知，本申请提供的一种网页篡改检测方法，包括：解析待检测网页得到对应待检测网页的标签信息，将所述标签信息作为待检测信息；在所述待检测信息中提取篡改特征信息；利用深度学习模型对所述篡改特征信息进行计算，得到所述待检测网页的篡改检测结果；其中，所述深度学习模型为预先利用与所述篡改特征信息对应的训练样本进行训练得到的深度学习模型。

由此可见，本申请提供一种网页篡改检测方法，首先解析待检测网页得到对应的标签信息，对标签信息进行篡改特征提取，得到篡改特征信息，并用深度学习模型对篡改特征信息进行计算，得到篡改检测结果。由于本方案中利用深度学习模型和待检测网页中的篡改特征信息对该网页进行篡改检测，而深度学习模型由于是根据篡改特征对应的训练样本训练出的模型，在计算过程中不是简单的匹配，而是具有一定的联想能力，当篡改特征信息与训练模型不完全相同时也可以得到更准确的检测结果，从而提高网页检测能力。

10 **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，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 为本申请实施例公开的一种网页篡改检测方法流程图；
- 图 2 为本申请实施例公开的一种具体的网页篡改检测方法流程图；
- 图 3 为本申请实施例公开的一种具体的网页篡改检测方法流程图；
- 图 4 为本申请实施例公开的一种具体的网页篡改检测方法流程图；
- 图 5 为本申请实施例公开的一种网页篡改检测系统结构示意图；
- 图 6 为本申请实施例公开的一种网页篡改检测装置结构示意图。

具体实施方式

下面将结合本申请实施例中的附图，对本申请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申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，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，都属于本申请保护的范围。

本申请实施例公开了一种网页篡改检测方法、系统、装置及计算机可读存储介质，以解决如何提高网页篡改检测能力的问题。

参见图1，本申请实施例提供的一种网页篡改检测方法，具体包括：

5 S101，解析待检测网页得到对应待检测网页的标签信息，将所述标签信息作为待检测信息。

具体地，首先确定待检测网页，并解析待检测网页中的标签信息，将标签信息作为待检测信息。

需要说明的是，网页的本质其实为HTML（超文本标记语言），对于HTML网页中是用多种标签来定义不同信息，例如标签<title>定义了文档的标题，<link>定义了一个文档和外部资源之间的关系。

10 在本步骤中，首先需要解析网页的DOM结构，提取title、超链接、正文等标签信息。需要说明的是，DOM（Document Object Model，文档对象模型），可以以一种独立于平台和语言的方式访问和修改一个文档的内容和结构，换句话说，这是表示和处理一个HTML或XML文档的常用方法。

15 S102，在所述待检测信息中提取篡改特征信息。

具体地，在检测信息中心提取篡改特征信息，篡改特征信息即用于标识网页被篡改的特征信息。

20 在本方案中，为了检测更加全面，使检测结果更加可靠，作为优选的，在待检测信息中提取至少两种篡改特征信息，也就是说，提取多维特征信息以进行后续的检测。

S103，利用深度学习模型对所述篡改特征信息进行计算，得到所述待检测网页的篡改检测结果；其中，所述深度学习模型为预先利用与所述篡改特征信息对应的训练样本进行训练得到的深度学习模型。

25 在本方案中，预先确定与篡改特征信息对应的训练模型，并对模型进行深度学习训练，从而得到深度学习模型，然后再利用深度学习模型对上述篡改特征信息进行计算，得到网页检测结果。

在一个优选的实施方式中，为了使检测结果更加准确，所述利用深度学习模型对所述篡改特征信息进行计算，得到所述待检测网页的篡改检测结果，包括：

将至少两个深度学习模型作为弱分类器对所述篡改特征信息进行计算，得到对应每个弱分类器的计算结果；

集成学习每个所述计算结果得到所述待检测网页的篡改结果。

在本方案中，将至少两个深度学习模型作为集成学习的弱分类器，从而利用至少两个深度学习模型对上述步骤提取到的篡改特征信息进行计算，可以综合每个深度学习模型的计算效果，来综合决策待检测网页的被篡改情况，使可以提高检测的准确性。

