Journal of Combinatorial Mathematics
and Combinatorial Computing
www.combinatorialpress.com/jcmcc

Combinatorial Press

Remote Image Tampering Detection Combining Deep Neural Networks

Meijing Zhang[1,✉], Yi Chen[2], Dongxing Wang[3]

[1] *Key University Laborary of Fujian Province Digitalized Cyber Crime Supervision Prevention Control, Fujian Police College, Fuzhou, Fujian, 350007, China*

[2] *Collaborative Innovation Research Center of Intelligent Policing, Fujian Police College, Fuzhou, Fujian, 350007, China*

[3] *Research Center of New-quality Public Security Combat Effectiveness, Fujian Police College, Fuzhou, Fujian, 350007, China*

ABSTRACT

In the current information age, image tampering detection technology is crucial to ensure the integrity and authenticity of digital media, and remote image tampering detection technology combined with deep neural networks has become a research hotspot. This paper adopts convolutional neural network as the main detection tool, and on the improved DPN network model, the feature fusion module based on the attention mechanism is used to fuse the two features in this paper. In this way, the image tampering detection technique based on dual-stream feature fusion is proposed in this paper. The precision, recall and F value of the detection algorithm in this paper are better than the comparison algorithm. When the image compression quality factor is reduced to 20, the precision rate, recall rate, and F value of this paper's algorithm do not appear to be greatly reduced, and the reduction is only 0.028, 0.041, and 0.042. This paper's image tampering detection algorithm, which fuses the frequency domain branching module and the attention mechanism feature fusion module, has a higher detection efficiency. And the Accuracy rate, Recall rate and F Value of this paper's algorithm on image level detection are 17.8%, 15.3% and 16.3% higher than that of DCT algorithm respectively. In conclusion, the remote image tampering technique combined with deep neural network provides an effective solution to ensure the authenticity and integrity of images.

Keywords: Image tampering detection, DPN network model, Attention mechanism, Feature fusion

1. Introduction

In today's mobile Internet era, digital images are used on a large scale as an information carrier, and uncountable images are uploaded to the Internet every day. In the field of image forensics, photographic images have been widely utilised as a kind of evidence that is difficult to modify and highly reliable, and is an effective means of proving the truth and reducing ambiguity [1-3]. Images

✉ Corresponding author.
E-mail address: zmjpaper@163.com (M. Zhang).
Received 01 February 2024; Revised 20 April 2024; Accepted 10 November 2024; Published Online 15 April 2025.
DOI: 10.61091/jcmcc127a-246

have been appearing as very common evidence in news papers, courtrooms and hearings. The irrefutability of an image is by default its main attribute, and one of the main bases on which an image is used to prove or disprove a point of view and assertion is that its content has not been tampered with [4-6].

In the era of information technology dominance, people can easily tamper images into non-real images that are difficult to recognise with the naked eye through some image editing tools [7-8]. The appearance of tampered images reduces the credibility of the images people see, and even spreads through the network media to cause disturbances to the social life of human beings. Digital image forensics is an important field of information security, which can be divided into two main branches, active forensics and passive forensics [9-12].

Active forensics technology is generally based on digital signatures and digital watermarks in the image, although the current research in this area has been more mature, but due to the digital watermarks and digital signatures need to be embedded in the generation of the image, the imaging equipment requirements are high, and generally need a special way of verification, resulting in the image of the active forensics dataset is difficult to obtain, limiting the scope of its application [13-15]. In contrast, passive forensic techniques do not require any embedded operation on the image in advance, but by directly analysing the content of the image and obtaining certain features to distinguish whether the image is true and complete, a feature that makes passive forensics more widely used in the field of computer vision than active forensics [16-18].

Image passive forensic techniques are mainly divided into image tampering detection, image source identification and identification of computer-generated images. Image tampering mainly includes copy-paste tampering and splicing tampering, the research content of this paper that through a series of steps to identify whether the image has been copy-paste tampering [19-20]. Copy-paste tampering is to copy a certain region in the image and paste it directly or through geometric transformation to other locations in the original image to achieve the purpose of covering or hiding, and the resulting image has two or even more similar regions [21-22]. As the forged regions in the tampered image come from homologous images with the same lighting, noise and other influences, the differences between the regions are extremely small, and some tampered images are even difficult to distinguish with the naked eye, which leads to a greater challenge for the detection of copy-pasted tampered images, and attracts more and more researchers to devote themselves to this task [23-24].

The dual-stream feature fusion image tampering detection technique proposed in this paper is based on the convolutional neural network model and introduces an improved Dual Path Network neural network as the neural network structure for the remote image tampering detection technique in this paper. In addition, an SRM filter is used to obtain the RGB colour domain feature information and noise domain feature information of the remote image, and the feature fusion module based on the attention mechanism is used to integrate the features of the two branches. In order to verify the performance of this detection technique, this paper proposes three performance evaluation metrics, namely Accuracy rate, Recall rate and F Value, and evaluates the practicality and security of this paper's technique through comparative experiments, ablation experiments, robustness analyses, and image-level detection.

2. Image tampering detection algorithm incorporating deep neural network algorithm

2.1. Remote Image Tampering and Detection Techniques

2.1.1. Image tampering techniques. Image tampering is the intentional modification of a digital image to deceive and mislead people about the authenticity of the image. In order to better detect tampering, it is important to understand image tampering techniques.

Several common image tampering techniques include copy-paste, splice tampering, fill tampering and hybrid tampering. By understanding these tampering methods, one can better understand and respond to tampering behaviours and improve the accuracy and robustness of image tampering detection.

1) Copy-paste tampering: copying a part of an image, rotating it, scaling it or adjusting its colour, and then pasting it into another part of the image area, in order to cover up, delete or replace the original image information.

2) Splicing tampering: splicing tampering refers to splicing two or more images together to make a new image.

