

WHAT IS CLAIMED IS:

1. A method of detecting image tampering, comprising:

A. carrying out block segmentation on a to-be-detected image to segment the to-be-detected image into a plurality of image small fragments, and extracting initial tampering detection features from all the image small fragments;

B. encoding the extracted initial tampering detection features with a predetermined encoder to generate complicated tampering features, and determining a tampering detection result corresponding to the to-be-detected image according to the generated complicated tampering features, wherein the tampering detection result comprises an image-tampered result and an image-not-tampered result;

wherein the step A comprises:

converting the to-be-detected image from a first color space into a second color space;

carrying out the block segmentation on the to-be-detected image to segment the to-be-detected image into $N \times M$ image small fragments, wherein N and M are positive integers;

applying a preset wavelet function to each second color space component of each image small fragment to obtain multiple corresponding pixel coefficient maps, calculating a tabulate statistics coefficient of each pixel coefficient map, and obtaining multiple tabulate statistics coefficients from each image small fragment, wherein the tabulate statistics coefficients are regarded as the initial tampering detection features of the corresponding image small fragments.

2. The method of detecting image tampering of claim 1, wherein the predetermined encoder is a stacked auto-encoder; the stacked auto-encoder is formed by stacking multiple layers of basic auto-encoders, and an output of each layer of auto-encoder is an input of the next layer of auto-encoder; the stacked auto-encoder also comprises a neural network multi-layer perceptron; the neural network multilayer perceptron is jointed with the last layer of auto-encoder, and is used for determining the tampering detection result corresponding to the to-be-detected image according to the generated complicated tampering features.

3. The method of detecting image tampering of claim 2, wherein the step B comprises:

encoding the initial tampering detection features of all the image small fragments with the predetermined encoder to generate the complicated tampering features of all the image small fragments;

determining first tampering detection results corresponding to all the image small fragments according to the complicated tampering features of all the image small

fragments, wherein the first tampering detection result comprise the image-tampered result and the image-not-tampered result;

if the first tampering detection result corresponding to one image small fragment is the image-tampered result, determining that the tampering detection result corresponding to the to-be-detected image is the image-tampered result.

4. The method of detecting image tampering of claim 3, wherein the stacked auto-encoder comprises an adjacent region perception layer for determining the tampering detection result corresponding to the to-be-detected image according to scene information of adjacent regions;

the step B further comprises:

calculating adjacent scene information of each image small fragment according to a preset algorithm, and determining a second tampering detection result corresponding to each image small fragment according to the adjacent scene information of each image small fragment, wherein the second tampering detection result comprises an image-tampered result and an image-not-tampered result;

if the second tampering detection result corresponding to one image small fragment is the image-tampered result, determining that the tampering detection result corresponding to the to-be-detected image is the image-tampered result;

if the second tampering detection results corresponding to all the image small fragments are all image-not-tampered results, but the first tampering detection result corresponding to one image small fragment is the image-tampered result, determining that the tampering detection result corresponding to the to-be-detected image is the image-not-tampered result.

5. The method of detecting image tampering of claim 1, wherein a training process of the predetermined encoder is as follows:

C. obtaining a preset number of image samples, and marking the tampering result of each image sample, wherein the tampering result comprises the image-tampered result and the image-not-tampered result;

D. carrying out block segmentation on each image sample to segment each image sample into $N*M$ image small fragments, wherein N and M are positive integers, and extracting initial tampering detection features from all the image small fragments of each image sample to extract the initial tampering detection features corresponding to each image sample;

E. classifying all the image samples into a first data set and a second data set according to a ratio of X to Y , wherein the number of image samples in the first data set is greater than that of image samples in the second data set, the first data set is used as a training set, and the second data set is used as a test set; and X is greater than 0, and Y is greater than 0;

F. training the encoder with the initial tampering detection features corresponding to all the image samples in the first data set, and verifying the accuracy rate of the trained encoder with the initial tampering detection features corresponding to all the image samples in the second data set;

G. if the accuracy rate of the trained encoder is greater than or equal to a preset accuracy rate, ending the training, or if the accuracy rate of the trained encoder is less than the preset accuracy rate, increasing the number of image samples, and repeatedly executing the steps D, E and F till the accuracy rate of the trained encoder is greater than or equal to the preset accuracy rate.

