

CLAIMS

1. A method for detecting webpage tampering, comprising:

parsing a to-be-detected webpage to obtain tag information corresponding to the to-be-detected webpage, and taking the tag information as to-be-detected information;

extracting tampering feature information from the to-be-detected information, wherein the tampering feature information comprises at least one of: a result of sentiment analysis on text information of the tag information, a result of semantic analysis on text information of the tag information, a suspiciousness detection result of link information of the tag information, and an expert-presupposed tampering feature; and

calculating the tampering feature information by using a deep learning model to obtain a tampering detection result of the to-be-detected webpage, wherein the deep learning model is obtained by pre-training on training samples corresponding to the tampering feature information.

2. The method according to claim 1, wherein before extracting the tampering feature information from the to-be-detected information, the method further comprises:

determining whether text information of the tag information includes a preset sensitive word;

if the text information includes the preset sensitive word, executing the step of extracting the tampering feature information from the to-be-detected information; and

if the text information does not include the preset sensitive word, determining that the tampering detection result of the to-be-detected webpage is the to-be-detected webpage being not tampered with.

3. The method according to claim 2, wherein determining whether the text information of the tag information includes the preset sensitive word comprises:

matching the text information of the tag information by using a preset rule to determine whether the tag information includes a word that meets the preset rule, wherein the preset rule

corresponds to the preset sensitive word, and each preset rule includes a relationship between a core sensitive word and a core sensitive word of the preset sensitive word.

4. The method according to claim 3, wherein before matching the text information of the tag information by using the preset rule to determine whether the tag information includes the word that meets the preset rule, the method further comprises:

determining whether the tag information includes the core sensitive word;

if the tag information includes the core sensitive word, executing the step of matching the text information of the tag information by using the preset rule to determine whether the tag information includes the word that meets the preset rule; and

if the tag information does not include the core sensitive word, determining that the tampering detection result of the to-be-detected webpage is the to-be-detected webpage being not tampered with.

5. The method according to claim 1, wherein calculating the tampering feature information by using the deep learning model to obtain the tampering detection result of the to-be-detected webpage comprises:

calculating the tampering feature information by using at least two deep learning models as weak classifiers, to obtain calculation results corresponding to each of the weak classifiers; and

performing ensemble learning on the calculation results to obtain the tampering result of the to-be-detected webpage.

6. The method according to claim 5, wherein if there are at least two types of the tampering feature information, the at least two deep learning models comprise:

deep learning models corresponding to each type of the tampering feature information obtained by training on training samples of each type of the tampering feature information;

calculating the tampering feature information by using the at least two deep learning models as the weak classifiers to obtain the calculation results corresponding to each of the weak classifiers comprises:

calculating, by using the at least two deep learning models as the weak classifiers, the tampering feature information corresponding to each of the deep learning models, to obtain the calculation results.

7. The method according to claim 5, wherein if there is one type of the tampering feature information, the at least two deep learning models comprise:

deep learning models respectively corresponding to at least two training algorithms obtained by training on the training sample of the tampering feature information using the at least two training algorithms;

calculating the tampering feature information by using the at least two deep learning models as the weak classifiers to obtain the calculation results corresponding to each of the weak classifiers comprises:

calculating the same tampering feature information by using the at least two deep learning models as the weak classifiers to obtain the calculation results corresponding to each of the weak classifiers.

8. The method according to claim 1, wherein before extracting the tampering feature information from the to-be-detected information, the method further comprises:

obtaining a picture in the to-be-detected webpage; and

identifying text information in the picture, and taking the text information in the picture as the to-be-detected information.

9. The method according to claim 1, wherein before extracting the tampering feature information from the to-be-detected information, the method further comprises:

parsing and executing JavaScript code in the to-be-detected webpage to jump to a target page corresponding to the JavaScript code; and

parsing the target page to obtain target tag information corresponding to the target page, and taking the target tag information as the to-be-detected information.

10. A system for detecting webpage tampering, comprising:

a to-be-detected webpage parsing module configured to parse a to-be-detected webpage to obtain tag information corresponding to the to-be-detected webpage, and take the tag information as to-be-detected information;

a to-be-detected information feature extraction module configured to extract tampering feature information from the to-be-detected information, wherein the tampering feature information comprises at least one of: a result of sentiment analysis on text information of the tag information, a result of semantic analysis on text information of the tag information, a suspiciousness detection result of link information of the tag information, and an expert-presupposed tampering feature; and

a calculation module configured to calculate the tampering feature information by using a deep learning model to obtain a tampering detection result of the to-be-detected webpage, wherein the deep learning model is obtained by pre-training on training samples corresponding to the tampering feature information.

11. The system according to claim 10, wherein the system further comprises:

a preset sensitive word detection module configured to determine whether text information of the tag information includes a preset sensitive word; if the text information includes the preset sensitive word, start the workflow corresponding to the to-be-detected information feature extraction module; if the text information does not include the preset sensitive word, determine that the tampering detection result of the to-be-detected webpage is the to-be-detected webpage being not tampered with.

12. The system according to claim 11, wherein the preset sensitive word detection module is configured to match the text information of the tag information by using a preset rule to determine whether the tag information includes a word that meets the preset rule,

wherein the preset rule corresponds to the preset sensitive word, and each preset rule includes a relationship between a core sensitive word and a core sensitive word of the preset sensitive word.

13. The system according to claim 12, wherein the system further comprises:

a core sensitive word detection module configured to determine whether the tag

information includes the core sensitive word; if the tag information includes the core sensitive word, start the workflow corresponding to the preset sensitive word detection module; if the tag information does not include the core sensitive word, determine that the tampering detection result of the to-be-detected webpage is the to-be-detected webpage being not tampered with.

14. The system according to claim 10, wherein the calculation module comprises:

a calculation unit configured to calculate the tampering feature information by using at least two deep learning models as weak classifiers, to obtain calculation results corresponding to each of the weak classifiers; and

an ensemble learning unit configured to perform ensemble learn on the calculation results to obtain the tampering result of the to-be-detected webpage.

15. The system according to claim 14, wherein if there are at least two types of the tampering feature information, the at least two deep learning models comprises:

deep learning models corresponding to each type of the tampering feature information obtained by training on training samples of each type of the tampering feature information,

the calculation unit is configured to calculate, by using the at least two deep learning models as the weak classifiers, the tampering feature information corresponding to each of the deep learning models, to obtain the calculation results.

16. The system according to claim 14, wherein if there are at least two types of the tampering feature information, the at least two deep learning models comprise:

deep learning models respectively corresponding to at least two training algorithms obtained by training on the training sample of the tampering feature information using the at least two training algorithms,

the calculation unit is configured to calculate the same tampering feature information by using the at least two deep learning models as the weak classifiers to obtain the calculation results corresponding to each of the weak classifiers.

17. The system according to claim 10, wherein the system further comprises:

a picture obtaining module configured to obtain a picture in the to-be-detected webpage;

and

a picture text information identification module configured to identify text information in the picture, and take the text information in the picture as the to-be-detected information.

18. A device for detecting webpage tampering, comprising:

a memory configured to store a computer program; and

a processor configured to execute the computer program to implement steps of the method for detecting webpage tampering according to any one of claims 1 to 9.

19. A computer-readable storage medium, wherein the computer-readable storage medium stores a computer program that, when executed by a processor, implements steps of the method for detecting webpage tampering according to any one of claims 1 to 9.