3) Touch-up tampering: It is the use of relevant image processing software to peel and stretch the content of the image and other operations, so as to achieve the role of repairing broken images or hiding image information.

4) Generation tampering: It learns the common features in the image by computer and generates images that are not available in real life according to the features.

5) Hybrid tampering: It refers to the combination of multiple tampering means on the image, such as splicing and embellishment operations at the same time. Due to the combination of multiple tampering means, hybrid tampering is often more difficult to detect.

2.1.2. Image tampering detection techniques. Image tampering detection technology is a technique for identifying and labelling tampered areas in an image, which can be divided into the following types according to the detection method:

1) Methods based on image visual features: this method analyzes the image based on its features, such as texture, colour, shape and so on.

2) Methods based on image compression: the compression algorithms used in the transmission and storage of digital images are used to detect whether the image has been tampered with.

3) Methods based on digital watermarking: special digital watermarks are embedded in the image and used to detect whether the image has been tampered with.

4) Deep learning based methods: deep neural networks are used to detect whether an image has been tampered with. By training on a large number of images, the deep neural network can learn the features and patterns of the image to determine whether the image has been tampered with.

2.1.3. Performance evaluation metrics for tamper detection. Evaluation metrics for image tampering detection are usually divided into two categories: detection performance metrics and lightweight evaluation metrics. In this paper, we use the detection performance metrics, including Recall, Precision and F Value. Assuming that the real number of tampered regions is N and the number of tampered regions detected by the algorithm is M, of which the number of correctly detected tampered regions is K, they are defined as follows:

1) Recall Rate: refers to the ratio of tampered regions correctly detected by the algorithm to the real tampered regions:

$$Recall = \frac{K}{N} \tag{1}$$

2) Accuracy rate: the ratio of tampered areas correctly detected by the algorithm to all tampered areas detected by the algorithm:

$$Precision = \frac{K}{M} \tag{2}$$

3) F Value: is an evaluation metric that combines precision and recall to assess the performance of a classification model. It is the reconciled average of precision and recall:

$$Fl = 2 \times \frac{\Pr ecision \times \mathrm{Re} call}{\Pr ecision + \mathrm{Re} call} \tag{3}$$

2.2. Deep neural network models

2.2.1. Convolutional neural network models. A deep convolutional neural network is a feed-forward neural network with a deep structure that contains many convolutional computational layers, which can provide an end-to-end approach to task analysis. In general, CNN structures typically contain multiple sets of learnable parameters and components. These components usually consist of an alternating cascade of four basic network layers: a convolutional layer, a pooling layer, an activation layer, and a regularisation layer. The overall structure of a CNN is shown in Figure 1.

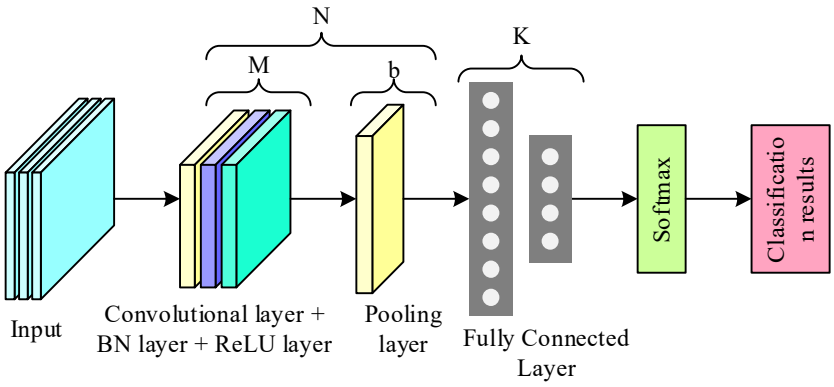

Fig. 1. General architexture of CNN

1) Convolutional Layer. In CNN, the input image is processed using a convolution operation with a number of convolution kernels of k. The convolution operation generates k new feature maps and uses them as input to the subsequent layers. In the following equation, Definition $F_j^{(n)}$ represents the j th output feature map in layer n:

$$F_j^{(n)} = \sum_i w_{ij}^{(n)} * F_i^{(n-1)} + b_j^{(n)} \tag{4}$$

In the above equation, * denotes 2-dimensional convolution, and $w_{ij}^{(n)}$ and $b_j^{(n)}$ denote convolution kernel weights and bias values, respectively.

2) Pooling layer. The image undergoes a series of convolutional layers to produce a large number of large-size feature maps. In order to reduce the dimensionality of the input features, a pooling layer is usually added after the convolution layer, which is defined as:

$$F_j^{(n+1)} = pool\left(F_j^n\right) \tag{5}$$

In the above equation, $pool(\ )$ represents pooling functions such as maximum pooling, average pooling and random pooling.

3) Activation layer. The activation layer is connected after the convolution layer to transform the input feature map with a nonlinear mapping, which is defined as:

$$F_j^{(n+1)} = f\left(F_j^n\right) \tag{6}$$

In the above equation, $f(\ )$ represents the activation functions such as TanH and ReLU.

4) Regularisation layer. To prevent the network from overfitting the training data, it is often necessary to add a regularisation layer to the network model. In the BN layer, learnable parameters $\{\gamma, \beta\}$ are used to ensure that the network parameters always follow a certain feature distribution. The

conversion of each data item x_i in a feature $B=\{x_1,x_2,\ldots,x_m\}$ of batch size m to y_i by these two parameters is achieved by the following equation:

$$y_i=\gamma\hat{x}_i+\beta \tag{7}$$

$$\hat{x}_i=\frac{x_i-E_M(x_i)}{\sqrt{Var_M(x_i)+\varepsilon}} \tag{8}$$

In the above equation, $E_M(x_i)$ and $Var_M(x_i)$ represent the mean and variance of x_i in batch B, respectively.