此外，每个深度学习模型在训练时，都需要避免过拟合的问题，即避免使模型使用过多参数过于复杂，从而使模型只适用当前训练数据，却不能适用其他数据的问题，而本方案中模型包括至少两个深度学习模型，即便其中一个出现了过拟合问题，而其他没有出现过拟合的深度学习模型也可以减轻整体模型的过拟合问题，从而可以较大程度上忽略单个弱分类器的过拟合问题，使整个模型的泛化能力更高，也就是说，使整个模型能够更容易的适应不同的数据。

需要说明的是，集成学习是使用一系列学习器进行学习，并使用某种规则把各个学习结果进行整合从而获得比单个学习器更好的学习效果的一种机器学习方法。

在本方案中，集成学习每个深度学习模型得到的计算结果，综合每个深度学习模型的计算效果，从而使整体检测结果的准确性更高。需要说明的是，整合每个深度学习模型的计算结果的具体规则在本方案中不做具体限定。

由于深度学习模型包括至少两个，因此，深度学习模型可以是对应每种特征都训练一个深度学习模型，即一种特征对应一个深度学习模型，也可以是利用至少两个算法对所有特征进行训练得到与每个算法对应的弱分类器，即一种算法对应一个深度学习模型。

因此，在一个具体的实施方式中，当所述篡改特征信息包括至少两种时，所述至少两个深度学习模型包括：

分别利用一种所述篡改特征信息的训练样本进行训练，得到的对应每种篡改特征信息的深度学习模型；

对应的，所述将至少两个深度学习模型作为弱分类器对所述篡改特征信息进行计算，得到对应每个弱分类器的计算结果，包括：

将至少两个所述深度学习模型作为弱分类器分别对与每种所述深度学习模型对应的所述篡改特征信息进行计算，得到计算结果。在本方案中，
5 每个深度学习模型的训练样本均与每种篡改特征的种类一致，也就是说，一个深度学习模型对应一种篡改特征信息，当有多个篡改特征信息时，也就对应多个深度学习模型。在进行计算时，利用与篡改特征信息对应的深度学习模型来计算相应的篡改特征信息，从而对于每个篡改特征信息来说，由于深度学习模型是针对自己训练得到的，所以深度学习模型对自己
10 进行计算更加适合，从而对自己进行计算的准确率也就相对较高。同样地，由于最终要结合多种篡改特征信息来更加全面的决策当前待检测网页的篡改检测结果，要对每一种深度学习模型计算出的计算结果进行集成学习，得到最终的篡改结果。

需要说明的是，本方案中，对每种篡改特征的训练数据进行训练时，
15 可以采用相同的算法，也可以采用不同的算法。

在另一个具体的实施方式中，当所述篡改特征信息包括一种篡改特征信息时，所述至少两个深度学习模型包括：

利用至少两种训练算法对所述篡改特征信息的训练样本进行训练得到的对应每种训练算法的深度学习模型；

20 对应的，所述将至少两个深度学习模型作为弱分类器对所述篡改特征信息进行计算，得到对应每个弱分类器的计算结果，包括：

将至少两个深度学习模型作为弱分类器对同一种所述篡改特征信息进行计算，得到对应每个弱分类器的计算结果。

在本方案中，确定篡改特征信息对应的训练样本，利用不同的算法，
25 如TextCNN，SVM等，分别对训练样本进行训练，得到对应不同算法的深度学习模型，由于每个算法都会有自己的长处也有自己短处，利用不同算法对应的不同的深度学习模型分别对所有的篡改特征信息进行计算，再集成学习所有的计算结果，可以博采众长，综合得到更准确的待检测网页的篡改检测结果。

需要说明的是，篡改检测结果一般是篡改程度的百分比，具体篡改结果以什么形式表现可以根据具体的弱分类器来确定，在本方案中不做具体限定。

由此可见，本申请提供一种网页篡改检测方法，首先解析待检测网页得到对应的标签信息，对标签信息进行篡改特征提取，得到篡改特征信息，并用深度学习模型对篡改特征信息进行计算，得到篡改检测结果。由于本方案中利用深度学习模型和待检测网页中的篡改特征信息对该网页进行篡改检测，而深度学习模型在计算过程中不是简单的匹配，而是根据训练特征具有一定的联想能力，因此，当篡改特征信息与训练模型有出入时也可以得到更准确的检测结果，从而提高网页检测能力。