6. A system of detecting image tampering, comprising:

an extraction module, which is used for carrying out block segmentation on a to-be-detected image to segment the to-be-detected image into a plurality of image small fragments, and extracting initial tampering detection features from all the image small fragments;

a detection module, which is used for encoding the extracted initial tampering detection features with a predetermined encoder to generate complicated tampering features, and determining a tampering detection result corresponding to the to-be-detected image according to the generated complicated tampering features, wherein the tampering detection result comprises an image-tampered result and an image-not-tampered result;

wherein the extraction module comprises:

a conversion unit, which is used for converting the to-be-detected image from a first color space into a second color space;

a segmentation unit, which is used for carrying out the block segmentation on the to-be-detected image to segment the to-be-detected image into $N \times M$ image small fragments, wherein N and M are positive integers;

an obtaining unit, which is used for applying preset wavelet function decomposition to each second color space component of each image small fragment to obtain multiple corresponding pixel coefficient maps, calculating a tabulate statistics coefficient of each pixel coefficient map, and obtaining multiple tabulate statistics coefficients from each image small fragment, wherein the tabulate statistics

coefficients are regarded as the initial tampering detection features of the corresponding image small fragments.

7. The system of detecting image tampering of claim 6, wherein the predetermined encoder is a stacked auto-encoder; the stacked auto-encoder is formed by stacking multiple layers of basic auto-encoders, and an output of each layer of auto-encoder is an input of the next layer of auto-encoder; the stacked auto-encoder also comprises a neural network multi-layer perceptron; the neural network multilayer perceptron is jointed with the last layer of auto-encoder, and is used for determining the tampering detection result corresponding to the to-be-detected image according to the generated complicated tampering features.

8. The system of detecting image tampering of claim 7, wherein the detection module is further used for:

encoding the initial tampering detection features of all the image small fragments with the predetermined encoder to generate the complicated tampering features of all the image small fragments;

determining first tampering detection results corresponding to all the image small fragments according to the complicated tampering features of all the image small fragments, wherein the first tampering detection results comprise the image-tampered results and the image-not-tampered result;

if the first tampering detection result corresponding to one image small fragment is the image-tampered result, determining that the tampering detection result corresponding to the to-be-detected image is the image-tampered result.

9. The system of detecting image tampering of claim 8, wherein the stacked auto-encoder comprises an adjacent region perception layer for determining the tampering detection result corresponding to the to-be-detected image according to scene information of adjacent regions;

the detection module is further used for:

calculating adjacent scene information of each image small fragment according to a preset algorithm, and determining a second tampering detection result corresponding to each image small fragment according to the adjacent scene information of each image small fragment, wherein the second tampering detection result comprises an image-tampered result and an image-not-tampered result;

if the second tampering detection result corresponding to one image small fragment is the image-tampered result, determining that the tampering detection result corresponding to the to-be-detected image is the image-tampered result;

if the second tampering detection results corresponding to all the image small fragments are all image-not-tampered results, but the first tampering detection result corresponding to one image small fragment is the image-tampered result, determining

that the tampering detection result corresponding to the to-be-detected image is the image-not-tampered result.

10. The system of detecting image tampering of claim 6, wherein a training process of the predetermined encoder is as follows:

C. obtaining a preset number of image samples, and marking the tampering result of each image sample, wherein the tampering result comprises the image-tampered result and the image-not-tampered result;

D. carrying out block segmentation on each image sample to segment each image sample into $N \times M$ image small fragments, wherein N and M are positive integers, and extracting initial tampering detection features from all the image small fragments of each image sample to extract the initial tampering detection features corresponding to each image sample;

E. classifying all the image samples into a first data set and a second data set according to a ratio of X to Y , wherein the number of image samples in the first data set is greater than that of image samples in the second data set, the first data set is used as a training set, and the second data set is used as a test set; and X is greater than 0, and Y is greater than 0;

F. training the encoder with the initial tampering detection features corresponding to all the image samples in the first data set, and verifying the accuracy rate of the trained encoder with the initial tampering detection features corresponding to all the image samples in the second data set;

G. if the accuracy rate of the trained encoder is greater than or equal to a preset accuracy rate, ending the training, or if the accuracy rate of the trained encoder is less than the preset accuracy rate, increasing the number of image samples, and repeatedly

executing the steps D, E and F till the accuracy rate of the trained encoder is greater than or equal to the preset accuracy rate.