2.2.2. Dual Path Neural Network DPN Model. ResNet in each residual block the output is superimposed on the output of the previous layer on the basis of the results of the convolution performed. It reduces the problem of vanishing in the information transfer process in a way. DenseNet, on the basis of forward propagation, each layer of the network receives the feature maps of all the layers in front of it and the data aggregation is done by splicing instead of summing as in Resnet. And for back propagation, the shallow network can get the gradient information of the deeper layers. DPN network is a fusion of the core ideas of ResNet and DenseNet to achieve complementary strengths and weaknesses [25]. The structure of each layer of the DPN network can be expressed by the following equation:

$$X_{res}=F(x)+x \tag{9}$$

$$X_{dense}=H_l([x_0,x_1,\ldots\ldots,x_{l-1}]) \tag{10}$$

$$X_{dual}=g(X_{res}+X_{dense}) \tag{11}$$

Where X_{res} is the output of ResNet training the previous layer of network, X_{dense} denotes the output of DenseNet training the previous layer of network, X_{dual} denotes the merging of X_{res} and X_{dense} in the pattern of concat, and g is the activation function, and in this paper, the relu activation function is used.The specific structure of the DPN network is shown in Fig. 2:

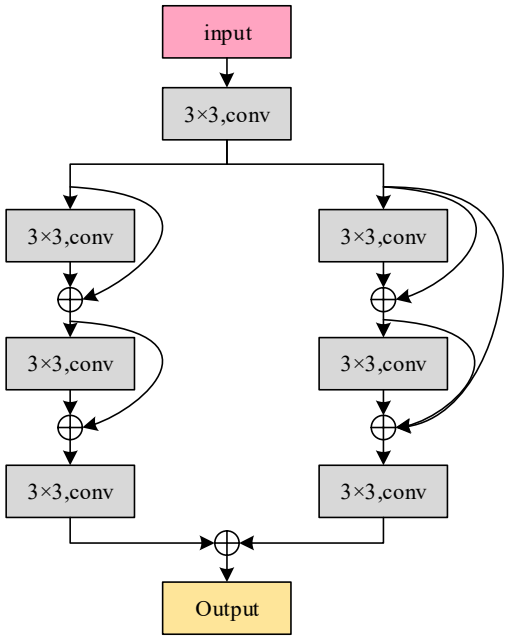

Fig. 2. Double path neural network

2.2.3. Attention Mechanisms in Neural Networks. Attention is an essential and complex cognitive function of humans, which refers to the ability to selectively focus on some information while ignoring others. Attention can generally be divided into two types: top-down conscious attention, known as focussed attention, and bottom-up unconscious attention, known as salient attention. Conscious attention is defined as the intentional, active focusing of the conscious mind on an object, whereas unconscious attention is driven by external stimuli, requires no active intervention, and is not task-related.

The attention mechanism in deep learning is a resource allocation scheme in the case of limited computational resources, which allocates limited computational resources to more important tasks [26]. When using neural networks to process input information, with the help of the human brain's attention mechanism, only some key information inputs are selected for processing to improve the efficiency of neural networks.

Denote by $X=[x_1,\ldots,x_N]\in\Re^{D\times N}$ the N sets of input information, where $x_n\left(n=[1,N]\right)$ is a D-dimensional vector. In order to save computational resources, only some task-relevant information is fed into the neural network. The computation of the attention mechanism is divided into two steps:

1) Calculation of the attention distribution: in order to select the information related to a specific task from the N input feature vectors, a representation related to the task, the query vector, referred to as q, is first introduced; meanwhile, the correlation between each input vector and the query vector is calculated by the scoring function $s(x,q)$. The following scoring functions are usually available:

Additive Modelling:

$$s(x,q)=v^T\tanh\left(Wx+Uq\right) \tag{12}$$

Dot product models:

$$s(x,q)=x^Tq \tag{13}$$

Scaling dot product models:

$$s(x,q)=\frac{x^Tq}{\sqrt{D}} \tag{14}$$

Bilinear Modelling:

$$s(x,q)=x^TWq \tag{15}$$

where W, U, and v are learnable parameters, D is the dimension of the input vector, and the query vector q can be dynamically generated or learnt parameters.

Given the query vector q related to the task, the index position of the selected information is denoted by i. To facilitate the computation, a soft information mechanism is used. The probability α_n of selecting the n th input vector given q and X is first calculated:

$$\begin{aligned}\alpha_n&=p\left(i=n\middle|X,q\right)=Soft\max\left(s\left(x_n,q\right)\right)\\&=\frac{\exp\left(s\left(x_n,q\right)\right)}{\sum_{i=1}^{N}\exp\left(s\left(x_j,q\right)\right)}\end{aligned} \tag{16}$$

where α_n is the attention distribution.

2) Weighted average: the attention distribution α_n can be used to characterise how much attention the n rd input vector receives when it comes to the task-related query q. The soft information selection mechanism is then used to summarise all the inputs, i.e:

$$Attention(X,q)=\sum_{n=1}^{N}\alpha_n x_n = E_{i\sim p(i|X,q)}[x_i] \tag{17}$$

Equation (14) is the soft attention mechanism, where the information selected is the expectation of all input vectors under the attention distribution.

Alternatively, there is hard attention, which focuses only on a particular input vector and selects the one with the highest probability, viz:

$$Attention(X,q)=x_{\tilde{n}} \tag{18}$$

where $\tilde{n}=\arg\max_{n=1}^{N}\alpha_n$ is the subscript corresponding to the input vector with the highest probability.