在前述实施例的基础上，本实施例对技术方案进行进一步说明和优化。具体如下：

在前述实施例中，所述至少两种篡改特征信息包括：

对所述标签信息的文本信息进行情感分析的结果和/或对所述标签信息的文本信息进行语义分析的结果和/或对所述标签信息的链接信息的可疑性检测结果和/或专家预设篡改特征。

需要说明的是，篡改网页经常会在网页中插入恶意文本，因此本申请使用自然语言处理（NLP）中的情感分析技术，来检查网页中是否含有恶意文本。具体地，可以根据标签信息，判断每个标签信息中的文本是否含有非法或消极内容，例如博彩广告。同时，本申请还可以使用情感分析判断网页文本整体的恶意性，即以整个网页的文本作为待检测文本的单位，进行恶意文本的检测。因此，情感分析的结果既可以包括恶意文本在各个标签的分布统计，如每个标签有几个恶意文本，也可以包括整个网页中恶意文本的概率，具体要以哪个结果作为篡改特征信息，在本方案中不做具体限定。

由于客户的多样性，部分客户网站自身业务容易引起误报，比如福彩网站由于包含双色球、时时彩等敏感信息，很容易被传统引擎所误报。因此，在本方案中，篡改特征信息还包括对标签信息的文本进行语义分析的

结果。在本方案中，确定标签信息中的可以文本与网站的主题的相关性，从而大幅度降低业务误报。相关性确定的方式在本方案中不做具体限定，可以根据实际情况确定，例如，可以将标签信息中文本信息的敏感词语映射为词向量，并确定网站的主体，同样映射为向量，通过确定敏感词向量与主题向量的距离可以确定敏感词是否为当前网页的业务，从而避免误报。因此，在本方案中，篡改特征信息可以包括可疑文本的个数、可疑文本与敏感词之间的距离统计、可疑文本与网站主题之间的距离统计等。

在本方案中，对于网页中的链接情况也进行检测。黑客篡改网站处理会在网页中插入恶意文本，还会插入恶意链接，因此为了检测更加全面，篡改特征信息中还可以包括链接相关的信息。因此可以预先通过模型学习大量的正常域名和恶意域名的文本特征信息，然后利用训练好的模型确定网页中的链接情况，再结合链接的网络关联情况，即该链接是否也被其他正常网站作为外链，即可确定当前网页中的链接是否为恶意连接。因此在本方案中，篡改特征信息可以包括可疑链接的统计、可疑链接的可疑程度、可疑链接出现的标签等。

在本方案中，还可以结合安全领域专家的知识，预设一些篡改特征信息。

篡改还会采用一些反检测技术，比如使用肉眼不可见的超小字体、使用特殊编码或颜色等，因此可以通过分析待检测网页的DOM结构，确定源码中是否有可以呈现上述反检测效果的异常行为，并将是否有异常行为作为篡改特征信息。

此外，反检测技术还会使用异常编码进行，例如，正常网页在查看其源代码时，可以直接看到文字。恶意文本为了隐藏恶意内容，会使用诸如HTML编码的技术，将文字编码成一些数字，人眼无法理解，此种HTML编码即可作为异常编码，因此，本方案还可以通过分析待检测网页的DOM结构，确定源码中是否有异常编码，并将是否有异常编码作为篡改特征信息。

下面对本申请实施例提供的一种具体的网页篡改检测方法进行介绍，下文描述的一种具体的网页篡改检测方法与上述任一实施例可以相互参

照。

参加图2，本申请实施例提供的一种具体的网页篡改检测方法，具体包括：

5 S201，解析待检测网页得到对应待检测网页的标签信息，将所述标签信息作为待检测信息。

S202，判断所述标签信息的文本信息中是否包括预设敏感词；若是，则执行S204，若否，则执行S203。

当待检测网页数目众多时，为了提高整体的检测效率，在本方案中需要

10 先过滤掉明显没有被篡改过的网页过滤掉。
而未被篡改的网页中通常不会含有敏感词，因此在本方案中可以先检测待检测网页的标签信息的文本信息中是否包括预设敏感词，如果有，则执行S204做进一步的篡改检测，如果没有则直接确定该网页为未被篡改网页，不再执行后续步骤，节省时间。