11. An electronic device, comprising a processing equipment and storage equipment, wherein the storage equipment stores an image tampering detection program comprising at least one computer readable instruction; and the at least one computer readable instruction is executed by the processing equipment to implement the following operations:

A. carrying out block segmentation on a to-be-detected image to segment the to-be-detected image into a plurality of image small fragments, and extracting initial tampering detection features from all the image small fragments;

B. encoding the extracted initial tampering detection features with a predetermined encoder to generate complicated tampering features, and determining a tampering detection result corresponding to the to-be-detected image according to the generated complicated tampering features, wherein the tampering detection result comprises an image-tampered result and an image-not-tampered result;

wherein the operation A comprises:

converting the to-be-detected image from a first color space into a second color space;

carrying out the block segmentation on the to-be-detected image to segment the to-be-detected image into $N \times M$ image small fragments, wherein N and M are positive integers;

applying preset wavelet function decomposition to each second color space component on each image small fragment to obtain multiple corresponding pixel coefficient maps, calculating a tabulate statistics coefficient of each pixel coefficient map, and obtaining multiple tabulate statistics coefficients from each image small fragment, wherein the tabulate statistics coefficients are regarded as the initial tampering detection features of the corresponding image small fragments.

12. The electronic device of claim 11, wherein the predetermined encoder is a stacked auto-encoder; the stacked auto-encoder is formed by stacking multiple layers of basic auto-encoders, and an output of each layer of auto-encoder is an input of the next layer of auto-encoders; the stacked auto-encoder also comprises a neural network multi-layer perceptron; the neural network multi-layer perceptron is jointed with the last layer of auto-encoder, and is used for determining the tampering detection result corresponding to the to-be-detected image according to the generated complicated tampering features.

13. The electronic device of claim 12, wherein the at least one computer readable instruction is executed by the processing equipment, during execution of the operation B, comprising:

encoding the initial tampering detection features of all the image small fragments with the predetermined encoder to generate the complicated tampering features of all the image small fragments;

determining first tampering detection results corresponding to all the image small fragments according to the complicated tampering features of all the image small fragments, wherein the first tampering detection results comprise the image-tampered results and the image-not-tampered results;

if the first tampering detection result corresponding to one image small fragment is the image-tampered result, determining that the tampering detection result corresponding to the to-be-detected image is the image-tampered result.

14. The electronic device of claim 13, wherein the stacked auto-encoder also comprises an adjacent region perception layer for determining the tampering detection result corresponding to the to-be-detected image according to scene information of adjacent regions; the at least one computer readable instruction is executed by the processing equipment, during execution of the operation B, comprising:

calculating adjacent scene information of each image small fragment according to a preset algorithm, and determining a second tampering detection result corresponding to each image small fragment according to the adjacent scene information of each image small fragment, wherein the second tampering detection result comprises an image-tampered result and an image-not-tampered result;

if the second tampering detection result corresponding to one image small fragment is the image-tampered result, determining that the tampering detection result corresponding to the to-be-detected image is the image-tampered result;

if the second tampering detection results corresponding to all the image small fragments are all image-not-tampered results, but the first tampering detection result corresponding to one image small fragment is the image-tampered result, determining that the tampering detection result corresponding to the to-be-detected image is the image-not-tampered result.

15. A computer readable storage medium, which stores at least one computer readable instruction executed by processing equipment to implement the following operations:

A. carrying out block segmentation on a to-be-detected image to segment the to-be-detected image into a plurality of image small fragments, and extracting initial tampering detection features from all the image small fragments;

B. encoding the extracted initial tampering detection features with a predetermined encoder to generate complicated tampering features, and determining a tampering detection result corresponding to the to-be-detected image according to the generated complicated tampering features, wherein the tampering detection result comprises an image-tampered result and an image-not-tampered result;

wherein the operation A comprises:

converting the to-be-detected image from a first color space into a second color space;

carrying out the block segmentation on the to-be-detected image to segment the to-be-detected image into $N \times M$ image small fragments, wherein N and M are positive integers;

applying preset wavelet function decomposition to each second color space component on each image small fragment to obtain multiple corresponding pixel coefficient maps, calculating a tabulate statistics coefficient of each pixel coefficient map, and obtaining multiple tabulate statistics coefficients from each image small fragment, wherein the tabulate statistics coefficients are regarded as the initial tampering detection features of the corresponding image small fragments.