Commonly, attention can also be expressed as key-value pair attention, where the input information is represented by a key-value pair (K,V), where the "key" K is used for the computation of the attention distribution α_n, and the "value" V is used for the computation of the aggregated information. Then given the task-related query vector q, the key-value pair attention can be obtained, i.e.:

$$Attention((K,V),q)=\sum_{n=1}^{N}\alpha_n v_n=\sum_{n=1}^{N}\frac{\exp(s(k_n,q))}{\sum_{i=1}\exp(s(k_j,q))}v_n \tag{19}$$

The process of selecting multiple sets of information from the input information centre by placing multiple key-value pair attentions in parallel is multi-head attention, then each attention can focus on a different part of the input information, i.e.:

$$Multiheadattention((K,V),Q)=Concat(head_1,head_2,\cdots,head_n) \tag{20}$$

where n denotes the number of long attention spans and $head_i=Attention((K,V),q_i)$.

2.3. Image tampering detection technique based on dual-stream feature fusion

2.3.1. Network model structural design. In this paper, an image tampering detection structure based on dual-stream multiscale attention mechanism feature fusion is proposed, and the model structure consists of RGB colour domain branch, Noise noise domain branch, SRM processing module, multiscale attention module, and feature fusion module. The network structure adopts the convolutional neural network as the main body, the improved Dual Path Network neural network as the backbone, the RGB colour domain branch and the Noise noise domain branch adopt the same network structure, in which the SRM filter is used to obtain the spatial information of the noise domain of the image to be detected as the input of the Noise noise domain branch. Finally, the features of the two branches are fused by the feature fusion module based on the attention mechanism. The structure of image tampering detection with dual-stream multi-scale attention mechanism feature fusion is shown in Fig. 3.

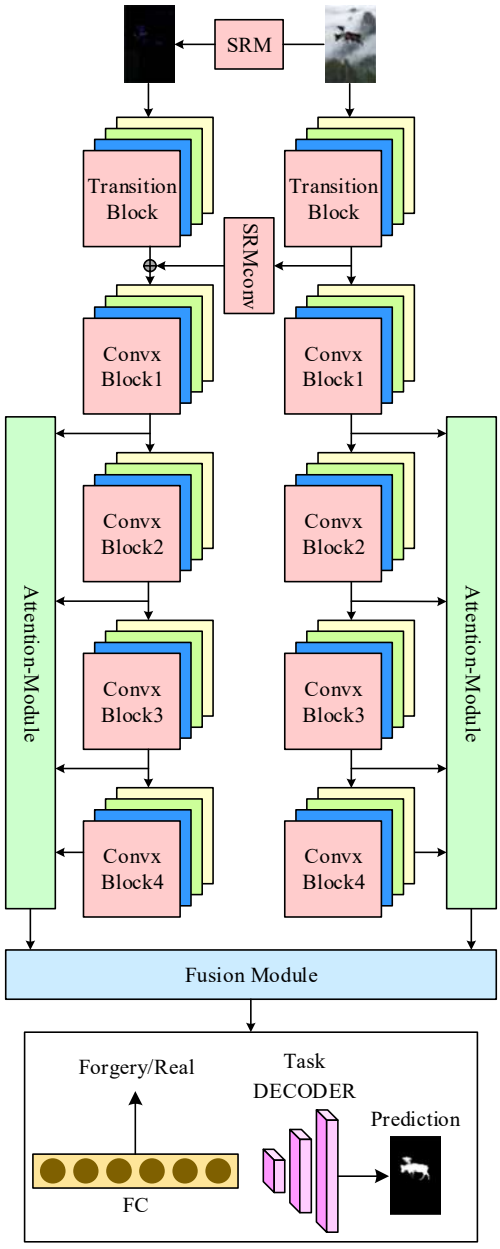

Fig. 3. Network model structure

The core idea of the image tampering detection method based on feature fusion with dual-stream multi-scale attention mechanism is based on the attention mechanism, which aims to synergise the feature information in the colour domain space and the feature information in the noise domain space, and extracts the image edge feature information using Sobel filters and the noise domain feature information of the image using SRM filters from the different network model structures for extracting the different modal feature information. Finally, the model achieves effective fusion of different features by collaboratively using the colour domain feature information and the noise domain information using the feature fusion module based on the attention mechanism, and the final obtained feature map is used for image tampering detection. The algorithm flow can be expressed by the following equation:

$$X_O = Fusi onModule(T_{rgb}, T_{noise}) \tag{21}$$

The RGB colour domain branch feature T_{rgb} and the noise feature T_{noise} are coordinated with each other. Finally, the features of the dual-stream branches are fused to obtain the final feature map, which is used to classify the image characters by obtaining the probability scores of different categories in the fully connected layer. For the image tampering localisation task, the decoder adopts the FCN network decoding method, which converts the size of the final feature vector into the size of the original image by inflated convolution to achieve image tampering detection and localisation.

2.3.2. SRM module. In this paper, SRM filter is used for noise extraction of the image, which is based on the difference between the pixel values and the surrounding pixel values to determine the tampered and non-tampered regions by the discontinuity between the noise [27].

By using three high pass filters for each channel of the image, three residual values are obtained for each channel, after which the three residual values are averaged to obtain a single channel noise map. The same operation is performed on the other two channels to obtain a three-channel noise map. The three convolution kernels are shown in equation (22):

$$k_1=\begin{bmatrix}-1&2&-2&2&-1\\2&-6&8&-6&2\\-2&8&-12&8&-2\\2&-6&8&-6&2\\-1&2&-2&2&-1\end{bmatrix}\quad k_2=\begin{bmatrix}0&0&0&0&0\\0&-1&2&-1&0\\0&2&-4&2&0\\0&-1&2&-1&0\\0&0&0&0&0\end{bmatrix}$$
$$k_3=\begin{bmatrix}0&0&0&0&0\\0&0&0&0&0\\0&1&-2&1&0\\0&0&0&0&0\\0&0&0&0&0\end{bmatrix} \tag{22}$$

2.3.3. Frequency domain branching module. In this study an SRM filter is used to convert the image to noise domain information and use it as an input channel for the noise flow branch. In addition, the early feature information in the RGB colour domain branch is used to guide the feature learning in the noise domain branch, which is combined with the early edge information to effectively capture the boundary tampering anomaly information.