15 在一个优选的实施方式中，利用预设规则对所述标签信息的文本信息进行匹配，判断所述标签信息中是否包括满足所述预设规则的词；其中所述预设规则对应预设敏感词，每条所述预设规则中包括预设敏感词的核心敏感词与所述核心敏感词之间的关系。

需要说明的是，如果利用传统的关键词匹配算法判断标签信息的文本信息中是否包括预设敏感词，也就是利用传统的关键词匹配算进行文本信息
20 信息与预设敏感词的匹配，例如，利用多模字符串匹配算进行匹配，则关键词的抗干扰能力差，容易被绕过。例如，预设敏感词为“娱乐城赌博”，当文本信息中在关键词中颠倒一个词中的顺序时，例如“赌博娱乐城”，再例如，在文本中的两个词之间加入其它的字或词，如“娱乐城的赌博”，则将不能够将该文本信息匹配到预设敏感词，从而会使检测出现漏洞。

25 因此，在本方案中，对应每个预设敏感词都有一个或多个规则，例如，对应一个预设敏感词，规则为允许其中的核心敏感词颠倒顺序，允许核心敏感词之间插入其他字符。需要说明的是，核心敏感词即为预设敏感词的核心词，如预设敏感词为“娱乐城赌博”，其核心敏感词为“娱乐城”、“赌博”。

在一个具体地实施方式中，核心敏感词的确定方式可以是对预设敏感词进行分词处理，从而得到对应的核心敏感词；也可以是通过在网页中收集得到的核心敏感词。

5 当通过在网页中收集得到核心敏感词时，可以包括但不限于以下方式：

收集大量正常网页和篡改网页；对网页进行分词，统计每个词语在篡改网页中出现的概率 $f1$ 和在正常网页出现的概率 $f2$ 。如果其差值 $d=f1-f2$ 大于预设阈值，则判断该词语为核心敏感词。

10 由于每一个预设敏感词都会对应有一个或多个规则，利用规则判断当前的文本是否为预设敏感词相比直接判断文本是否与预设敏感词相同会耗费更多的时间与计算资源，因此，在本方案中，提供一个优选的实施方式，在本方案中，所述利用对应预设敏感词的规则对所述标签信息的文本信息进行匹配，判断所述标签信息中是否包括满足所述预设敏感词的规则的词之前，还包括：

15 判断所述标签信息是否包括所述核心敏感词；

若是，则执行所述利用对应预设敏感词的规则对所述标签信息的文本信息进行匹配，判断所述标签信息中是否包括满足所述预设敏感词的规则的词的步骤；

若否，则确定所述待检测网页的篡改检测结果为未被篡改。

20 在本方案中，首先判断标签信息中是否包括核心敏感词，即先进行传统的关键词匹配，匹配当前标签信息中的文本是否有核心敏感词，如果包括核心敏感词再执行后续的步骤，如果不包括核心敏感词，则直接确定当前待检测网页的篡改结果为未被篡改。

S203，确定所述待检测网页的篡改检测结果为未被篡改。

25 S204，在所述待检测信息中提取篡改特征信息；

S205，利用深度学习模型对所述篡改特征信息进行计算，得到所述待检测网页的篡改检测结果；其中，所述深度学习模型为预先利用与所述篡改特征信息对应的训练样本进行训练得到的深度学习模型。

有关S204、S205均已在上述实施例中介绍，此处将不再赘述。

下面对本申请实施例提供的一种具体的网页篡改检测方法进行介绍，下文描述的一种具体的网页篡改检测方法与上述任一实施例可以相互参照。

5 参见图3，本申请实施例提供的一种具体的网页篡改检测方法，具体包括：

 S301，解析待检测网页得到对应待检测网页的标签信息，将所述标签信息作为待检测信息。

 S302，获取所述待检测网页中的图片。

10 S303，识别所述图片中的文本信息，将所述图片中的文本信息作为待检测信息。

 需要说明的是，图片篡改是另一种网页篡改的类型，即在被入侵网页中插入恶意图片，而图片中的信息并不能直接利用上述针对文本的篡改检测方法进行检测，因此在本方案中，首先会获取到待检测网页中的图片，
15 然后对图片进行识别，提取其中的文本信息，将图片的文本信息也作为待检测信息，然后执行后续检测的步骤。需要说明的是，有关图片识别的相关技术已在现有技术中相对成熟，如OCR（Optical Character Recognition，光学字符识别）技术，因此，在本方案中不再进行赘述。

 因此，本方案对图片篡改也可以进行检测。

20 S304，在所述待检测信息中提取篡改特征信息。

 S305，利用深度学习模型对所述篡改特征信息进行计算，得到所述待检测网页的篡改检测结果；其中，所述深度学习模型为预先利用与所述篡改特征信息对应的训练样本进行训练得到的深度学习模型。S301、S304、S305的具体内容可以参见上述实施例，在本方案中不再进行赘述。

25

下面对本申请实施例提供的一种具体的网页篡改检测方法进行介绍，下文描述的一种具体的网页篡改检测方法与上述任一实施例可以相互参照。

 参见图4，本申请实施例提供的一种具体的网页篡改检测方法，具体包

括:

S401, 解析待检测网页得到对应待检测网页的标签信息, 将所述标签信息作为待检测信息。

5 S402, 解析执行所述待检测网页中的JavaScript代码, 以跳转到所述JavaScript代码对应的目标页面。

S403, 解析所述目标页面得到对应所述目标页面的目标标签信息, 将所述目标标签信息作为待检测信息。

需要说明的是, 在html网页中, 除了文本信息、链接信息、图片信息, 还可能会有JavaScript代码, 用户浏览器加载JavaScript代码可以被定向到另一个网页中, 如果JavaScript代码为恶意代码, 即加载该代码时会跳转到恶意网页中。

10

因此, 在本方案中为了可以检测出此种篡改情况, 首先需要解析执行待检测网页中的JavaScript代码, 从而跳转到该代码对应的目标页面, 然后解析目标页面的目标标签信息, 并将其作为待检测信息, 同样执行后续的篡改检测步骤, 从而可以检测出待检测网页的JavaScript代码的篡改情况, 使检测更加全面, 检测结果更加准确。

15

需要说明的是, 本申请不限于JavaScript代码, 也可以是其他具有跳转页面效果的代码。

S404, 在所述待检测信息中提取篡改特征信息。

20 S405, 利用深度学习模型对所述篡改特征信息进行计算, 得到所述待检测网页的篡改检测结果; 其中, 所述深度学习模型为预先利用与所述篡改特征信息对应的训练样本进行训练得到的深度学习模型。S401、S404、S405的具体内容可以参见上述实施例, 在本方案中不再进行赘述。下面对本申请实施例提供的一种网页篡改检测系统进行介绍, 下文描述的一种网页篡改检测系统与上述任一实施例可以相互参照。

25

参见图5, 本申请实施例提供的一种网页篡改检测系统, 具体包括:

待检测网页解析模块501, 用于解析待检测网页得到对应待检测网页的标签信息, 将所述标签信息作为待检测信息。

待检测信息特征提取模块502, 用于在所述待检测信息中提取篡改特征

信息;

计算模块503, 用于利用深度学习模型对所述篡改特征信息进行计算, 得到所述待检测网页的篡改检测结果; 其中, 所述深度学习模型为预先利用与所述篡改特征信息对应的训练样本进行训练得到的深度学习模型。

5 优选的, 所述系统还包括:

预设敏感词检测模块, 用于判断所述标签信息的文本信息中是否包括预设敏感词; 若是, 则启动所述待检测信息特征提取模块502对应的工作流程; 若否, 则确定所述待检测网页的篡改检测结果为未被篡改。