The input X is subjected to multiple convolution operations to obtain early feature vectors, the obtained features are fused with the low-level feature vectors of the noise domain branch by a learnable SRM convolution kernel finally the final noise domain feature information is obtained by going through the same network structure as that of the RGB domain branch. T_{noise} The process equation can be expressed as follows:

$$X_{ef}=add\left(X_h, SRMconv\left(Convx_1\left(X\right)\right)\right) \tag{23}$$

$$T_{noise}=Convx_x\left(X_{ef}\right) \tag{24}$$

where X_{ef} denotes an early noise feature that has been guided by RGB colour domain features, and $Convx_x$ denotes a convolutional block in a DPN neural network.

2.3.4. Feature Fusion Module. The RGB colour domain T_{rgb} feature information and Noise noise domain T_{noise} feature information are obtained in the above dual-stream image tampering process. The feature fusion in this paper is similar to the Last fusion fusion mechanism inside multimodal fusion.

In this paper, we adopt a fusion method based on the attention mechanism, and the feature fusion module is shown in Fig. 4. The effective fusion of two branches is achieved by giving different weights to their feature information. Firstly, the T_{rgb} and T_{noise} branches are spliced, and then a set of fusion weights are obtained by local and global attention and then by the corresponding sigmoid, and different weights are given to the two branches to be summed up, so as to realise the soft selection of feature information. The execution process can be represented by the following equation:

$$T_{cat} = F_{cat}\left(T_{rgb} + T_{noise}\right) \tag{25}$$

$$wei = sigmoid\left(F_{global}\left(T_{cat}\right) + F_{local}\left(T_{cat}\right)\right) \tag{26}$$

$$X_o = 2 * T_{rgb} * wei + 2 * T_{noise} * \left(1 - wei\right) \tag{27}$$

where T_{cat} denotes concatenate, F_{global} denotes local attention, F_{local} denotes global attention, and X_o denotes fused feature information. Subsequently, X_o is used for the tamper detection task after passing through a series of fully connected layers, and X_o is used for the image tamper detection localisation task by converting the output size to the same size as the input X through the FC head of the FCN fully convolutional neural network after multiple expansion convolutions.

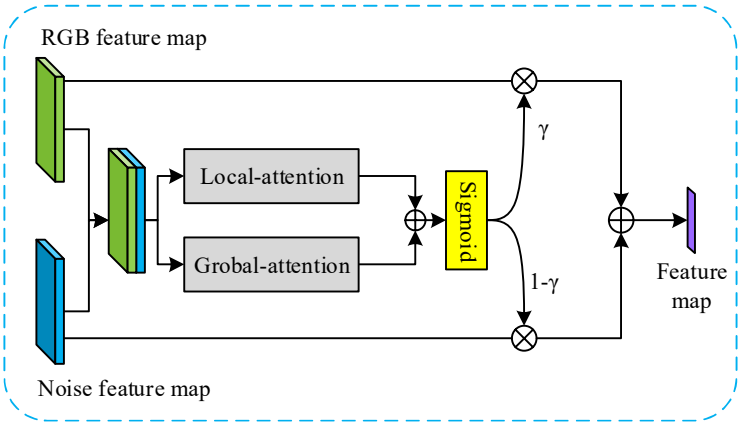

Fig. 4. Feature fusion module

3. Performance testing of remote image tampering detection technology

3.1. Comparative experiments

In order to verify the effectiveness of the algorithm in this paper, this section selects several current image tampering algorithms with better detection effect for experimental comparison, the comparison algorithms are: LSTM, RTAG, BLK, DCT, NADQ and AttRUNet, including the algorithms proposed in this paper, which are recorded as Algorithm Models 1-7 in order to carry out fair experimental comparisons, the TIFF-formatted image data is converted into zero-compression JPEG format image data. Fifty sets of image data are randomly selected from CASIA and Coumbia datasets as test objects.

Fig. 5 shows the average values of precision, recall and F of the detection results of each of the seven groups of algorithmic models on 50 sets of image data. From the figure, it can be seen that the detection results of this paper's algorithm are better than the other six comparative algorithms in terms of the three sets of evaluation parameters precision rate and F. The precision rate, recall and F value of this paper's algorithm are 0.862, 0.911 and 0.871 respectively, which are 16.1%, 15.3% and 17.8% better than the next best algorithm (DCT).

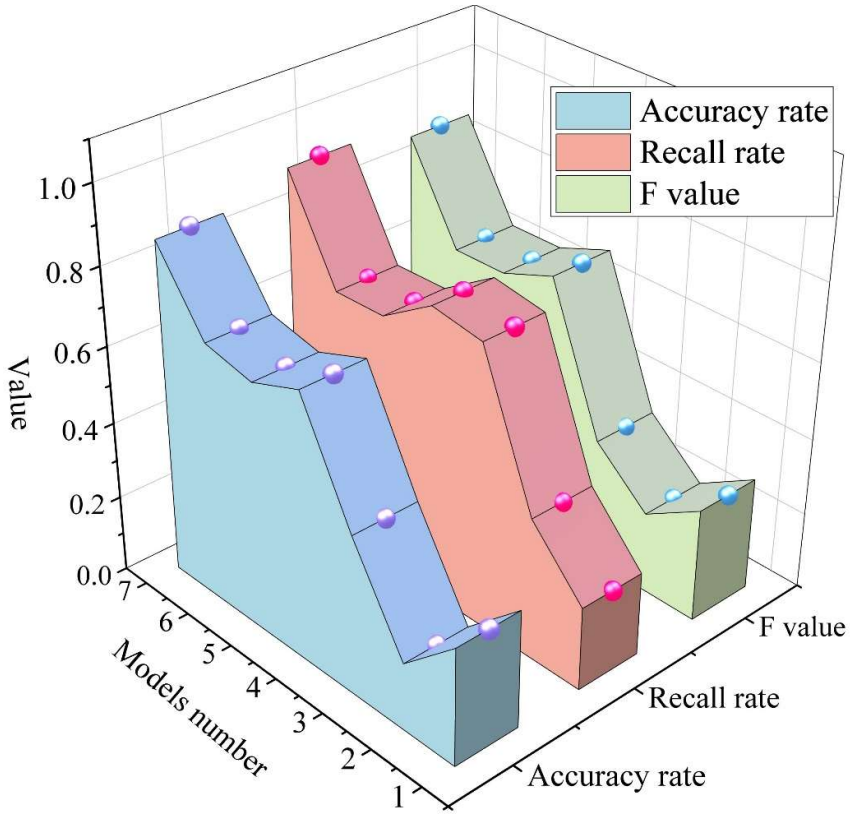

Fig. 5. The algorithm is based on the test results of the data of 50 groups

3.2. Robustness analysis

In order to further verify the robustness of this algorithm, this paper chooses to compare the evaluation parameter detection results with the above second best performing algorithmic model DCT under different types and degrees of attacks (including JPEG image compression attack and Gaussian noise pollution attack). The precision, recall, and F value detection results under different attack types are shown in Fig. 6.

The left side of the figure represents the detection results of the two algorithms under different degrees of JPEG image compression attacks (e.g., when the quality factor is 100, i.e., it means no compression). The right side represents the detection results of the algorithms under Gaussian noise pollution attacks with different variances (the mean value defaults to 0).

The data in the figure shows that under the JPEG image compression attack with different quality factors, the DCT algorithm has a significant decreasing trend in the range of quality factors from 100 to 20. When the quality factor is 20, the precision, recall, and F value of DCT algorithm are 0.241, 0.324, and 0.362 respectively, and its detection results are basically invalid. In contrast, the algorithm in this paper is 0.817, 0.883, and 0.822, respectively, demonstrating better and more stable detection results. Similarly, under the Gaussian noise pollution attack with different variances, the detection effect of this algorithm is also better than that of the DCT algorithm.

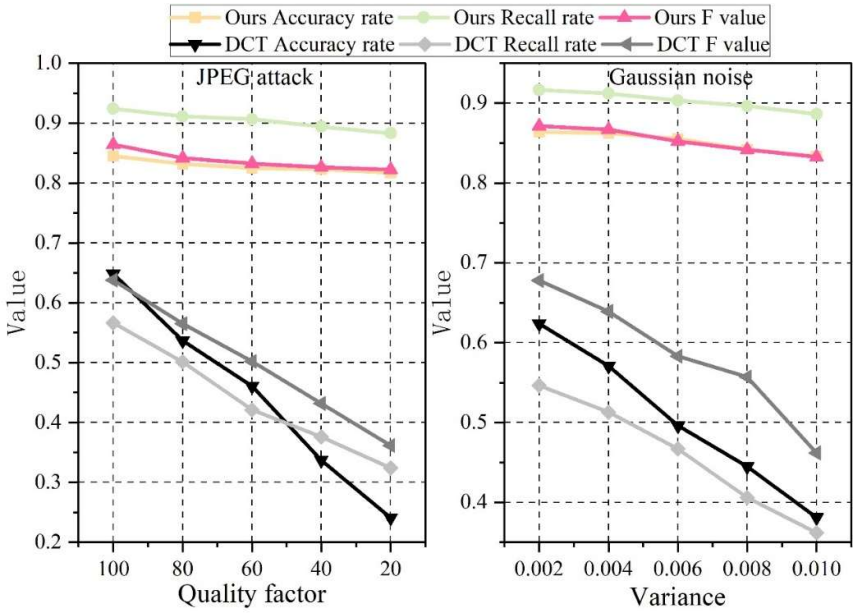

Fig. 6. The accuracy rate of different attack types and the recall rate of the recall rate

3.3. Ablation experiments

In order to test the role of the model structure on the network level and to detect the impact of the designed module structure on the detection results, four model structures are used in this section for the ablation experiments, namely, the original DPN (denoted as P-DPN), the model DPN without the use of pre-populated feature extraction module (denoted as U-DPN), the DPN without the attention module (denoted as N-DPN), and the improved proposed in this paper DPN model, were tested on CASIA and Columbia datasets respectively, and three evaluation metrics, namely, Accuracy rate, Recall rate and F Value, were used. The results of the ablation experiments are shown in Fig. 7.

Through ablation experiments, it was found that experimenting on the two selected datasets, the introduction of the frequency domain module and the attention module into the neural network structure greatly improved the detection efficiency of the model. For example, on the CASIA dataset, the Accuracy Rate, Recall rate, and F Value evaluation index values are improved from 0.693, 0.737, and 0.689 to 0.892, 0.918, and 0.876, respectively, and this can be seen that there exists a greater research value of image tampering in terms of the frequency-domain feature extraction and the attention mechanism.