10 优选的, 所述预设敏感词检测模块具体为用于利用预设规则对所述标签信息的文本信息进行匹配, 判断所述标签信息中是否包括满足所述预设规则的词的模块;

其中, 所述预设规则对应预设敏感词, 每条所述预设规则中包括预设敏感词的核心敏感词与所述核心敏感词之间的关系。

优选的, 所述系统还包括:

15 核心敏感词检测模块, 用于判断所述标签信息是否包括所述核心敏感词; 若是, 则启动所述预设敏感词检测模块对应的工作流程; 若否, 则确定所述待检测网页的篡改检测结果为未被篡改。

优选的, 所述篡改特征信息包括:

20 对所述标签信息的文本信息进行情感分析的结果和/或对所述标签信息的文本信息进行语义分析的结果和/或对所述标签信息的链接信息的可疑性检测结果和/或专家预设篡改特征。

优选的, 所述计算模块503, 包括:

计算单元, 用于将至少两个深度学习模型作为弱分类器对所述篡改特征信息进行计算, 得到对应每个弱分类器的计算结果;

25 集成学习单元, 用于集成学习每个所述计算结果得到所述待检测网页的篡改结果。

优选的, 当所述篡改特征信息包括至少两种时, 所述至少两个深度学习模型包括:

分别利用一种所述篡改特征信息的训练样本进行训练, 得到的对应每

种篡改特征信息的深度学习模型；

对应的，所述计算单元具体用于将至少两个所述深度学习模型作为弱分类器分别对与每种所述深度学习模型对应的所述篡改特征信息进行计算，得到计算结果。

- 5 优选的，当所述篡改特征信息包括至少两种时，所述至少两个深度学习模型包括：

利用至少两种训练算法对所述篡改特征信息的训练样本进行训练得到的对应每种训练算法的深度学习模型；

- 10 对应的，所述计算单元具体用于将至少两个深度学习模型作为弱分类器对同一种所述篡改特征信息进行计算，得到对应每个弱分类器的计算结果。

优选的，所述系统还包括：

图片获取模块，用于获取所述待检测网页中的图片；

- 15 图片文本信息识别模块，用于识别所述图片中的文本信息，将所述图片中的文本信息作为待检测信息。

优选的，所述系统还包括：

代码解析模块，用于解析执行所述待检测网页中的JavaScript代码，以跳转到所述JavaScript代码对应的目标页面；

- 20 目标页面解析模块，用于解析所述目标页面得到对应所述目标页面的目标标签信息，将所述目标标签信息作为待检测信息。

- 25 本实施例的网页篡改检测系统用于实现前述的网页篡改检测方法，因此网页篡改检测系统中的具体实施方式可见前文中的网页篡改检测方法的实施例部分，例如，待检测网页解析模块501，待检测信息特征提取模块502，第一计算模块503，第二计算模块504，分别用于实现上述网页篡改检测方法中步骤S101，S102，S103和S104，所以，其具体实施方式可以参照相应的各个部分实施例的描述，在此不再赘述。

下面对本申请实施例提供的一种网页篡改检测装置进行介绍，下文描述的一种网页篡改检测装置与上述任一实施例可以相互参照。

参见图6, 本申请实施例提供的一种网页篡改检测装置, 具体包括:

存储器100, 用于存储计算机程序;

处理器200, 用于执行所述计算机程序时实现如上述任一实施例所述网页篡改检测方法的步骤。

- 5 具体的, 存储器100包括非易失性存储介质、内存储器。该非易失性存储介质存储有操作系统和计算机可读指令, 该内存储器为非易失性存储介质中的操作系统和计算机可读指令的运行提供环境。处理器200为网页篡改检测装置提供计算和控制能力, 可以实现上述任一网页篡改检测方法实施例所提供的步骤。

10

在上述实施例的基础上, 作为优选实施方式, 所述网页篡改检测装置还包括:

- 输入接口300, 用于获取外部导入的计算机程序、参数和指令, 经处理器控制保存至存储器中。该输入接口300可以与输入装置相连, 接收用户手
15 动输入的参数或指令。该输入装置可以是显示屏上覆盖的触摸层, 也可以是终端外壳上设置的按键、轨迹球或触控板, 也可以是键盘、触控板或鼠标等。