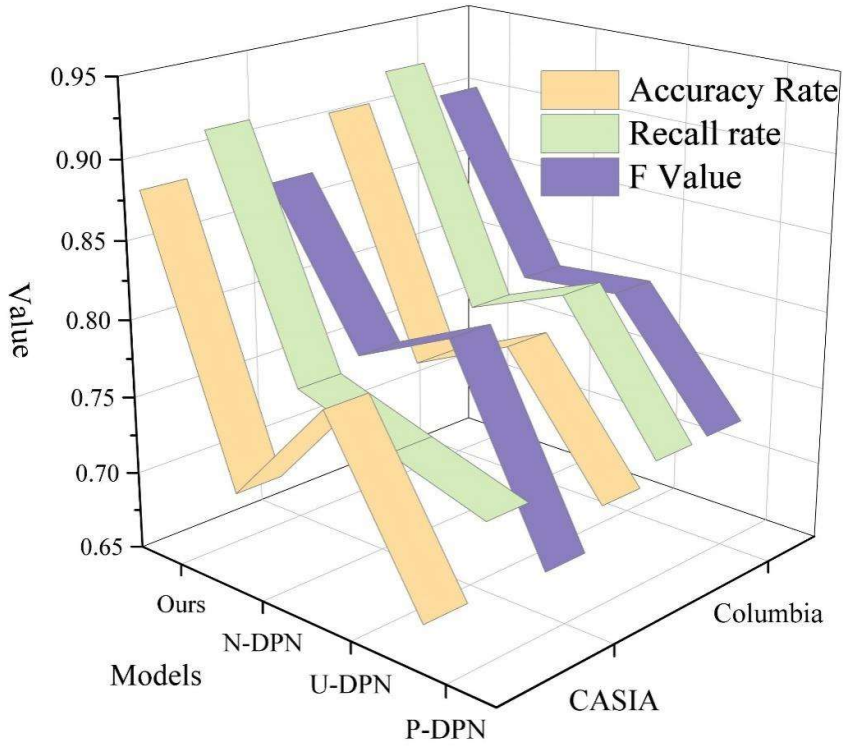

Fig. 7. Ablation experiment results

3.4. Image-level detection

In order to compare the performance of this paper's image tampering detection algorithm other detection algorithms for detecting common splicing tampering at the image level. In this section, 200 tampered images and 200 real images are randomly selected from two datasets CASIA and Columbia for testing. The detection mean and error values of each algorithm are recorded.

Fig. 8 shows the image level detection results of all the algorithms. Algorithm numbers 1-6 in the figure are comparison algorithms, algorithm 7 is this paper's algorithm, and the shading in the figure is the average error of different algorithms on the detection metrics of the selected images. As can be seen from the figure, the detection evaluation values of Accuracy rate, Recall rate and F Value of this paper's algorithm on the selected images are 0.913, 0.937 and 0.876 respectively, while the average values of the three indexes of DCT algorithm, which is the best performer among the comparison algorithms, are only 0.735, 0.784 and 0.713 respectively. In this paper, we propose an image tampering detection algorithm outperforms other detection algorithms, confirming that the algorithm in this paper can correctly learn different images of tampered and untampered regions and classify tampered and real images.

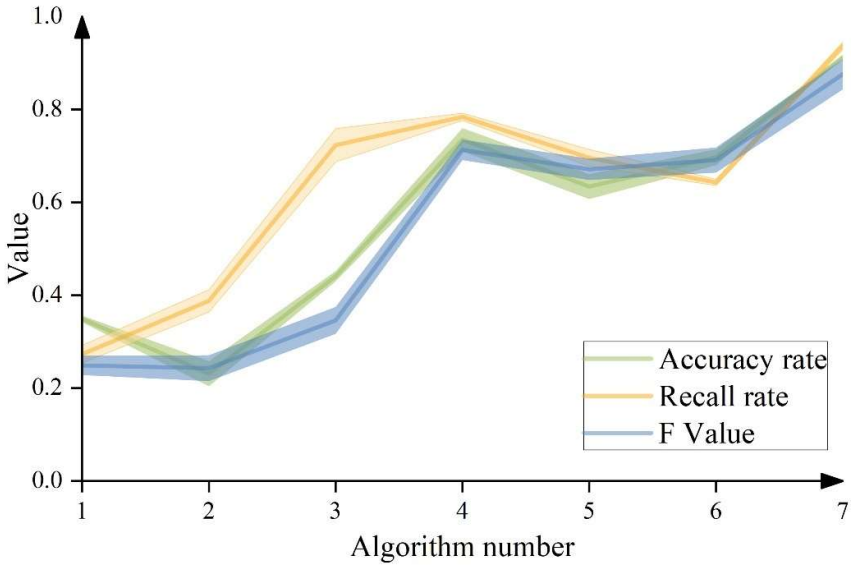

Fig. 8. Image level detection of all algorithms

4. Conclusion

In this paper, a dual stream feature fusion based image tampering detection technique is proposed with an improved Dual Path Network neural network as the network structure. The acquired colour domain feature information and noise domain feature information are feature fused with a feature fusion module that combines the attention mechanism. And the performance of this paper's detection technique is evaluated through simulation experiments.

The precision, recall, and F value of the detection algorithm in this paper are 16.1%, 15.3%, and 17.8% higher than the most effective comparison algorithm (DCT), respectively. Its performance is much better than the comparison algorithm.

As the JPEG image compression and Gaussian noise pollution attack intensity rises, the algorithm in this paper shows better detection effect. For example, when the image compression quality factor is 20, the precision rate, recall rate, and F value of this paper's algorithm are 0.817, 0.883, and 0.822, respectively, with no significant decrease.

The ablation experiments found that the image tampering detection algorithm in this paper, which fuses the frequency domain branching module and the attention mechanism feature fusion module, has higher detection efficiency. The Accuracy Rate, Recall rate, and F Value evaluation index values are improved by 19.9%, 18.1%, and 18.7%, respectively, compared with the original DPN model.

The image level detection results show that the proposed algorithm in this paper can classify tampered images and real images more accurately than the comparison algorithm.

Acknowledgements

Fujian Provincial Department of Finance's 2023 Provincial Direct Unit Science and Technology Special Project (Second Batch) (FuJian Finance Directive [2023] No. 891).

References

[1] Zheng, L., Zhang, Y., & Thing, V. L. (2019). A survey on image tampering and its detection in real-world photos. Journal of Visual Communication and Image Representation, 58, 380-399.

[2] González Fernández, E., Sandoval Orozco, A. L., García Villalba, L. J., & Hernandez-Castro, J. (2018). Digital image tamper detection technique based on spectrum analysis of CFA artifacts. Sensors, 18(9), 2804.