显示单元400, 用于显示处理器发送的数据。该显示单元40可以为PC机上的显示屏、液晶显示屏或者电子墨水显示屏等。

- 20 网络端口500, 用于与外部各终端设备进行通信连接。该通信连接所采用的通信技术可以为有线通信技术或无线通信技术, 如移动高清链接技术(MHL)、通用串行总线(USB)、高清多媒体接口(HDMI)、无线保真技术(WiFi)、蓝牙通信技术、低功耗蓝牙通信技术、基于IEEE802.11s的通信技术等。

25

本申请还提供了一种计算机可读存储介质, 其上存储有计算机程序, 所述计算机程序被处理器执行时可以实现上述实施例所提供的步骤。该存储介质可以包括: U盘、移动硬盘、只读存储器(Read-Only 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。

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。

5 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本申请。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申请的精神或范围的情况下，在其它实施例中实现。因此，本申请将不会被限制于本文所示的
10 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、一种网页篡改检测方法，其特征在于，包括：

解析待检测网页得到对应待检测网页的标签信息，将所述标签信息作为待检测信息；

5 在所述待检测信息中提取篡改特征信息；

利用深度学习模型对所述篡改特征信息进行计算，得到所述待检测网页的篡改检测结果；其中，所述深度学习模型为预先利用与所述篡改特征信息对应的训练样本进行训练得到的深度学习模型。

2、根据权利要求1所述的方法，其特征在于，所述在所述待检测信息
10 中提取篡改特征信息之前，还包括：

判断所述标签信息的文本信息中是否包括预设敏感词；

若是，则执行所述在所述待检测信息中提取篡改特征信息的步骤；

若否，则确定所述待检测网页的篡改检测结果为未被篡改。

3、根据权利要求2所述的方法，其特征在于，所述判断所述标签信息
15 的文本信息中是否包括预设敏感词，包括：

利用预设规则对所述标签信息的文本信息进行匹配，判断所述标签信息中是否包括满足所述预设规则的词；其中所述预设规则对应预设敏感词，每条所述预设规则中包括预设敏感词的核心敏感词与所述核心敏感词之间的关系。

20 4、根据权利要求3所述的方法，其特征在于，所述利用预设规则对所述标签信息的文本信息进行匹配，判断所述标签信息中是否包括满足所述预设规则的词之前，还包括：

判断所述标签信息是否包括所述核心敏感词；

若是，则执行所述利用预设规则对所述标签信息的文本信息进行匹配，

25 判断所述标签信息中是否包括满足所述预设规则的词；

若否，则确定所述待检测网页的篡改检测结果为未被篡改。

5、根据权利要求1所述的方法，其特征在于，所述篡改特征信息包括：

对所述标签信息的文本信息进行情感分析的结果和/或对所述标签信息的文本信息进行语义分析的结果和/或对所述标签信息的链接信息的可

疑性检测结果和/或专家预设篡改特征。

6、根据权利要求1所述的方法，其特征在于，所述利用深度学习模型对所述篡改特征信息进行计算，得到所述待检测网页的篡改检测结果，包括：

- 5 将至少两个深度学习模型作为弱分类器对所述篡改特征信息进行计算，得到对应每个弱分类器的计算结果；

集成学习每个所述计算结果得到所述待检测网页的篡改结果。

7、根据权利要求6所述的方法，其特征在于，当所述篡改特征信息包括至少两种时，所述至少两个深度学习模型包括：

- 10 分别利用一种所述篡改特征信息的训练样本进行训练，得到的对应每种篡改特征信息的深度学习模型；

对应的，所述将至少两个深度学习模型作为弱分类器对所述篡改特征信息进行计算，得到对应每个弱分类器的计算结果，包括：

- 15 将至少两个所述深度学习模型作为弱分类器分别对与每种所述深度学习模型对应的所述篡改特征信息进行计算，得到计算结果。

8、根据权利要求6所述的方法，其特征在于，当所述篡改特征信息包括一种篡改特征信息时，所述至少两个深度学习模型包括：

利用至少两种训练算法对所述篡改特征信息的训练样本进行训练得到的对应每种训练算法的深度学习模型；

- 20 对应的，所述将至少两个深度学习模型作为弱分类器对所述篡改特征信息进行计算，得到对应每个弱分类器的计算结果，包括：

将至少两个深度学习模型作为弱分类器对同一种所述篡改特征信息进行计算，得到对应每个弱分类器的计算结果。

- 25 9、根据权利要求1所述的方法，其特征在于，所述在所述待检测信息中提取篡改特征信息之前，还包括：

获取所述待检测网页中的图片；

识别所述图片中的文本信息，将所述图片中的文本信息作为待检测信息。

10、根据权利要求1所述的方法，其特征在于，所述在所述待检测信息

中提取篡改特征信息之前,还包括:

解析执行所述待检测网页中的JavaScript代码,以跳转到所述JavaScript代码对应的目标页面;

5 解析所述目标页面得到对应所述目标页面的目标标签信息,将所述目标标签信息作为待检测信息。

11、一种网页篡改检测系统,其特征在于,包括:

待检测网页解析模块,用于解析待检测网页得到对应待检测网页的标签信息,将所述标签信息作为待检测信息;

10 待检测信息特征提取模块,用于在所述待检测信息中提取篡改特征信息;

计算模块,用于利用深度学习模型对所述篡改特征信息进行计算,得到所述待检测网页的篡改检测结果;其中,所述深度学习模型为预先利用与所述篡改特征信息对应的训练样本进行训练得到的深度学习模型。

12、根据权利要求11所述的系统,其特征在于,还包括:

15 预设敏感词检测模块,用于判断所述标签信息的文本信息中是否包括预设敏感词;若是,则启动所述待检测信息特征提取模块对应的工作流程;若否,则确定所述待检测网页的篡改检测结果为未被篡改。

20 13、根据权利要求12所述的系统,其特征在于,所述预设敏感词检测模块具体为用于利用预设规则对所述标签信息的文本信息进行匹配,判断所述标签信息中是否包括满足所述预设规则的词的模块;

其中,所述预设规则对应预设敏感词,每条所述预设规则中包括预设敏感词的核心敏感词与所述核心敏感词之间的关系。

14、根据权利要求13所述的系统,其特征在于,还包括:

25 核心敏感词检测模块,用于判断所述标签信息是否包括所述核心敏感词;若是,则启动所述预设敏感词检测模块对应的工作流程;若否,则确定所述待检测网页的篡改检测结果为未被篡改。

15、根据权利要求11所述的系统,其特征在于,所述计算模块包括:

计算单元,用于将至少两个深度学习模型作为弱分类器对所述篡改特征信息进行计算,得到对应每个所述弱分类器的计算结果;

集成学习单元，用于集成学习每个所述计算结果得到所述待检测网页的篡改结果。

16、根据权利要求15所述的系统，其特征在于，当所述篡改特征信息包括至少两种时，所述至少两个深度学习模型包括：

- 5 分别利用一种所述篡改特征信息的训练样本进行训练，得到的对应每种篡改特征信息的深度学习模型；

对应的，所述计算单元具体用于将至少两个所述深度学习模型作为弱分类器分别对与每种所述深度学习模型对应的所述篡改特征信息进行计算，得到计算结果。

- 10 17、根据权利要求15所述的系统，其特征在于，当所述篡改特征信息包括至少两种时，所述至少两个深度学习模型包括：

利用至少两种训练算法对所述篡改特征信息的训练样本进行训练得到的对应每种训练算法的深度学习模型；

- 15 对应的，所述计算单元具体用于将至少两个深度学习模型作为弱分类器对同一种所述篡改特征信息进行计算，得到对应每个所述弱分类器的计算结果。

18、根据权利要求11所述的系统，其特征在于，还包括：

图片获取模块，用于获取所述待检测网页中的图片；

- 20 图片文本信息识别模块，用于识别所述图片中的文本信息，将所述图片中的文本信息作为待检测信息。

19、一种网页篡改检测装置，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10任一项所述网页篡改检测方法的步骤。

- 25 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10任一项所述网页篡改检测方法的步骤。