[3] Manjunatha, S., & Patil, M. M. (2021, February). Deep learning-based technique for image tamper detection. In 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV) (pp. 1278-1285). IEEE.

[4] Asaad, A., & Jassim, S. (2017). Topological data analysis for image tampering detection. In Digital Forensics and Watermarking: 16th International Workshop, IWDW 2017, Magdeburg, Germany, August 23-25, 2017, Proceedings 16 (pp. 136-146). Springer International Publishing.

[5] Diallo, B., Urruty, T., Bourdon, P., & Fernandez-Maloigne, C. (2019). Improving robustness of image tampering detection for compression. In MultiMedia Modeling: 25th International Conference, MMM 2019, Thessaloniki, Greece, January 8–11, 2019, Proceedings, Part I 25 (pp. 387-398). Springer International Publishing.

[6] Zhuang, P., Li, H., Tan, S., Li, B., & Huang, J. (2021). Image tampering localization using a dense fully convolutional network. IEEE Transactions on Information Forensics and Security, 16, 2986-2999.

[7] Vega, E. A. A., Fernández, E. G., Orozco, A. L. S., & Villalba, L. J. G. (2020). Image tampering detection by estimating interpolation patterns. Future Generation Computer Systems, 107, 229-237.

[8] Molina-Garcia, J., Garcia-Salgado, B. P., Ponomaryov, V., Reyes-Reyes, R., Sadovnychiy, S., & Cruz-Ramos, C. (2020). An effective fragile watermarking scheme for color image tampering detection and self-recovery. Signal Processing: Image Communication, 81, 115725.

[9] Bondi, L., Lameri, S., Güera, D., Bestagini, P., Delp, E. J., & Tubaro, S. (2017, July). Tampering detection and localization through clustering of camera-based CNN features. In 2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW) (pp. 1855-1864). IEEE.

[10] Doan, T. N. C., Retraint, F., & Zitzmann, C. (2021). Image tampering detection based on a statistical model. Multimedia Tools and Applications, 80(21), 32905-32924.

[11] Chennamma, H. R., & Madhushree, B. (2023). A comprehensive survey on image authentication for tamper detection with localization. Multimedia Tools and Applications, 82(2), 1873-1904.

[12] Zhang, D., Chen, X., Li, F., Sangaiah, A. K., & Ding, X. (2020). Seam - Carved Image Tampering Detection Based on the Cooccurrence of Adjacent LBPs. Security and Communication Networks, 2020(1), 8830310.

[13] Alshanbari, H. S. (2021). Medical image watermarking for ownership & tamper detection. Multimedia tools and applications, 80(11), 16549-16564.

[14] Bourouis, S., Alroobaea, R., Alharbi, A. M., Andejany, M., & Rubaiee, S. (2020). Recent advances in digital multimedia tampering detection for forensics analysis. Symmetry, 12(11), 1811.

[15] Bhalerao, S., Ansari, I. A., & Kumar, A. (2021). A secure image watermarking for tamper detection and localization. Journal of Ambient Intelligence and Humanized Computing, 12(1), 1057-1068.

[16] Sarkar, D., Palit, S., Som, S., & Dey, K. N. (2020). Large scale image tamper detection and restoration. Multimedia Tools and Applications, 79(25), 17761-17791.

[17] Ulutas, G., Ustubioglu, A., Ustubioglu, B., V Nabiyev, V., & Ulutas, M. (2017). Medical image tamper detection based on passive image authentication. Journal of digital imaging, 30, 695-709.

[18] Abdelhakim, A., Saleh, H. I., & Abdelhakim, M. (2019). Fragile watermarking for image tamper detection and localization with effective recovery capability using K-means clustering. Multimedia Tools and Applications, 78(22), 32523-32563.

[19] da Costa, K. A., Papa, J. P., Passos, L. A., Colombo, D., Del Ser, J., Muhammad, K., & de Albuquerque, V. H. C. (2020). A critical literature survey and prospects on tampering and anomaly detection in image data. Applied Soft Computing, 97, 106727.

[20] Yuan, X., Li, X., & Liu, T. (2021). Gauss–Jordan elimination-based image tampering detection and self-recovery. Signal Processing: Image Communication, 90, 116038.

[21] Bammey, Q., von Gioi, R. G., & Morel, J. M. (2018, April). Automatic detection of demosaicing image artifacts and its use in tampering detection. In 2018 IEEE Conference on Multimedia Information Processing and Retrieval (MIPR) (pp. 424-429). IEEE.

[22] Gull, S., Loan, N. A., Parah, S. A., Sheikh, J. A., & Bhat, G. M. (2020). An efficient watermarking technique for tamper detection and localization of medical images. Journal of ambient intelligence and humanized computing, 11, 1799-1808.

[23] Rajput, V., & Ansari, I. A. (2020). Image tamper detection and self-recovery using multiple median watermarking. Multimedia Tools and Applications, 79(47), 35519-35535.

[24] Li, H., Luo, W., Qiu, X., & Huang, J. (2017). Image forgery localization via integrating tampering possibility maps. IEEE Transactions on Information Forensics and Security, 12(5), 1240-1252.

[25] Tong Fu,Liquan Chen,Yuan Gao & Huiyu Fang. (2024). DCANet: CNN model with dual-path network and improved coordinate attention for JPEG steganalysis. Multimedia Systems(4),230-230.

[26] Fatih CELIK,Kemal CELIK & Ayse CELIK. (2024). Enhancing brain tumor classification through ensemble attention mechanism. Scientific Reports(1),22260-22260.

[27] Wellington A. Silva & Laurinda L. N. Reis. (2018). Phase fault attenuation in SRM based on generalized predictive control and filter design. Electrical Engineering(3),1481-1489.